CISA

Number: CISA
Passing Score: 800
Time Limit: 120 min
File Version: 1

CISA

Sections

1. The process of Auditing Information System
2. Governance and Management of IT
3. Information System Acquisition, Development and Implementation
4. Information System Operations, Maintenance and Support
5. Protection of Information Assets

Exam A

QUESTION 1
You are part of a security staff at a highly profitable bank and each day, all traffic on the network is logged for later review. Every Friday when major deposits are made you're seeing a series of bits placed in the "Urgent Pointer" field of a TCP packet. This is only 16 bits which isn't much but it concerns you because:

A. This could be a sign of covert channeling in bank network communications and should be investigated.
B. It could be a sign of a damaged network cable causing the issue.
C. It could be a symptom of malfunctioning network card or drivers and the source system should be checked for the problem.
D. It is normal traffic because sometimes the previous fields 16-bit checksum value can over run into the urgent pointer's 16-bit field causing the condition.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:
The Urgent Pointer is used when some information has to reach the server ASAP. When the TCP/IP stack at the other end sees a packet using the Urgent Pointer set, it is duty bound to stop all ongoing activities and immediately send this packet up the stack for immediate processing. Since the packet is plucked out of the processing queue and acted upon immediately, it is known as an Out Of Band (OOB)packet and the data is called Out Of Band (OOB) data.

The Urgent Pointer is usually used in Telnet, where an immediate response (e.g. the echoing of characters) is desirable.

Covert Channels are not directly synonymous with backdoors. A covert channel is simply using a communication protocol in a way it was not intended to be used or sending data without going through the proper access control mechanisms or channels. For example, in a Mandatory Access Control systems a user at secret has found a way to communicate information to a user at Confidential without going through the normal channels.

In this case the Urgent bit could be used for a few reasons:

1. It could be to attempt a Denial of service where the host receiving a packet with the Urgent bit set will give immediate attention to the request and will be in wait state until the urgent message is receive, if the sender does not send the urgent message then it will simply sit there doing nothing until it times out. Some of the TCP/IP stacks used to have a 600 seconds time out, which means that for 10 minutes nobody could use the port. By sending thousands of packet with the URGENT flag set, it would create a very effective denial of service attack.
2. It could be used as a client server application to transmit data back and forward without going through the proper channels. It would be slow but it is possible to use reserved fields and bits to transmit data outside the normal communication channels. The other answers are incorrect

Reference:

http://www.fas.org/irp/nsa/rainbow/tg030.htm document covering the subject of covert channels and also see: http://gray-world.net/papers.shtml which is a large collection of documents on Covert Channels

QUESTION 2
Sam is the security Manager of a financial institute. Senior management has requested he performs a risk analysis on all critical vulnerabilities reported by an IS auditor. After completing the risk analysis, Sam has observed that for a few of the risks, the cost benefit analysis shows that risk mitigation cost (countermeasures,

controls, or safeguard) is more than the potential lost that could be incurred. What kind of a strategy should Sam recommend to the senior management to treat these risks?

A. Risk Mitigation
B. Risk Acceptance
C. Risk Avoidance
D. Risk transfer

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:
Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

For your exam you should know below information about risk assessment and treatment:

A risk assessment, which is a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls. A risk assessment is carried out, and the results are analyzed. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. Security can be quite complex, even for well-versed security professionals, and it is easy to apply too much security, not enough security, or the wrong security controls, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of resources that should be applied to protecting against those risks in a sensible manner.
A risk analysis has four main goals:
Identify assets and their value to the organization.
Identify vulnerabilities and threats.
Quantify the probability and business impact of these potential threats.
Provide an economic balance between the impact of the threat and the cost of the countermeasure.

Treating Risk

Risk Mitigation

Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented. Examples of risk mitigation can be seen in everyday life and are readily apparent in the information technology world. Risk Mitigation involves applying appropriate control to reduce risk. For example, to lessen the risk of exposing personal and financial information that is highly sensitive and confidential organizations put countermeasures in place, such as firewalls, intrusion detection/prevention systems, and other mechanisms, to deter malicious outsiders from accessing this highly sensitive information. In the underage driver example, risk mitigation could take the form of driver education for the youth or establishing a policy not allowing the young driver to use a cell phone while driving, or not letting youth of a certain age have more than one friend in the car as a passenger at any given time.

Risk Transfer

Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way. The family is evaluating whether to permit an underage driver to use the family car. The family decides that it is important for the youth to be mobile, so it transfers the financial risk of a youth being in an accident to the insurance company, which provides the family with auto insurance. It is important to note that the transfer of risk may be accompanied by a cost. This is certainly true for the insurance example presented earlier, and can be seen in other insurance instances, such as liability insurance for a vendor or the insurance taken out by companies to protect against hardware and software theft or destruction. This may also be true if an organization must purchase and implement security controls in order to make their organization less desirable to attack. It is important to remember that not all risk can be transferred. While financial risk is simple to transfer through insurance, reputational risk may almost never be fully transferred.

Risk Avoidance

Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized. For example, have you ever heard a friend, or parents of a friend, complain about the costs of insuring an underage driver? How about the risks that many of these children face as they become mobile? Some of these families will decide that the child in question will not be allowed to drive the family car, but will rather wait until he or she is of legal age (i.e., 18 years of age) before committing to owning, insuring, and driving a motor vehicle.

In this case, the family has chosen to avoid the risks (and any associated benefits) associated with an underage driver, such as poor driving performance or the cost of insurance for the child. Although this choice may be available for some situations, it is not available for all. Imagine a global retailer who, knowing the risks associated with doing business on the Internet, decides to avoid the practice. This decision will likely cost the company a significant amount of its revenue (if, indeed, the company has products or services that consumers wish to purchase). In addition, the decision may require the company to build or lease a site in each of the locations, globally, for which it wishes to continue business. This could have a catastrophic effect on the company's ability to continue business operations

Risk Acceptance

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

For example, an executive may be confronted with risks identified during the course of a risk assessment for their organization. These risks have been prioritized by high, medium, and low impact to the organization. The executive notes that in order to mitigate or transfer the low-level risks, significant costs could be involved. Mitigation might involve the hiring of additional highly skilled personnel and the purchase of new hardware, software, and office equipment, while transference of the risk to an insurance company would require premium payments. The executive then further notes that minimal impact to the organization would occur if any of the reported low-level threats were realized. Therefore, he or she (rightly) concludes that it is wiser for the organization to forgo the costs and accept the risk. In the

young driver example, risk acceptance could be based on the observation that the youngster has demonstrated the responsibility and maturity to warrant the parent's trust in his or her judgment.

The following answers are incorrect:

Risk Transfer - Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way.

Risk Avoidance - Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized.

Risk Mitigation -Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented.

Reference:
CISA Review Manual 2014 Page number 51
and
Official ISC2 guide to CISSP CBK 3rd edition page number 534-539

QUESTION 3
Which of the following security control is intended to avoid an incident from occurring?

A. Deterrent
B. Preventive
C. Corrective
D. Recovery

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:
Preventive controls are intended to avoid an incident from occurring

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker
Corrective - Corrective control fixes components or systems after an incident has occurred
Recovery - Recovery controls are intended to bring the environment back to regular operations

Reference:

CISA Review Manual 2014 Page number 44
and
Official ISC2 CISSP guide 3rd edition Page number 50 and 51

QUESTION 4
Which of the following control fixes a component or system after an incident has occurred?

A. Deterrent
B. Preventive
C. Corrective
D. Recovery

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:
Corrective control fixes components or systems after an incident has occurred

For your exam you should know below information about different security controls

Deterrent Controls
Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents

associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker

Preventive - Preventive controls are intended to avoid an incident from occurring
Recovery - Recovery controls are intended to bring the environment back to regular operations

Reference:

CISA Review Manual 2014 Page number 44
and
Official ISC2 CISSP guide 3rd edition Page number 50 and 51

QUESTION 5
Which of the following security control is intended to bring environment back to regular operation?

A. Deterrent
B. Preventive
C. Corrective
D. Recovery

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:

Recovery controls are intended to bring the environment back to regular operations
For your exam you should know below information about different security controls

Deterrent Controls
Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls
When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls
Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker

Preventive - Preventive controls are intended to avoid an incident from occurring

Corrective - Corrective control fixes components or systems after an incident has occurred

Reference:

CISA Review Manual 2014 Page number 44
and
Official ISC2 CISSP guide 3rd edition Page number 50 and 51

QUESTION 6
Which of the following is NOT an example of preventive control?

A. Physical access control like locks and door
B. User login screen which allows only authorize user to access website
C. Encrypt the data so that only authorize user can view the same
D. Duplicate checking of a calculations

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:

The word NOT is used as a keyword in the question. You need to find out a security control from given options which in not preventive. Duplicate checking of a calculation is a detective control and not a preventive control.

For your exam you should know below information about different security controls

Deterrent Controls
Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.
The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the

likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or

more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls
Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations. For your exam you should know below information about different security controls

Deterrent Controls
Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker’s appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls
Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function.

Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls

must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls
Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:
The other examples belong to Preventive control.

Reference:
CISA Review Manual 2014 Page number 44
and
Official ISC2 CISSP guide 3rd edition Page number 50 and 51

QUESTION 7
Which of the following audit assess accuracy of financial reporting?

A. Compliance Audit
B. Financial Audit
C. Operational Audit
D. Forensic audit

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

For your exam you should know below information about different types of audit:

What is an audit?
An audit in general terms is a process of evaluating an individual or organization's accounts. This is usually done by an independent auditing body. Thus, audit involves a competent and independent person obtaining evidence and evaluating it objectively with regard to a given entity, which in this case is the subject of audit, in order to establish conformance to a given set of standards. Audit can be on a person, organization, system, enterprise, project or product.

Compliance Audit
A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

What, precisely, is examined in a compliance audit will vary depending upon whether an organization is a public or private company, what kind of data it handles and if it transmits or stores sensitive financial data. For instance, SOX requirements mean that any electronic communication must be backed up and secured with reasonable disaster recovery infrastructure. Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements. Financial services companies that transmit credit card data are subject to PCI DSS requirements. In each case, the organization must be able to demonstrate compliance by producing an audit trail, often generated by data from event log management software.

Financial Audit
A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Operational Audit

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

The Institute of Internal Auditor (IIA) defines Operational Audit as a systematic process of evaluating an organization's effectiveness, efficiency and economy of operations under management's control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement.

Objectives

To appraise the effectiveness and efficiency of a division, activity, or operation of the entity in meeting organizational goals.
To understand the responsibilities and risks faced by an organization.
To identify, with management participation, opportunities for improving control.
To provide senior management of the organization with a detailed understanding of the Operations.

Integrated Audits
An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

IS Audit
An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

Will the organization's computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company's valuable asset (its information) and establish methods of minimizing those risks.

Forensic Audit
Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

The following answers are incorrect:

Compliance Audit - A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

Operational Audit - Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives.[1] Operational audit is a more comprehensive form of an Internal audit.

Forensic Audit - Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

Reference:

CISA Review Manual 2014 Page number 44
http://searchcompliance.techtarget.com/definition/compliance-audit
http://en.wikipedia.org/wiki/Financial_audit
http://en.wikipedia.org/wiki/Operational_auditing
http://en.wikipedia.org/wiki/Information_technology_audit
http://www.investorwords.com/16445/forensic_audit.html

QUESTION 8
Which of the following audit risk is related to exposure of a process or entity to be audited without taking into account the control that management has implemented?

A. Inherent Risk
B. Control Risk
C. Detection Risk
D. Overall Audit Risk

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:

Inherent Risk is the risk level or exposure of a process or entity to be audited without taking into account the control that management has implemented. Inherent risk exists independent of an audit and can occur because of the nature of the business.

For your exam you should know below information about audit risk:

Audit risk (also referred to as residual risk) refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR), and can be calculated thus:

AR = IR × CR × DR

Inherent Risk

Auditors must determine risks when working with clients. One type of risk to be aware of is inherent risk. While assessing this level of risk, you ignore whether the client has internal controls in place (such as a secondary review of financial statements) in order to help mitigate the inherent risk. You consider the strength of the internal controls when assessing the client's control risk. Your job when assessing inherent risk is to evaluate how susceptible the financial statement assertions are to material misstatement given the nature of the client's business. A few key factors can increase inherent risk.

Environment and external factors: Here are some examples of environment and external factors that can lead to high inherent risk:

Rapid change: A business whose inventory becomes obsolete quickly experiences high inherent risk.
Expiring patents: Any business in the pharmaceutical industry also has inherently risky environment and external factors. Drug patents eventually expire, which means the company faces competition from other manufacturers marketing the same drug under a generic label. State of the economy: The general level of economic growth is another external factor affecting all businesses.
Availability of financing: Another external factor is interest rates and the associated availability of financing. If your client is having problems meeting its short-term cash payments, available loans with low interest rates may mean the difference between your client staying in business or having to close its doors.
Prior-period misstatements: If a company has made mistakes in prior years that weren't material (meaning they weren't significant enough to have to change), those errors still exist in the financial statements. You have to aggregate prior-period misstatements with current year misstatements to see if you need to ask the client to adjust the account for the total misstatement.

You may think an understatement in one year compensates for an overstatement in another year. In auditing, this assumption isn't true. Say you work a cash register and one night the register comes up $20 short. The next week, you somehow came up $20 over my draw count. The $20 differences are added together to represent the total amount of your mistakes which is $40 and not zero. Zero would indicate no mistakes at all had occurred.

Susceptibility to theft or fraud: If a certain asset is susceptible to theft or fraud, the account or balance level may be considered inherently risky. For example, if a client has a lot of customers who pay in cash, the balance sheet cash account is going to have risk associated with theft or fraud because of the fact that cash is more easily diverted than customer checks or credit card payments.

Looking at industry statistics relating to inventory theft, you may also decide to consider the inventory account as inherently risky. Small inventory items can further increase the risk of this account valuation being incorrect because those items are easier to conceal (and therefore easier to steal).

Control Risk
Control risk has been defined under International Standards of Auditing (ISAs) as following:

The risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's internal control.

In simple words control risk is the probability that a material misstatement exists in an assertion because that misstatement was not either prevented from entering entity's financial information or it was not detected and corrected by the internal control system of the entity.

It is the responsibility of the management and those charged with governance to implement internal control system and maintain it appropriately which includes managing control risk.

There can be many reasons for control risk to arise and why it cannot be eliminated absolutely. But some of them are as follows:

Cost-benefit constraints
Circumvention of controls
Inappropriate design of controls
Inappropriate application of controls
Lack of control environment and accountability
Novel situations
Outdated controls
Inappropriate segregation of duties

Detection Risk
Detection Risk is the risk that the auditors fail to detect a material misstatement in the financial statements.

An auditor must apply audit procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit procedures may result in a material misstatement remaining undetected by the auditor. Some detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions.
Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed testing.

The following answers are incorrect:
Control Risk - The risk that material error exist that would not be prevented or detected on timely basis by the system of internal controls.

Detection risk - The risk that material errors or misstatements that have occurred will not be detected by an IS auditor.
Overall audit risk - The probability that information or financial report may contain material errors and that the auditor may not detect an error that has occurred. An objective in formulating the audit approach is to limit the audit risk in the area under security so the overall audit risk is at sufficiently low level at the completion of the examination.

Reference:

CISA review manual 2014 page number 50
http://en.wikipedia.org/wiki/Audit_risk
http://www.dummies.com/how-to/content/how-to-assess-inherent-risk-in-an-audit.html
http://pakaccountants.com/what-is-control-risk/ http://accounting-simplified.com/audit/risk-assessment/audit-risk.html

QUESTION 9
Which of the following statement INCORRECTLY describes the Control self-assessment (CSA) approach?

A. CSA is policy or rule driven
B. CSA Empowered/accountable employees
C. CSA focuses on continuous improvement/learning curve
D. In CSA, Staffs at all level, in all functions, are the primary control analyst.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:

The word INCORRECTLY is the keyword used in the question. You need to find out an option which incorrectly describes Control Self-assessment.

For your exam you should know the information below about control self-assessment:

Control self-assessment is an assessment of controls made by the staff and management of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal controls of the organization are reliable. Benefits of CSA

Early detection of risk
More efficient and improved internal controls
Creation of cohesive teams through employee involvement
Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives
Increased employee awareness of organizational objectives, and knowledge of risk and internal controls
Highly motivated employees
Improved audit training process
Reduction in control cost
Assurance provided to stakeholders and customers

Traditional and CSA attributes
Traditional Historical CSA
Assign duties/supervises staff Empowered/accountable employees
Policy/rule driven Continuous improvement/learning curve
Limited employee participation Extensive employee participation and training
Narrow stakeholders focus Broad stakeholders focus
Auditors and other specialist Staff at all level, in all functions, are the primary control analysts

The following answers are incorrect:

The other options specified are correctly describes about CSA.

Reference:
CISA review manual 2014 page number 61, 62 and 63

QUESTION 10
Statistical sampling is NOT based on which of the following audit sample techniques?

A. Haphazard Sampling

B. Random Sampling
C. Cell Sampling
D. Fixed interval sampling

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Explanation:
The NOT keyword is used in the question. You need find out an option which is NOT an example of statistical sampling. Statistical sampling is NOT based on Haphazard sampling.
For your exam you should know the information below

Audit samples are selected for the purpose of collecting representative evidence to be subjected to either compliance testing or substantive testing. The auditor should consider a selection technique that will provide the most relevant evidence supported by appropriate analytical procedures.
Two basic types of audit samples can be designed by the auditor to fulfill their requirements:
statistical and no statistical. Below Figure shows the various audit samples, as well as their testing methods. Care is given to the selection process in order to avoid drawing the wrong conclusion from the wrong sample. This is referred to as a sampling risk. Let's look at each of these samples more closely.

Statistical Sampling
Statistical sampling uses mathematical techniques that result in an outcome that is mathematically quantifiable. Statistical samples are usually presented as a percentage. The purpose of statistical sampling is to gain an objective representation. Samples are selected by an objective mathematical process. The auditor should be aware that if the client has strong internal controls, the sample sizes may be smaller because the odds of fraud or failure will be lower.
Examples of statistical sampling include the following:

Random sampling Samples are selected at random.
Cell sampling Random selection is performed at predefined intervals.
Fixed interval sampling The sample existing at every n + interval increment is selected for testing.

No statistical Sampling
No statistical sampling is based on the auditor's judgment (also referred to as judgmental sampling). The auditor determines the sample size, the method of generating the sample, and the number of items to be analyzed. The results of judgmental sampling are unlikely to represent the actual population. This is a subjective process usually based on elements of risk or materiality. An example of no statistical sampling includes haphazard sampling, in which the samples are randomly drawn for testing.
After the samples are selected, the next step is to perform compliance tests or substantive testing.

Conducting Audit Testing As stated earlier, the basic test methods used will be either compliance testing or substantive testing. Appropriate audit samples will have to be generated for the test.

Compliance Testing
Compliance testing tests for the presence or absence of something. Compliance testing includes verifying that policies and procedures have been put in place, and checking that user access rights, program change control procedures, and system audit logs have been activated. An example of a compliance test is comparing the list of persons with physical access to the data center against the HR list of current employees.

Compliance testing is based on one of the following types of audit samples:

Attribute sampling Generally popular in compliance testing. The objective is to determine whether an attribute is present or absent in the subject sample. The result is specified by the rate of occurrence—for example, the presence of 1 in 100 units would be 1 percent.
Stop-and-go sampling Used when few errors are expected. Stop-and-go allows the test to occur without excessive effort in sampling and provides the opportunity to stop testing at the earliest possible opportunity. It is a simple form of testing to reinforce any claim that errors are unlikely in the sample population.

Discovery sampling A 100 percent sampling used to detect fraud or when the likelihood of evidence existing is low. Forensics is an excellent example of discovery sampling. This is an attempt to discover evidence.
Precision, or expected error rate The precision rate indicates the acceptable margin of error between audit samples and the total quantity of the subject population. This is usually expressed as a percentage, such as 5 percent. To obtain a very low error rate, it is necessary to use a very large sample in testing. Auditors are justified in using a smaller sample size when the total population is expected to be error-free. A larger sample is required when errors are expected to be present in the population. The larger sample can yield a higher average. When errors are expected, the auditor must examine more data to determine whether the actual errors are within a tolerable error rate (maximum errors you would accept).
Error levels may be determined by reviewing the findings of a prior audit and by considering changes in the organization's procedures. Use the risk-based audit strategy to determine whether your samples and tests are telling the truth about the audited.

Substantive Testing
Substantive testing seeks to verify the content and integrity of evidence. Substantive tests may include complex calculations to verify account balances, perform physical inventory counts, or execute sample transactions to verify the accuracy of supporting documentation. Substantive tests use audit samples selected by dollar value or to project (forecast or estimate) a total for groups with related characteristics.

Substantive testing is based on one of the following types of audit samples:

Variable sampling Used to designate dollar values or weights (effectiveness) of an entire subject population by prorating from a smaller sample. Consider the challenge of counting large volumes of currency by its weight. Variable sampling could be used to count currency by multiplying the physical weight of one unit by the total weight of the combined sample, and then multiplying by the face value printed on the bill or coin. A demonstration is a single $50 bill weighing 1.0 gram, with the entire sample of $50 bills weighing 61 grams altogether. The combined sample weight would indicate a total quantity of 61 bills for an estimated dollar value of $3,050. This is a common technique for forecasting quantity and value of inventory based on particular characteristics.

Unsatisfied mean estimation Used in an attempt to project an estimated total for the whole subject population.
Stratified mean estimation Used to calculate an average by group, similar to demographics, whereby the entire population is divided (stratified) into smaller groups based on similar characteristics.
Examples are teenagers from the ages of 13 to 19, people from the ages of 20 to 29, people from the ages of 30 to 39, and those who are male or female, smokers or nonsmokers, and so on. Difference estimation Used to determine the difference between audited and unaudited claims of value.

The following answers are incorrect:

The other options like Random Sampling, Cell Sampling and Fixed Interval Sampling are examples of Statistical sampling.

Reference:

CISA review manual 2014 page number 55 to 56
CISA certified information system auditor study guide Second Edition Page Number 98 to 101

QUESTION 11
An organization performs nightly backups but does not have a formal policy. An IS auditor should **FIRST**:

A. evaluate current backup procedures
B. escalate to senior management
C. document a policy for the organization
D. recommend automated backup

Correct Answer: A
Section: The process of Auditing Information System
Explanation
Explanation/Reference:

QUESTION 12
In a follow-up audit, an IS auditor notes that management has addressed the original findings in a different way than originally agreed upon. The auditor should **FIRST:**

A. mark the recommendation as satisfied and close the finding
B. verify if management's action mitigates the identified risk

C. re-perform the audit to assess the changed control environment
D. escalate the deviation to the audit committee

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 13
An organization is considering outsourcing the processing of customer insurance claims. An IS auditor notes that customer data will be sent offshore for processing. Which of the following would be the **BEST** way to address the risk of exposing customer data?

A. Require background checks on all service provider personnel involved in the processing of data.
B. Recommend the use of a service provider within the same country as the organization.
C. Consider whether the service provider has the ability to meet service level agreements (SLAs).
D. Assess whether the service provider meets the organization's data protection policies.

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 14
An IS audit team is evaluating the documentation related to the most recent application user-access review performed by IT and business management. It is determined the user list was not system-generated. Which of the following should be the **GREATEST** concern?
A. Source of the user list reviewed
B. Availability of the user list reviewed
C. Confidentiality of the user list reviewed
D. Completeness of the user list reviewed

Correct Answer: A

Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 15
Which of the following should an IS auditor determine **FIRST** when evaluating additional hardware required to support the acquisition of a new accounting system?

A. A training program has been developed to support the new accounting system.
B. The supplier has experience supporting accounting systems.
C. The hardware specified will be compliant with the current IT strategy.
D. The hardware will be installed in a secure and environmentally controlled area.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 16
A company requires that all program change requests (PCRs) be approved and all modifications be automatically logged. Which of the following IS audit procedures will **BEST** determine whether unauthorized changes have been made to production programs?

A. Review a sample of PCRs for proper approval throughout the program change process.
B. Trace a sample of program changes from the log to completed PCR forms.
C. Use source code comparison software to determine whether any changes have been made to a sample of programs since the last audit date.
D. Trace a sample of complete PCR forms to the log of all program changes.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 17
An IS auditor submitted audit reports and scheduled a follow-up audit engagement with a client. The client has requested to engage the services of the same auditor to develop enhanced controls. What is the **GREATEST** concern with this request?

A. It would require the approval of the audit manager.
B. It would be beyond the original audit scope.
C. It would a possible conflict of interest.
D. It would require a change to the audit plan.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 18
The risk that the IS auditor will not find an error that has occurred is identified by which of the following terms?

A. Control
B. Prevention
C. Inherent
D. Detection

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 19
An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the **BEST** recommendation by the IS auditor?

A. Improve the change management process
B. Perform a configuration review
C. Establish security metrics
D. Perform a penetration test

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 20
An IS auditor reviewing a new application for compliance with information privacy principles should be the **MOST** concerned with:

A. nonrepudiation
B. collection limitation
C. availability
D. awareness

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 21
Which of the following is the **PRIMARY** reason for an IS auditor to issue an interim audit report?

A. To avoid issuing a final audit report
B. To enable the auditor to complete the engagement in a timely manner
C. To provide feedback to the auditee for timely remediation
D. To provide follow-up opportunity during the audit

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 22
Which of the following conditions would be of **MOST** concern to an IS auditor assessing the risk of a successful brute force attack encrypted data at rest?

A. Use of symmetric encryption
B. Use of asymmetric encryption
C. Random key generation
D. Short key length

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 23
In which of the following SDLC phases would the IS auditor expect to find that controls have been incorporated into system specifications?

A. Development
B. Implementation
C. Design
D. Feasibility

Correct Answer: B
Section: The process of Auditing Information System
Explanation
Explanation/Reference:

QUESTION 24
An IS auditor observes a system performance monitoring tool which states that a server critical to the organization averages high CPU utilization across a cluster of four virtual servers throughout the audit period. To determine if further investigation is required, an IS auditor should review:

A. the system process activity log
B. system baselines
C. the number of CPUs allocated to each virtual machine
D. organizational objectives

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 25
An IS auditor has discovered that a cloud-based application was not included in an application inventory that was used to confirm the scope of an audit. The business process owner explained that the application will be audited by a third party in the next year. The auditor's **NEXT** step should be to:

A. evaluate the impact of the cloud application on the audit scope
B. revise the audit scope to include the cloud-based application
C. review the audit report when performed by the third party

D. report the control deficiency to senior management

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 26
Which of the following should **MOST** concern an IS auditor reviewing an intrusion detection system (IDS)?

A. Number of false negatives

B. Number of false positives
C. Legitimate traffic blocked by the system
D. Reliability of IDS logs

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 27
An IS auditor considering the risks associated with spooling sensitive reports for off-line printing will be the **MOST** concerned that:

A. data can easily be read by operators
B. data can more easily be amended by unauthorized persons
C. unauthorized copies of reports can be printed
D. output will be lost if the system should fail

Correct Answer: C

Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 28
Before concluding that internal controls can be relied upon, the IS auditor should:

A. discuss the internal control weaknesses with the auditee
B. document application controls
C. conduct tests of compliance
D. document the system of internal control

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
QUESTION 29
The IS auditor has identified a potential fraud perpetrated by the network administrator. The IS auditor should:

A. issue a report to ensure a timely resolution
B. review the audit finding with the audit committee prior to any other discussions
C. perform more detailed tests prior to disclosing the audit results
D. share the potential audit finding with the security administrator

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 30

Which of the following should be of **MOST** concern to an IS auditor reviewing the public key infrastructure (PKI) for enterprise e-mail?

A. The private key certificate has not been updated.
B. The certificate revocation list has not been updated.
C. The certificate practice statement has not been published.
D. The PKI policy has not been updated within the last year.

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 31
An IS auditor observes that the CEO has full access to the enterprise resource planning (ERP) system. The IS auditor should **FIRST**:

A. accept the level of access provided as appropriate
B. recommend that the privilege be removed
C. ignore the observation as not being material to the review
D. document the finding as a potential risk

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 32
The **GREATEST** risk when performing data normalization is:

A. the increased complexity of the data model
B. duplication of audit logs
C. reduced data redundancy

D. decreased performance

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is the **BEST** way to evaluate the effectiveness of access controls to an internal network?

A. Perform a system penetration test
B. Test compliance with operating procedures
C. Review access rights
D. Review router configuration tables

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
QUESTION 34
An internal control audit has revealed a control deficiency related to a legacy system where the compensating controls no longer appear to be effective. Which of the following would **BEST** help the information security manager determine the security requirements to resolve the control deficiency?

A. Cost-benefit analysis
B. Gap analysis
C. Risk assessment
D. Business case

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 35
An audit of the quality management system (QMS) begins with an evaluation of the:

A. organization's QMS policy
B. sequence and interaction of QMS processes
C. QMS processes and their application
D. QMS document control procedures

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 36
An IS auditor is conducting a review of a healthcare organization's IT policies for handling medical records. Which of the following is MOST important to verify?

A. A documented policy approval process is in place
B. Policy writing standards are consistent
C. The policies comply with regulatory requirements
D. IT personnel receive ongoing policy training

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 37
Audit management has just completed the annual audit plan for the upcoming year, which consists entirely of high-risk processes. However, it is determined that there are insufficient resources to execute the plan. What should be done NEXT?

A. Remove audits from the annual plan to better match the number of resources available
B. Reduce the scope of the audits to better match the number of resources available
C. Present the annual plan to the audit committee and ask for more resources
D. Review the audit plan and defer some audits to the subsequent year

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 38
If concurrent update transactions to an account are not processed properly, which of the following will be affected?

A. Integrity
B. Confidentiality
C. Availability
D. Accountability

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
QUESTION 39
Which of the following is the MOST appropriate responsibility of an IS auditor involved in a data center renovation project?

A. Performing independent reviews of responsible parties engaged in the project
B. Ensuring the project progresses as scheduled and milestones are achieved
C. Performing day-to-day activities to ensure the successful completion of the project
D. Providing sign off on the design of controls for the data center

Correct Answer: A

Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 40
During a privileged access review, an IS auditor observes many help desk employees have privileges within systems not required for their job functions. Implementing which of the following would have prevented this situation?

A. Separation of duties
B. Multi-factor authenticationC. Least privilege access
D. Privileged access reviews

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 41
An IS auditor discovered abnormalities in a monthly report generated from a system upgraded six months ago. Which of the following should be the auditor's FIRST course of action?

A. Inspect source code for proof of abnormalities
B. Perform a change management review of the system
C. Schedule an access review of the system
D. Determine the impact of abnormalities in the report

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 42
An IS auditor conducting audit follow-up activities learns that some previously agreed-upon corrective actions have not been taken and that the associated risk has been accepted by senior management. If the auditor disagrees with management's decision, what is the BEST way to address the situation?

A. Repeat the audit with audit scope only covering areas with accepted risks
B. Report the issue to the chief audit executive for resolution
C. Recommend new corrective actions to mitigate the accepted risk
D. Take no action since management's decision has been made

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 43
During a security audit, an IS auditor is tasked with reviewing log entries obtained from an enterprise intrusion prevention system (IPS). Which type of risk would be associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration?

A. Inherent risk
B. Sampling risk
C. Control risk
D. Detection risk

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
QUESTION 44
An IS auditor is analyzing a sample of accesses recorded on the system log of an application. The auditor intends to launch an intensive investigation if one exception is found. Which sampling method would be appropriate?

A. Discovery sampling

B. Variable sampling
C. Stratified sampling
D. Judgmental sampling

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 45
An IS auditor is assessing risk associated with peer-to-peer file sharing within an organization. Which of the following should be of GREATEST concern?

A. File-sharing policies have not been reviewed since last year
B. Only some employees are required to attend security awareness training
C. Not all devices are running antivirus programs
D. The organization does not have an efficient patch management process

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 46
An IS auditor is reviewing an organization's incident management processes and procedures. Which of the following observations should be the auditor's GREATEST concern?

A. Ineffective incident classification
B. Ineffective incident prioritization
C. Ineffective incident detection
D. Ineffective post-incident review

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 47
An IS auditor is conducting a pre-implementation review to determine a new system's production readiness. The auditor's PRIMARY concern should be whether:

A. the project adhered to the budget and target date
B. users were involved in the quality assurance (QA) testing
C. there are unresolved high-risk items
D. benefits realization has been evidenced

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 48
An IS auditor reviewing the threat assessment for a data center would be MOST concerned if:

A. all identified threats relate to external entities
B. some of the identified threats are unlikely to occur
C. neighboring organizations' operations have been included
D. the exercise was completed by local management

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 49
Which of the following should an IS auditor verify when auditing the effectiveness of virus protection?

A. Frequency of IDS log reviews
B. Currency of software patch application
C. Schedule for migration to production
D. Frequency of external Internet access

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 50
Which of the following should be reviewed FIRST when planning an IS audit?

A. Recent financial information
B. Annual business unit budget
C. IS audit standards
D. The business environment

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 51
An auditor notes the administrator user ID is shared among three financial managers to perform month-end updates. Which of the following is the BEST recommendation to ensure the administrator ID in the financial system is controlled effectively?

A. Implement use of individual software tokens

B. Conduct employee awareness training
C. Institute user ID logging and monitoring
D. Ensure data in the financial systems has been classified

Correct Answer:
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
A

QUESTION 52
An IS auditor is involved with a project and finds an IT project stakeholder wants to make a change that could affect both the project scope and schedule. Which of the following would be the MOST appropriate action for the project manager with respect to the change request?

A. Recommend to the project sponsor whether to approve the change
B. Modify the project plan as a result of the change
C. Evaluate the impact of the change
D. Ignore out-of-scope requests

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 53
Which of the following should an IS auditor expect to see in a network vulnerability assessment?

A. Misconfiguration and missing updates
B. Malicious software and spyware
C. Security design flaws
D. Zero-day vulnerabilities

Correct Answer: C

Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 54
An IS auditor is evaluating the security of an organization's data backup process, which includes the transmission of daily incremental backups to a dedicated offsite server. Which of the following findings poses the GREATEST risk to the organization?

A. Backup transmissions are not encrypted
B. Backup transmissions occasionally fail
C. Data recovery testing is conducted once per year
D. The archived data log is incomplete

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 55
When continuous monitoring systems are being implemented, an IS auditor should FIRST identify:

A. the location and format of output files
B. applications that provide the highest financial risk
C. high-risk areas within the organization
D. the controls on which to focus

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

Correct Answer:
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
QUESTION 56
During a follow-up audit, an IS auditor concludes that a previously identified issue has not been adequately remediated. The auditee insists the risk has been addressed. The auditor should:

A. recommend an independent assessment by a third party
B. report the disagreement according to established procedures
C. follow-up on the finding next year
D. accept the auditee's position and close the finding

A

QUESTION 57
An organization allows employee use of personal mobile devices for corporate email. Which of the following should be the GREATEST IS audit concern?

A. Email forwarding to private devices requires excessive network bandwidth
B. There is no corporate policy for the acceptable use of private devices
C. There is no adequate tracking of the working time spent out-of-hours
D. The help desk is not able to fully support different kinds of private devices

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 58

Which of the following findings would be of GREATEST concern to an IS auditor reviewing an organization's newly implemented online security awareness program?

A. Only new employees are required to attend the program
B. The timing for program updates has not been determined
C. Metrics have not been established to assess training results
D. Employees do not receive immediate notification of results

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 59
Which of the following is MOST important for an IS auditor to ensure is included in a global organization's online data privacy notification to customers?

A. Consequences to the organization for mishandling the data
B. Consent terms including the purpose of data collection
C. Contact information for reporting violations of consent
D. Industry standards for data breach notification

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 60
Which of the following is **MOST** important for an IS auditor to review when evaluating the effectiveness of an organization's incident response process?

A. Past incident response actions
B. Incident response staff experience and qualifications

Correct Answer:
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
C. Results from management testing of incident response procedures
D. Incident response roles and responsibilities

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 61
Which of the following observations would an IS auditor consider the **GREATEST** risk when conducting an audit of a virtual server farm for potential software vulnerabilities?

A. The hypervisor is updated quarterly.
B. Guest operating systems are updated monthly.
C. Antivirus software has been implemented on the guest operating system only.
D. A variety of guest operating systems operate on one virtual server.

C

QUESTION 62
An IS auditor is mapping controls to risk for an accounts payable system. What is the **BEST** control to detect errors in the system?

A. Alignment of the process to business objectives
B. Quality control review of new payments
C. Management approval of payments
D. Input validation

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 63
When auditing a quality assurance plan, an IS auditor should be **MOST** concerned if the:

A. quality assurance function is separate from the programming function.
B. SDLC is coupled with the quality assurance plan.
C. quality assurance function is periodically reviewed by internal audit.
D. scope of quality assurance activities is undefined.

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 64
The **PRIMARY** reason for an IS auditor to use data analytics techniques is to reduce which type of audit risk?
A. Technology risk
B. Inherent risk
C. Detection risk
D. Control risk

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

Correct Answer:
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 65

While reviewing similar issues in an organization's help desk system, an IS auditor finds that they were analyzed independently and resolved differently. This situation **MOST** likely indicates a deficiency in:

A. IT service level management.
B. change management.
C. configuration management.
D. problem management.

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 66

An auditor is creating an audit program in which the objective is to establish the adequacy of personal data privacy controls in a payroll process. Which of the following would be **MOST** important to include?

A. Approval of data changes
B. Audit logging of administrative user activity
C. Segregation of duties controls
D. User access provisioning

C

QUESTION 67

While reviewing a hot site, the IS auditor discovers that one type of hardware platform is not installed. The IS auditor should **FIRST**:

A. recommend the purchase and installation of hardware at the hot site.
B. report the finding immediately to senior IS management.
C. determine the business impact of the absence of the hardware.
D. establish the lead time for delivery of a new machine.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 68
Which of the following is the **MOST** important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

A. Peak activity periods for the business
B. Remediation dates included in management responses
C. Availability of IS audit resources
D. Complexity of business processes identified in the audit

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 69
An IS auditor has obtained a large data set containing multiple fields and non-numeric data for analysis. Which of the following activities will **MOST** improve the quality of conclusions derived from the use of a data analytics tool for this audit?

A. Data anonymization
B. Data classification

Correct Answer:
Section: The process of Auditing Information System
Explanation

Explanation/Reference:
C. Data stratification
D. Data preparation

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 70
Which of the following is the **MOST** important requirement for an IS auditor to evaluate when reviewing a transmission of personally identifiable information (PII) between two organizations?

A. Completeness
B. Timeliness
C. Necessity
D. Accuracy

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 71
An IS auditor reviewed the business case for a proposed investment to virtualize an organization's server infrastructure. Which of the following is **MOST** likely to be included among the benefits in the project proposal?

A. Fewer operating system licenses
B. Better efficiency of logical resources

C. Reduced hardware footprint
D. Less memory and storage space

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 72
Which of the following would be the **MOST** efficient audit approach, given that a compliance-based approach was adopted in the previous year?

A. Validate all applications using test data.
B. Interview systems personnel to evaluate all automated controls.
C. Evaluate the controls surrounding changes to programs.
D. Perform a review of significant transactions posted within the system.

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 73
An IS auditor will be testing accounts payable controls by performing data analytics on the entire population transactions. Which of the following is **MOST** important for the auditor to confirm when sourcing the population data?

A. There is no privacy information in the data.
B. The data analysis tools have been recently updated.
C. The data can be obtained in a timely manner.
D. The data is taken directly from the system.

Explanation/Reference:

Correct Answer: A
Section: The process of Auditing Information System
Explanation
QUESTION 74
Which of the following should be of **GREATEST** concern to an IS auditor reviewing actions taken during a forensic investigation?

A. The investigation report does not indicate a conclusion.
B. An image copy of the attacked system was not taken.
C. The proper authorities were not notified.
D. The handling procedures of the attacked system are not documented.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 75
An IS audit report highlighting inadequate network internal controls is challenged because no serious incident has ever occurred. Which of the following actions performed during the audit would have **BEST** supported the findings?

A. Compliance testing
B. Threat risk assessment
C. Penetration testing
D. Vulnerability assessment

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 76

Which of the following is the **PRIMARY** reason for an IS auditor to use computer-assisted audit techniques (CAATs)?

A. To efficiently test an entire population
B. To perform direct testing of production data
C. To conduct automated sampling for testing
D. To enable quicker access to information

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 77
An IS auditor is planning to audit an organization's infrastructure for access, patching, and change management. Which of the following is the **BEST** way to prioritize the systems?

A. Complexity of the environment
B. Criticality of the system
C. System hierarchy within the infrastructure
D. System retirement plan

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 78
Which of the following would be the **GREATEST** concern to an IS auditor reviewing an IT outsourcing arrangement?
Explanation/Reference:

A. Several IT personnel perform the same functions as the vendor.
B. The contract does not include a renewal option.
C. Development of KPIs that will be used was assigned to the vendor.
D. Some penalties were waived during contract negotiations.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

D.

QUESTION 79
To **BEST** evaluate the effectiveness of a disaster recovery plan, the IS auditor should review the:

A. test plan and results of past tests.
B. plans and procedures in the business continuity plan.
C. capacity of backup facilities.
D. hardware and software inventory.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 80
An internal audit department recently established a quality assurance (QA) program as part of its overall audit program. Which of the following activities should be included as part of the QA program requirements?

A. Reporting program results to the board
B. Reviewing audit standards periodically
C. Analyzing user satisfaction reports from business lines
D. Conducting long-term planning for internal audit staffing

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

Explanation/Reference:

QUESTION 81
An IS auditor has observed gaps in the data available to the organization for detecting incidents. Which of the following would be the **BEST** recommendation to improve the organization's security incident response capability?

A. Document procedures for incident escalation.
B. Document procedures for incident classification.
Correlate security logs collected from multiple sources.
Centralize alerts and security log information.

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 82
When reviewing the effectiveness of data center operations, the IS auditor would **FIRST** establish that system performance:

A. is monitored and reported against agreed service levels.
B. reflects the expected usage levels established at implementation.
C. meets the expected targets specified by the manufacturer.
D. is within generally accepted reliability levels for that system.

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 83

C.

D.

Which of the following is the **MOST** important for an IS auditor to do during an exit meeting with an auditee?

A. Ensure that the facts presented in the report are correct.
B. Specify implementation dates for the recommendations.
C. Request input in determining corrective action.
D. Communicate the recommendations to senior management.

Correct Answer: A
Section: The process of Auditing Information System
Explanation
QUESTION 84
An IS auditor finds that confidential company data has been inadvertently leaked through social engineering. The **MOST** effective way to help prevent a recurrence of this issue is to implement:

A. penalties to staff for security policy breaches.
B. a third-party intrusion prevention solution.
C. a security awareness program.
D. data loss prevention (DLP) software.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 85
An organization is developing data classification standards and has asked internal audit for advice on aligning the standards with best practices. Internal audit would **MOST** likely recommend the standards should be:

A. based on the results of an organization-wide risk assessment.
Explanation/Reference:

B. based on the business requirements for confidentiality of the information.
C. aligned with the organization's segregation of duties requirements.
D. based on the business requirements for authentication of the information.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 86
Internal audit reports should be **PRIMARILY** written for and communicated to:

A. audit management, as they are responsible for the quality of the audit.
B. external auditors, as they provide an opinion on the financial statements. auditees, as they will eventually have to implement the recommendations.

C.

D.

senior management, as they should be informed about the identified risks.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 87
Which of the following should be done **FIRST** to effectively define the IT audit universe for an entity with multiple business lines?

A. Identify aggregate residual IT risk for each business line.
B. Obtain a complete listing of the entity's IT processes.
C. Obtain a complete listing of assets fundamental to the entity's businesses.
D. Identify key control objectives for each business line's core processes.

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 88
An IS auditor determines that a business continuity plan has not been reviewed and approved by management. Which of the following is the **MOST** significant risk associated with this situation?

A. Continuity planning may be subject to resource constraints.
B. The plan may not be aligned with industry best practice.
C. Critical business processes may not be addressed adequately.
D. The plan has not been reviewed by risk management.

Correct Answer: D

Section: The process of Auditing Information System
Explanation

Explanation/Reference:
QUESTION 89
Which of the following is **MOST** important when planning a network audit?

A. Determination of IP range in use
B. Isolation of rogue access points
C. Identification of existing nodes
D. Analysis of traffic content

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 90
IS audit is asked to explain how local area network (LAN) servers can contribute to a rapid dissemination of viruses. The IS auditor's **BEST** response is that:

A. the server's software is the prime target and is the first to be infected.
B. the server's operating system exchanges data with each station starting at every log-on.
C. the server's file sharing function facilitates the distribution of files and applications.
D. users of a given server have similar usage of applications and files.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

C.

D.

QUESTION 91
During a review of an application system, an IS auditor identifies automated controls designed to prevent the entry of duplicate transactions. What is the **BEST** way to verify that the controls work as designed?

A. Implement periodic reconciliations.
B. Review quality assurance (QA) test results.
Use generalized audit software for seeking data corresponding to duplicate transactions.
Enter duplicate transactions in a copy of the live system.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 92
During business process reengineering (BPR) of a bank's teller activities, an IS auditor should evaluate:

A. the impact of changed business processes.
B. the cost of new controls.
C. BPR project plans.
D. continuous improvement and monitoring plans.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 93
A large insurance company is about to replace a major financial application. Which of the following is the IS auditor's **PRIMARY** focus when conducting the preimplementation review?

A. Procedure updates
B. Migration of data
C. System manuals
D. Unit testing

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

C.

QUESTION 94
An audit team has a completed schedule approved by the audit committee. After starting some of the scheduled audits, executive management asked the team to immediately audit an additional process. There are not enough resources available to add the additional audit to the schedule. Which of the following is the **BEST** course of action?

A. Revise the scope of scheduled audits.
B. Propose a revised audit schedule.
C. Approve overtime work to ensure the audit is completed.
D. Consider scheduling the audit for the next period.

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 95
During a vulnerability assessment, an IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer orders via credit card. The IS auditor should **FIRST**:

A. notify management.
B. redesign the customer order process.
C. document the finding in the report.
D. suspend credit card processing.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is the **PRIMARY** objective of the IS audit function?

A. Perform reviews based on standards developed by professional organizations.
B. Reports to management on the functioning of internal controls.
C. Certify the accuracy of financial data.
D. Facilitate extraction of computer-based data for substantive testing.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 97
A database administrator (DBA) extracts a user listing for an auditor as testing evidence. Which of the following will provide the **GREATEST** assurance that the user listing is reliable?

A. Requesting a query that returns the count of the users.
B. Requesting a copy of the query that generated the user listing
C. Obtaining sign-off from the DBA to attest that the list is complete
D. Witnessing the DBA running the query in-person

Correct Answer:
Section: The process of Auditing Information System

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 98
During an audit, it is discovered that several suppliers with standing orders have been deleted from the supplier master file. Which of the following controls would have **BEST** prevented such an occurrence?

A. Logical relationship check
B. Existence check
C. Table look-ups
D. Referential integrity

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 99
Which of the following should be of **GREATEST** concern to an IS auditor reviewing the controls for a continuous software release process?

A. Release documentation is not updated to reflect successful deployment.
B. Test libraries have not been reviewed in over six months.
C. Developers are able to approve their own releases.
D. Testing documentation is not attached to production releases.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 100
While executing follow-up activities, an IS auditor is concerned that management has implemented corrective actions that are different from those originally discussed and agreed with the audit function. In order to resolve the situation, the IS auditor's **BEST** course of action would be to:

A. determine whether the alternative controls sufficiently mitigate the risk and record the results.
B. reject the alternative controls and re-prioritize the original issue as high risk.
C. postpone follow-up activities and escalate the alternative controls to senior audit management.
D. schedule another audit due to the implementation of alternative controls.

A

Correct Answer:
Section: The process of Auditing Information System

Explanation

Explanation/Reference:

QUESTION 101
Which of the following communication modes should be of **GREATEST** concern to an IS auditor evaluating end-user networking?

A. System-to-system
B. Peer-to-peer
C. Host-to-host
D. Client-to-server

Correct Answer: B
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 102
An IS auditor is reviewing an organization's sales and purchasing system due to ongoing data quality issues. An analysis of which of the following would provide the **MOST** useful information to determine the revenue loss?

A. Correlation between the number of issues and average downtime
B. Cost of implementing data validation controls within the system
C. Comparison of the cost of data acquisition and loss in sales revenue
D. Correlation between data errors and loss in value of transactions

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 103
During a help desk review, an IS auditor determines the call abandonment rate exceeds agreed-upon service levels. What conclusions can be drawn from this finding?

A. There are insufficient telephone lines available to the help desk.
B. There is insufficient staff to handle the help desk call volume.
C. Help desk staff are unable to resolve a sufficient number of problems on the first call.
D. Users are finding solutions from alternative sources.

Correct Answer: B
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 104
When reviewing backup policies, an IS auditor **MUST** verify that backup intervals of critical systems do not exceed which of the following?

A. Recovery point objective (RPO)
B. Recovery time objective (RTO)
C. Service level objective (SLO)
D. Maximum acceptable outage (MAO)

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 105
Which of the following projects would be **MOST** important to review in an audit of an organization's financial statements?

Correct Answer:
Section: The process of Auditing Information System

Explanation

Explanation/Reference:

A. Resource optimization of the enterprise resource planning (ERP) system
B. Security enhancements to the customer relationship database
C. Automation of operational risk management processes
D. Outsourcing of the payroll system to an external service provider

C

QUESTION 106
An IS auditor reviewing the use of encryption finds that the symmetric key is sent by an email message between the parties. Which of the following audit responses is correct in this situation?

A. An audit finding is recorded, as the key should be asymmetric and therefore changed.
B. No audit finding is recorded, as it is normal to distribute a key of this nature in this manner.
C. No audit finding is recorded, as the key can only be used once.
D. An audit finding is recorded as the key should be distributed in a secure manner.

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 107
Which of the following is the **GREATEST** risk resulting from conducting periodic reviews of IT over several years based on the same audit program?

A. The amount of errors will increase because the routine work promotes inattentiveness.
B. Detection risk is increased because auditees already know the audit program.
C. Audit risk is increased because the programs might not be adapted to the organization's current situation.
D. Staff turnover in the audit department will increase because fieldwork becomes less interesting.

Correct Answer: C
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 108
What is the **FIRST** step an auditor should take when beginning a follow-up audit?

Correct Answer:
Section: The process of Auditing Information System

Explanation

Explanation/Reference:

Review workpapers from the previous audit.

B. Gather evidence of remediation to conduct tests of controls.
C. Review previous findings and action plans.
D. Meet with the auditee to discuss remediation progress.

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 109
Following an IS audit, which of the following types of risk would be **MOST** critical to communicate to key stakeholders?

A. Control
B. Residual
C. Audit
D. Inherent

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 110
During an audit of information security procedures of a large retailer's online store, an IS auditor notes that operating system (OS) patches are automatically deployed upon release. Which of the following should be of **GREATEST** concern to the auditor?

A. Patches are in conflict with current licensing agreements.

A.
B. Patches are pushed from the vendor increasing Internet traffic.
C. Patches are not reflected in the configuration management database.
D. Patches are not tested before installation on critical servers.

QUESTION 111
Which of the following is the **BEST** way to address ongoing concerns with the quality and accuracy of internal audits?

A. Engage an independent review of the audit function.
B. Require peer reviews of audit workpapers.
C. Implement performance management for IS auditors.
D. Require IS audit management to lead exit meetings.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 112
An IS auditor finds that periodic reviews of read-only users for a reporting system are not being performed. Which of the following should be the IS auditor's **NEXT** course of action?

A. Obtain a verbal confirmation from IT for this exemption.
B. Review the list of end-users and evaluate for authorization.
C. Verify management's approval for this exemption.
D. Report this control process weakness to senior management.

Correct Answer: C
Section: The process of Auditing Information System
Explanation
Correct Answer: D
Section: The process of Auditing Information System

Explanation

Explanation/Reference:
Explanation/Reference:

QUESTION 113
Which of the following activities would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA)?
Developing the CSA questionnaire
B. Developing the remediation plan
C. Implementing the remediation plan
D. Partially completing the CSA

Correct Answer: C
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 114
Which of the following audit procedures would be **MOST** conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

A. Interviews with knowledgeable users
B. Use of test transactions
C. Review of source code
D. Review of program documentation

Correct Answer: B
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

A.

QUESTION 115

An IS audit reveals that an organization is not proactively addressing known vulnerabilities. Which of the following should the IS auditor recommend the organization do **FIRST**?

A. Verify the disaster recovery plan (DRP) has been tested.
B. Ensure the intrusion prevention system (IPS) is effective.
C. Confirm the incident response team understands the issue.
D. Assess the security risks to the business.

QUESTION 116

As part of an IS audit, the auditor notes the practices listed below. Which of the following would be a segregation of duties concern?

A. Operators are degaussing magnetic tapes during night shifts.
B. System programmers have logged access to operating system parameters.
C. System programmers are performing the duties of operators.
D. Operators are acting as tape librarians on alternate shifts.

Correct Answer: D
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 117

During an audit, the client learns that the IS auditor has recently completed a similar security review at a competitor. The client inquires about the competitor's audit results. What is the **BEST** way for the auditor to address this inquiry?

A. Explain that it would be inappropriate to discuss the results of another audit client.
B. Escalate the question to the audit manager for further action.
C. Discuss the results of the audit omitting specifics related to names and products.

Correct Answer: D
Section: The process of Auditing Information System

Explanation

Explanation/Reference:
D. Obtain permission from the competitor to use the audit results as examples for future clients.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 118
Which of the following IS audit recommendations would **BEST** help to ensure appropriate mitigation will occur on control weaknesses identified during an audit?
Assign actions to responsible personnel and follow up.
B. Report on progress to the audit committee.
C. Perform a cost-benefit analysis on remediation strategy.
D. Implement software to input the action points from the IS audit.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 119
During a database audit, an IS auditor noted frequent problems due to the growing size of the order tables. Which of the following is the **BEST** recommendation in this situation?

A. Develop an archiving approach.
B. Periodically delete completed orders.
C. Build more table indices.
D. Migrate to a different database management system.

A.
Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 120
Which of the following procedures should an IS auditor complete **FIRST** when evaluating the adequacy of IT key performance indicators (KPIs)?

A. Independently calculate the accuracy of the KPIs.
B. Review KPIs that indicate poor IT performance.
C. Validate the KPI thresholds.
D. Determine whether the KPIs support IT objectives.

QUESTION 121
Which of the following is **MOST** important for an IS auditor to consider when determining an appropriate sample size in situations where selecting the entire population is not feasible?

A. Tolerable error
B. Accessibility of the data
C. Data integrity
D. Responsiveness of the auditee

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

Correct Answer: D
Section: The process of Auditing Information System

Explanation

Explanation/Reference:

QUESTION 122

An IS auditor finds that a mortgage origination team receives customer mortgage applications via a shared repository. Which of the following test procedures is the **BEST** way to assess whether there are adequate privacy controls over this process?

A. Validate whether the encryption is compliant with the organization's requirements.
B. Validate that data is entered accurately and timely.
C. Validate whether documents are deleted according to data retention procedures.
D. Validate whether complex passwords are required.

Correct Answer: A
Section: The process of Auditing Information System
Explanation

Explanation/Reference:

QUESTION 123

Which of the following is **MOST** important for an IS auditor to determine when evaluating a database for privacy-related risks?

A. Whether copies of production data are masked
B. Whether the integrity of the data dictionary is maintained
C. Whether data import and export procedures are approved
D. Whether all database tables are normalized

Correct Answer: B
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 124
Which of the following is **MOST** important for an IS auditor to consider when evaluating a Software as a Service (SaaS) arrangement?

A. Total cost of ownership
B. Frequency of software updates
C. Physical security
D. Software availability

Correct Answer: D
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 125
Which of the following findings should be of **GREATEST** concern for an IS auditor when auditing the effectiveness of a phishing simulation test administered for staff members?

A. Staff members were not notified about the test beforehand.
B. Test results were not communicated to staff members.
C. Staff members who failed the test did not receive follow-up education.

D. Security awareness training was not provided prior to the test.

Correct Answer: C
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 126
After the release of an application system, an IS auditor wants to verify that the system is providing value to the organization. The auditor's **BEST** course of action would be to:

A. review the results of compliance testing.
B. quantify improvements in client satisfaction.
C. confirm that risk has declined since the application system release.
D. perform a gap analysis against the benefits defined in the business case.

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 127
What is an IS auditor's **BEST** recommendation for management if a network vulnerability assessment confirms that critical patches have not been applied since the last assessment?

A. Implement a process to test and apply appropriate patches.
B. Apply available patches and continue periodic monitoring.
C. Configure servers to automatically apply available patches.
D. Remove unpatched devices from the network.

Correct Answer: A

Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 128
During a review of a production schedule, an IS auditor observes that a staff member is not complying with mandatory operational procedures. The auditor's **NEXT** step should be to:

A. determine why the procedures were not followed.
B. include the noncompliance in the audit report.
C. note the noncompliance in the audit working papers.
D. issue an audit memorandum identifying the noncompliance.

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 129
An IS auditor conducts a review of a third-party vendor's reporting of key performance indicators (KPIs). Which of the following findings should be of **MOST** concern to the auditor?

A. Some KPIs are not documented.
B. KPIs have never been updated.
C. KPIs data is not being analyzed.
D. KPIs are not clearly defined.

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 130
An IS auditor discovers a recurring software control process issue that severely impacts the efficiency of a critical business process. Which of the following is the **BEST** recommendation?

A. Replace the malfunctioning system.
B. Determine the compensating controls.
C. Identify other impacted processes.

Determine the root cause of the issue.

Correct Answer: D
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 131
Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS auditor has been asked to conduct a control assessment. The auditor's **BEST** course of action would be to determine if:

A. the domain controller was classified for high availability.
B. the network traffic was being monitored.
C. the patches were updated.
D. the logs were monitored.

Correct Answer: D
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 132
Which of the following should be of **GREATEST** concern to an IS auditor conducting an audit of an organization's backup processes?

A. A written backup policy is not available.
B. Backup failures are not resolved in a timely manner.
C. The restoration process is slow due to connectivity issues.
D. The service levels are not achieved.

Correct Answer: D

D.

Section: The process of Auditing Information
System Explanation

Explanation/Reference:
QUESTION 133
Performance monitoring tools report that servers are consistently above the recommended utilization capacity. Which of the following is the **BEST** recommendation of the IS auditor?

A. Develop a capacity plan based on usage projections.
B. Deploy load balancers.
C. Monitor activity logs.
D. Add servers until utilization is at target capacity.

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 134
Which of the following would be **MOST** critical for an IS auditor to look for when evaluating fire precautions in a manned data center located in the upper floor of a multi-story building?

A. Existence of handheld fire extinguishers in highly visible locations
B. Documentation of regular inspections by the local fire department
C. Adequacy of the HVAC system throughout the facility
D. Documentation of tested emergency evacuation plans

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 135
The **MOST** effective method for an IS auditor to determine which controls are functioning in an operating system is to:

A. compare the current configuration to the corporate standard.
B. consult with the systems programmer.
C. consult with the vendor of the system.
compare the current configuration to the default configuration.

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 136
A legacy application is running on an operating system that is no longer supported by the vendor. If the organization continues to use the current application, which of the following should be the IS auditor's **GREATEST** concern?

A. Potential exploitation of zero-day vulnerabilities in the system
B. Inability to update the legacy application database
C. Increased cost of maintaining the system
D. Inability to use the operating system due to potential license issues

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 137
A 5-year audit plan provides for general audits every year and application audits on alternating years. To achieve higher efficiency, the IS audit manager would **MOST** likely:

D.

A. proceed with the plan and integrate all new applications.
B. alternate between control self-assessment (CSA) and general audits every year.
C. implement risk assessment criteria to determine audit priorities.
D. have control self-assessments (CSAs) and formal audits of applications on alternating years.

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:
QUESTION 138
Which of the following would be an IS auditor's **GREATEST** concern when evaluating a cybersecurity incident response plan?

A. The plan has not been recently tested.
B. Roles and responsibilities are not detailed for each process.
C. Stakeholder contact details are not up-to-date.
D. The plan does not include incident response metrics.

Correct Answer: B
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 139
Which of the following is an IS auditor’s **BEST** course of action upon learning that preventive controls have been replaced with detective and corrective controls?

A. Report the issue to management as the risk level has increased.
B. Recommend the implementation of preventive controls in addition to the other controls.
C. Verify the revised controls enhance the efficiency of related business processes.
D. Evaluate whether new controls manage the risk at an acceptable level.

Correct Answer: D

Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 140
Which of the following should the IS auditor do **FIRST** to ensure data transfer integrity for Internet of Things (IoT) devices?

A. Verify access control lists to the database where collected data is stored.
B. Confirm that acceptable limits of data bandwidth are defined for each device.
C. Ensure that message queue telemetry transport (MQTT) is used.
Determine how devices are connected to the local network.

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 141
An IS auditor finds that corporate mobile devices used by employees have varying levels of password settings. Which of the following would be the **BEST** recommendation?

A. Update the acceptable use policy for mobile devices.
B. Notify employees to set passwords to a specified length.
C. Encrypt data between corporate gateway and devices.
D. Apply a security policy to the mobile devices.

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

D.

QUESTION 142
When planning an application audit, it is **MOST** important to evaluate risk factors by interviewing:

A. process owners.
B. application owners.
C. IT management.
D. application users.

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:
QUESTION 143
The scheduling of audit follow-ups should be based **PRIMARILY** on:

A. costs and audit efforts involved.
B. auditee and auditor time commitments.
C. the risk and exposure involved.
D. control and detection processes.

Correct Answer: C
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 144
A vendor service level agreement (SLA) requires backups to be physically secured. An IS audit of the backup system revealed a number of the backup media were missing. Which of the following should be the auditor's **NEXT** step?

A. Recommend a review of the vendor's contract.
B. Recommend identification of the data stored on the missing media.

C. Notify executive management.
D. Include the missing backup media finding in the audit report.

Correct Answer: B
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 145
During a review of an organization's IT incident management practices, the IS auditor finds the quality of incident resolution documentation is poor. Which of the following is the **BEST** recommendation to help address this issue?

A. Have service desk staff create documentation be choosing from pre-selected answers in the service management tool.
B. Require service desk staff to open incident tickets only when they have sufficient information.
C. Revise incident resolution procedures and provide training for service desk staff on the applicable updates.
Require peer review of resolution documentation followed by service desk management sign off.

Correct Answer: C
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 146
What is an IS auditor's **BEST** course of action when provided with a status update indicating audit recommendations related to segregation of duties for financial staff have been implemented?

A. Verify sufficient segregation of duties controls are in place.
B. Request documentation of the segregation of duties policy and procedures.
C. Note the department's response in the audit workpapers and records.
D. Confirm with the business that the recommendations are implemented.

D.

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 147
When reviewing capacity monitoring, an IS auditor notices several incidents where storage capacity limits were reached, while the average utilization was below 30%. Which of the following would the IS auditor **MOST** likely identify as the root cause?

A. The IT response to the alerts was too slow.
B. The amount of data produced was unacceptable for operations.
C. The storage space should have been enlarged in time.
D. The dynamics of the utilization were not properly taken into account.

Correct Answer: D
Section: The process of Auditing Information
System Explanation

Explanation/Reference:
QUESTION 148
An IS auditor is reviewing the process followed in identifying and prioritizing the critical business processes. This process is part of the:

A. balanced scorecard.
B. business impact analysis (BIA).
C. operations component of the business continuity plan (BCP).
D. enterprise risk management plan.

Correct Answer: C
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 149
When assessing a business case as part of a post-implementation review, the IS auditor must ensure that the:

A. feasibility of alternative project approaches has been assessed.
B. business case has not been amended since project approval.
C. quality assurance measures have been applied throughout the project.
D. amendments to the business case have been approved.

Correct Answer: D
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 150
Which of the following should be of **GREATEST** concern to an IS auditor reviewing an organization's information security program?

A. The program was not formally signed off by the sponsor.
B. Key performance indicators (KPIs) are not established.
C. Not all IT staff are aware of the program.

D.

The program was last updated five years ago.

Correct Answer: B
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 151
Which of the following is the **MOST** appropriate document for granting authority to an external IS auditor in an audit engagement with a client organization?

A. Approved statement of work
B. Formally approved audit charter
C. An internal memo to all concerned parties
D. Request for proposal for audit services

Correct Answer: A
Section: The process of Auditing Information System Explanation

Explanation/Reference:

QUESTION 152
Which of the following is **MOST** important for an IS auditor to evaluate when determining the effectiveness of an information security program?

A. Percentage of users aware of the objectives of the security program
B. Percentage of policy exceptions that were approved with justification
C. Percentage of desired control objectives achieved
D. Percentage of reported security incidents

Explanation/Reference:

Correct Answer: C
Section: The process of Auditing Information
System Explanation
QUESTION 153
Which of the following should be the **GREATEST** concern to an IS auditor evaluating an organization's policies?

A. Policies are not formally approved by the management.
B. Policies are nor formally acknowledged and signed by employees.
C. Policies do not provide adequate protection to the organization.
D. Policies are not reviewed and updated frequently.

Correct Answer: C
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 154
An IS auditor is evaluating the access controls at a multinational company with a shared network infrastructure. Which of the following is **MOST** important?

A. Simplicity of end-to-end communication paths
B. Remote network administration
C. Common security policies
D. Logging of network information at user level

Correct Answer: C
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 155

Which of the following should be an IS auditor's **PRIMARY** concern when evaluating an organization's information security policies, procedures, and controls for third-party vendors?

A. The third-party vendors have their own information security requirements.
B. The organization is still responsible for protecting the data.
C. Noncompliance is easily detected.
D. The same procedures and controls are used for all third-party vendors.

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 156
During a follow-up audit, an IS auditor finds that some critical recommendations have not been addressed as management has decided to accept the risk. Which of the following is the IS auditor's **BEST** course of action?

A. Adjust the annual risk assessment accordingly.
B. Require the auditee to address the recommendations in full.
C. Evaluate senior management's acceptance of the risk.
D. Update the audit program based on management's acceptance of risk.

Correct Answer: C
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 157
Explanation/Reference:

As part of a follow-up of a previous year's audit, an IS auditor has increased the expected error rate for a sample. The impact will be:

A. degree of assurance increases.
B. standard deviation decreases.
C. sampling risk decreases.
D. required sample size increases.

Correct Answer: D
Section: The process of Auditing Information
System Explanation
QUESTION 158
During a vendor management database audit, an IS auditor identifies multiple instances of duplicate vendor records. In order to prevent recurrence of the same issue, which of the following would be the IS auditor's **BEST** recommendation to management?

A. Perform system verification checks for unique data values on key fields.
B. Request senior management approval of all new vendor details.
C. Run system reports of full vendor listings periodically to identify duplication.
D. Build a segregation of duties control into the vendor creation process.

Correct Answer: A
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 159
During the implementation of a new system, an IS auditor must assess whether certain automated calculations comply with the regulatory requirements. Which of the following is the **BEST** way to obtain this assurance?

A. Inspect user acceptance test results.
B. Re-perform the calculation with audit software.
C. Review sign-off documentation.
D. Review the source code related to the calculation.

Correct Answer: B
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 160
An IS auditor has been asked to review a recently implemented quality management system (QMS). Which of the following should be the auditor's **PRIMARY** focus?

A. Training materials prepared for coaching employees
B. Processes to measure the performance of business critical transactions
C. Documentation standard of the implemented QMS system
D. Stability of the implemented QMS system over a period of time

Correct Answer: B
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 161
Which of the following should be the **PRIMARY** concern of an IS auditor during a review of an external IT service level agreement (SLA) for computer operations?

A. No employee succession plan
B. Changes in services are not tracked
C. Lack of software escrow provisions
D. Vendor has exclusive control of IT resources

Explanation/Reference:

Correct Answer: B
Section: The process of Auditing Information
System Explanation

Explanation/Reference:

QUESTION 162
An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's **BEST** recommendation should be to:

A. reclassify the data to a lower level of confidentiality.
B. recommend corrective actions to be taken by the security administrator.
C. implement a strong password schema for users.
D. require the business owner to conduct regular access reviews.

Correct Answer: B
Section: The process of Auditing Information
System Explanation
QUESTION 163
During a review of the IT strategic plan, an IS auditor finds several IT initiatives focused on delivering new systems and technology are not aligned with the organization's strategy. Witch of the following would be the IS auditor's **BEST** recommendation?

A. Reassess the return on investment for the IT initiatives
B. Modify IT initiatives that do not map to business strategies
C. Utilize a balanced scorecard to align IT initiatives to business strategies
D. Reassess IT initiatives that do not map business strategies

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 164

An organization has outsourced some of its subprocesses to a service provider. When scoping the audit of the provider, the organization's internal auditor should **FIRST**:

A. evaluate operational controls of the provider
B. discuss audit objectives with the provider
C. review internal audit reports of the provider
D. review the contract with the provider

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 165
An organization was severely impacted after an advanced persistent threat (APT) attack. Afterwards, it was found that the initial breach happened a month prior to the attack. Management's **GREATEST** concern should be:

A. results of the past internal penetration test
B. the effectiveness of monitoring processes
C. the installation of critical security patches

Explanation/Reference:

D. external firewall policies

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 166
Software quality assurance (QA) reviews are planned as part of system development. At which stage in the development process should the first review be initiated?

A. At pre-implementation planning
B. As a part of the user requirements definition
C. Immediately prior to user acceptance testing
D. During the feasibility study

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 167
Which of the following is the **MOST** effective way of ensuring that business units comply with an information security governance framework?

A. Conducting information security awareness training
B. Performing security assessments and gap analyses
C. Integrating security requirements with processes
D. Conducting a business impact analysis (BIA)

Correct Answer: C

Section: Governance and Management of IT
Explanation

Explanation/Reference:
QUESTION 168
Which of the following is **MOST** important to the successful implementation of an information security governance framework across the organization?

A. The existing organizational security culture
B. Security management processes aligned with security objectives
C. Organizational security controls deployed in line with regulations
D. Security policies that adhere to industry best practices

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 169
Which of the following is the **MOST** effective way to achieve the integration of information security governance into corporate governance?

A. Ensure information security aligns with IT strategy.
B. Provide periodic IT balanced scorecards to senior management.
C. Align information security budget requests to organizational goals.
D. Ensure information security efforts support business goals.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 170

In the absence of technical controls, what would be the **BEST** way to reduce unauthorized text messaging on company-supplied mobile devices?

A. Update the corporate mobile usage policy to prohibit texting.
B. Conduct a business impact analysis (BIA) and provide the report to management.
C. Stop providing mobile devices until the organization is able to implement controls.
D. Include the topic of prohibited texting in security awareness training.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 171
Which of the following is the **BEST** way to demonstrate to senior management that organizational security practices comply with industry standards?

A. A report on the maturity of controls
B. Up-to-date policy and procedures documentation
C. Existence of an industry-accepted framework
D. Results of an independent assessment

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 172
Following significant organizational changes, which of the following is the **MOST** important consideration when updating the IT policy?

A. The policy is integrated into job descriptions.
B. The policy is endorsed by senior executives.
C. The policy is compliant with relevant laws and regulations.

D. The policy is aligned with industry standards and best practice.

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 173
Which of the following is the **FIRST** consideration when developing a data retention policy?

A. Determining the backup cycle based on retention period
B. Designing an infrastructure storage strategy
C. Identifying the legal and contractual retention period for data
D. Determining the security access privileges to the data

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 174
A review of Internet security disclosed that users have individual user accounts with the Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only corporate network is used. The organization should **FIRST**:

A. use a proxy server to filter out Internet sites that should not be accessed.
B. keep a manual log of Internal access.
C. monitor remote access activities.
D. include a statement in its security policy about Internet use.

Correct Answer: D

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 175
Which of the following **BEST** indicates a need to review an organization's information security policy?

A. Completion of annual IT risk assessment
B. Increasing complexity of business transactions
C. Increasing exceptions approved by management
D. High number of low-risk findings in the audit report

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 176
Which of the following is a directive control?

A. Establishing an information security operations team
B. Updating data loss prevention software
C. Implementing an information security policy
D. Configuring data encryption software

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 177
An organization's IT security policy requires annual security awareness training for all employees. Which of the following would provide the **BEST** evidence of the training's effectiveness?

A. Results of a social engineering test
B. Interviews with employees
C. Decreased calls to the incident response team
D. Surveys completed by randomly selected employees

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 178
Which type of risk would **MOST** influence the selection of a sampling methodology?

A. Control
B. Inherent
C. Residual
D. Detection

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 179
Which of the following will **BEST** protect an organization against spear phishing?

A. Email content filtering

B. Acceptable use policy
C. End-user training
D. Antivirus software

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 180
Which of the following is **MOST** likely to be included in an enterprise information security policy?

A. Password composition requirements
B. Consequences of noncompliance
C. Audit trail review requirements
D. Security monitoring strategy

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 181
Which of the following processes is the **FIRST** step in establishing an information security policy?

A. Security controls evaluation
B. Business risk assessment
C. Review of current global standards
D. Information security audit

Correct Answer: B

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 182
A cloud service provider is unable to provide an independent assessment of controls. Which of the following is the **BEST** way to obtain assurance that the provider can adequately protect the organization's information?

A. Check references supplied by the provider's other customers.
B. Invoke the right to audit per the contract.
C. Review the provider's information security policy.
D. Review the provider's self-assessment.

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 183
Which of the following would **BEST** help to ensure compliance with an organization's information security requirements by an IT service provider?
A. Defining the business recovery plan with the IT service provider
B. Requiring an external security audits of the IT service provider
C. Defining information security requirements with internal IT
D. Requiring regular reporting from the IT service provider

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 184
Which of the following provides the **GREATEST** assurance that an organization allocates appropriate resources to respond to information security events?

A. Incident classification procedures
B. Threat analysis and intelligence reports
C. An approved IT staffing plan
D. Information security policies and standards.

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 185
When the inherent risk of a business activity is lower than the acceptable risk level, the **BEST** course of action would be to:

A. implement controls to mitigate the risk.
B. report compliance to management.
C. review the residual risk level.
D. monitor for business changes.

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 186
An information security manager is concerned that executive management does not support information security initiatives. Which of the following is the **BEST** way to address this situation?

A. Demonstrate alignment of the information security function with business needs.

B. Escalate noncompliance concerns to the internal audit manager.
C. Report the risk and status of the information security program to the board.
D. Revise the information security strategy to meet executive management's expectations.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 187
The **PRIMARY** reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:

A. maintain compliance with industry best practices.
B. serve as evidence of security awareness training.
C. assign accountability for transactions made with the user's ID.
D. maintain an accurate record of users' access rights.

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 188
Which of the following would provide the **MOST** reliable evidence to indicate whether employee access has been deactivated in a timely manner following termination?
A. Comparing termination forms with dates in the HR system
B. Reviewing hardware return-of-asset forms
C. Interviewing supervisors to verify employee data is being updated immediately
D. Comparing termination forms with system transaction log entries

Correct Answer: D

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 189
Which of the following is the **MOST** effective way to ensure security policies are relevant to organizational business practices?

A. Leverage security steering committee contribution.
B. Obtain senior management sign-off.
C. Integrate industry best practices.
D. Conduct an organization-wide security audit.

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 190
Which of the following is the **PRIMARY** role of a data custodian?

A. Processing information
B. Securing information
C. Classifying information
D. Validating information

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 191
The **PRIMARY** focus of a training curriculum for members of an incident response team should be:

A. technology training.
B. security awareness.
C. external corporate communication.
D. specific role training.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 192
Which of the following should be the **PRIMARY** objective of the information security incident response process?

A. Minimizing negative impact to critical operations
B. Communicating with internal and external parties
C. Classifying incidents
D. Conducting incident triage

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 193
Which of the following is **MOST** important when selecting an information security metric?

A. Defining the metric in quantitative terms
B. Aligning the metric to the IT strategy

C. Defining the metric in qualitative terms
D. Ensuring the metric is repeatable

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 194
Which of the following is the **PRIMARY** purpose of conducting a business impact analysis (BIA)?

A. Identifying risk mitigation options
B. Identifying key business risks
C. Identifying critical business processes
D. Identifying the threat environment

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 195
Which of the following would **BEST** assist an information security manager in gaining strategic support from executive management?

A. Research on trends in global information security breaches
B. Risk analysis specific to the organization
C. Annual report of security incidents within the organization
D. Rating of the organization's security based on international standards

Correct Answer: B

Section: Governance and Management of IT
Explanation

Explanation/Reference:
QUESTION 196
An information security manager has developed a strategy to address new information security risks resulting from recent changes in the business. Which of the following would be **MOST** important to include when presenting the strategy to senior management?

A. The impact of organizational changes on the security risk profile
B. The costs associated with business process changes
C. Results of benchmarking against industry peers
D. Security controls needed for risk mitigation

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 197
Which of the following is the **FIRST** step when conducting a business impact analysis?

A. Identifying critical information resources
B. Identifying events impacting continuity of operations
C. Analyzing past transaction volumes
D. Creating a data classification scheme

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 198
Which of the following findings would have the **GREATEST** impact on the objective of a business intelligence system?

A. Key control have not been tested in a year.
B. Decision support queries use database functions proprietary to the vendor.
C. The hot site for disaster recovery does not include the decision support system.
D. Management reports have not been evaluated since implementation.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 199
When reviewing an organization's IT governance processes, which of the following provides the **BEST** indication that information security expectations are being met at all levels?

A. Achievement of established security metrics
B. Approval of the security program by senior management
C. Utilization of an internationally recognized security standard
D. Implementation of a comprehensive security awareness program

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 200
Which of the following is the **MOST** important benefit of involving IS audit when implementing governance of enterprise IT?

A. Identifying relevant roles for an enterprise IT governance framework

B. Verifying that legal, regulatory and contractual requirements are being met
C. Making decisions regarding risk response and monitoring of residual risk
D. Providing independent and objective feedback to facilitate improvement of IT processes

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:
QUESTION 201
Which of the following is **MOST** important for an IS auditor to consider during a review of the IT governance of an organization?

A. Funding allocations
B. Risk management methodology
C. Defined service levels
D. Decision making responsibilities

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 202
Which of the following findings should be of **MOST** concern to an IS auditor when evaluating information security governance within an organization?

A. The data center manager has final sign-off on security projects.
B. The information security oversight committee meets quarterly.
C. The information security department has difficulty filling vacancies.
D. Information security policies were last updated two years ago.

Correct Answer: C
Section: Governance and Management of IT

Explanation

Explanation/Reference:

QUESTION 203
When reviewing business continuity plan (BCP) test results, it is **MOST** important for the IS auditor to determine whether the test:

A. verifies the ability to resume key business operations.
B. considers changes to the systems environment.
C. assesses the capability to retrieve vital records.
D. follows up on activities that occurred since the previous test.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 204
The **BEST** method an organization can employ to align its business continuity plan (BCP) and disaster recovery plan (DRP) with core business needs is to:

A. execute periodic walk-throughs of the plans.
B. update the business impact analysis (BIA) for significant business changes.
C. outsource the maintenance of the BCP and disaster recovery plan to a third party.
D. include BCP and disaster recovery plan responsibilities as a part of new employee training.

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 205

Which of the following is **MOST** important to include in a business continuity plan (BCP)?

A. Vendor contact information B.
Documentation of critical systems

C. Documentation of data center floor plans
D. Backup site location information

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 206
An organization wants to test business continuity using a scenario in which there are many remote workers trying to access production data at the same time. Which of the following is the **BEST** testing method in this situation?

A. Application failover testing.
B. Network stress testing.
C. Alternate site testing.
D. Network penetration testing.

Correct Answer: B

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 207
Which of the following is the **MOST** important prerequisite for implementing a data loss prevention (DLP) tool?

A. Identifying where existing data resides and establishing a data classification matrix.
B. Requiring users to save files in secured folders instead of a company-wide shared drive
C. Reviewing data transfer logs to determine historical patterns of data flow
D. Developing a DLP policy and requiring signed acknowledgement by users

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 208
An organization's IT security policy states that user IDs must uniquely identify individuals and that users should not disclose their passwords. An IS auditor discovers that several generic user IDs are being used. Which of the following is the **MOST** appropriate course of action for the auditor?

A. Investigate the noncompliance.
B. Include the finding in the final audit report.
C. Recommend disciplinary action.
D. Recommend a change in security policy.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 209
Which of the following observations noted during a review of the organization's social media practices should be of **MOST** concern to the IS auditor?

A. The organization does not require approval for social media posts.
B. More than one employee is authorized to publish on social media on behalf of the organization.
C. Not all employees using social media have attended the security awareness program.
D. The organization does not have a documented social media policy.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 210
An IS auditor is conducting a review of an organization's information systems and discovers data that is no longer needed by business applications. Which of the following would be the IS auditor's **BEST** recommendation?

A. Ask the data custodian to remove it after confirmation from the business user.
B. Assess the data according to the retention policy.
C. Back up the data to removable media and store in a secure area.
D. Keep the data and protect it using a data classification policy.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 211
Which of the following provides an IS auditor the **MOST** assurance that an organization is compliant with legal and regulatory requirements?

A. The IT manager is responsible for the organization's compliance with legal and regulatory requirements.
B. Controls associated with legal and regulatory requirements have been identified and tested.

C. Senior management has provided attestation of legal and regulatory compliance.
D. There is no history of complaints or fines from regulators regarding noncompliance.

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 212
An IS auditor is reviewing IT policies and found that most policies have not been reviewed in over 3 years. The **MOST** significant risk is that the policies do not reflect:

A. current legal requirements.
B. the vision of the CEO.
C. the mission of the organization.
D. current industry best practices.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 213
What is the **BEST** way for an IS auditor to address the risk associated with over-retention of personal data after identifying a large number of customer records retained beyond the retention period defined by law?

A. Recommend automating deletion of records beyond the retention period.
B. Schedule regular internal audits to identify records for deletion.
C. Report the retention period noncompliance to the regulatory authority.
D. Escalate the over-retention issue to the data privacy officer for follow-up.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 214
During an audit of identity and access management, an IS auditor finds that the engagement audit plan does not include the testing of controls that regulate access by third parties. Which of the following would be the auditor's **BEST** course of action?

A. Plan to test these controls in another audit.
B. Escalate the deficiency to audit management.
C. Add testing of third-party access controls to the scope of the audit.
D. Determine whether the risk has been identified in the planning documents.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 215
An organization that has suffered a cyber attack is performing a forensic analysis of the affected users' computers. Which of the following should be of **GREATEST** concern for the IS auditor reviewing this process?

A. The chain of custody has not been documented.
B. The legal department has not been engaged.
C. An imagining process was used to obtain a copy of the data from each computer.
D. Audit was only involved during extraction of the information.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 216
Which of the following is the **PRIMARY** role of an IS auditor with regard to data privacy?

A. Ensuring compliance with data privacy laws
B. Communicating data privacy requirements to the organization
C. Drafting the organization's data privacy policy
D. Verifying that privacy practices match privacy statements

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 217
Which of the following controls will **BEST** ensure that the board of directors receives sufficient information about IT?

A. The CIO reports on performance and corrective actions in a timely manner.
B. Regular meetings occur between the board, the CIO, and a technology committee.
C. The CIO regularly sends IT trend reports to the board.
D. Board members are knowledgeable about IT, and the CIO is consulted on IT issues.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:
QUESTION 218
The **MOST** effective way to determine if IT is meeting business requirements is to establish:

A. industry benchmarks.

B. organizational goals.
C. a capability model.
D. key performance indicators (KPIs).

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 219
Which of the following roles combined with the role of a database administrator (DBA) will create a segregation of duties conflict?

A. Quality assurance
B. Systems analyst
C. Application end user
D. Security administrator

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 220
When testing segregation of duties, which of the following audit techniques provides the **MOST** reliable evidence?

A. Observing daily operations for the area in scope
B. Evaluating the department structure via the organizational chart
C. Reviewing departmental procedure handbooks
D. Interviewing managers and end users
Correct Answer: A

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 221
Which of the following would **BEST** provide executive management with current information on IT-related costs and IT performance indicators?

A. IT dashboard
B. Risk register
C. IT service-management plan
D. Continuous audit reports

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 222
Which of the following will **MOST** effectively help to manage the challenges associated with end user-developed application systems?

A. Developing classifications based on risk
B. Introducing redundant support capacity
C. Prohibiting creation of executable files
D. Applying control practices used by IT

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 223
In the IT department where segregation of duties is not feasible due to a limited number of resources, a team member is performing the functions of computer operator and reviewer of application logs. Which of the following would be the IS auditor's **BEST** recommendation?

A. Develop procedures to verify that the application logs are not modified.
B. Prevent the operator from performing application development activities.
C. Assign an independent second reviewer to verify the application logs.
D. Restrict the computer operator's access to the production environment.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 224
A core business unit relies on an effective legacy system that does not meet the current security standards and threatens the enterprise network. Which of the following is the **BEST** course of action to address the situation?

A. Require that new systems that can meet the standards be implemented.
B. Document the deficiencies in the risk register.
C. Develop processes to compensate for the deficiencies.
D. Disconnect the legacy system from the rest of the network.

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 225
A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server. Which of the following would **MOST** effectively allow the hospital to avoid paying the ransom?

A. A continual server replication process
B. A property tested offline backup system
C. A property configured firewall
D. Employee training on ransomware

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 226
Which of the following is **MOST** likely to be included in computer operating procedures in a large data center?

A. Instructions for job scheduling
B. Procedures for resequencing source code
C. Procedures for utility configuration
D. Guidance on setting security parameters

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 227
What is the **PRIMARY** benefit to executive management when audit, risk, and security functions are aligned?

A. More efficient incident handling
B. Reduced number of assurance reports
C. More effective decision making
D. More timely risk reporting

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 228
Reevaluation of risk is **MOST** critical when there is:

A. resistance to the implementation of mitigating controls
B. a change in security policy
C. a management request for updated security reports
D. a change in the threat landscape

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 229
Which of the following **BEST** enables staff acceptance of information security policies?

A. Strong senior management support
B. Adequate security funding
C. Computer-based training
D. A robust incident response program

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 230
An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the **BEST** assurance that the third party's contract programmers comply with the organization's security policies?

A. Perform periodic security assessments of the contractors' activities.
B. Conduct periodic vulnerability scans of the application.
C. Include penalties for noncompliance in the contracting agreement.
D. Require annual signed agreements of adherence to security policies.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 231
What is the **FIRST** line of defense against criminal insider activities?

A. Validating the integrity of personnel
B. Monitoring employee activities
C. Signing security agreements by critical personnel
D. Stringent and enforced access controls

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 232
Which of the following is the **MOST** important factor when an organization is developing information security policies and procedures?

A. Cross-references between policies and procedures
B. Inclusion of mission and objectives

C. Compliance with relevant regulations
D. Consultation with management

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 233
Which of the following requires a consensus by key stakeholders on IT strategic goals and objectives?
A. Balanced scorecards
B. Benchmarking
C. Maturity models
D. Peer reviews

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 234
An organization's information security department is creating procedures for handling digital evidence that may be used in court. Which of the following would be the **MOST** important consideration from a risk standpoint?

A. Ensuring the entire security team reviews the evidence
B. Ensuring that analysis is conducted on the original data
C. Ensuring the original data is kept confidential
D. Ensuring the integrity of the data is preserved

Correct Answer: D

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 235
Which of the following is the **BEST** approach to make strategic information security decisions?

A. Establish regular information security status reporting
B. Establish business unit security working groups
C. Establish periodic senior management meetings
D. Establish an information security steering committee

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 236
The **MAIN** purpose of documenting information security guidelines for use within a large, international organization is to:

A. ensure that all business units have the same strategic security goals
B. provide evidence for auditors that security practices are adequate
C. explain the organization's preferred practices for security
D. ensure that all business units implement identical security procedures

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 237
Which of the following would be the **MOST** important information to include in a business case for an information security project in a highly regulated industry?

A. Industry comparison analysis
B. Critical audit findings
C. Compliance risk assessment
D. Number of reported security incidents

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 238
Which of the following is the **BEST** course of action for an information security manager to align security and business goals?
A. Reviewing the business strategy
B. Actively engaging with stakeholders
C. Conducting a business impact analysis
D. Defining key performance indicators

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 239
An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the **MOST** useful information for planning purposes?

A. Results from a business impact analysis

B. Results from a gap analysis
C. An inventory of security controls currently in place
D. Deadline and penalties for noncompliance

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 240
The **MOST** important objective of security awareness training for business staff is to:

A. understand intrusion methods
B. reduce negative audit findings
C. increase compliance
D. modify behavior

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 241
Which of the following is the **BEST** reason to certify an organization to an international security standard?

A. The certification covers enterprise security end-to-end.
B. The certification reduces information security risk.
C. The certification ensures that optimal controls are in place.
D. The certification delivers value to stakeholders.

Correct Answer: D

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 242
An organization's IT department is undertaking a large virtualization project to reduce its physical server footprint. Which of the following should be the **HIGHEST** priority of the information security manager?

A. Determining how incidents will be managed
B. Selecting the virtualization software
C. Being involved as the design stage of the project
D. Ensuring the project has appropriate security funding

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 243
Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed **NEXT**?
A. Schedule the target end date for implementation activities.
B. Budget the total cost of implementation activities.
C. Develop an implementation strategy.
D. Calculate the residual risk for each countermeasure.

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 244
Which of the following presents the GREATEST concern when implementing data flow across borders?

A. Software piracy laws
B. National privacy laws
C. Political unrest
D. Equipment incompatibilities

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 245
When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs due to scope creep?

A. Problem management
B. Quality management
C. Change management
D. Risk management

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 246
Which of the following is the MOST important reason to use statistical sampling?

A. The results are more defensible
B. It ensures that all relevant cases are covered

C. It reduces time required for testing
D. The results can reduce error rates

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 247
Which of the following is MOST critical to the success of an information security program?

A. Integration of business and information security
B. Alignment of information security with IT objectives
C. Management's commitment to information security
D. User accountability for information security

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 248
The MOST important reason why an IT risk assessment should be updated on a regular basis is to:

A. utilize IT resources in a cost-effective manner
B. comply with data classification changes
C. comply with risk management policies
D. react to changes in the IT environment

Correct Answer: D

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 249
Which of the following groups is **MOST** likely responsible for the implementation of IT projects?

A. IT steering committee
B. IT compliance committee
C. IT strategy committee
D. IT governance committee

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 250
The CIO of an organization is concerned that the information security policies may not be comprehensive. Which of the following should an IS auditor recommend be performed **FIRST**?

A. Obtain a copy of their competitor's policies.
B. Determine if there is a process to handle exceptions to the policies.
C. Establish a governance board to track compliance with the policies.
D. Compare the policies against an industry framework.

Correct Answer: C
Section: Governance and Management of IT
Explanation
Explanation/Reference:

QUESTION 251
An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality. Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed **FIRST**?

A. Data impacting business objectives
B. Data supporting financial statements
C. Data reported to the regulatory body
D. Data with customer personal information

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 252
An IS auditor has been asked to advise on the design and implementation of IT management best practices. Which of the following actions would impair the auditor's independence?

A. Providing consulting advice for managing applications
B. Designing an embedded audit module
C. Implementing risk response on management's behalf
D. Evaluating the risk management process

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 253

Management decided to accept the residual risk of an audit finding and not take the recommended actions. The internal audit team believes the acceptance is inappropriate and has discussed the situation with executive management. After this discussion, there is still disagreement regarding the decision. Which of the following is the **BEST** course of action by internal audit?

A. Report this matter to the audit committee without notifying executive management.
B. Document in the audit report that management has accepted the residual risk and take no further actions.
C. Report the issue to the audit committee in a joint meeting with executive management for resolution.
D. Schedule another meeting with executive management to convince them of taking action as recommended.

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 254
An IS auditor has completed a service level management audit related to order management services provided by a third party. Which of the following is the **MOST** significant finding?

A. The third party has offshore support arrangements.
B. Penalties for missing service levels are limited.
C. The service level agreement does not define how availability is measured.
D. Service desk support is not available outside the company's business hours.

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 255
To help ensure the accuracy and completeness of end-user computing output, it is **MOST** important to include strong:

A. reconciliation controls.
B. change management controls.
C. access management controls.
D. documentation controls.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 256
Rather than decommission an entire legacy application, an organization's IT department has chosen to replace specific modules while maintaining those still relevant. Which of the following artifacts is **MOST** important for an IS auditor to review?

A. IT service management catalog and service level requirements
B. Security requirements for legacy data masking and data destruction
C. Applicable licensing agreements for the application
D. Future state architecture and requirements

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 257
Which of the following is the **MOST** important consideration for an organization when strategizing to comply with privacy regulations?

A. Ensuring there are staff members with in-depth knowledge of the privacy regulations
B. Ensuring up-to-date knowledge of where customer data is saved
C. Ensuring regularly updated contracts with third parties that process customer data
D. Ensuring appropriate access to information systems containing privacy information.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 258
Which of the following is the MOST important aspect relating to employee termination?

A. The details of employee have been removed from active payroll files.
B. Company property provided to the employee has been returned.
C. User ID and passwords of the employee have been deleted.
D. The appropriate company staff are notified about the termination.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:
Explanation:
Even though Logical access to information by a terminated employee is possible if the ID and password of the terminated employee has not been deleted this is only one part of the termination procedures. If user ID is not disabled or deleted, it could be possible for the employee without physical access to visit the company's networks remotely and gain access to the information.

Please note that this can also be seen in a different way: the most important thing to do could also be to inform others of the person's termination, because even if user ID's and passwords are deleted, a terminated individual could simply socially engineer their way back in by calling an individual he/she used to work with and ask them for access. He could intrude on the facility or use other weaknesses to gain access to information after he has been terminated.

By notifying the appropriate company staff about the termination, they would in turn initiate account termination, ask the employee to return company property, and all credentials would be withdrawn for the individual concerned. This answer is more complete than simply disabling account.

It seems harsh and cold when this actually takes place, but too many companies have been hurt by vengeful employees who have lashed out at the company when their positions were revoked for one reason or another. If an employee is disgruntled in any way, or the termination is unfriendly, that employee's accounts should be disabled right away, and all passwords on all systems changed.

For your exam you should know the information below:

Employee Termination Processes
Employees join and leave organizations every day. The reasons vary widely, due to retirement, reduction in force, layoffs, termination with or without cause, relocation to another city, career opportunities with other employers, or involuntary transfers. Terminations may be friendly or unfriendly and will need different levels of care as a result.

Friendly Terminations
Regular termination is when there is little or no evidence or reason to believe that the termination is not agreeable to both the company and the employee. A standard set of procedures, typically maintained by the human resources department, governs the dismissal of the terminated employee to ensure that company property is returned, and all access is removed. These procedures may include exit interviews and return of keys, identification cards, badges, tokens, and cryptographic keys. Other property, such as laptops, cable locks, credit cards, and phone cards, are also collected. The user manager notifies the security department of the termination to ensure that access is revoked for all platforms and facilities. Some facilities choose to immediately delete the accounts, while others choose to disable the accounts for a policy defined period, for example, 30 days, to account for changes or extensions in the final termination date. The termination process should include a conversation with the departing associate about their continued responsibility for confidentiality of information.

Unfriendly Terminations
Unfriendly terminations may occur when the individual is fired, involuntarily transferred, laid off, or when the organization has reason to believe that the individual has the means and intention to potentially cause harm to the system. Individuals with technical skills and higher levels of access, such as the systems administrators, computer programmers, database administrators, or any individual with elevated privileges, may present higher risk to the environment. These individuals could alter files, plant logic bombs to create system file damage at a future date, or remove sensitive information. Other disgruntled users could enter erroneous data into the system that may not be discovered for several months. In these situations, immediate termination of systems access is warranted at the time of termination or prior to notifying the employee of the termination. Managing the people aspect of security, from pre-employment to postemployment, is critical to ensure that trustworthy, competent resources are employed to further the business objectives that will protect company information. Each of these actions contributes to preventive, detective, or corrective personnel controls.

The following answers are incorrect:
The other options are less important.

Reference:

CISA review manual 2014 Page number 99
Harris, Shun (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 129). McGraw-Hill. Kindle Edition.

QUESTION 259
In which of the following cloud computing service model are applications hosted by the service provider and made available to the customers over a network?

A. Software as a service
B. Data as a service
C. Platform as a service
D. Infrastructure as a service

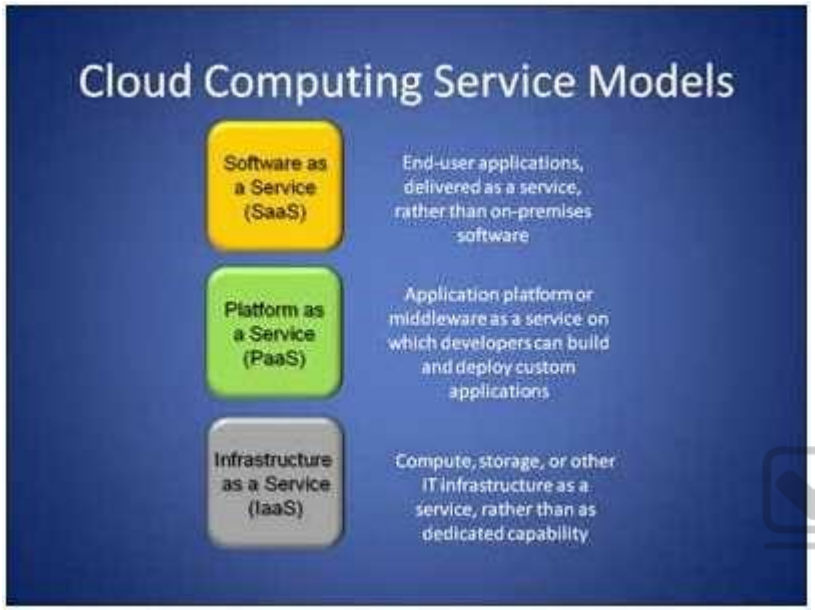
Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:
Explanation:
Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. Seas is closely related to the ASP (application service provider) and on demand computing software delivery models.

For your exam you should know below information about Cloud Computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. Cloud computing service model

Cloud computing service models



Software as a Service (Seas)
Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for Seas. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for Seas distribution.

Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network based access to a single copy of an application created specifically for Seas distribution and use.

Benefits of the Seas model include:

easier administration

automatic updates and patch management compatibility: All users will have the same version of software. easier collaboration, for the same reason global accessibility.

Platform as a Service (Peas)
Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Cloud providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment. Where Iasi is the “raw IT network,” Peas is the software environment that runs on top of the IT network.

Platform as a Service (Peas) is an outgrowth of Software as a Service (Seas), a software distribution model in which hosted software applications are made available to customers over the Internet. Peas has several advantages for developers. With Peas, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

On the downside, Peas involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

Infrastructure as a Service (Iasi)
Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them.

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a peruse basis.

The following answers are incorrect:

Data as a service - Data Provided as a service rather than needing to be loaded and prepared on premises.
Platform as a service - Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.
Infrastructure as a service - Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations,

including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Reference:

CISA review manual 2014 page number 102
Official ISC2 guide to CISSP 3rd edition Page number 689 http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

QUESTION 260
Which of the following cloud computing service model is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components?

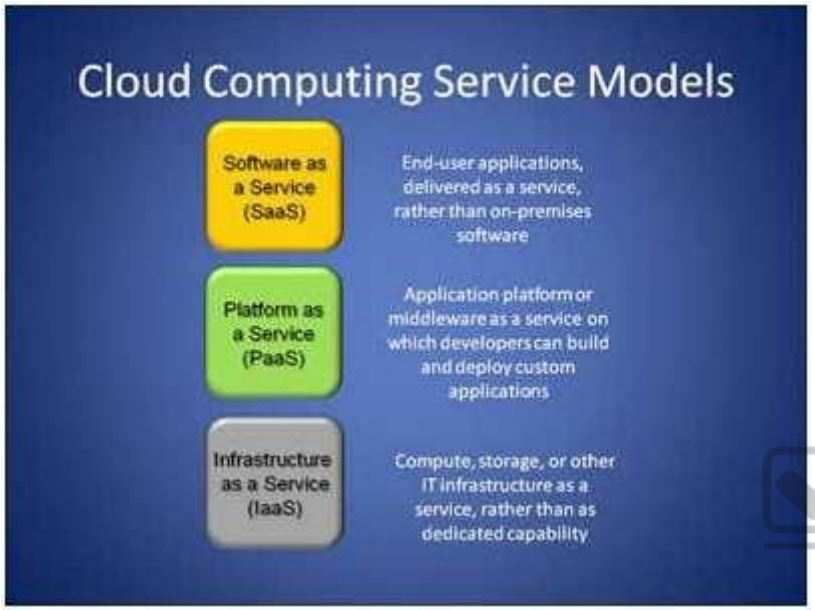
A. Software as a service
B. Data as a service
C. Platform as a service
D. Infrastructure as a service

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:
Explanation:
Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a peruse basis.

For your exam you should know below information about Cloud Computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. Cloud Computing



Cloud computing service models:
Cloud computing service models

Software as a Service (Seas)
Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for Seas. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for Seas distribution.

Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network based access to a single copy of an application created specifically for Seas distribution and use.

Benefits of the Seas model include:

easier administration automatic updates and patch
management compatibility: All users will have the same
version of software.
easier collaboration, for the same reason
global accessibility.

Platform as a Service (Peas)
Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Cloud providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment. Where Iasi is the “raw IT network,” Peas is the software environment that runs on top of the IT network.

Platform as a Service (Peas) is an outgrowth of Software as a Service (Seas), a software distribution model in which hosted software applications are made available to customers over the Internet. Peas has several advantages for developers. With Peas, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

On the downside, Peas involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

Infrastructure as a Service (Iasi)
Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them.

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a peruse basis.

Characteristics and components of Iasi include:

Utility computing service and billing model.
Automation of administrative tasks.

Dynamic scaling.
Desktop virtualization.
Policy-based services.
Internet connectivity.

Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).

The following answers are incorrect:

Data as a service - Data Provided as a service rather than needing to be loaded and prepared on premises.

Software as a service - Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. Seas is closely related to the ASP (application service provider) and on demand computing software delivery models.

Platform as a service - Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Reference:

CISA review manual 2014 page number 102
Official ISC2 guide to CISSP 3rd edition Page number 689 http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS
http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

QUESTION 261
Which of the following cloud deployment model is provisioned for open use by the general public?

A. Private Cloud
B. Community Cloud
C. Public Cloud
D. Hybrid Cloud

Correct Answer: C
Section: Governance and Management of IT

Explanation

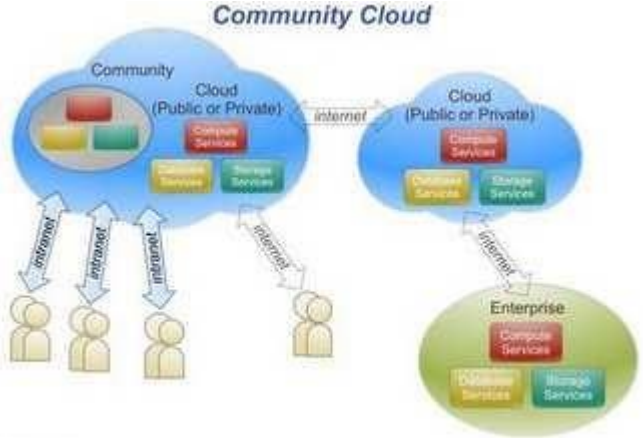
Explanation/Reference:
Explanation:
In Public cloud, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

For your exam you should know below information about Cloud Computing deployment models:

Private cloud
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

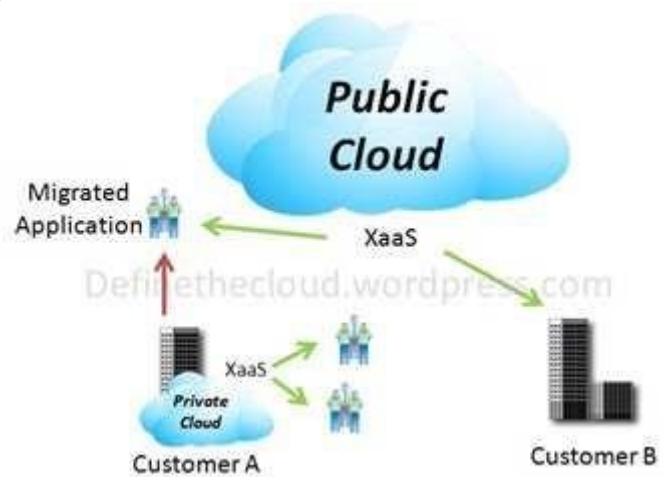
Private Cloud

Community Cloud
The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. Community Cloud



Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Public Cloud



Hybrid cloud
The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)
hybrid cloud

The following answers are incorrect:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Reference:

CISA review manual 2014 page number 102
Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

QUESTION 262
Which of the following step of PDCA establishes the objectives and processes necessary to deliver results in accordance with the expected output?

A. Plan
B. Do
C. Check
D. Act

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:
Explanation:
Plan - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition." The steps in each successive PDCA cycle are:

PLAN
Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.
DO
Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.
CHECK
Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".
ACT
Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:
DO - Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.
CHECK - Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences
ACT -Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product

Reference:

CISA review manual 2014 page number 107

QUESTION 263
Which of the following step of PDCA implement the plan, execute the process and make product?

A. Plan
B. Do
C. Check
D. Act

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:
Explanation:
Do - Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition." The steps in each successive PDCA cycle are:

PLAN
Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.
DO
Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.
CHECK
Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".
ACT
Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:

PLAN - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals).
CHECK - Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences
ACT -Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product

Reference:
CISA review manual 2014 page number 107

QUESTION 264
Which of the following step of PDCA study the actual result and compares it against the expected result?

A. Plan
B. Do
C. Check
D. Act

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:
Explanation:
Check - Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition." The steps in each successive PDCA cycle are:

PLAN
Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.
DO
Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.
CHECK
Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".
ACT
Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:

PLAN - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals).

DO - Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

ACT -Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product

Reference:

CISA review manual 2014 page number 107

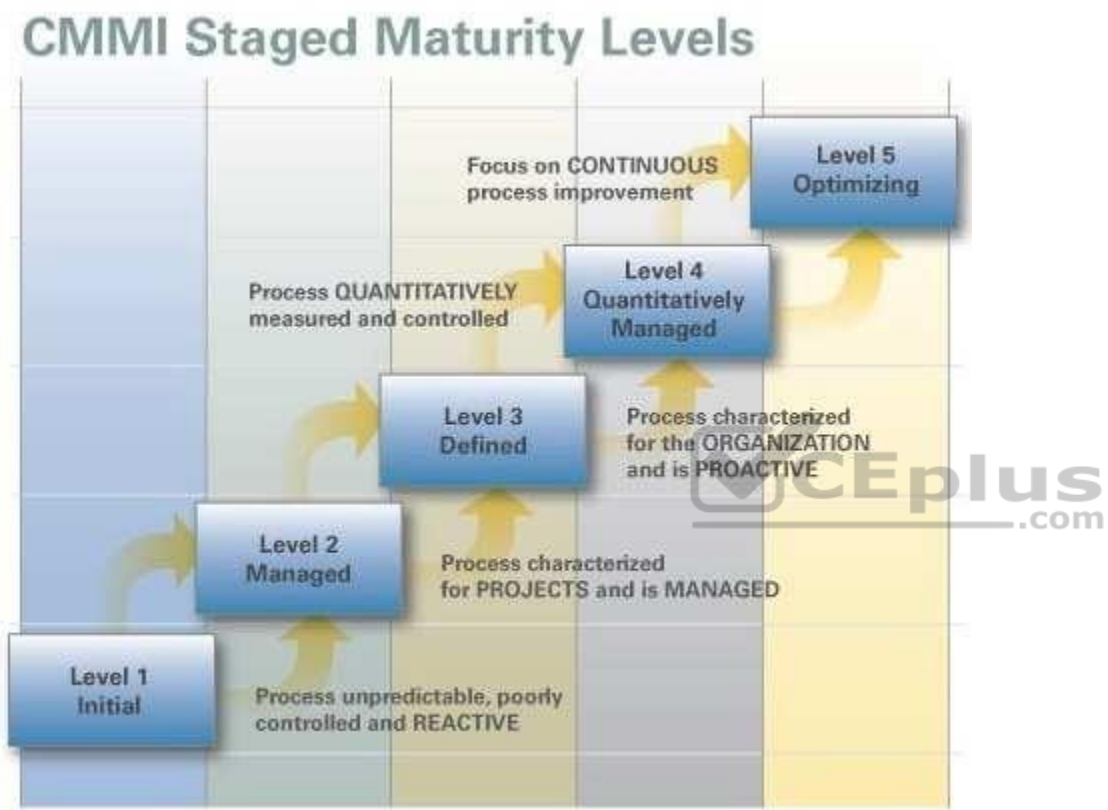
QUESTION 265
Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?

A. Initial, Managed, Defined, Quantitatively managed, optimized
B. Initial, Managed, Defined, optimized, Quantitatively managed
C. Initial, Defined, Managed, Quantitatively managed, optimized
D. Initial, Managed, Quantitatively managed, Defined, optimized

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:
Explanation:
Maturity model

A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainable produce required outcomes.



A maturity model can be used as a benchmark for comparison and as an aid to understanding - for example, for comparative assessment of different organizations where there is something in common that can be used as a basis for comparison. In the case of the CMM, for example, the basis for comparison would be the organizations' software development processes.

Structure

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

Common Features: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

Key Practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.

Levels
There are five levels defined along the continuum of the model and, according to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief".

Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.
Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted.
Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the last being Work Instructions). Managed - the process is quantitatively managed in accordance with agreed-upon metrics. Optimizing - process management includes deliberate process optimization/improvement.

Within each of these maturity levels are Key Process Areas which characteristic that level, and for each such area there are five factors: goals, commitment, ability, measurement, and verification. These are not necessarily unique to CMM, representing — as they do — the stages that organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/ feasible.

Level 1 - Initial (Chaotic)
It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable
It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined
It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 - Managed
It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5 - Optimizing
It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

The following answers are incorrect:
The other option specified in the option does not provide correct sequence.

Reference:

CISA review manual 2014 Page number 188
CISSP Official study guide page number 693

QUESTION 266
A maturity model can be used to aid the implementation of IT governance by identifying:

A. critical success factors (CSF)
B. performance drivers

C. improvement opportunities
D. accountabilities

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 267
The effectiveness of an information security governance framework will **BEST** be enhanced if:

A. consultants review the information security governance framework
B. a culture of legal and regulatory compliance is promoted by management
C. IS auditors are empowered to evaluate governance activities
D. risk management is built into operational and strategic activities

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 268
Which of the following **BEST** demonstrates effective information security management within an organization?

A. Employees support decisions made by information security management.
B. Excessive risk exposure in one department can be absorbed by other departments.
C. Information security governance is incorporated into organizational governance.
D. Control ownership is assigned to parties who can accept losses related to control failure.

Correct Answer: C

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 269
A multinational organization is introducing a security governance framework. The information security manager's concern is that regional security practices differ. Which of the following should be evaluated **FIRST**?

A. Local regulatory requirements
B. Local IT requirements
C. Cross-border data mobility
D. Corporate security objectives

Correct Answer: A
Section: Governance and Management of IT
Explanation
Explanation/Reference:

QUESTION 270
When facilitating the alignment of corporate governance and information security governance, which of the following is the **MOST** important role of an organization's security steering committee?

A. Obtaining support for the integration from business owners
B. Obtaining approval for the information security budget
C. Evaluating and reporting the degree of integration
D. Defining metrics to demonstrate alignment

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 271
Which of the following is a **PRIMARY** responsibility of an information security governance committee?

A. Approving the purchase of information security technologies
B. Approving the information security awareness training strategy
C. Reviewing the information security strategy
D. Analyzing information security policy compliance reviews

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 272
What is the **MOST** effective way to ensure security policies and procedures are up-to-date?

A. Verify security requirements are being identified and consistently applied.
B. Align the organization's security practices with industry standards and best practice.
C. Define and document senior management's vision for the direction of the security
D. Prevent security documentation audit issues from being raised

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 273
Which of the following findings would be of **GREATEST** concern to an IS auditor performing an information security audit of critical server log management activities?

A. Log records can be overwritten before being reviewed.

B. Logging procedures are insufficiently documented.
C. Log records are dynamically into different servers.
D. Logs are monitored using manual processes.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 274
The **BEST** way to validate whether a malicious act has actually occurred in an application is to review:

A. segregation of duties
B. access controls
C. activity logs
D. change management logs

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:
QUESTION 275
An IS auditor finds that application servers had inconsistent configurations leading to potential security vulnerabilities. Which of the following should the auditor recommend **FIRST**?

A. Enforce server baseline standards.
B. Improve change management processes using a workflow tool.
C. Hold the application owner accountable for monitoring metrics.
D. Use a single vendor for the application servers.

Correct Answer: A

Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 276
Implementing a strong password policy is part of an organization's information security strategy for the year. A business unit believes the strategy may adversely affect a client's adoption of a recently developed mobile application and has decided not to implement the policy. Which of the following would be the information security manager's **BEST** course of action?

A. Analyze the risk and impact of not implementing the policy
B. Develop and implement a password policy for the mobile application
C. Escalate non-implementation of the policy to senior management
D. Benchmark with similar mobile applications to identify gaps

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 277
In a multinational organization, local security regulations should be implemented over global security policy because:

A. global security policies include unnecessary controls for local businesses
B. business objectives are defined by local business unit managers
C. requirements of local regulations take precedence
D. deploying awareness of local regulations is more practical than of global policy

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 278
Which of the following is a step in establishing a security policy?

A. Developing platform-level security baselines.
B. Developing configurations parameters for the network,
C. Implementing a process for developing and maintaining the policy.
D. Creating a RACI matrix.

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 279
Which of the following is **MOST** important for the IS auditor to verify when reviewing the development process of a security policy?

A. Evidence of active involvement of key stakeholders
B. Output from the enterprise's risk management system
C. Identification of the control framework
D. Evidence of management approval

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:
QUESTION 280
Which of the following should be the **PRIMARY** reason to establish a social media policy for all employees?

A. To publish acceptable messages to be used by employees when posting

B. To raise awareness and provide guidance about social media risks
C. To restrict access to social media during business hours to maintain productivity
D. To prevent negative public social media postings and comments

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 281
A small organization is experiencing rapid growth and plans to create a new information security policy. Which of the following is **MOST** relevant to creating the policy?

A. Industry standards
B. The business impact analysis (BIA)
C. The business objectives
D. Previous audit recommendations

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 282
A CEO requests access to corporate documents from a mobile device that does not comply with organizational policy. The information security manager should **FIRST**:

A. evaluate the business risk
B. evaluate a third-party solution
C. initiate an exception approval process
D. deploy additional security controls

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 283
Which of the following is **MOST** important to consider when developing a bring your own device (BYOD) policy?

A. Supported operating systems
B. Procedure for accessing the network
C. Application download restrictions
D. Remote wipe procedures

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 284
An IT steering committee assists the board of directors to fulfill IT governance duties by:

A. developing IT policies and procedures for project tracking.
B. focusing on the supply of IT services and products.
C. overseeing major projects and IT resource allocation.
D. implementing the IT strategy.

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 285
Which of the following can provide assurance that an IT project has delivered its planned benefits?

A. User acceptance testing (UAT)
B. Steering committee approval
C. Post-implementation review
D. Quality assurance evaluation

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 286
Which of the following is **MOST** important when evaluating the retention period for a cloud provider's client data backups?

A. Cost of data storage
B. Contractual commitments
C. Previous audit recommendations
D. Industry best practice

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 287
Which of the following is **MOST** important to include in a contract with a software development service provider?

A. A list of key performance indicators (KPIs)
B. Ownership of intellectual property

C. Service level agreement (SLA)
D. Explicit contract termination requirements

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 288
Which of the following is a distinguishing feature at the highest level of a maturity model?

A. There are formal standards and procedures.
B. Projects are controlled with management supervision.
C. A continuous improvement process is applied.
D. Processes are monitored continuously.

Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 289
The **PRIMARY** purpose of a precedence diagramming method in managing IT projects is to:

A. monitor project scope creep.
B. identify the critical path.
C. identify key milestones.
D. minimize delays and overruns.

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 290
Which of the following is the **PRIMARY** risk when business units procure IT assets without IT involvement?

A. Corporate procurement standards are not followed.
B. The business units want IT to be responsible for maintenance costs.
C. Data security requirements are not considered.
D. System inventory becomes inaccurate.

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 291
Which of the following would be **MOST** important to update once a decision has been made to outsource a critical application to a cloud service provider?

A. Project portfolio
B. IT resource plan
C. IT budget
D. Business impact analysis (BIA)

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 292
Communicating which of the following would **BEST** encourage management to initiate appropriate actions following the receipt of report findings?

A. Risk implications of the observations
B. Strict deadlines to close all observations
C. Statistical sampling used to derive observations
D. Recommendations that align with the business strategy

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 293
Which of the following is the **BEST** key performance indicator (KPI) for determining how well the IT policy is aligned to the business requirements?

A. Number of approved exceptions to the policy
B. Total cost of policy breaches
C. Total cost to support the policy
D. Number of inquiries regarding the policy

Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 294
An external audit team is deciding whether to rely on internal audit's work for an annual compliance audit. Which of the following is the **GREATEST** consideration when making this decision?

A. Independence of the internal audit department from management's influence
B. Professional certifications held by the internal audit team members
C. Years of experience each of the internal auditors have in performing compliance audits
D. The level of documentation maintained by internal audit and the methods used to collect evidence

Correct Answer: D
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 295
Which of the following methods would **BEST** ensure that IT strategy is in line with business strategy?

A. Break-even-point analysis
B. IT value analysis
C. Critical path analysis
D. Business impact analysis (BIA)

Correct Answer: B
Section: Governance and Management of IT
Explanation

Explanation/Reference:

QUESTION 296
The **MAIN** consideration when designing an incident escalation plan should be ensuring that:

A. information assets are classified.
B. appropriate stakeholders are involved.
C. high-impact risks have been identified.
D. requirements cover forensic analysis.

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 297
Which of the following should be an information security manager's **MOST** important consideration when conducting a physical security review of a potential outsourced data center?

A. Environmental factors of the surrounding location
B. Proximity to law enforcement
C. Availability of network circuit connections
D. Distance of the data center from the corporate office

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 298
Which of the following is **MOST** important for an information security manager to ensure is included in a business case for a new system?

A. Intangible benefits of the system
B. Risk associated with the system
C. Effectiveness of controls
D. Audit-logging capabilities

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 299
During a post-incident review. the sequence and correlation of actions must be analyzed **PRIMARLY** based on:

A. interviews with personnel

B. a consolidated event time line
C. logs from systems involved
D. documents created during the incident

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 300
The **BEST** way to obtain funding from senior management for a security awareness program is to:
A. meet regulatory requirements
B. produce an impact analysis report of potential breaches
C. demonstrate that the program will adequately reduce risk
D. produce a report of organizational risks

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 301
In a cloud technology environment, which of the following would pose the **GREATEST** challenge to the investigation of security incidents?

A. Data encryption
B. Access to the hardware
C. Compressed customer data
D. Non-standard event logs

Correct Answer: B

Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 302
When considering whether to adopt bring your own device (BYOD), it is **MOST** important for the information security manager to ensure that:

A. security controls are applied to each device when joining the network
B. business leaders have an understanding of security risks
C. users have read and signed acceptable use agreements
D. the applications are tested prior to implementation

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation
Explanation/Reference:

QUESTION 303
The GREATEST benefit of using a prototyping approach in software development is that it helps to:

A. decrease the time allocated for user testing and review
B. minimize scope changes to the system
C. conceptualize and clarify requirements
D. improve efficiency of quality assurance (QA) testing

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 304
A company is using a software developer for a project. At which of the following points should the software quality assurance (QA) plan be developed?

A. As part of software definition
B. During the feasibility phase
C. Prior to acceptance testing
D. As part of the design phase

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 305
To develop meaningful recommendations for findings, which of the following is MOST important for an IS auditor to determine and understand?

A. Criteria
B. Responsible party
C. Impact
D. Root cause

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 306
Which of the following would BEST demonstrate that an effective disaster recovery plan (DRP) is in place?

A. Periodic risk assessment
B. Full operational test

C. Frequent testing of backups
D. Annual walk-through testing

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 307
Which of the following practices associated with capacity planning provides the GREATEST assurance that future incidents related to server performance will be prevented?

A. Anticipating current service level agreements (SLAs) will remain unchanged
B. Prorating the current processing workloads
C. Negotiating agreements to acquire required cloud services
D. Duplicating existing disk drive systems to improve redundancy and data storage

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
QUESTION 308
A change to the scope of an IT project has been formally submitted to the project manager. What should the project manager do NEXT?

A. Update the project plan to reflect the change in scope
B. Discuss the change with the project team and determine if it should be approved
C. Escalate the change to the change advisory board for approval
D. Determine how the change will affect the schedule and budget

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 309
The MOST important function of a business continuity plan is to:

A. ensure that the critical business functions can be recovered
B. provide procedures for evaluating tests of the business continuity plan
C. provide a schedule of events that has to occur if there is a disaster
D. ensure that all business functions are restored

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 310
Which of the following would be MOST useful for determining whether the goals of IT are aligned with the organization's goals?

A. Balanced scorecard
B. Enterprise architecture
C. Key performance indicators
D. Enterprise dashboard

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 311
A company has implemented an IT segregation of duties policy. In a role-based environment, which of the following roles may be assigned to an approach developer?

A. IT operator
B. Database administration
C. System administration
D. Emergency support

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 312
What is the **BEST** indicator of successful implementation of an organization's information security policy?

A. Reduced number of successful phishing incidents
B. Reduced number of help desk calls
C. Reduced number of noncompliance penalties incurred
D. Reduced number of false-positive security events

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
QUESTION 313
An organization is in the process of deciding whether to allow a bring your own device (BYOD) program. If approved, which of the following should be the **FIRST** control required before implementation?

A. Device baseline configurations
B. Device registration
C. An acceptable use policy
D. An awareness program

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 314
A CIO has asked an IS auditor to implement several security controls for an organization's IT processes and systems. The auditor should:

A. perform the assignment and future audits with due professional care.
B. obtain approval from executive management for the implementation.
C. refuse due to independence issues.
D. communicate the conflict of interest to audit management.

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 315
A start-up company acquiring servers for its order-taking system is unable to predict the volume of transactions. Which of the following is **MOST** important for the company to consider?

A. Scalability
B. Configuration
C. Optimization
D. Compatibility

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 316
When developing a risk-based IS audit plan, the **PRIMARY** focus should be on functions:

A. considered important by IT management.
B. with the most ineffective controls.
C. with the greatest number of threats.
D. considered critical to business operations.

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 317
Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?

A. Bridge
B. Repeater

C. Router
D. Gateway

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:
A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.

Important Note:

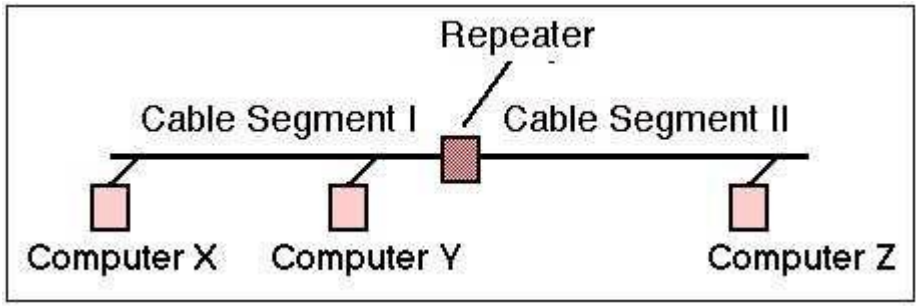
For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.

The second thing you must remembers is the fact that a gateway act as a translation device.
It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.

For your exam you should know the information below:

Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.
A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

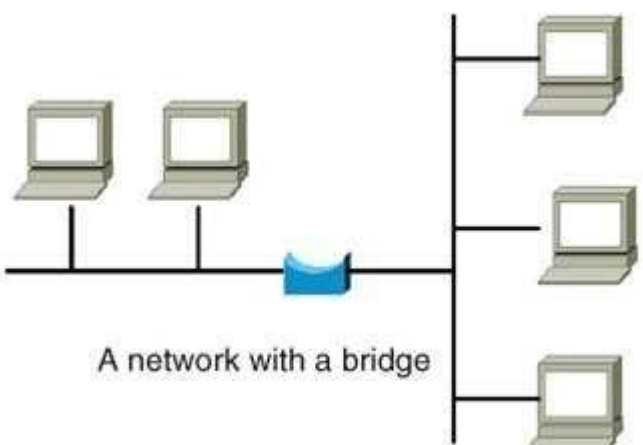
Repeater



Bridges

A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge



Routers

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It

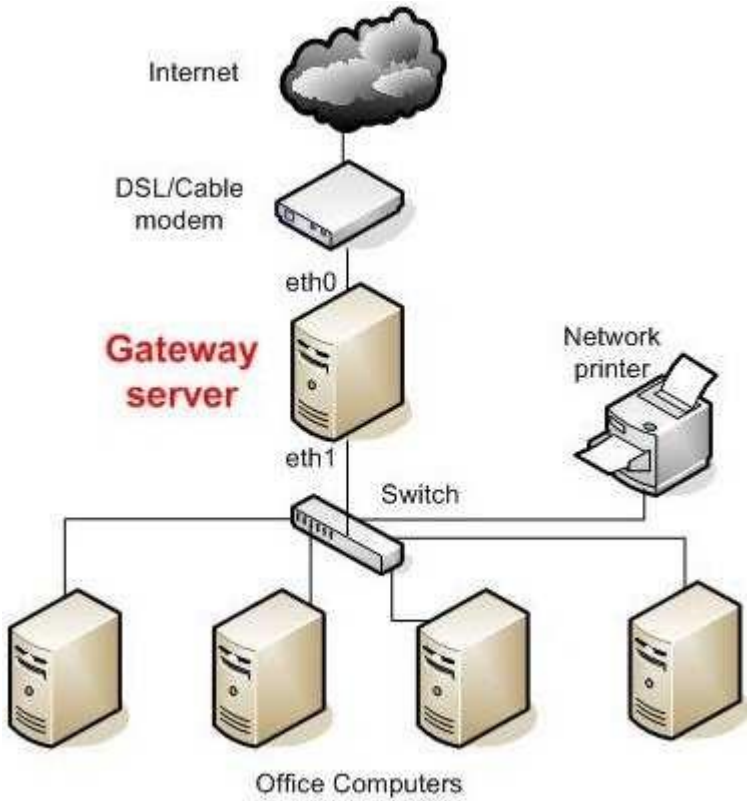
can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch

Switches
Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways
Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server



The following answers are incorrect:

Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.

Reference:
CISA review manual 2014 Page number 263
Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

QUESTION 318
Why would a database be renormalized?

A. To ensure data integrity
B. To increase processing efficiency
C. To prevent duplication of data
D. To save storage space

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:
A database is renormalized when there is a need to improve processing efficiency.

There is, however, a risk to data integrity when this occurs. Since it implies the introduction of duplication, it will not likely allow saving of storage space.

Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 109).

QUESTION 319
Which of the following is not a common method of multiplexing data?

A. Analytical multiplexing
B. Time-division multiplexing
C. Asynchronous time-division multiplexing

D. Frequency division multiplexing

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:
Generally, the methods for multiplexing data include the following:
Time-division multiplexing (TDM): information from each data channel is allocated bandwidth based on pre-assigned time slots, regardless of whether there is data to transmit.
Asynchronous time-division multiplexing (ATDM): information from data channels is allocated bandwidth as needed, via dynamically assigned time slots.
Frequency division multiplexing (FDM): information from each data channel is allocated bandwidth based on the signal frequency of the traffic.
Statistical multiplexing: Bandwidth is dynamically allocated to any data channels that have information to transmit.
Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

QUESTION 320
Which of the following ISO/OSI layers performs transformations on data to provide a standardized application interface and to provide common communication services such as encryption?

A. Application layer
B. Session layer
C. Presentation layer
D. Transport layer

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation
The presentation layer (ISO/OSI layer 6) performs transformations on data to provide a standardized application interface and to provide common communication services such as encryption, text compression and reformatting. The function of the presentation layer is to ensure that the format of the data submitted by the application layer conforms to the applicable network standard.

Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 119).

QUESTION 321
Which of the following is NOT a defined ISO basic task related to network management?

A. Fault management
B. Accounting resources
C. Security management
D. Communications management

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation
Explanation/Reference:
Explanation:
Fault management: Detects the devices that present some kind of fault.
Configuration management: Allows users to know, define and change remotely the configuration of any device.
Accounting resources: Holds the records of the resource usage in the WAN.
Performance management: Monitors usage levels and sets alarms when a threshold has been surpassed.
Security management: Detects suspicious traffic or users and generates alarms accordingly.

Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 137).

QUESTION 322
What is the most effective means of determining that controls are functioning properly within an operating system?

A. Interview with computer operator
B. Review of software control features and/or parameters
C. Review of operating system manual
D. Interview with product vendor

Correct Answer: B

Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:
Various operating system software products provide parameters and options for the tailoring of the system and activation of features such as activity logging. Parameters are important in determining how a system runs because they allow a standard piece of software to be customized to diverse environments. The reviewing of software control features and/or parameters is the most effective means of determining how controls are functioning within an operating system and of assessing and operating system's integrity.

The operating system manual should provide information as to what settings can be used but will not likely give any hint as to how parameters are actually set. The product vendor and computer operator are not necessarily aware of the detailed setting of all parameters.

The review of software control features and/or parameters would be part of your security audit. A security audit is typically performed by an independent third party to the management of the system. The audit determines the degree with which the required controls are implemented.

A security review is conducted by the system maintenance or security personnel to discover vulnerabilities within the system. A vulnerability occurs when policies are not followed, miscon figurations are present, or flaws exist in the hardware or software of the system. System reviews are sometimes referred to as a vulnerability assessment.

Reference:

Schneider, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Security Operations, Page 1054, for users with the Kindle edition look at Locations 851-855
and
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 102).

QUESTION 323
Which of the following characteristics pertaining to databases is not true?

A. A data model should exist and all entities should have a significant name.
B. Justifications must exist for normalized data.
C. No NULLs should be allowed for primary keys.
D. All relations must have a specific cardinality.

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:
Justifications should be provided when data is renormalized, not when it is normalized, because it introduces risk of data inconsistency. Renormalization is usually introduced for performance purposes.

Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).

QUESTION 324
Who is responsible for reviewing the result and deliverables within and at the end of each phase, as well as confirming compliance with requirements?

A. Project Sponsor
B. Quality Assurance
C. User Management
D. Senior Management

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation
Explanation/Reference:
Explanation:
Quality Assurance personnel review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

For CISA exam you should know below information about roles and responsibilities of groups/individuals that may be involved in the development process are summarized below:

Senior Management – Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

User Management – Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training. User management is concerned primarily with the following questions:

Are the required functions available in the software?
How reliable is the software?
How effective is the software?
Is the software easy to use?
How easy is to transfer or adapt old data from preexisting software to this environment?
Is it possible to add new functions?
Does it meet regulatory requirement?

Project Steering Committee – Provides overall directions and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be compromised of senior representative from each business area that will be significantly impacted by the proposed new system or system modifications.

System Development Management – Provides technical support for hardware and software environment by developing, installing and operating the requested system.

Project Manager – Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall directions, ensures appropriate representation of the affected departments, ensures that the project adheres local standards, ensures that deliverable meet the quality expectation of key stakeholder, resolve interdepartmental conflict, and monitors and controls cost of the project timetables.

Project Sponsor – Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

System Development Project Team – Completes assigned tasks, communicates effectively with user by actively involving them in the development process, works according to local standards, and advise the project manager of necessary plan deviations.

User Project Team – Completes assigned tasks, communicate effectively with the system developers by actively involving themselves in the development process as Subject Matter Expert (SME) and works according to local standards, and advise the project manager of expected and actual project deviations.

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

The following were incorrect answers:

Project Sponsor – Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

User Management – Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training.

Senior Management – Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

Reference:

CISA review manual 2014 Page number 150

QUESTION 325
Who is responsible for providing technical support for the hardware and software environment by developing, installing and operating the requested system?

A. System Development Management
B. Quality Assurance
C. User Management
D. Senior Management

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:
System Development Management provides technical support for hardware and software environment by developing, installing and operating the requested system.

For the CISA exam you should know the information below about roles and responsibilities of groups/individuals that may be involved in the development process are summarized below:

Senior Management – Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

User Management – Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training. User management is concerned primarily with the following questions:

Are the required functions available in the software?
How reliable is the software?
How effective is the software?
Is the software easy to use?
How easy is to transfer or adapt old data from preexisting software to this environment?
Is it possible to add new functions?
Does it meet regulatory requirement?

Project Steering Committee – Provides overall directions and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be compromised of senior representative from each business area that will be significantly impacted by the proposed new system or system modifications.

System Development Management – Provides technical support for hardware and software environment by developing, installing and operating the requested system.

Project Manager – Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall directions, ensures appropriate representation of the affected departments, ensures that the project adheres local standards, ensures that deliverable meet the quality expectation of key stakeholder, resolve interdepartmental conflict, and monitors and controls cost of the project timetables.

Project Sponsor – Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

System Development Project Team – Completes assigned tasks, communicates effectively with user by actively involving them in the development process, works according to local standards, and advise the project manager of necessary plan deviations.

User Project Team – Completes assigned tasks, communicate effectively with the system developers by actively involving themselves in the development process as Subject Matter Expert (SME) and works according to local standards, and advise the project manager of expected and actual project deviations.

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

The following were incorrect answers:

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

User Management – Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training.

Senior Management – Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

Reference:
CISA review manual 2014 Page number 150

QUESTION 326
Which of the following statement correctly describes the difference between QAT and UAT?

A. QAT focuses on technical aspect of the application and UAT focuses on functional aspect of the application
B. UAT focuses on technical aspect of the application and QAT focuses on functional aspect of the application
C. UAT and QAT both focuses on functional aspect of the application
D. UAT and QAT both focuses on technical aspect of the application

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Final Acceptance Testing -It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.
For CISA exam you should know below types of testing:

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.
Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team. The following specific analysis may be carried out during system testing.

Recovery Testing – Checking the system's ability to recover after a software or hardware failure.

Security Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems.

Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour.

Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process.

Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process.

Performance Testing – Comparing the system performance to other equivalent systems using well defined benchmarks.

Final Acceptance Testing – It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.
QAT focuses on documented specifications and the technology employed. It verifies that application works as documented by testing the logical design and the technology itself. It also ensures that the application meet the documented technical specifications and deliverables. QAT is performed primarily by IS department. The participation of end user is minimal and on request. QAT does not focus on functionality testing.

UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods include: Definition of test strategies and procedure. Design of test cases and scenarios Execution of the tests.
Utilization of the result to verify system readiness.
Acceptance criteria are defined criteria that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production possible.

The following were incorrect answers:
The other presented options incorrectly describe the difference between QAT and UAT

Reference:
CISA review manual 2014 Page number 166

QUESTION 327
Which of the following type of testing uses a set of test cases that focus on control structure of the procedural design?

A. Interface testing
B. Unit Testing
C. System Testing
D. Final acceptance testing

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Unit testing is the testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.

For CISA exam you should know below types of testing:

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.

Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team. The following specific analysis may be carried out during system testing.

Recovery Testing – Checking the system's ability to recover after a software or hardware failure.

Security Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems.

Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour.

Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process.

Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process.

Performance Testing – Comparing the system performance to other equivalent systems using well defined benchmarks.

Final Acceptance Testing – It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.
QAT focuses on documented specifications and the technology employed. It verifies that application works as documented by testing the logical design and the technology itself. It also ensures that the application meet the documented technical specifications and deliverables. QAT is performed primarily by IS department. The participation of end user is minimal and on request. QAT does not focus on functionality testing.
UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods include: Definition of test strategies and procedure. Design of test cases and scenarios Execution of the tests.
Utilization of the result to verify system readiness.
Acceptance criteria are defined criteria that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production possible.

The following were incorrect answers:

Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team.

Final Acceptance Testing – During this testing phase the defined methods of testing to apply should be incorporated into the organization's QA methodology.

Reference:

CISA review manual 2014 Page number 166

QUESTION 328
Which of the following type of testing has two major categories: QAT and UAT?

A. Interface testing
B. Unit Testing
C. System Testing
D. Final acceptance testing

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 329
Which of the following is the process of feeding test data into two systems – the modified system and alternative system and comparing the result?

A. Parallel Test
B. Black box testing
C. Regression Testing
D. Pilot Testing

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Parallel testing is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing – An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing – A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing – Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing – An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing – The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing – This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Sociability Testing – The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web

development, changes to the desktop environment. Multiple application may run on the user's desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs) , making operating system registry or configuration file modification, and possibly extra memory utilization.

The following were incorrect answers:

Regression Testing – The process of returning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Black Box Testing – An integrity based form of testing associated with testing components of an information system's "functional" operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Pilot Testing – A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities Reference:

CISA review manual 2014 Page number 167

QUESTION 330
Which of the following statement correctly describes the difference between black box testing and white box testing?

A. Black box testing focuses on functional operative effectiveness where as white box assesses the effectiveness of software program logic
B. White box testing focuses on functional operative effectiveness where as black box assesses the effectiveness of software program logic
C. White box and black box testing focuses on functional operative effectiveness of an information systems without regard to any internal program structure
D. White box and black box testing focuses on the effectiveness of the software program logic

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing – An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user

acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing – A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing – Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing – An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing – The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing – This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Sociability Testing – The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user’s desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs) , making operating system registry or configuration file modification, and possibly extra memory utilization.

The following were incorrect answers:
The other options presented does not provides correct difference between black box and white box testing.
Reference:

CISA review manual 2014 Page number 167

QUESTION 331
Which of the following data validation control validates input data against predefined range values?

A. Range Check
B. Table lookups

C. Existence check
D. Reasonableness check

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

In the Range Check control data should not exceed a predefined range of values

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check – Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check – Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check – Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification – The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check – new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Reference:

CISA review manual 2014 Page number 215

QUESTION 332
Which of the following control make sure that input data comply with predefined criteria maintained in computerized table of possible values?

A. Range Check B.
Table lookups
C. Existence check
D. Reasonableness check

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

In table lookups input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check – Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check – Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check – Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification – The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check – new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Range Check – Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Reference:

CISA review manual 2014 Page number 215

QUESTION 333
While implementing an invoice system, Lily has implemented a database control which checks that new transactions are matched to those previously input to ensure that they have not already been entered. Which of the following control is implemented by Lily?

A. Range Check
B. Duplicate Check
C. Existence check
D. Reasonableness check

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

In a duplicate check control new transaction are matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check – Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check – Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check – Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification – The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check – new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his/her date of birth.

The following were incorrect answers:

Range Check – Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Reference:

CISA review manual 2014 Page number 215

QUESTION 334
William has been assigned a changeover task. He has to break the older system into deliverable modules. Initially, the first module of the older system is phased out using the first module of a new system. Then, the second module of the old system is phased out, using the second module of the newer system and so forth until reaching the last module. Which of the following changeover system William needs to implement?

A. Parallel changeover
B. Phased changeover
C. Abrupt changeover
D. Pilot changeover

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

In phased changeover approach, the older system is broken into deliverables modules. Initially, the first module of older system is phased out using the first module of a new system. Then, the second module of the newer system is phased out, using the second module of the newer system and so forth until reaching the last module.
Some of the risk areas that may exist in the phased changeover area includes:

Resource challenge
Extension of the project life cycle to cover two systems.
Change management for requirements and customizations to maintain ongoing support of the older systems.

Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacing (new) system.

Changeover to newer system involves four major steps or activities
Conversion of files and programs; test running on test bed
Installation of new hardware, operating system, application system and the migrated data.
Training employees or user in groups
Scheduling operations and test running for go-live or changeover

Some of the risk areas related to changeover includes:

Asset safeguarding
Data integrity
System effectiveness
Change management challenges
Duplicate or missing records

The following were incorrect answers:

Parallel changeover – This technique includes running the old system, then running both the old and new systems in parallel and finally full changing over to the new system after gaining confidence in the working of new system.

Abrupt changeover – In the abrupt changeover approach the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once changeover to the new system takes place.

Pilot changeover – Not a valid changeover type.

Reference:
CISA review manual 2014 Page number 172

QUESTION 335
Which of the following fourth generation language depends on self-contained database management systems?

A. Query and report generator
B. Embedded database 4GLs
C. Relational database 4GL
D. Application generators

Correct Answer: B

Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Embedded database 4GLsare depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

For CISA exam you should know below mentioned types of 4GLs

Query and report generator – These specialize language can extract and produce reports. Recently more powerful language has been produced that can access database records, produce complex on-line output and be developed in an almost natural language.

Embedded database 4GLs – These depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

Relational database 4GLs – These high level language products are usually an optional feature on vendor's DBMS product line. These allow the application developer to make better use of DBMS product, but they often are not end-user-oriented. Example include SQL+ MANTIS and NATURAL.

Application generators – These development tools generate lower level programming languages(3GL) such as COBOL and C. The application can be further tailored and customized. Data processing development personnel, not end user, use application generators.

The following were incorrect answers:

Query and report generator – These specialize language can extract and produce reports.
Relational database 4GLs – These high level language products are usually an optional feature on vendor's DBMS product line.
Application generators – These development tools generate lower level programming languages(3GL) such as COBOL and C.

Reference:
CISA review manual 2014 Page number 209

QUESTION 336
Which of the following component of an expert system allows the expert to enter knowledge into the system without the traditional mediation of a software engineer?

A. Decision tree

B. Rules
C. Semantic nets
D. Knowledge interface

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Knowledge interface allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

For CISA Exam you should know below information about Artificial Intelligence and Expert System
Artificial intelligence is the study and application of the principles by which:

Knowledge is acquired and used
Goals are generated and achieved
Information is communicated
Collaboration is achieved
Concepts are formed
Languages are developed

Two main programming languages that have been developed for artificial intelligence are LISP and PROLOG.
Expert system are compromised primary components, called shells, when they are not populated with particular data, and the shells are designed to host new expert system.

Keys to the system is the knowledge base (KB), which contains specific information or fact patterns associated with a particular subject matter and the rule for interpreting these facts. The KB interface with a database in obtaining data to analyze a particular problem in deriving an expert conclusion. The information in the KB can be expressed in several ways:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.
Rule – Expressing declarative knowledge through the use of if-then relationships. For example, if a patient's body temperature is over 39 degrees Celsius and their pulse is under 60, then they might be suffering from a certain disease.

Semantic nets – Consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of a data.

Additionally, the inference engine shown is a program that uses the KB and determines the most appropriate outcome based on the information supplied by the user. In addition, an expert system includes the following components

Knowledge interface – Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

Data Interface – Enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

The following were incorrect answers:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule - Expressing declarative knowledge through the use of if-then relationships.

Semantic nets – Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.

Reference:

CISA review manual 2014 Page number 187

QUESTION 337
An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model outline the major process of an organization and the external parties with which business interacts?

A. Context Diagrams
B. Activity Diagrams
C. Swim-lane diagrams
D. Entity relationship diagrams

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Context diagram – Outline the major processes of an organization and the external parties with which business interacts.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.
To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse – This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer – This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram – Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Context diagram – Outline the major processes of an organization and the external parties with which business interacts.
Activity or swim-lane diagram – De-construct business processes.

Reference:

CISA review manual 2014 Page number 188

QUESTION 338
Which of the following layer of an enterprise data flow architecture represents subset of information from the core Data Warehouse selected and organized to meet the needs of a particular business unit or business line?

A. Data preparation layer
B. Desktop Access Layer
C. Data Mart layer
D. Data access layer

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Data Mart layer – Data mart represents subset of information from the core Data Warehouse selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure. For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse – This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer – This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.
Entity relationship diagram – Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.
The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer – his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Reference:

CISA review manual 2014 Page number 188

QUESTION 339
Which of the following layer of an enterprise data flow architecture is responsible for data copying, transformation in Data Warehouse (DW) format and quality control?

A. Data Staging and quality layer
B. Desktop Access Layer
C. Data Mart layer
D. Data access layer

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.
For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse – This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer – This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.
Entity relationship diagram – Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Mart layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer – his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Reference:

CISA review manual 2014 Page number 188

QUESTION 340
Which of the following layer of an enterprise data flow architecture represents subsets of information from the core data warehouse?

A. Presentation layer
B. Desktop Access Layer
C. Data Mart layer
D. Data access layer

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Data Mart layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure. For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse – This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer – This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram – Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.
The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data access layer – his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Reference:

CISA review manual 2014 Page number 188

QUESTION 341
Which of the following layer in in an enterprise data flow architecture is directly death with by end user with information?

A. Desktop access layer
B. Data preparation layer
C. Data mart layer
D. Data access layer

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:
Presentation/desktop access layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.
To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:
Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.
Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Data mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.
Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Reference:

CISA review manual 2014 Page number 188

QUESTION 342
ISO 9126 is a standard to assist in evaluating the quality of a product. Which of the following is defined as a set of attributes that bear on the existence of a set of functions and their specified properties?

A. Reliability
B. Usability
C. Functionality
D. Maintainability

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

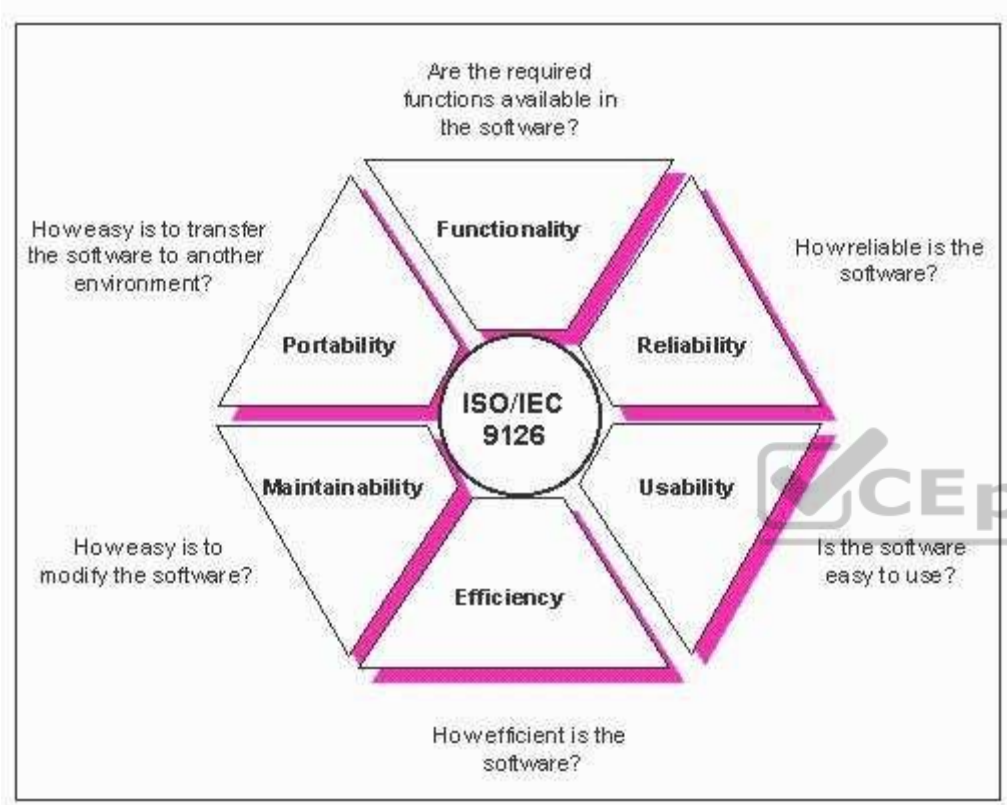
Explanation/Reference:
Explanation:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties.
The functions are those that satisfy stated or implied needs.
Suitability
Accuracy
Interoperability
Security
Functionality Compliance

For CISA Exam you should know below information about ISO 9126 model:

ISO/IEC 9126 Software engineering — Product quality was an international standard for the evaluation of software quality. It has been replaced by ISO/IEC 25010:2011.[1] The fundamental objective of the ISO/IEC 9126 standard is to address some of the well-known human biases that can adversely affect the delivery and perception of a software development project. These biases include changing priorities after the start of a project or not having any clear definitions of "success." By clarifying, then agreeing on the project priorities and subsequently converting abstract priorities (compliance) to measurable values (output data can be validated against schema X with zero intervention), ISO/IEC 9126 tries to develop a common understanding of the project's objectives and goals.

ISO 9126



The standard is divided into four parts:

Quality model
External metrics
Internal metrics
Quality in use metrics.

Quality Model
The quality model presented in the first part of the standard, ISO/IEC 9126-1,[2] classifies software quality in a structured set of characteristics and subcharacteristics as follows:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs.
Suitability
Accuracy
Interoperability
Security
Functionality Compliance

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.
Maturity
Fault Tolerance
Recoverability
Reliability Compliance

Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.
Understandability
Learn ability
Operability
Attractiveness
Usability Compliance

Efficiency - A set of attributes that bear on the relationship between the level of performance of the software and the amount of resources used, under stated conditions.
Time Behavior
Resource Utilization
Efficiency Compliance

Maintainability - A set of attributes that bear on the effort needed to make specified modifications.
Analyzability
Changeability
Stability
Testability
Maintainability Compliance

Portability - A set of attributes that bear on the ability of software to be transferred from one environment to another.
Adaptability
Install ability
Co-Existence
Replace ability
Portability Compliance

Each quality sub-characteristic (e.g. adaptability) is further divided into attributes. An attribute is an entity which can be verified or measured in the software product. Attributes are not defined in the standard, as they vary between different software products.

Software product is defined in a broad sense: it encompasses executables, source code, architecture descriptions, and so on. As a result, the notion of user extends to operators as well as to programmers, which are users of components such as software libraries.

The standard provides a framework for organizations to define a quality model for a software product. On doing so, however, it leaves up to each organization the task of specifying precisely its own model. This may be done, for example, by specifying target values for quality metrics which evaluates the degree of presence of quality attributes.

Internal Metrics
Internal metrics are those which do not rely on software execution (static measure)

External Metrics
External metrics are applicable to running software.
Quality in Use Metrics

Quality in use metrics are only available when the final product is used in real conditions.
Ideally, the internal quality determines the external quality and external quality determines quality in use.

This standard stems from the GE model for describing software quality, presented in 1977 by McCall et al., which is organized around three types of Quality Characteristics:

Factors (To specify): They describe the external view of the software, as viewed by the users.
Criteria (To build): They describe the internal view of the software, as seen by the developer.
Metrics (To control): They are defined and used to provide a scale and method for measurement.

ISO/IEC 9126 distinguishes between a defect and a nonconformity, a defect being The nonfulfillment of intended usage requirements, whereas a nonconformity is The nonfulfillment of specified requirements. A similar distinction is made between validation and verification, known as V&V in the testing trade.

The following were incorrect answers:

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.
Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.
Maintainability - A set of attributes that bear on the effort needed to make specified modifications.

Reference:

CISA review manual 2014 Page number 188

QUESTION 343
Which of the following ACID property ensures that transaction will bring the database from one valid state to another?

A. Atomicity
B. Consistency
C. Isolation D. Durability

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

For CISA exam you should know below information about ACID properties in DBMS:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors, and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other. Providing isolation is the main goal of concurrency control. Depending on concurrency control method, the effects of an incomplete transaction might not even be visible to another transaction.[citation needed]

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

The following were incorrect answers:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other.

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

Reference:

CISA review manual 2014 Page number 218

QUESTION 344

Which of the following is an estimation technique where the results can be measure by the functional size of an information system based on the number and complexity of input, output, interface and queries?

A. Functional Point analysis
B. Gantt Chart
C. Time box management
D. Critical path methodology

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation:

For CISA exam you should know below information about Functional Point Analysis:

Function Point Analysis (FPA) is an ISO recognized method to measure the functional size of an information system. The functional size reflects the amount of functionality that is relevant to and recognized by the user in the business. It is independent of the technology used to implement the system.

The unit of measurement is "function points". So, FPA expresses the functional size of an information system in a number of function points (for example: the size of a system is 314 fop's). The functional size may be used:

To budget application development or enhancement costs
To budget the annual maintenance costs of the application portfolio
To determine project productivity after completion of the project
To determine the Software Size for cost estimating

All software applications will have numerous elementary processes or independent processes to move data. Transactions (or elementary processes) that bring data from outside the application domain (or application boundary) to inside that application boundary are referred to as external inputs. Transactions (or elementary processes) that take data from a resting position (normally on a file) to outside the application domain (or application boundary) are referred as either an external outputs or external inquiries. Data at rest that is maintained by the application in question is classified as internal logical files. Data at rest that is maintained by another application in question is classified as external interface files.

Types of Function Point Counts:

Development Project Function Point Count
Function Points can be counted at all phases of a development project from requirements up to and including implementation. This type of count is associated with new development work. Scope creep can be tracked and monitored by understanding the functional size at all phase of a project. Frequently, this type of count is called a baseline function point count.

Enhancement Project Function Point Count

It is common to enhance software after it has been placed into production. This type of function point count tries to size enhancement projects. All production applications evolve over time. By tracking enhancement size and associated costs a historical database for your organization can be built. Additionally, it is important to understand how a Development project has changed over time.

Application Function Point Count
Application counts are done on existing production applications. This "baseline count" can be used with overall application metrics like total maintenance hours. This metric can be used to track maintenance hours per function point. This is an example of a normalized metric. It is not enough to examine only maintenance, but one must examine the ratio of maintenance hours to size of the application to get a true picture. Productivity:

The definition of productivity is the output-input ratio within a time period with due consideration for quality.
Productivity = outputs/inputs (within a time period, quality considered)

The formula indicates that productivity can be improved by (1) by increasing outputs with the same inputs, (2) by decreasing inputs but maintaining the same outputs, or (3) by increasing outputs and decreasing inputs change the ratio favorably.

Software Productivity = Function Points / Inputs

Effectiveness vs. Efficiency:
Productivity implies effectiveness and efficiency in individual and organizational performance. Effectiveness is the achievement of objectives. Efficiency is the achievement of the ends with least amount of resources.

Software productivity is defined as hours/function points or function points/hours. This is the average cost to develop software or the unit cost of software. One thing to keep in mind is the unit cost of software is not fixed with size. What industry data shows is the unit cost of software goes up with size.

Average cost is the total cost of producing a particular quantity of output divided by that quantity. In this case to Total Cost/Function Points. Marginal cost is the change in total cost attributable to a one-unit change in output.

There are a variety of reasons why marginal costs for software increase as size increases. The following is a list of some of the reasons

As size becomes larger complexity increases.
As size becomes larger a greater number of tasks need to be completed.
As size becomes larger there is a greater number of staff members and they become more difficult to manage.

Function Points are the output of the software development process. Function points are the unit of software. It is very important to understand that Function Points remain constant regardless who develops the software or what language the software is developed in. Unit costs need to be examined very closely. To calculate average unit cost all items (units) are combined and divided by the total cost. On the other hand, to accurately estimate the cost of an application each component cost needs to be estimated.

Determine type of function point count
Determine the application boundary
Identify and rate transactional function types to determine their contribution to the unadjusted function point count. Identify and rate data function types to determine their contribution to the unadjusted function point count.
Determine the value adjustment factor (VAF) Calculate the adjusted function point count.

To complete a function point count knowledge of function point rules and application documentation is needed. Access to an application expert can improve the quality of the count. Once the application boundary has been established, FPA can be broken into three major parts

FPA for transactional function types
FPA for data function types
FPA for GSCs

Rating of transactions is dependent on both information contained in the transactions and the number of files referenced, it is recommended that transactions are counted first. At the same time a tally should be kept of all FTR's (file types referenced) that the transactions reference. Every FTR must have at least one or more transactions. Each transaction must be an elementary process. An elementary process is the smallest unit of activity that is meaningful to the end user in the business. It must be self-contained and leave the business in consistent state

The following were incorrect answers:

Critical Path Methodology - The critical path method (CPM) is an algorithm for scheduling a set of project activities

Gantt Chart - A Gantt chart is a type of bar chart, developed by Henry Gantt in the 1910s, that illustrates a project schedule. Gantt charts illustrate the start and finish dates of the terminal elements and summary elements of a project. Terminal elements and summary elements comprise the work breakdown structure of the project. Modern Gantt charts also show the dependency (i.e. precedence network) relationships between activities. Gantt charts can be used to show current schedule status using percent-complete shadings and a vertical "TODAY" line as shown here.

Time box Management - In time management, a time boxing allocates a fixed time period, called a time box, to each planned activity. Several project management approaches use time boxing. It is also used for individual use to address personal tasks in a smaller time frame. It often involves having deliverables and deadlines, which will improve the productivity of the user.

Reference:

CISA review manual 2014 Page number 154

QUESTION 345

Following a recent acquisition, an information security manager has been requested the outstanding risk reported early in the acquisition process. Which of the following would be the manager's **BEST** course of action?

A. Perform a vulnerability assessment of the acquired company's infrastructure.
B. Re-evaluate the risk treatment plan for the outstanding risk.
C. Re-assess the outstanding risk of the acquired company.
D. Add the outstanding risk to the acquiring organization's risk registry

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 346
A manufacturing company is implementing application software for its sales and distribution system. Which of the following is the **MOST** important reason for the company choose a centralized online database?

A. Enhanced data redundancy
B. Elimination of multiple points of failure
C. Elimination of the need for data normalization
D. Enhanced integrity controls

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 347
An organization has replaced all of the storage devices at its primary data center with new, higher capacity units. The replaced devices have been installed at the disaster recovery site to replace older units. An IS auditor's **PRIMARY** concern would be whether:

A. the procurement was in accordance with corporate policies and procedures
B. the relocation plan has been communicated to all concerned parties
C. a hardware maintenance contract is in place for both old and new storage devices
D. the recovery site devices can handle the storage requirements

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 348
A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon. The **MOST** effective plan of action would be to:

A. use analytical tools to produce exception reports from the system and performance monitoring software
B. re-install the system and performance monitoring software
C. evaluate replacement systems and performance monitoring software
D. restrict functionality of system monitoring software to security-related events

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 349
The **PRIMARY** objective of conducting a post-implementation review is to:

A. determine if project management methodology was applied consistently
B. verify that the information system meets the intended objectives
C. determine if testing documentation was sufficient
D. allow employees to provide feedback on the information system

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
QUESTION 350
The **MOST** significant reason for using key performance indicators (KPIs) to track the progress of IT projects against initial targets is that they:

A. influence management decisions to outsource IT projects
B. identify which projects may require additional funding
C. provide timely indication of when corrective actions need to be taken
D. identify instances where increased stakeholder engagement is required

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 351
An organization has implemented an automated match between purchase orders, goods receipts, and invoices. Which of the following risks will this control **BEST** mitigate?

A. Customer discounts not being applied
B. A legitimate transaction being paid multiple times
C. Invalid payments being processed by the system
D. Delay of purchase orders

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 352
A multinational organization is integrating its existing payroll system with a human resource information system. Which of the following should be of **GREATEST** concern to the IS auditor?

A. System documentation
B. Currency conversion

Explanation/Reference:

C. Application interfaces
D. Scope creep

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 353
An online retailer is receiving customer about receiving different items from what they ordered on the organization's website. The root cause has been traced to poor data quality. Despite efforts to clean erroneous data from the system, multiple data quality issues continue to occur. Which of the following recommendations would be the **BEST** way to reduce the likelihood of future occurrences?

A. Implement business rules to validate employee data entry.
B. Invest in additional employee training for data entry.
C. Assign responsibility for improving data quality.
D. Outsource data cleansing activities to reliable third parties.

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 354
Which of the following are the **PRIMARY** considerations when determining the timing of remediation testing?

A. The level of management and business commitment to implementing agreed action plans
B. The difficulty of scheduling resources and availability of management for a follow-up engagement
C. The availability and competencies of control owners for implementing the agreed action
D. The significance of the reported findings and the impact if corrective actions are not taken

D

QUESTION 355
Which of the following is the **BEST** way to control the concurrent use of licensed software?

A. User self-discipline.
B. Monitor by system administrator.
C. Surprise audit conducted by vendors.
D. Metering software

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 356
When determining the specifications for a server supporting an online application using more than a hundred endpoints, which of the following is the **MOST** important factor to be considered?

A. High availability of different systems
B. Cost-benefit comparison between the available systems
C. Reputation of the vendors and their customer base
D. Transaction volume estimate during peak periods

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Correct Answer:
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

Explanation/Reference:

QUESTION 357
Following an unauthorized disclosure of data, an organization needs to implement data loss prevention (DLP) measures. The IS auditor's **BEST** recommendation should be to:

A. install DLP software on corporate servers to prevent recurrence.
B. monitor and block outgoing emails based on common DLP criteria.
C. restrict removable media access on all computer systems.
D. establish a risk and control framework.

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 358
Which of the following is the **BEST** time for an IS auditor to perform a post-implementation review?

A. When the system has stabilized.
B. After the completion of user testing.
C. Before decommissioning the legacy system.
D. Immediately after the new system goes into production.

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 359
What is the **PRIMARY** advantage of prototyping as part of systems development?

A. Maximizes user satisfaction
B. Eliminates the need for internal controls
C. Increases accuracy in reporting
D. Reduces the need for compliance testing

A

QUESTION 360
What is the **BEST** population to select from when testing that programs are migrated to production with proper approval?

A. List of changes provided by application programming managers
B. List of production programs
C. Completed change request forms
D. Change advisory board meeting minutes

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 361
An organization has implemented data storage hardware. Which of the following should an IS auditor review to assess if IT is maximizing storage and network utilization?

A. Capacity management plans

Correct Answer:
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

B. Downtime statistics
C. The quality management systems
D. Routine and non-routine job schedules

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 362
When evaluating the recent implementation of an intrusion detection system (IDS), an IS auditor should be **MOST** concerned with inappropriate:

A. encryption.

B. training.
C. tuning.
D. patching.

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 363
Which of the following procedures should be implemented prior to disposing of surplus computer equipment to employees?

A. Use operating system commands to delete all files from the hard drive.
B. Have the employee receiving the machine sign a nondisclosure agreement.
C. Use application delete commands to remove files.
D. Overwrite the hard drive with random data.

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 364
Which of the following controls should be implemented to **BEST** minimize system downtime for maintenance?

A. Nightly full backups
B. Virtualization
C. Warm site
D. Clustering

D

QUESTION 365
The **MOST** efficient way to confirm that an ERP system being implemented satisfies business expectations is to utilize which of the following types of testing?

A. Parallel
B. Pilot
C. Sociability
D. Alpha

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

Correct Answer:
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 366
An organization plans to implement a virtualization strategy enabling multiple operating systems on a single host. Which of the following should be the **GREATEST** concern with this strategy?

A. Adequate storage space
B. Complexity of administration
C. Network bandwidth
D. Application performance

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 367
An organization considers implementing a system that uses a technology that is not in line with the organization's IT strategy. Which of the following is the **BEST** justification for deviating from the IT strategy?

A. The system has a reduced cost of ownership.
B. The organization has staff familiar with the technology.
C. The business benefits are achieved even with extra costs.
D. The system makes use of state-of-the-art technology.

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 368
Which of the following methodologies is **MOST** appropriate to use for developing software with incomplete requirements?

A. Process-based
B. Critical chain
C. Waterfall
D. Agile

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 369
Which of the following is **MOST** important to the effective management of an end user-developed application?

A. Implementing best practice folder structures
B. Continuous monitoring to facilitate prompt escalation of issues
C. Assigning risk ratings based on probability and impact
D. Stress testing the application through use of data outliers

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation
Explanation/Reference:

QUESTION 370
A development team has designed a new application and incorporated best practices for secure coding. Prior to launch, which of the following is the IS auditor's **BEST** recommendation to mitigate the associated security risk?

A. User acceptance testing
B. Unit testing
C. Integration testing
D. Penetration testing

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 371
Which of the following should be reviewed **FIRST** when assessing the effectiveness of an organization's network security procedures and controls?

A. Data recovery capability
B. Inventory of authorized devices
C. Vulnerability remediation
D. Malware defenses

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 372
An organization is implementing the use of mobile devices that will connect to sensitive corporate applications. Which of the following is the **BEST** recommendation to mitigate risk of data leakage?

A. Remote data wipe
B. GPS tracking software
C. Encrypted RFID tags
D. Data encryption

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 373
The **PRIMARY** responsibility of a project steering committee is to:

A. ensure that each project deadline is met
B. undertake final acceptance of the system for implementation
C. ensure that systems developed meet business needs
D. provide day-to-day guidance and oversight

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 374

As IS auditor discovers that due to resource constraints, a database administrator (DBA) is responsible for developing and executing changes into the production environment. Which of the following should the auditor do **FIRST**?

A. Identify whether any compensating controls exist
B. Report a potential segregation of duties (SoD) violation
C. Determine whether another database administrator could make the changes
D. Ensure a change management process is followed prior to implementation

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 375
When implementing a new risk assessment methodology, which of the following is the **MOST** important requirement?

A. The methodology must be approved by the chief executive officer.
B. Risk assessments must be reviewed annually.
C. Risk assessments must be conducted by certified staff.
D. The methodology used must be consistent across the organization.

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 376
Which of the following is the **MOST** likely reason an organization would use Platform as a Service (PaaS)?

A. To operate third-party hosted applications
B. To install and manage operating systems

C. To establish a network and security architecture
D. To develop and integrate its applications

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 377
Which of the following is the **BEST** approach to reduce unnecessary duplication of compliance activities?

A. Integrating of assurance efforts
B. Automation of controls
C. Standardization of compliance requirements
D. Documentation of control procedures

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 378
Which of the following sites would be **MOST** appropriate in the case of a very short recovery time objective (RTO)?

A. Mobile
B. Redundant
C. Shared
D. Warm

Correct Answer: B

Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 379
Which of the following is the **GREATEST** risk associated with the lack of an effective data privacy program?

A. Failure to prevent fraudulent transactions
B. Inability to manage access to private or sensitive data
C. Inability to obtain customer confidence
D. Failure to comply with data-related regulations

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
QUESTION 380
A design company has multiple name and address files for its customers in several of its independent systems. Which of the following is the **BEST** control to ensure that the customer name and address agree across all files?

A. Use of hash totals on customer records
B. Periodic review of each master file by management
C. Matching of records and review of exception reports
D. Use of authorized master file change forms

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 381
Which of the following is the client organization's responsibility in a Software as a Service (SaaS) environment?

A. Detecting unauthorized access
B. Ensuring that users are properly authorized
C. Ensuring the data is available when needed
D. Preventing insertion of malicious code

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 382
An existing system is being replaced with a new application package. User acceptance testing (UAT) should ensure that:

A. data from the old system has been converted correctly
B. the new system functions as expected
C. the new system is better than the old system
D. there is a business need for the new system

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 383
An employee of an organization has reported losing a smartphone that contains sensitive information. The **BEST** step to address this situation should be to:

A. terminate the device connectivity
B. escalated to the user's management

C. disable the user's access to corporate resources
D. remotely wipe the device

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 384
Which of the following is the **BEST** physical security solution for granting and restricting access to individuals based on their unique access needs?

A. Bolting door locks
B. Cipher locks
C. Closed-circuit television (CCTV)
D. Electronic badge system

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
QUESTION 385
Which of the following methods should be used to purge confidential data from write-once optical media?

A. Degauss the media.
B. Destroy the media.
C. Remove the references to data from the access index.
D. Write over the data with null values.

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 386
In a typical network architecture used for e-commerce, a load balancer is normally found between the:

A. routers and the web servers.
B. mail servers and the mail repositories.
C. users and the external gateways.
D. databases and the external gateways.

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 387
An organization is choosing key performance indicators (KPIs) for its information security management. Which of the following KPIs would provide stakeholders with the **MOST** useful information about whether information security risk is being managed?

A. Time from initial reporting of an incident to appropriate escalation
B. Time from identifying a security threat to implementing a solution
C. The number of security controls implemented
D. The number of security incidents during the past quarter

B

QUESTION 388
Which of the following control checks would utilize data analytics?

A. Evaluating configuration settings for the credit card application system
B. Reviewing credit card applications submitted in the past month for blank data fields
C. Attempting to submit credit card applications with blank data fields
D. Reviewing the business requirements document for the credit card application system

Correct Answer: D
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 389
Which of the following is the **BEST** way to control scope creep during application system development?

A. Involve key stakeholders.
B. Implement project steering committee review.
C. Implement a quality management system.
D. Establish key performance indicators (KPIs).

Correct Answer: B
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

Correct Answer:
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
QUESTION 390
An organization has an approved bring your own device (BYOD) program. Which of the following is the **MOST** effective method to enforce application control on personal devices?

A. Implement a mobile device management solution.
B. Establish a mobile device acceptable use policy.
C. Implement a web application firewall.
D. Educate users regarding the use of approved applications.

Correct Answer: A
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 391
An emergency change was made to an IT system as a result of a failure. Which of the following should be of **GREATEST** concern to the organization's information security manager?

A. The operations team implemented the change without regression testing.
B. The change did not include a proper assessment of risk.
C. Documentation of the change was made after implementation.
D. The information security manager did not review the change prior to implementation.

Correct Answer: B
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 392
The **MOST** important factors in determining the scope and timing for testing a business continuity plan are:

A. manual processing capabilities and the test location.
B. the importance of the function to be tested and the cost of testing.
C. the experience level of personnel and the function location.
D. prior testing results and the degree of detail of the business continuity plan.

B

QUESTION 393
Which of the following will identify a deviation in the information security management process from generally accepted standards of good practices?

A. Gap analysis
B. Risk assessment
C. Business impact analysis (BIA)
D. Penetration testing

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 394
Which of the following is **MOST** important for an organization to complete prior to developing its disaster recovery plan (DRP)?

A. Support staff skill gap analysis
B. Comprehensive IT inventory

Correct Answer:
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
C. Business impact analysis (BIA)
D. Risk assessment

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

QUESTION 395
An application development team is also promoting changes to production for a critical financial application. Which of the following would be the **BEST** control to reduce the associated risk?

A. Implementing a change management code review
B. Implementing a peer review process
C. Performing periodic audits
D. Submitting change logs to the business manager for review

Correct Answer: A
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 396
A web application is developed in-house by an organization. Which of the following would provide the **BEST** evidence to an IS auditor that the application is secure from external attack?

A. Penetration test results
B. Database application monitoring logs

C. Code review by a third party
D. Web application firewall implementation

Correct Answer: A
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 397
Which of the following is the **BEST** methodology to use for estimating the complexity of developing a large business application?

A. Function point analysis
B. Software cost estimation
C. Work breakdown structure
D. Critical path analysis

A

QUESTION 398
An organization is considering allowing users to connect personal devices to the corporate network. Which of the following should be done **FIRST**?

A. Configure users on the mobile device management solution.
B. Create inventory records of personal devices.
C. Implement an acceptable use policy.
D. Conduct security awareness training.

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Correct Answer:
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Explanation/Reference:

QUESTION 399
Which of the following is critical to the successful establishment of an enterprise IT architecture?

A. A well-defined data migration policy
B. Comparison of the architecture with that of other organizations
C. An architecture encompassing only critical systems
D. Organizational support for standardization

Correct Answer: D
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 400
Which of the following is **MOST** important in determining a project's feasibility?

A. The organization's main competitor has initiated a similar project.
B. The IT steering committee endorses the project.
C. A project management methodology is established.
D. The project's value is established in an approved business case.

Correct Answer: D
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 401

Which of the following **BEST** helps to identify errors during data transfer?

A. Decrease the size of data transfer packets.
B. Test the integrity of the data transfer.
C. Review and verify the data transfer sequence numbers.
D. Enable a logging process for data transfer.

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 402
To create a digital signature in a message using asymmetric encryption, it is necessary to:

A. first use a symmetric algorithm for the authentication sequence.
B. encrypt the authentication sequence using a public key.
C. transmit the actual digital signature in unencrypted clear text.
D. encrypt the authentication sequence using a private key.

Correct Answer: D

Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 403
What is the **PRIMARY** benefit of prototyping as a method of system development?

A. Reduces the need for testing.
B. Minimizes the time the IS auditor has to review the system.
C. Increases the likelihood of user satisfaction.
D. Eliminates the need for documentation.

Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 404
Which of the following methods **BEST** ensures that a comprehensive approach is used to direct information security activities?

A. Creating communication channels
B. Promoting security training
C. Establishing a steering committee
D. Holding periodic meetings with business owners

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 405
An organization's marketing department has requested access to cloud-based collaboration sites for exchanging media files with external marketing companies. As a result, the information security manager has been asked to perform a risk assessment. Which of the following should be the **MOST** important consideration?

A. The information to be exchanged
B. Methods for transferring the information
C. Reputations of the external marketing companies
D. The security of the third-party cloud provider

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 406
A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value can be mitigated by:

A. requiring the recipient to use a different hash algorithm.
B. generating hash output that is the same size as the original message.
C. using a secret key in conjunction with the hash algorithm.
D. using the sender's public key to encrypt the message.

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 407
Which of the following is the **MOST** effective data loss control when connecting a personally owned mobile device to the corporate email system?

A. A senior manager must approve each new connection.
B. Email synchronization must be prevented when connected to a public Wi-Fi hotspot.
C. Email must be stored in an encrypted format on the mobile device.

D. Users must agree to allow the mobile device to be wiped if it is lost.

Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 408
A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The **GREATEST** weakness under this system architecture is that:

A. an incident involving unauthorized access to data cannot be tied to a specific user.
B. when multiple sessions with the same application ID collide, the database locks up.
C. users can gain direct access to the application ID and circumvent data controls.
D. the database becomes unavailable if the password of the application ID expires.

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 409
Which of the following is the **MOST** effective mitigation strategy to protect confidential information from insider threats?

A. Implementing authentication mechanisms
B. Performing an entitlement review process
C. Defining segregation of duties
D. Establishing authorization controls.

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 410
Labeling information according to its security classification:
A. reduces the need to identify baseline controls for each classification.
B. reduces the number and type of countermeasures required.
C. enhances the likelihood of people handling information securely.
D. affects the consequences if information is handled insecurely.

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 411
Which of the following **MOST** effectively prevents internal users from modifying sensitive data?

A. Network segmentation
B. Multi-factor authentication
C. Acceptable use policies
D. Role-based access controls

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 412
Which of the following is the **PRIMARY** benefit to an organization using an automated event monitoring solution?

A. Enhanced forensic analysis
B. Improved response time to incidents

C. Improved network protection
D. Reduced need for manual analysis

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:

QUESTION 413
Which of the following should be **PRIMARILY** included in a security training program for business process owners?

A. Application vulnerabilities
B. List of security incidents reported
C. Application recovery time
D. Impact of security risks

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 414
During an annual security review of an organization's servers, it was found that the customer service team's file server, which contains sensitive customer data, is accessible to all user IDs in the organization. Which of the following should the information security manager do **FIRST**?

A. Report the situation to the data owner.
B. Remove access privileges to the folder containing the data.
C. Train the customer service team on properly controlling file permissions.
D. Isolate the server from the network.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 415
Which of the following is the **BEST** way to improve the timely reporting of information security incidents? A.

Perform periodic simulations with the incident response team.

B. Incorporate security procedures in help desk processes.
C. Integrate an intrusion detection system (IDS) in the DMZ.
D. Regularly reassess and update the incident response plan.

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 416
The **MOST** important reason to use a centralized mechanism to identify information security incidents is to:

A. prevent unauthorized changes to networks.
B. comply with corporate policies.
C. detect potential fraud.
D. detect threats across environments.

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 417
An organization has detected sensitive data leakage caused by an employee of a third-party contractor. What is the **BEST** course of action to address this issue?

A. Include security requirements in outsourcing contracts.
B. Activate the organization's incident response plan.
C. Limit access to the third-party contractor.
D. Terminate the agreement with the third-party contractor.

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
QUESTION 418
During an IS audit of a data center, it was found that programmers are allowed to make emergency fixes to operational programs. Which of the following should be the IS auditor's PRIMARY recommendation?

A. Bypass use ID procedures should be put in place to ensure that the changes are subject to after-the-event approval and testing
B. The ability to undertake emergency fixes should be restricted to selected key personnel
C. Programmers should be allowed to implement emergency fixes only after obtaining verbal agreement from the application owner
D. Emergency program changes should be subject to program migration and testing procedures before they are applied to operational systems

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 419
Which of the following is the GREATEST concern associated with control self-assessments?

A. Employees may have insufficient awareness of controls
B. Controls may not be assessed objectively
C. Communication between operational management and senior management may not be effective
D. The assessment may not provide sufficient assurance to stakeholders

Correct Answer: B

Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 420
Several remote users have been unable to communicate with a secured network news transfer protocol (NNTP) server. Of the following, the MOST likely cause is:

A. the use of a password cracker
B. a hacker impersonating the server
C. a hacker using a sniffer

D. a replay attack by an eavesdropper

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 421
Which of the following MOST effectively provides assurance of ongoing service delivery by a vendor?

A. Regular status reporting provided by the vendor
B. Short incident response time by the vendor
C. Pre-defined service and operational level agreements
D. Regular monitoring by service management team

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 422
Which of the following tests is MOST likely to detect an error in one subroutine resulting from a recent change in another subroutine?

A. Stress testing
B. Regression testing
C. User acceptance testing
D. Black-box testing

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation
QUESTION 423

Reconciliations have identified data discrepancies between an enterprise data warehouse and a revenue system for key financial reports. What is the GREATEST risk to the organization in this situation?

A. The key financial reports may no longer be produced
B. Financial reports may be delayed
C. Undetected fraud may occur
D. Decisions may be made based on incorrect information

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 424
Which of the following is the MOST important feature of access control software?

A. Authentication
B. Violation reporting
C. Nonrepudiation
D. Identification

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 425
For several years, a vendor has been providing offsite backup media and record storage for a bank. Due to familiarity with bank employees, the vendor does not consistently require authorization forms from them to retrieve media. Which of the following is the GREATEST risk from this situation?

Explanation/Reference:

A. Bank employees can inappropriately obtain sensitive records
B. Backup tapes may not be available
C. Chain of custody could not be validated
D. The vendor provides the incorrect media to employees

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 426
Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

A. Validity check
B. Reasonableness check
C. Parity check
D. Limit check

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 427
A firewall has been installed on the company's web server. Which concern does the firewall address?

A. Availability of the information
B. Unauthorized modification of information by internal users
C. Accessing information by the outside world
D. Connectivity to the Internet

Correct Answer: C

Section: Information System Operations, Maintenance and Support
Explanation

QUESTION 428
An organization is within a jurisdiction where new regulations have recently been announced to restrict cross-border data transfer of personally identifiable information (PII). Which of the following IT decisions will MOST likely need to be assessed in the context of this change?

A. Hosting the payroll system at an external cloud service provider
B. Purchasing cyber insurance from an overseas insurance company
C. Applying encryption to database hosting PII data
D. Hiring IT consultants from overseas

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 429
A recent audit concluded that an organization's information security system was weak and that monitoring would likely fail to detect penetration. Which of the following would be the MOST appropriate recommendation?

A. Look continually for new criminal behavior and attacks on sensitive data
B. Establish a clear policy related to security and the handling of sensitive data
C. Encrypt sensitive data while strengthening the system
D. Identify and periodically remove sensitive data that is no longer needed

Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

Explanation/Reference:

QUESTION 430
A data breach has occurred at a third-party vendor used by an organization to outsource the processing of its customer data. What should be management's FIRST course of action?

A. Activate the disaster recovery plan
B. Notify the insurance company of the potential claim
C. Activate the incident management process
D. Take legal action against the service provider for reputation damage

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 431
During an external assessment of network vulnerability, which of the following activities should be performed FIRST?

A. Collect network information
B. Implement an intrusion detection system (IDS)
C. Monitor the network
D. Review policies

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 432
Which of the following would BEST prevent data from being orphaned?

A. Referential integrity
B. Table partitioning
C. Input validation checks
D. Table indexes

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation
QUESTION 433
Which of the following is the MOST reliable network connection medium in an environment where there is strong electromagnetic interference?

A. Coaxial cable
B. Fiber optic cable
C. Shielded twisted-pair cable
D. Wireless link

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 434
When consolidating several applications from two outdated servers onto one new server, which of the following is the GREATEST concern?

A. Increased software licensing cost
B. Maintenance requires more coordination
C. Decreased utilization of capacity
D. Increased network traffic

Explanation/Reference:

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 435
An organization is considering replacing physical backup tapes stored offsite with real-time on-line backup to a storage area network (SAN) located in the primary data center. Which of the following is the GREATEST risk?

A. Archived data may not satisfy data retention requirements
B. A single disaster could cause significant data loss
C. Backups may require excessive storage space
D. Implementation could cause significant cost increases

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 436
Which of the following procedures would BEST contribute to the reliability of information in a data warehouse?

A. Retaining only current data
B. Storing only a single type of data
C. Maintaining archive data
D. Maintaining current metadata

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 437
Which of the following is the PRIMARY responsibility of an organization's information security function?

A. Reviewing unauthorized attempts to access sensitive files
B. Managing the organization's security procedures
C. Approving access to data files
D. Installing network security programs

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 438

The risk of communication failure in an e-commerce environment is BEST minimized through the use of:

A. alternative or diverse routing
B. compression software to minimize transmission duration
C. a packet filtering firewall to reroute messages
D. functional or message acknowledgments

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 439
Which of the following could be used to evaluate the effectiveness of IT operations?

A. Total cost of ownership
B. Net present value
C. Balanced scorecard
D. Internal rate of return

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 440
The **MOST** important reason for documenting all aspects of a digital forensic investigation is that documentation:

A. provides traceability for independent investigation by third parties.
B. ensures compliance with corporate incident response policies.
C. ensures the process will be repeatable in future investigations.
D. meets IT audit documentation standards.

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 441
When conducting a follow-up audit on an organization's firewall configuration, the IS auditor discovered that the firewall had been integrated into a new system that provides both firewall and intrusion detection capabilities. The IS auditor should:

A. consider the follow-up audit unnecessary since the firewall is no longer being used.
B. assess whether the integrated system addresses the identified risk.
C. review the compatibility of the new system with existing network controls.
D. evaluate whether current staff is able to support the new system.

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 442
Which of the following entities is **BEST** suited to define the data classification levels within an organization?

A. Database administrator based on the data schema
B. Legal compliance team based on the application regulations
C. Business owner responsible for the respective data
D. System administrator responsible for data security controls

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 443
An IT organization's incident response plan is which type of control?
A. Preventive
B. Corrective
C. Detective
D. Directive

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 444
Which of the following is an example of a preventive control in an accounts payable system?

A. The system only allows payments to vendors who are included in the system's master vendor list.
B. Policies and procedures are clearly communicated to all members of the accounts payable department.
C. The system produces daily payment summary reports that staff use to compare against invoice totals.
D. Backups of the system and its data are performed on a nightly basis and tested periodically.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 445
The information security function in a large organization is **MOST** effective when:

A. decentralized as close to the user as possible.
B. the function reports directly to the IS operations manager.
C. partnered with the IS development team to determine access rights.
D. established at a corporate-wide level.

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:

QUESTION 446
Which of the following is the **MOST** likely result of the ongoing deterioration of a detective control?

A. Increased number of data loss events
B. Increased security incident response time
C. Decreased effectiveness of root cause analysis
D. Decreased overall recovery time

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 447
Following the discovery of inaccuracies in a data warehouse, an organization has implemented data profiling, cleansing, and handling filters to enhance the quality of data obtained from connected sources. Which type of control has been applied?

A. Preventive control

B. Corrective control
C. Compensating control
D. Detective control

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:

QUESTION 448
Which of the following is the **BEST** approach for performing a business impact analysis (BIA) of a supply-chain management application?

A. Circulating questionnaires to key internal stakeholders
B. Interviewing groups of key stakeholders
C. Accepting IT personnel's view of business issues
D. Reviewing the organization's policies and procedures

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 449
Which of the following **BEST** provides continuous availability of network bandwidth for critical application services?

A. Configuration management
B. Cloud computing
C. Problem management
D. Quality of service (QoS)

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 450
The objective of using coding standards for systems development is to:

A. facilitate program maintenance.
B. facilitate user testing.
C. ensure the completeness of requirements.
D. ensure that business needs are met.

Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 451
Which of the following sampling techniques is commonly used in fraud detection when the expected occurrence rate is small and the specific controls are critical?

A. Discovery sampling
B. Monetary unit sampling
C. Stop-or-go sampling
D. Random sampling

Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 452

The IS auditor of a power company finds that the radio link to a remote mountain site is experiencing systematic outages under specific weather conditions. The communications manager explains that increasing the radio power would require a new license and would help little. What is the **MOST** appropriate action by the IS auditor?

A. Recommend that the site's data collection and transmission be non-interruptible.
B. Review the installation license, permissions and associated costs.
C. Recommend that the site's hardware be upgraded to record data during outages.
D. Gather additional information to identify threats, vulnerabilities, and impact.

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
QUESTION 453
Most access violations are:

A. Accidental
B. Caused by internal hackers
C. Caused by external hackers
D. Related to Internet

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.
Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 192).

QUESTION 454
Which of the following is NOT a component of IPSec?

A. Authentication Header
B. Encapsulating Security Payload
C. Key Distribution Center
D. Internet Key Exchange

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference: Explanation:
AH, ESP and IKE are the three main components of IPSec. A KDC (Key Distribution Center) is a component of Kerberos, not IPSec.
Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 217).

QUESTION 455
As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains small enhancements and fixes?

A. Major software Release
B. Minor software Release
C. Emergency software release
D. General software Release

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:

Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

For CISA exam you should know below information about software release management:

Software Release Management is the process of ensuring releases can be reliably planned, scheduled and successfully transitioned (deployed) to Test and Live Environments. Software Release Management is not just about "automating the path to production" although that is certainly an important part. It also about adopting a holistic view of application changes, using the "Release" as the container to ensure that changes are packaged, released and tested in a repeatable and controlled manner. Release Management is often likened to the conductor of an orchestra, with the individual changes to be implemented the various instruments within it. Software Release Management is intrinsically linked with the more well understood and adopted Software Change and Configuration Management disciplines.

Software Release management is a process through which software is made available to user. Each update or upgrade of a Configuration Item is referred to as a release.

There are three levels of releases. These levels related to releasing hardware or software into your IT infrastructure. Some may be a single change, others may implement many changes at a time.
Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.
Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

The following were incorrect answers:
Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

General software Release – Not a valid type of software release.

Reference:
CISA review manual 2014 Page number 244

QUESTION 456
In which of the following database models is the data represented in terms of tulles and grouped into relations?

A. Hierarchical database model
B. Network database model
C. Relational database model

D. Object-relational database model

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

For your exam you should know below information about database models:

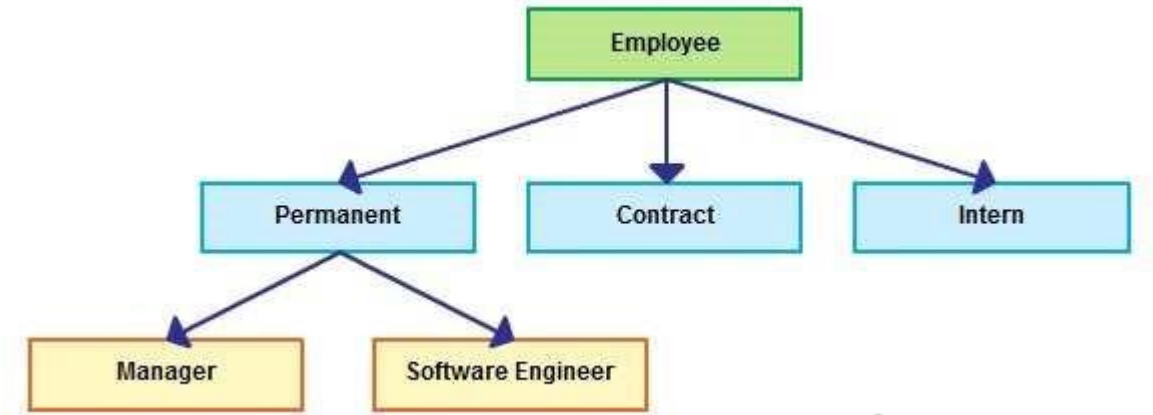
A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:
Hierarchical database model
Network model
Relational model
Object-relational database models

Hierarchical database model
In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.

This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.

Hierarchical database model



Network database model

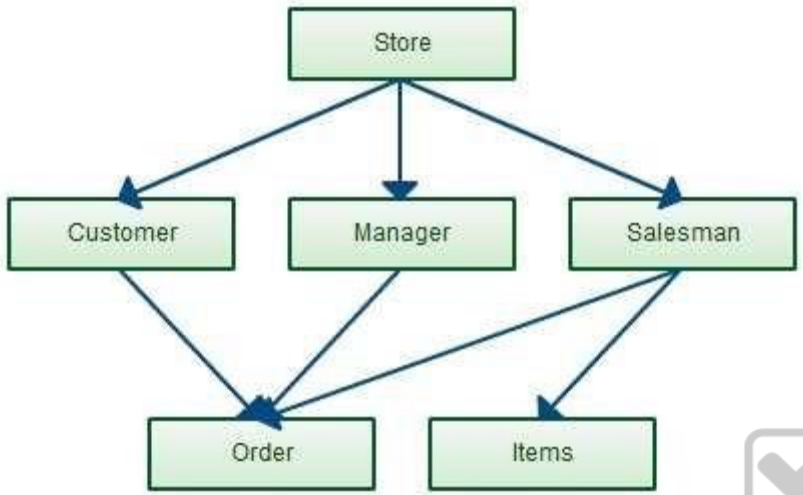
The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.

The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of B. At the same time another set may be defined where B is the owner of A. Thus all the sets comprise a general directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.

The network model is able to represent redundancy in data more efficiently than in the hierarchical model, and there can be more than one path from an ancestor node to a descendant. The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values.

Network Database model

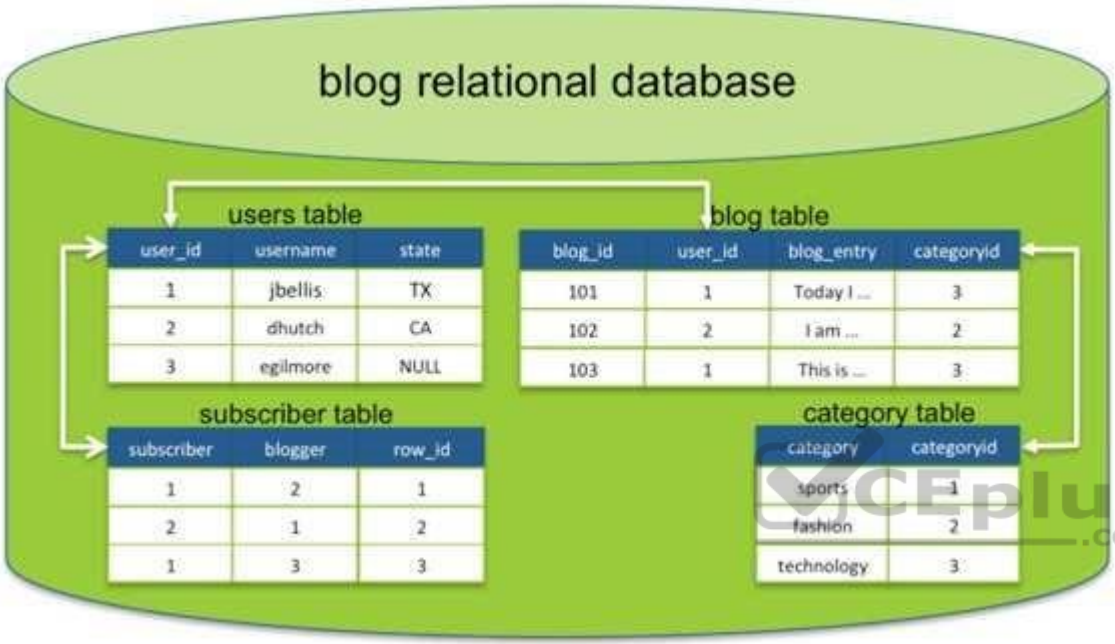


Relational database model
In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

In the relational model, related records are linked together with a "key".

The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.

Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.
Relational database model



Object-relational database Model

An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.

Example of an object-oriented database model

An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:

Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

Network database model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.
Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

Reference:

CISA review manual 2014 Page number 254

QUESTION 457
Which of the following type of a computer network covers a limited area such as a home, office or campus?

A. LAN
B. WAN
C. SAN
D. PAN

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:

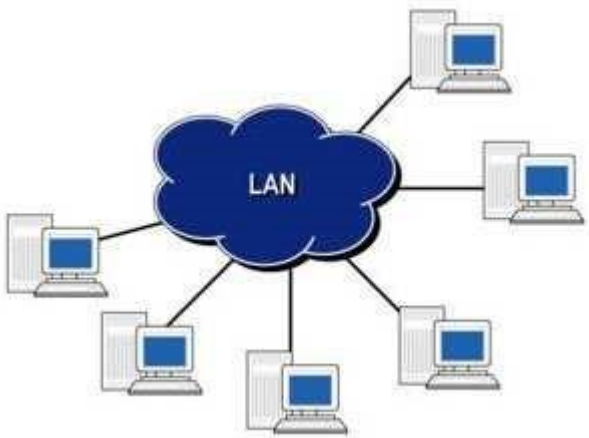
A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

For your exam you should know below information about computer networks:

Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

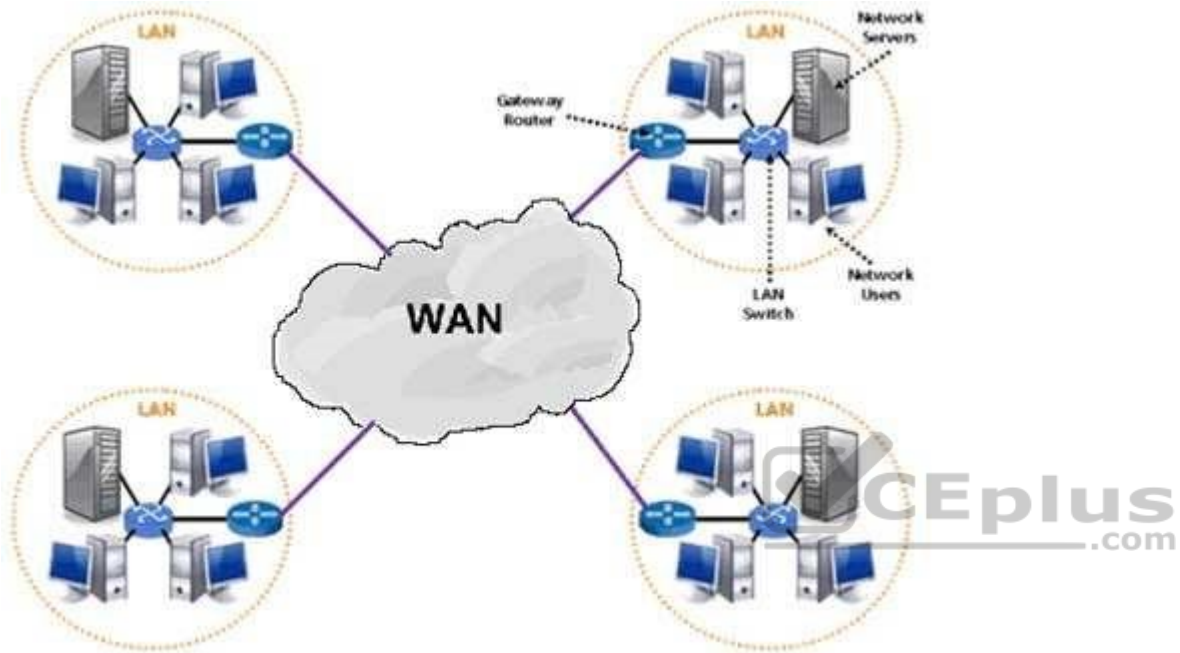
Local Area Network



Wide Area Network

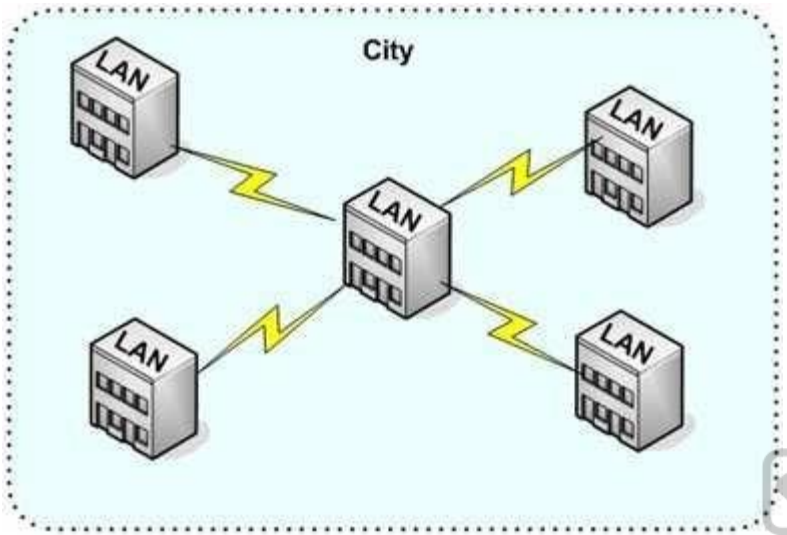
A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

Wide Area Network



Metropolitan Area Network
A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

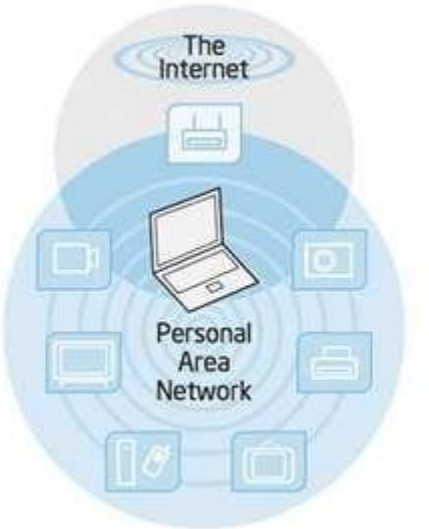


Metropolitan Area Network (MAN)

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Storage Area Network
A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

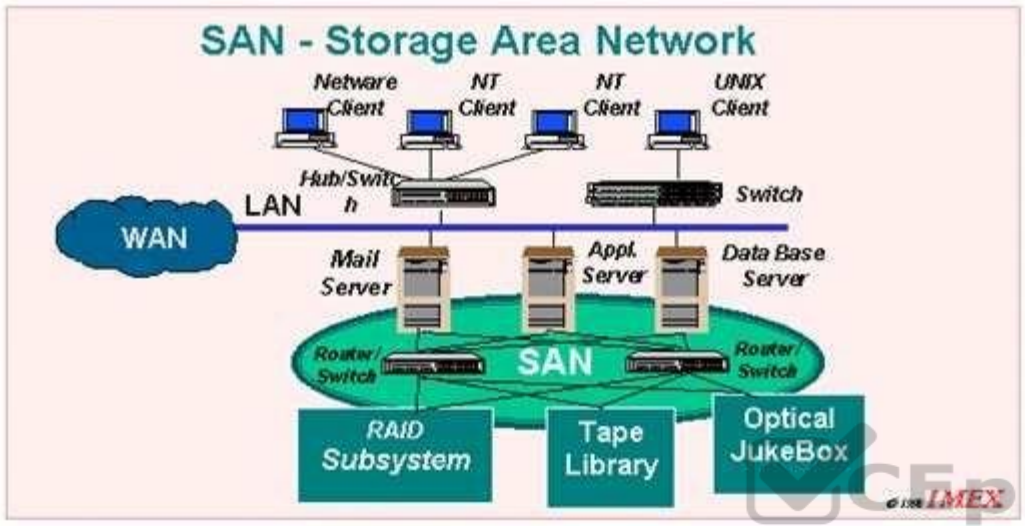


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

The following were incorrect answers:
PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).
WAN - A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.
SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Reference:

CISA review manual 2014 Page number 258

QUESTION 458

Which of the following type of a computer network is a WAN that are limited to a city?

A. LAN
B. MAN
C. SAN
D. PAN

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

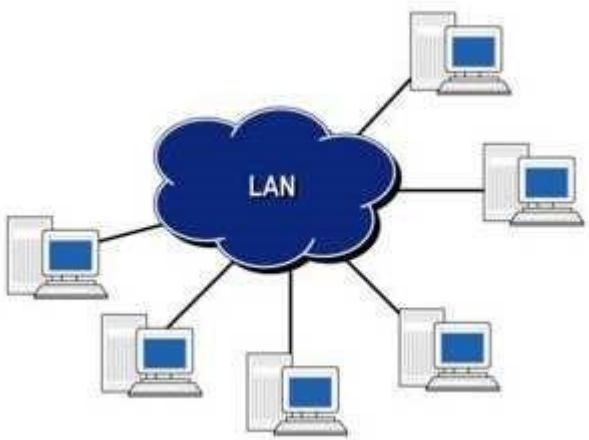
Explanation/Reference:
Explanation:

MAN - A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN.

For your exam you should know below information about computer networks:

Local Area Network (LAN)
A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

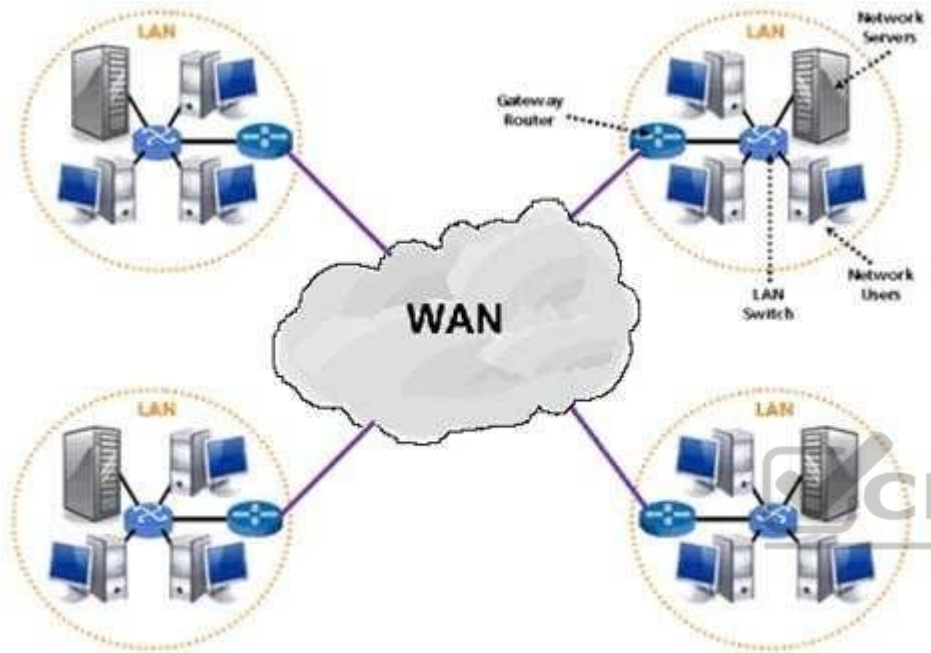
Local Area Network



Wide Area Network

A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

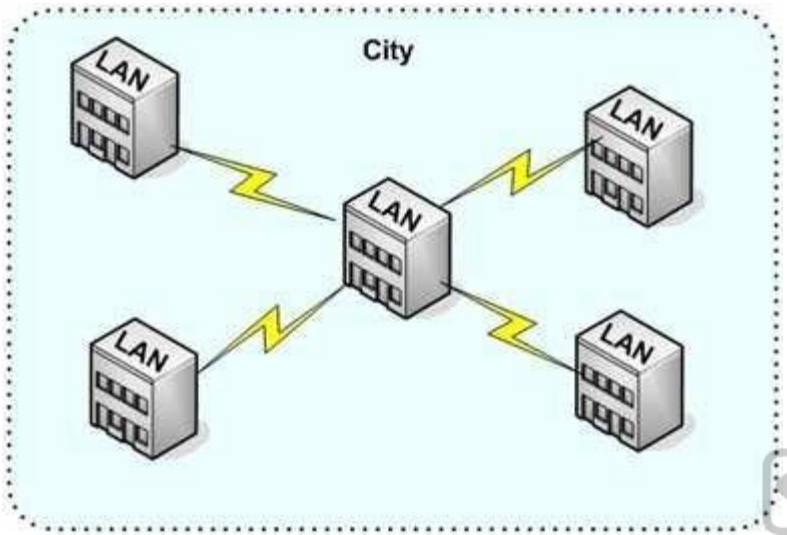
Wide Area Network



Metropolitan Area Network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

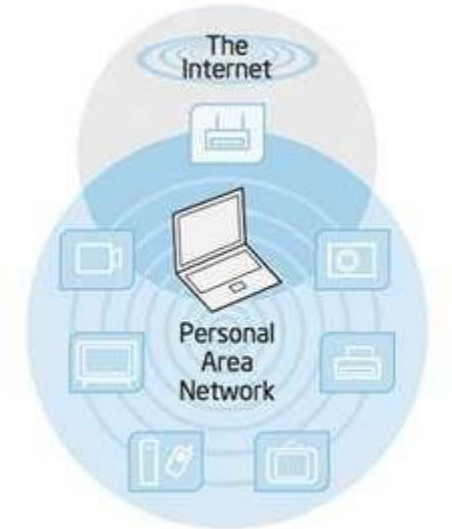


Metropolitan Area Network (MAN)

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Storage Area Network
A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

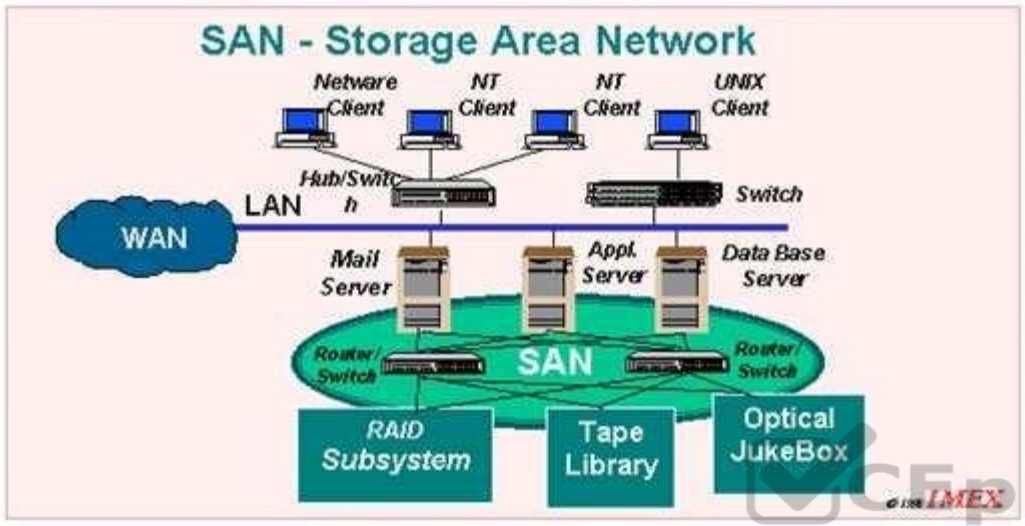


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

The following were incorrect answers:

PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Reference:

CISA review manual 2014 Page number 258

QUESTION 459
Which of the following type of a computer network are variation of LAN and are dedicated to connecting storage devices to servers and other computing devices?
A. LAN
B. MAN
C. SAN
D. PAN

Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

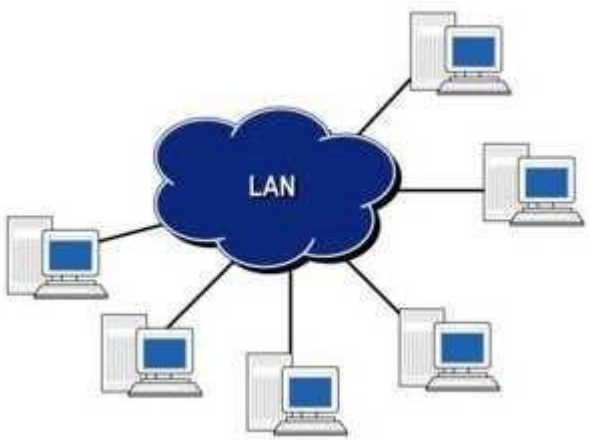
Explanation/Reference:
Explanation:

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

For your exam you should know below information about computer networks:

Local Area Network (LAN)
A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

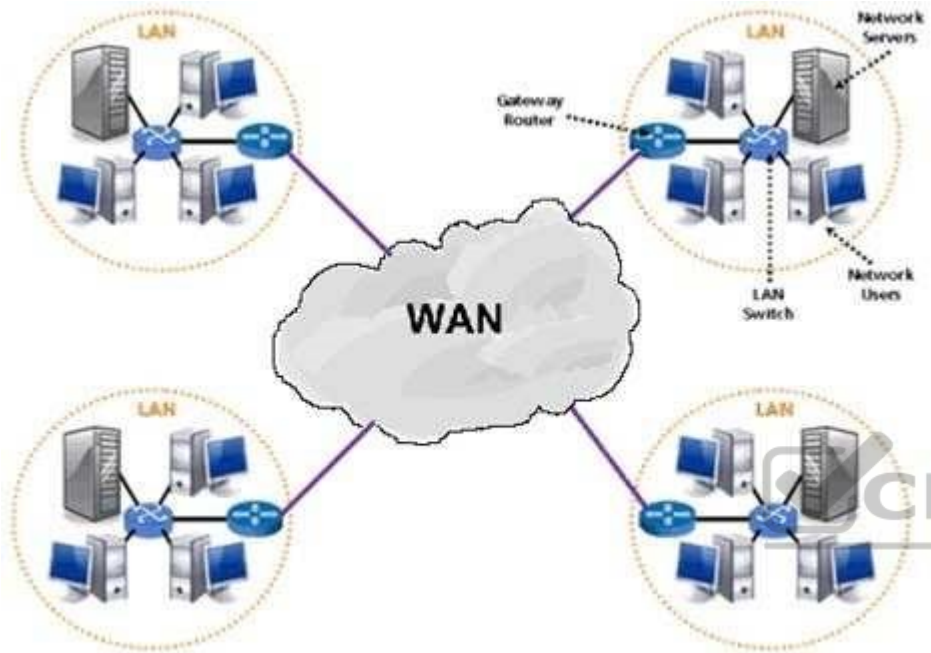
Local Area Network



Wide Area Network

A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

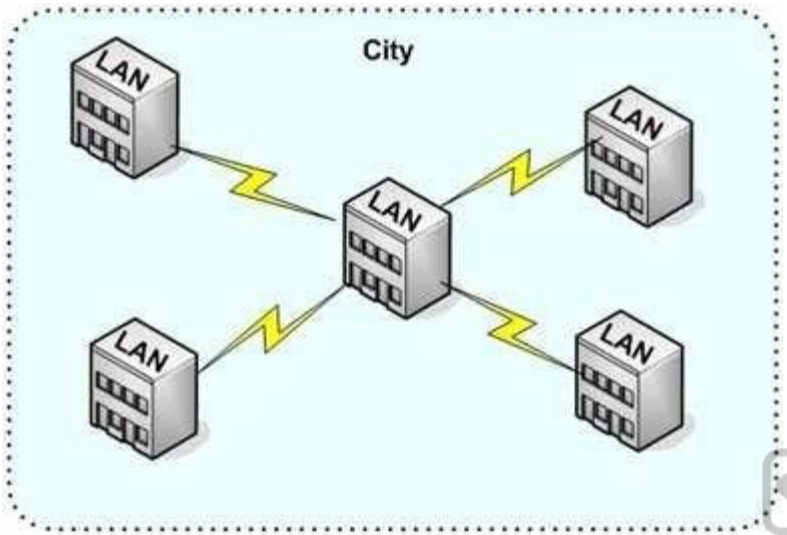
Wide Area Network



Metropolitan Area Network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

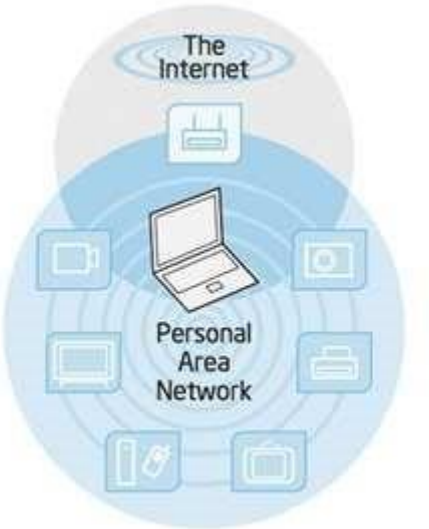


Metropolitan Area Network (MAN)

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Storage Area Network
A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

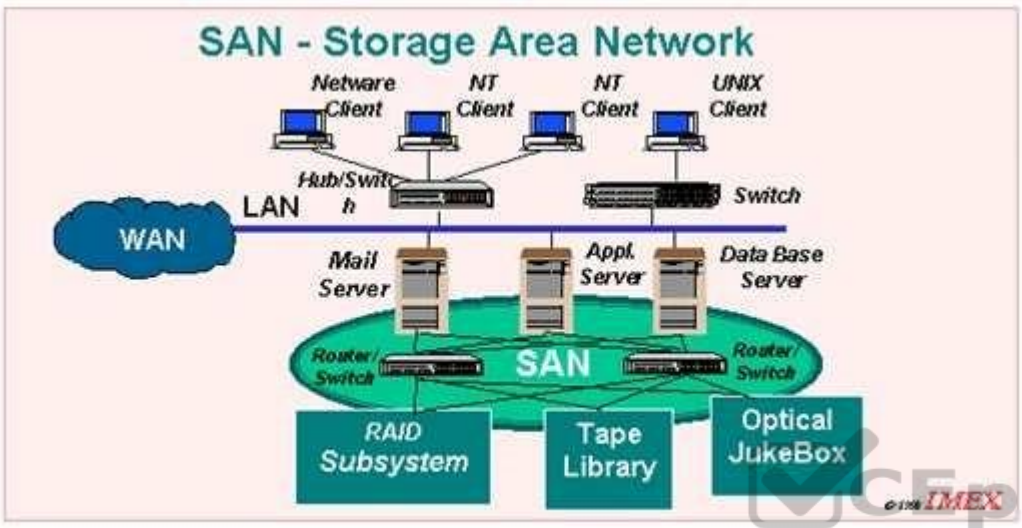


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

The following were incorrect answers:
PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

MAN - A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Reference:

CISA review manual 2014 Page number 258

QUESTION 460
Which of the following type of network service maps Domain Names to network IP addresses or network IP addresses to Domain Names?
A. DHCP
B. DNS
C. Directory Service
D. Network Management

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.
Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine. Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:
Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.
Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.
Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network
Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Reference:

CISA review manual 2014 Page number 258

QUESTION 461
Which of the following type of network service stores information about the various resources in a central database on a network and help network devices locate services?

A. DHCP

B. DNS
C. Directory Service
D. Network Management

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference: Explanation:

A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.
Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.
Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:
Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.
Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.
Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network
Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Domain Name System(DNS) - Translates the names of network nodes into network IP address.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.
Reference:
CISA review manual 2014 Page number 258

QUESTION 462
Which of the following type of network service is used by network computer to obtain an IP addresses and other parameters such as default gateway, subnet mask?

A. DHCP
B. DNS
C. Directory Service
D. Network Management

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.
Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.
Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:
Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.
Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.
Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network
Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:
Directory Service - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Domain Name System(DNS) - Translates the names of network nodes into network IP address.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Reference:

CISA review manual 2014 Page number 258

QUESTION 463
Which of the following layer of an OSI model transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier?

A. Transport Layer
B. Network Layer
C. Data Link Layer
D. Physical Layer

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

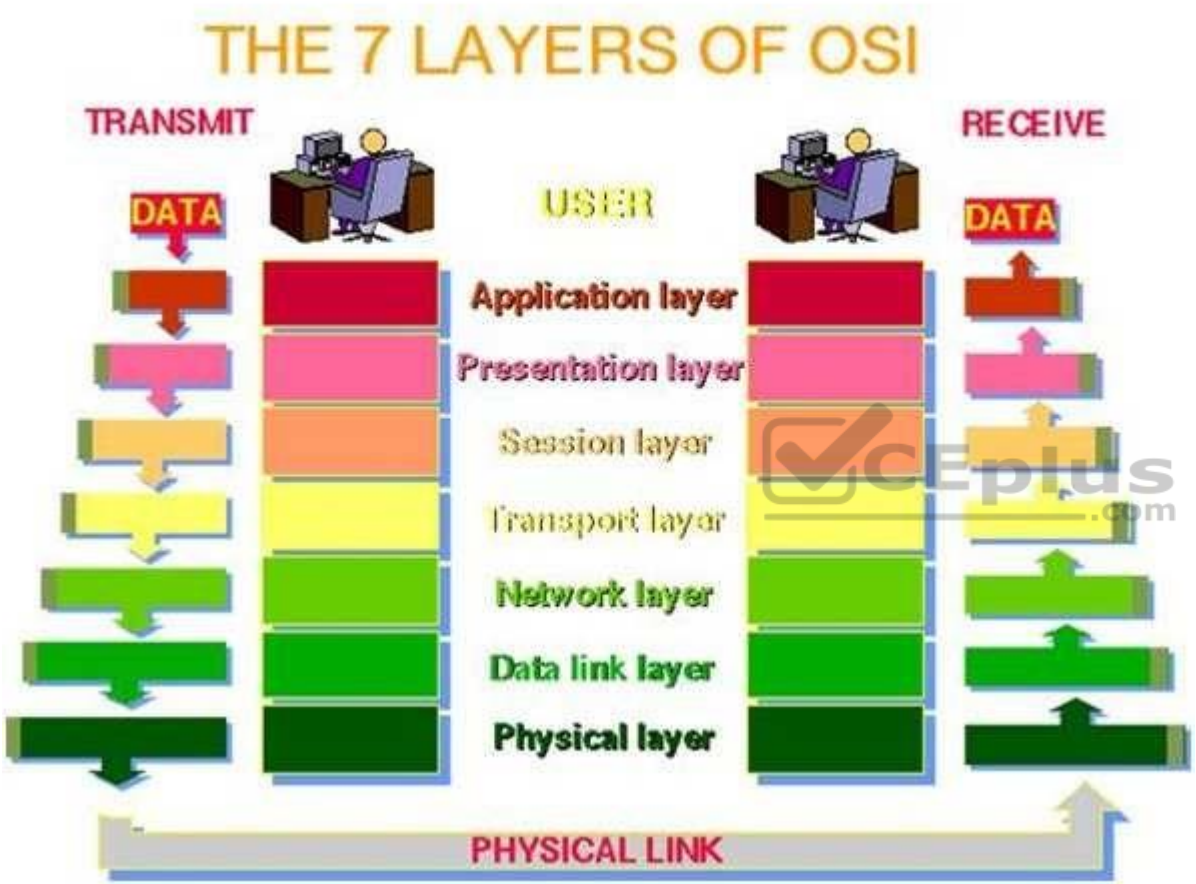
Explanation/Reference:
Explanation:

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal. OSI Model



PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1
How the receiving station knows when a "bit-time" starts
How the receiving station delimits a frame

DATA LINK LAYER
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.
Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available. Frame sequencing: transmits/receives frames sequentially.
Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet
The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER
The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:
Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail) Network
virtual terminals

The following were incorrect answers:
Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.
Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.
Data link layer - The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. Reference:

CISA review manual 2014 Page number 260

QUESTION 464
Which of the following statement INCORRECTLY describes network device such as a Router?

A. Router creates a new header for each packet
B. Router builds a routing table based on MAC address
C. Router does not forward broadcast packet
D. Router assigns a different network address per port

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
The INCORRECTLY keyword is used in the question. You need to find out a statement which is not valid about router. Router builds a routing table based on IP address and not on MAC address.
Difference between Router and Bridge:
Router
Bridge

Creates a new header for each packet
Does not alter header. Only reads the header Builds routing table based on IP address
Build forwarding table based on MAC address Assigns a different network address per port

Use the same network address for all ports

Filters traffic based on IP address
Filter traffic based on MAC address

Does not forward broadcast packet

Forward broadcast packet
Does not forward traffic that contain destination address unknown to the router

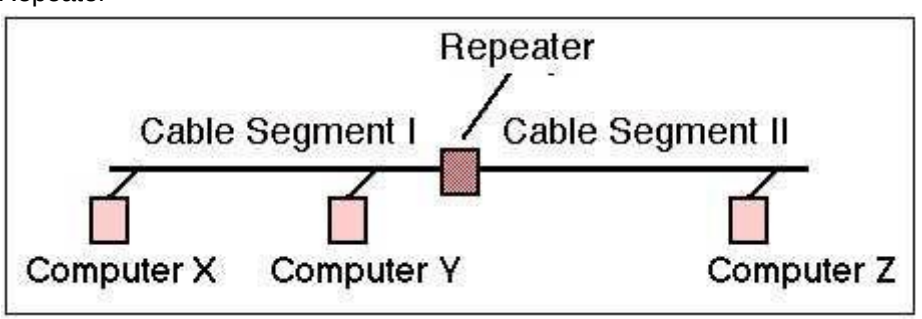
Forward traffic if destination address is unknown to bridge

For your exam you should know below information about network devices:

Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

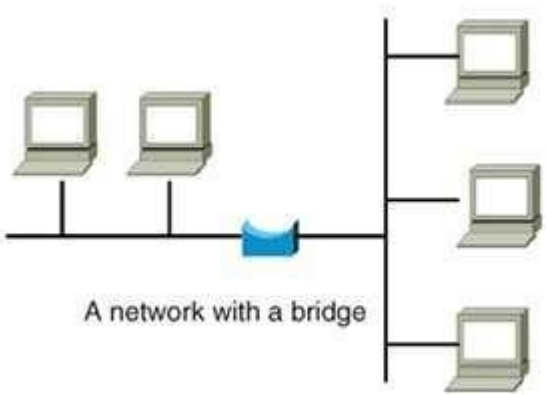
Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.
A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Repeater



Bridges
A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge



Routers

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch

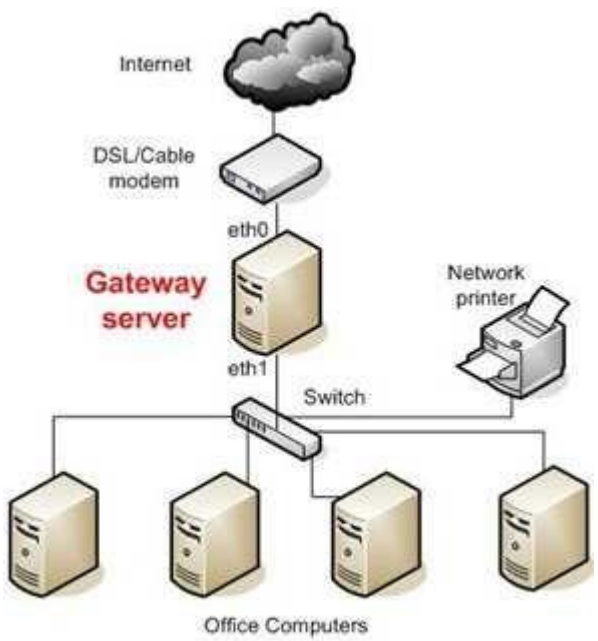
Switches

Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways
Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions.

Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

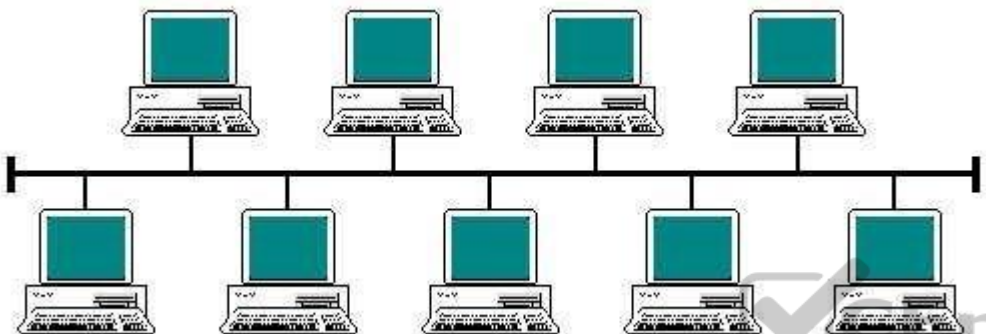
Gateway Server



The following were incorrect answers:
The other options presented correctly describes about Router.

Reference:
CISA review manual 2014 Page number 263

QUESTION 465
Identify the LAN topology from below diagram presented below:



bus topology

A. Bus
B. Star
C. Ring
D. Mesh

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:
For your exam you should know the information below related to LAN topologies:

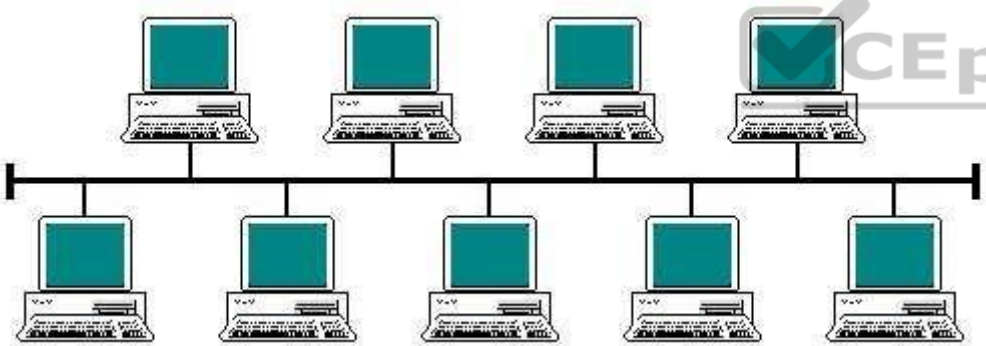
LAN Topologies
Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down. Bus topology



Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

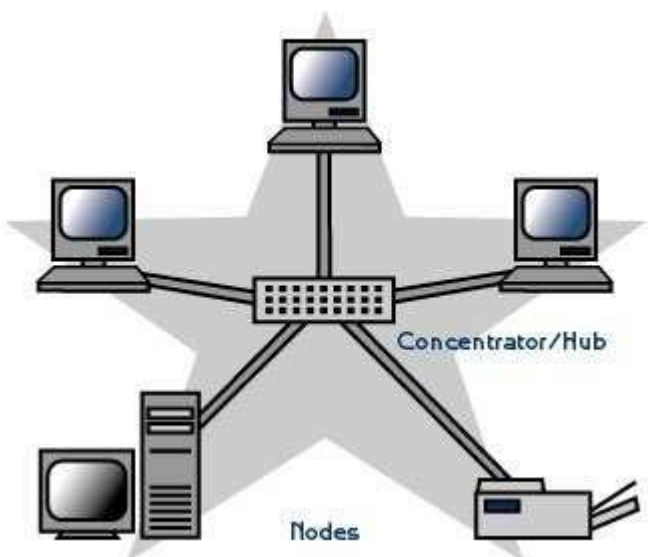
Star

In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure. Star Topology

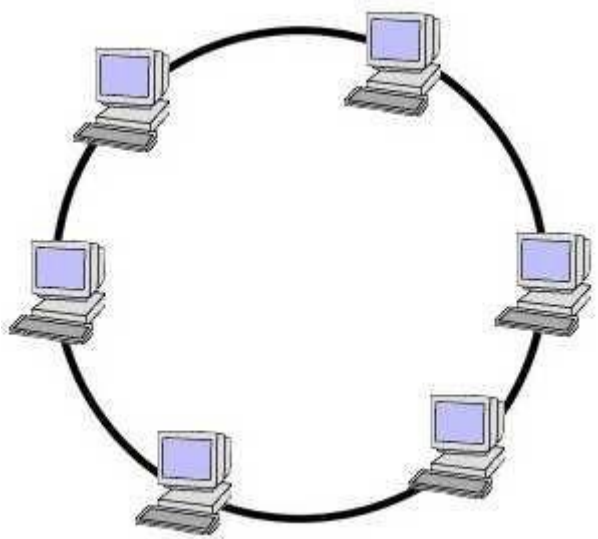


Ring

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

Ring Topology

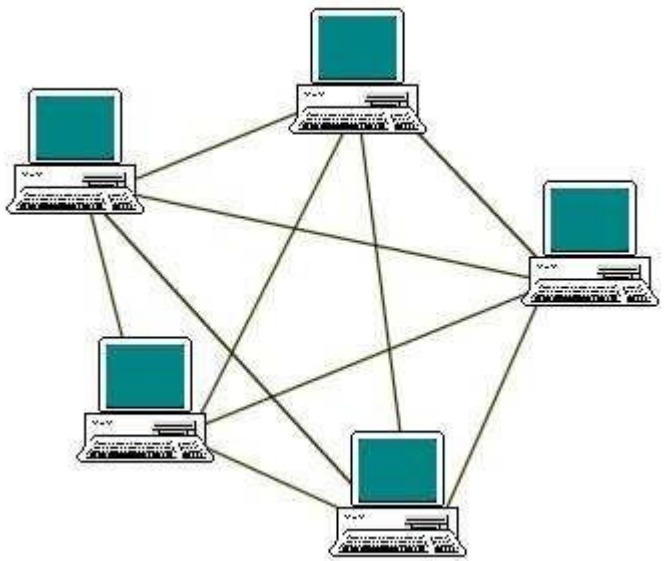


Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.

Mesh Topology



Fully connected mesh topology
A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology
The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

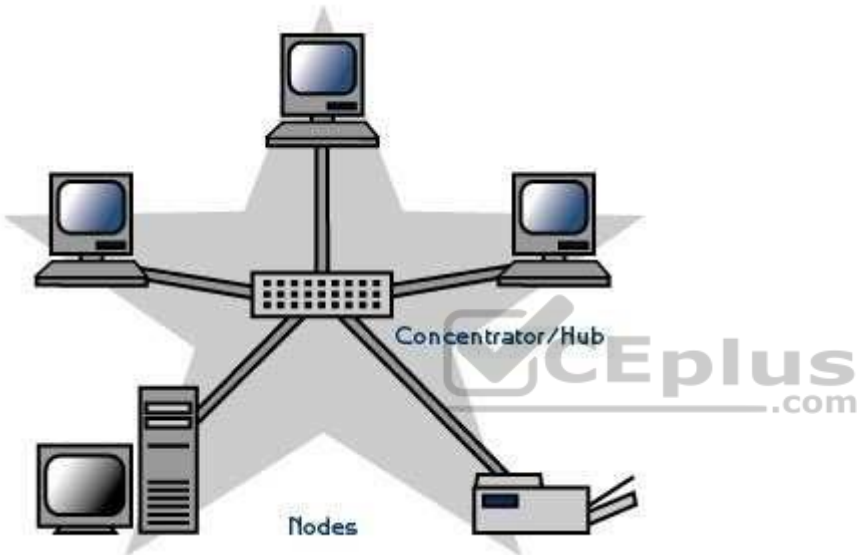
The following answers are incorrect:

The other options presented are not valid.

Reference:

CISA review manual 2014, Page number 262

QUESTION 466
Identify the network topology from below diagram presented below:



Network Topology

A. Bus
B. Star
C. Ring
D. Mesh

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference: Explanation:

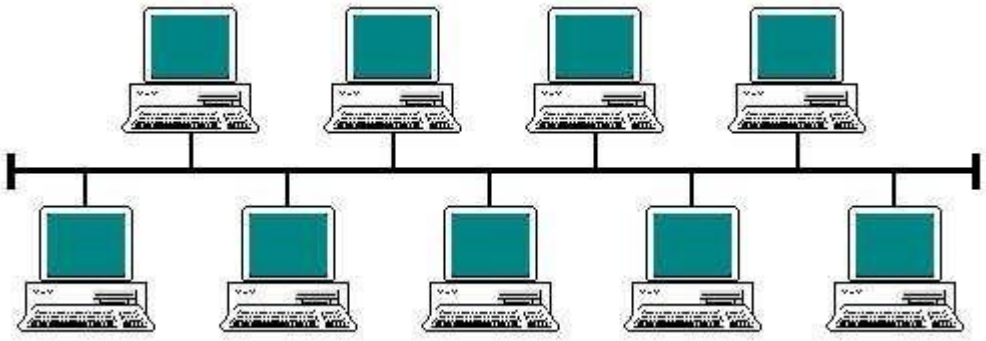
For your exam you should know the information below related to LAN topologies:

LAN Topologies
Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.
Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus
In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down. Bus topology

Graphic from:



Linear bus
The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

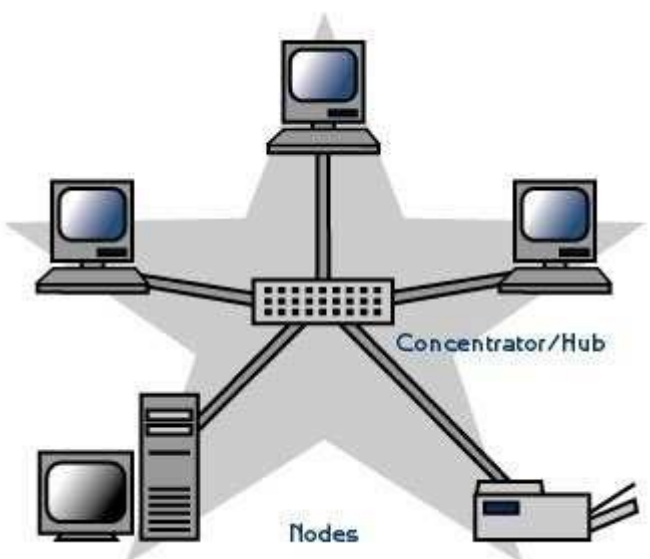
Star

In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure. Star Topology

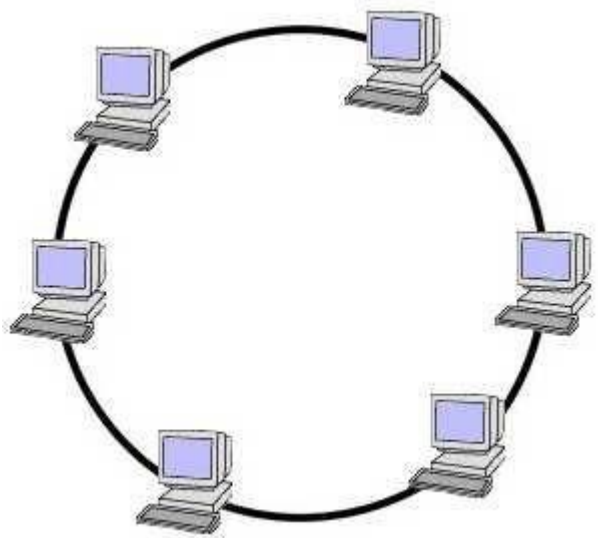


Ring

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

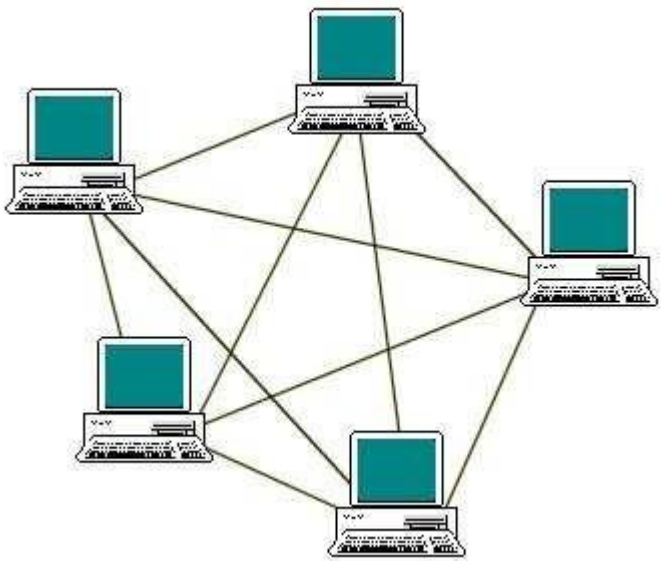
Ring Topology



Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.
Mesh Topology



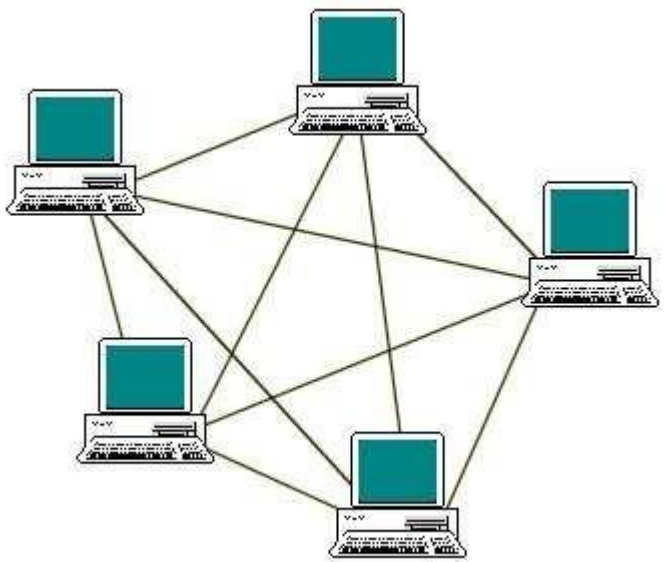
Fully connected mesh topology
A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology
The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:
The other options presented are not valid.

Reference:
CISA review manual 2014, Page number 262

QUESTION 467
Identify the network topology from below diagram presented below:



Network Topology

A. Bus
B. Star
C. Ring
D. Mesh

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:

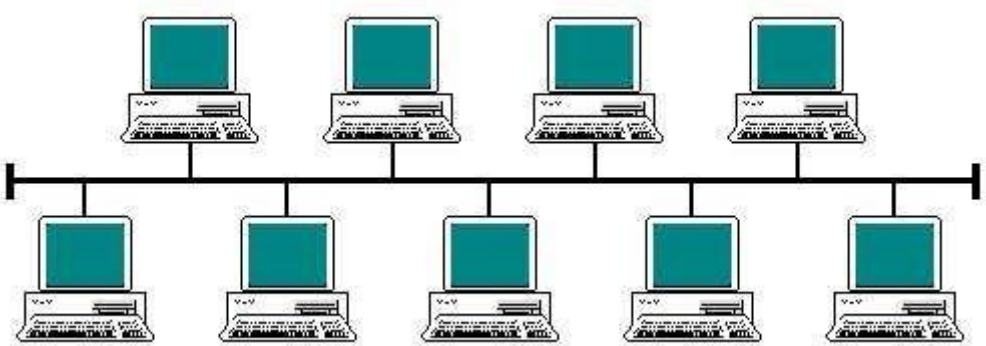
For your exam you should know the information below related to LAN topologies:

LAN Topologies
Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus
In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down. Bus topology



Linear bus
The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

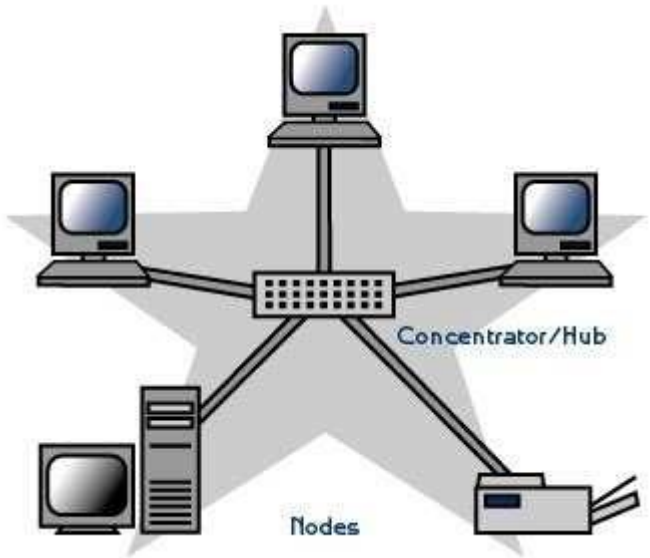
The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Star

In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.
All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure. Star Topology

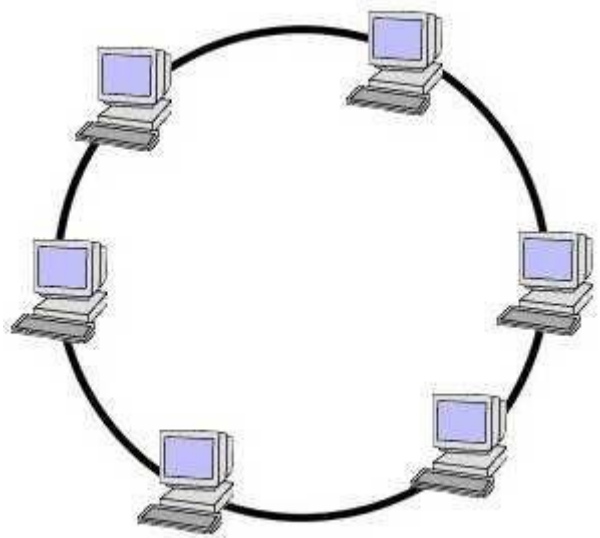


Ring

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

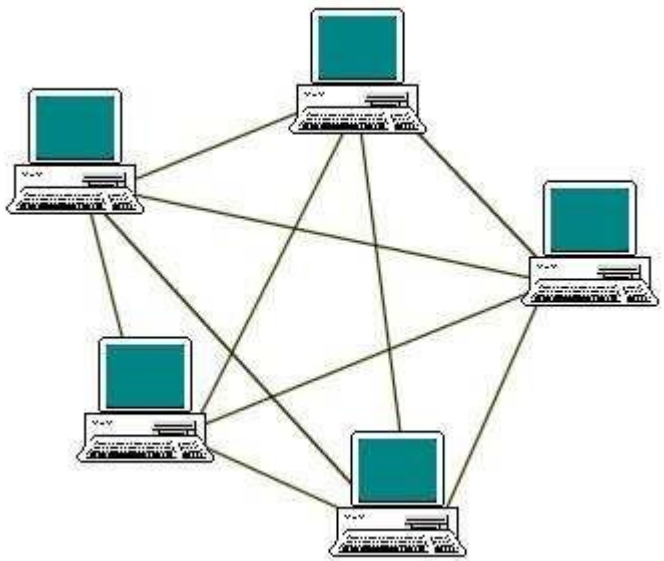
Ring Topology



Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.
Mesh Topology



Fully connected mesh topology
A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology
The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:
The other options presented are not valid.

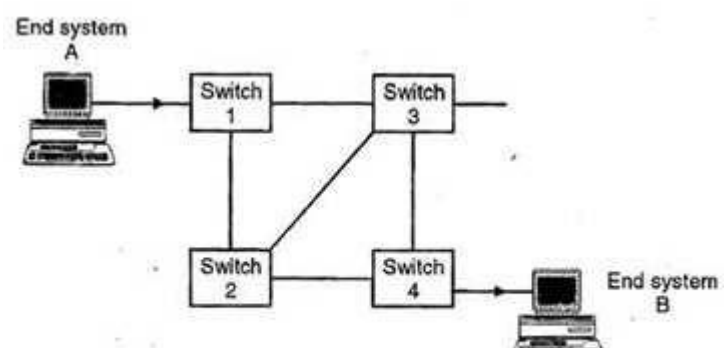
Reference:
CISA review manual 2014, Page number 262

QUESTION 468
In which of the following WAN message transmission technique does two network nodes establish a dedicated communications channel through the network before the nodes may communicate?

A. Message Switching
B. Packet switching
C. Circuit switchingD. Virtual Circuits

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

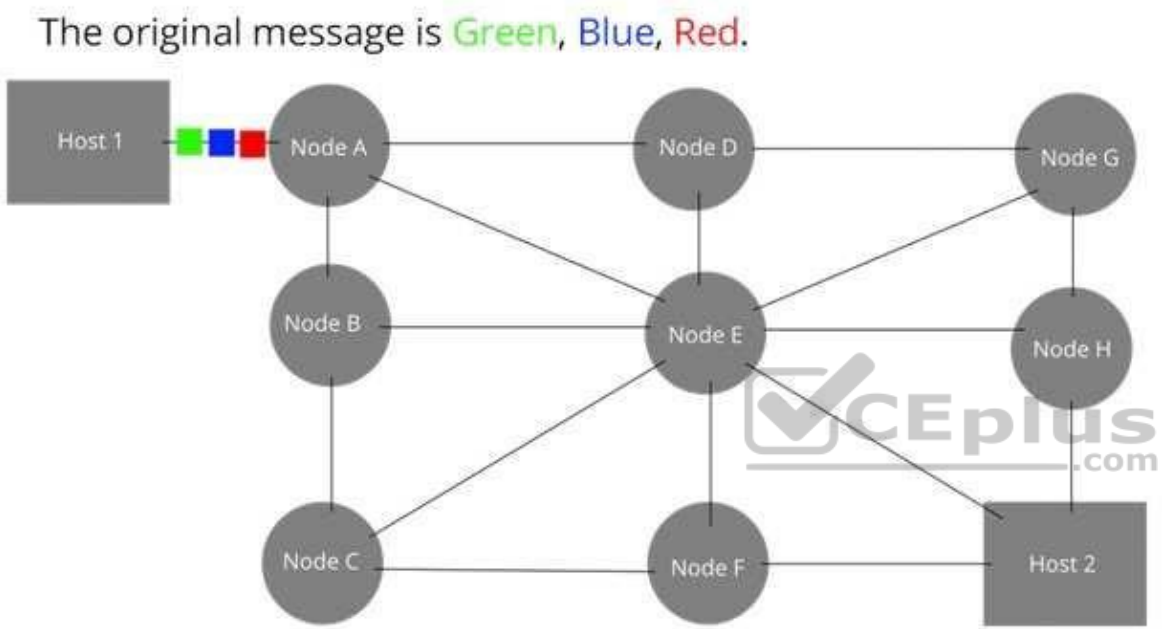
Explanation/Reference:
Explanation:
For your exam you should know below information about WAN message transmission technique: Message Switching
Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.
Message Switching



Message switched data network

Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Packet Switching



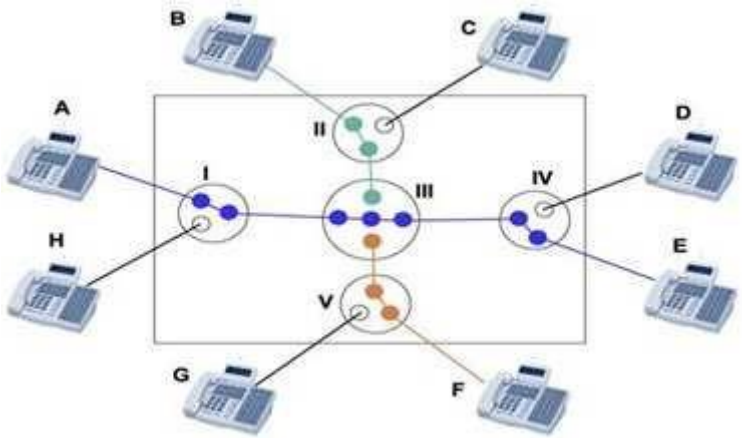
Circuit Switching
Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching



See a table below comparing Circuit Switched versus Packet Switched networks:
Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Virtual circuit
In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.
Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes, varying bit rate generated by the application, varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:
The other options presented are not valid choices.

Reference:
CISA review manual 2014 Page number 265

QUESTION 469
Which of the following statement INCORRECTLY describes Asynchronous Transfer Mode (ATM) technique?

A. ATM uses cell switching method
B. ATM is high speed network technology used for LAN, MAN and WAN
C. ATM works at session layer of an OSI model
D. Data are segmented into fixed size cell of 53 bytes

Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:
The keyword INCORRECTLY is used within the question. You need to find out a statement which was incorrectly describe Asynchronous Transfer Mode.ATM operates at data link layer of an OSI model

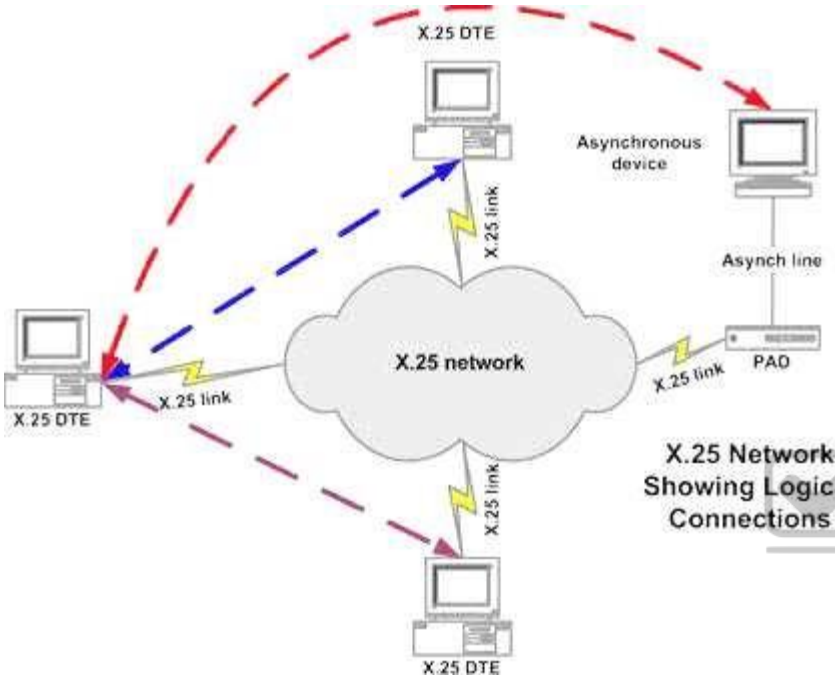
For your exam you should know below information about WAN Technologies:

Point-to-point protocol
PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred. Point-to-point protocol X.25

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.
X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.
Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).
X.25 works at network and data link layer of an OSI model.



X.25 Network Showing Logical Connections

X.25

Frame Relay

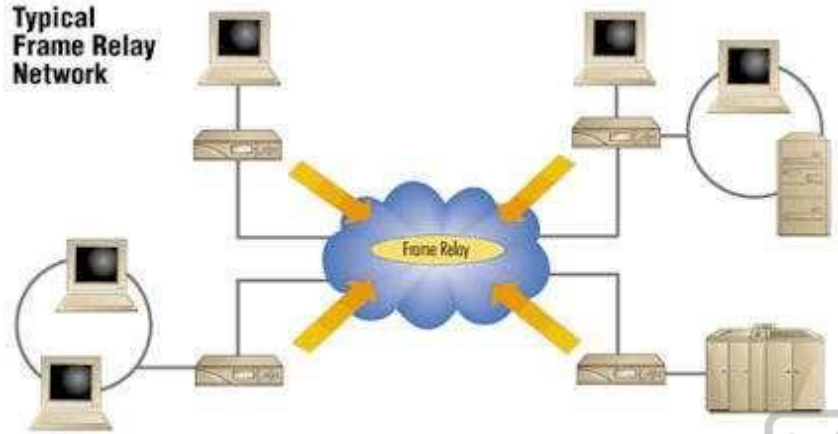
Works on a packet switching
Operates at data link layer of an OSI model
Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

Two main types of equipment's are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

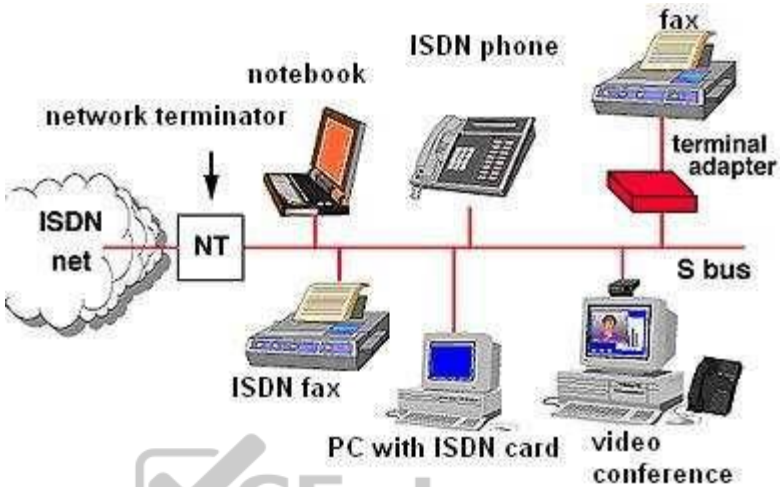
The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.



Frame Relay

Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.
Same copper telephone wire is used.

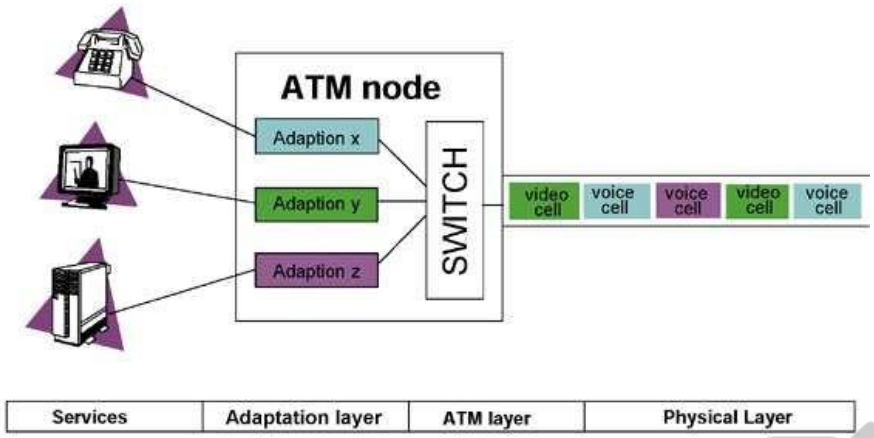


Provide digital point-to-point circuit switching medium.

ISDN

Asynchronous Transfer Mode (ATM)

Uses Cell switching method
High speed network technology used for LAN, MAN and WAN
Like a frame relay it is connection oriented technology which creates and uses fixed channel
Data are segmented into fixed size cell of 53 bytes
Some companies have replaces FDDI back-end with ATM

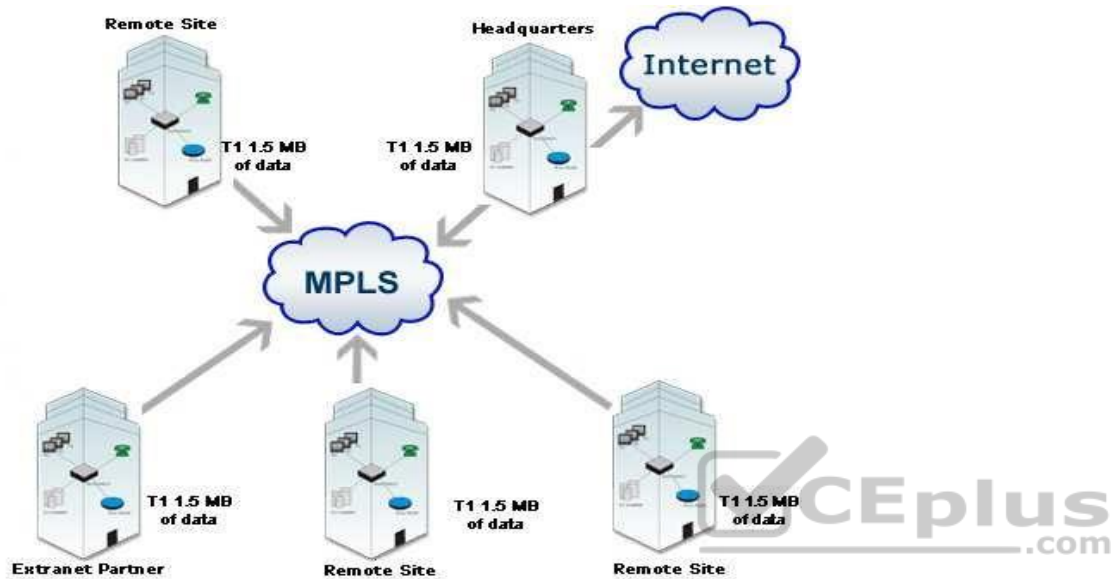


Asynchronous Transfer Mode

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:
The other options presented correctly describes Asynchronous Transfer Mode.

Reference:
CISA review manual 2014 page number 266

QUESTION 470
Which of the following protocol does NOT work at the Application layer of the TCP/IP Models?

A. HTTP
B. FTP
C. NTP
D. TCP

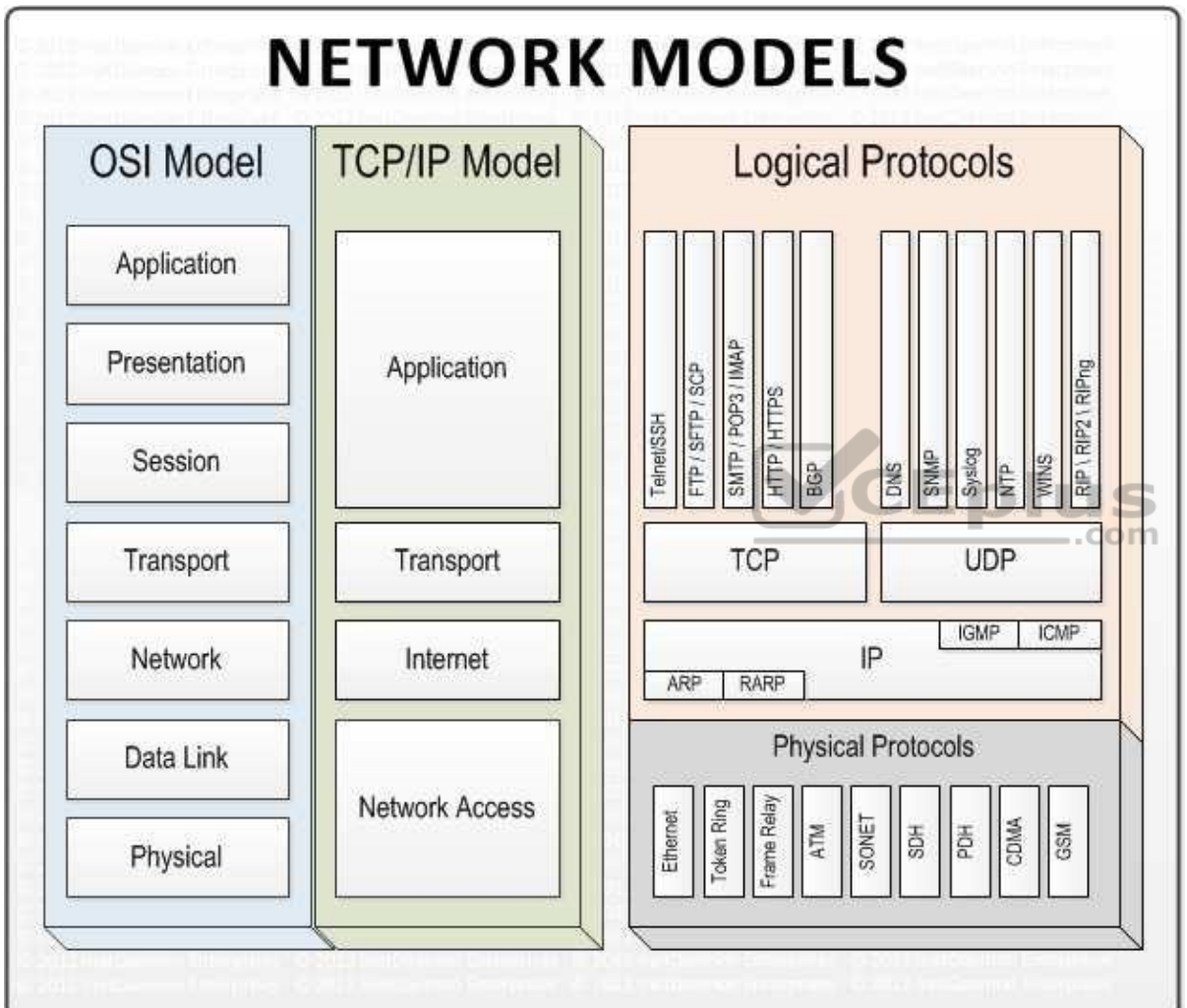
Correct Answer: D

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
The NOT keyword is used in the question. You need to find out a protocol which does not work at application layer. TCP protocol works at transport layer of a TCP/IP models.

For your exam you should know below information about TCP/IP model:

Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

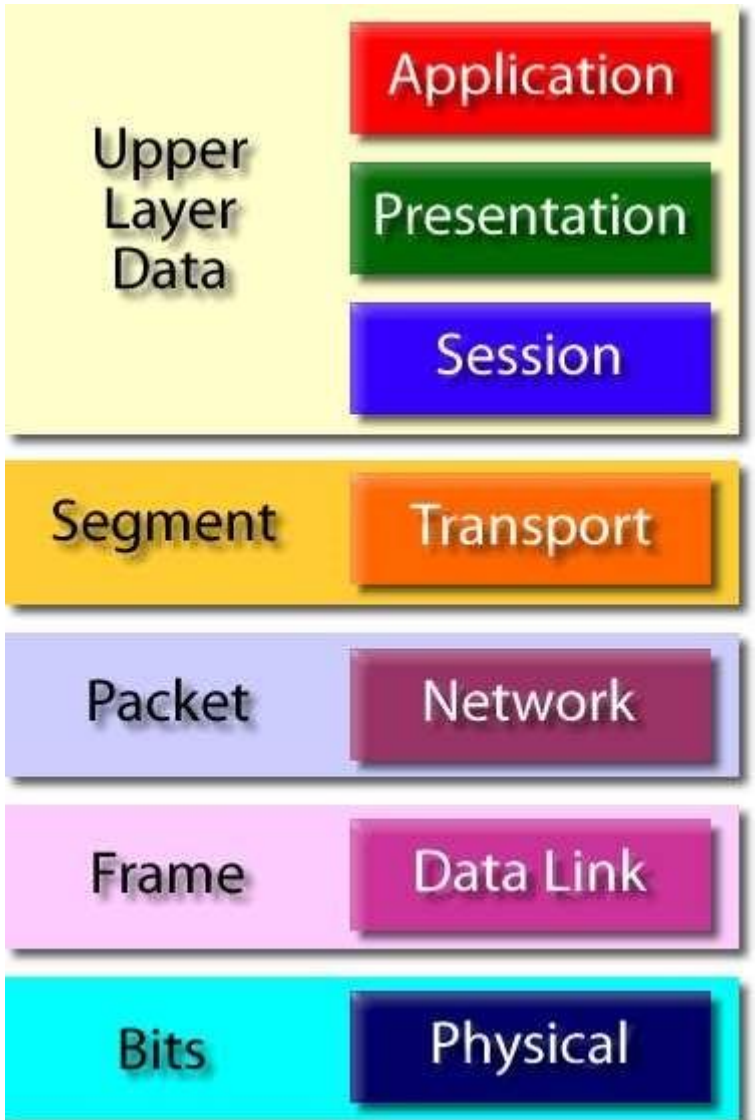
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each

other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:

HTTP, FTP and NTP protocols works at application layer in TCP/IP model.
Reference:

CISA review manual 2014 page number 272

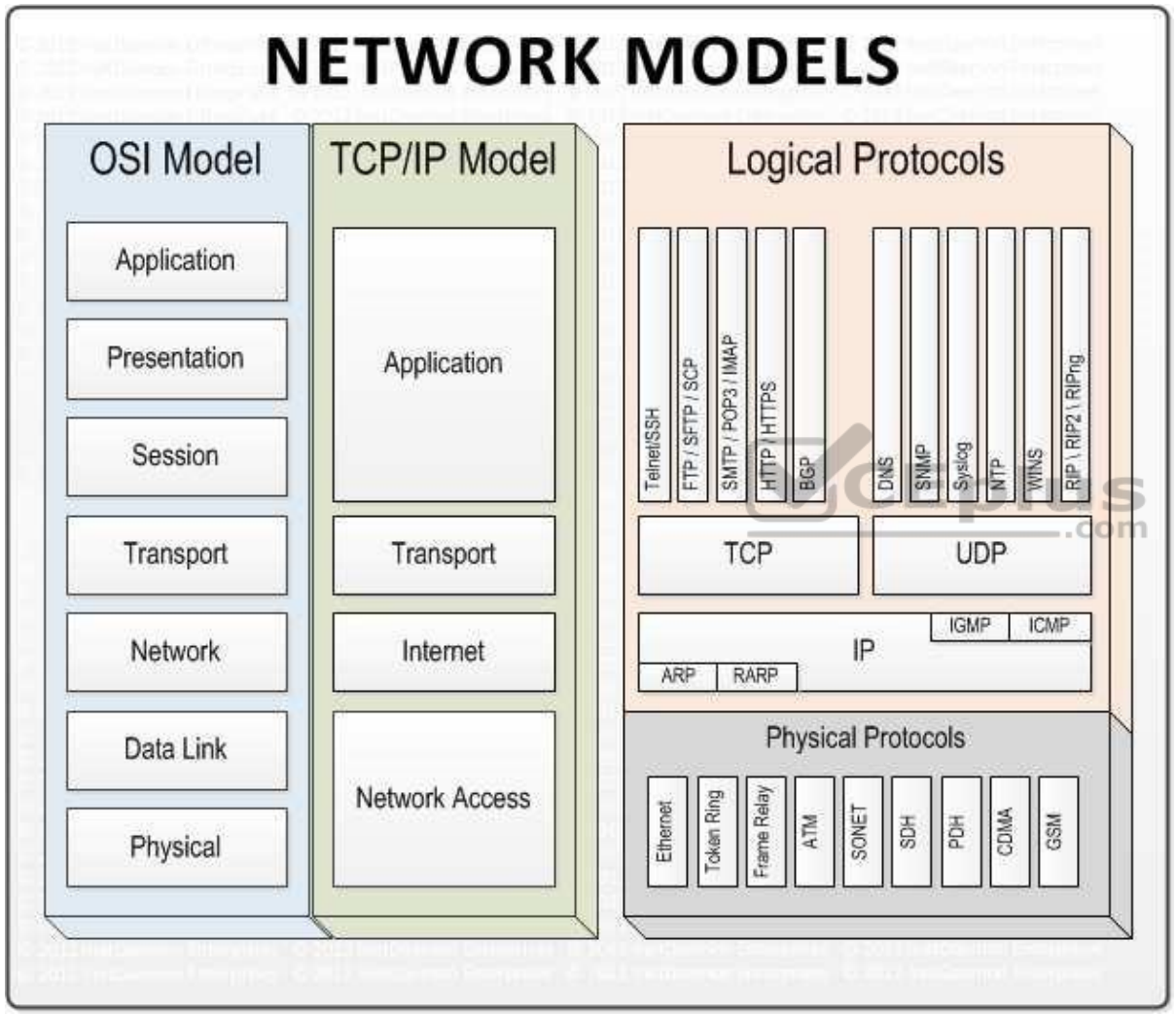
QUESTION 471
Which of the following is the protocol data unit (PDU) of application layer in TCP/IP model?

A. Data
B. Segment
C. Packet
D. Frame

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
Application layer's PDU is data.

For your exam you should know below information about TCP/IP model: Network models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer
Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

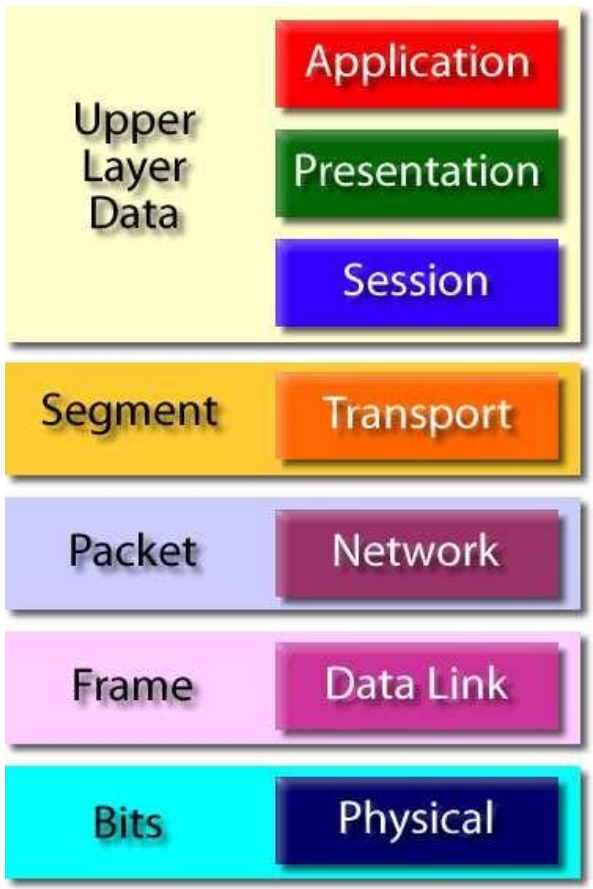
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:

Segment – Transport layer PDU
Packet – Network interface layer PDU
Frame/bit – LAN or WAN interface layer PDU

Reference:
CISA review manual 2014 page number 272

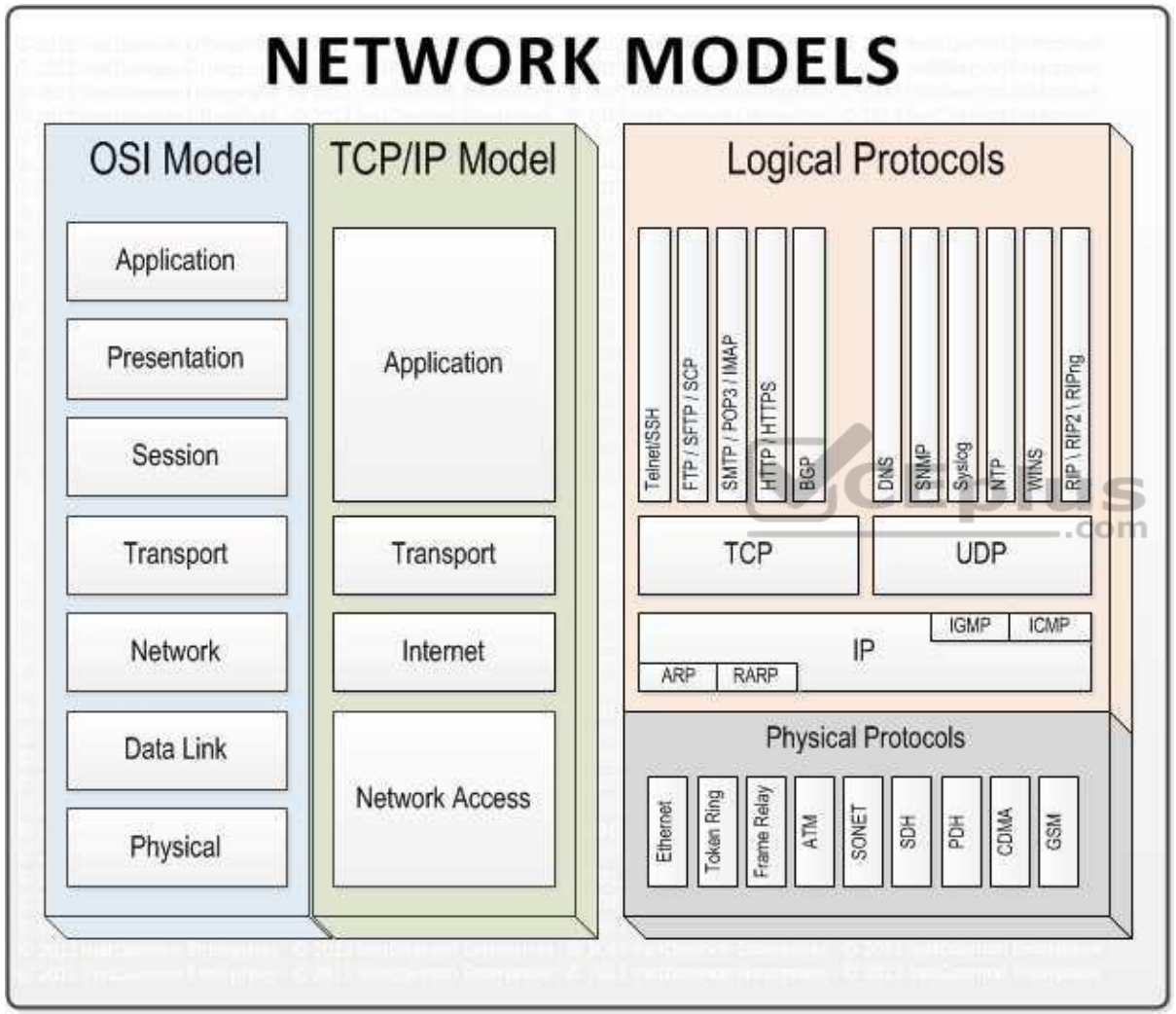
QUESTION 472
Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

A. Data
B. Segment
C. Packet
D. Frame

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
For your exam you should know below information about TCP/IP model:

Network models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer
Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

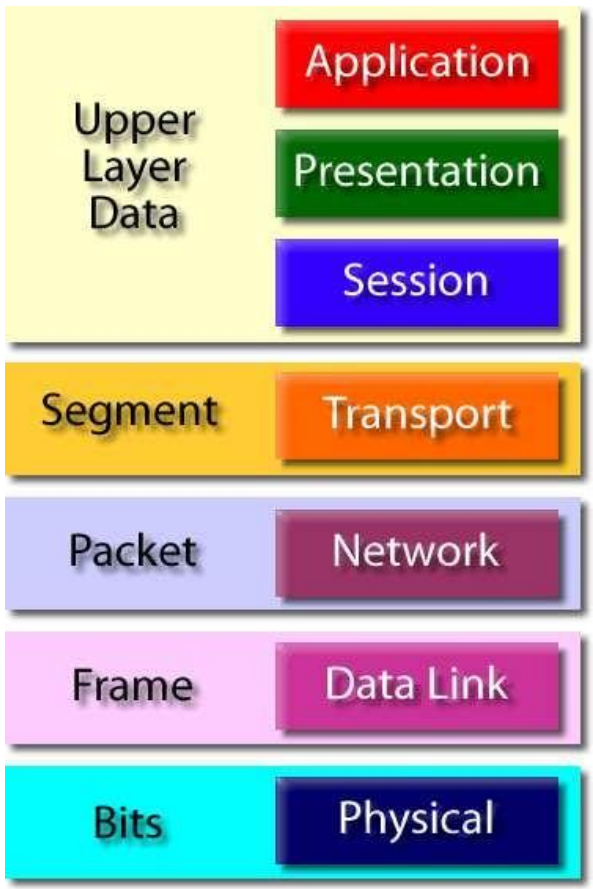
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:

Data – Application layer PDU
Packet – Network interface layer PDU Frame/bit – LAN or WAN interface layer PDU

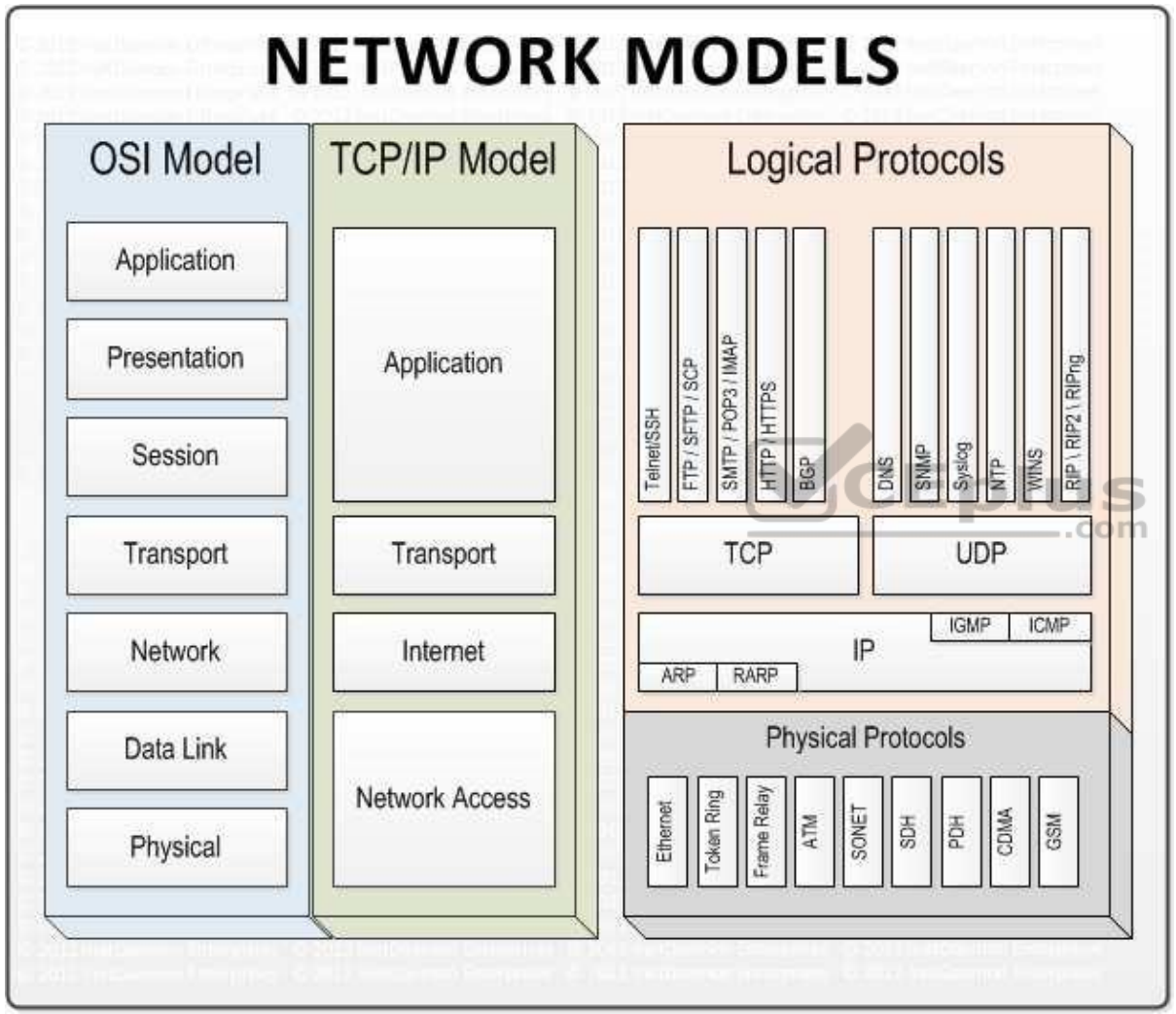
Reference:
CISA review manual 2014 page number 272

QUESTION 473
Which of the following is protocol data unit (PDU) of data at LAN or WAN interface layer in TCP/IP model?

A. Data
B. Segment
C. Packet
D. Frame and bits

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
For your exam you should know below information about TCP/IP model: Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer
Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

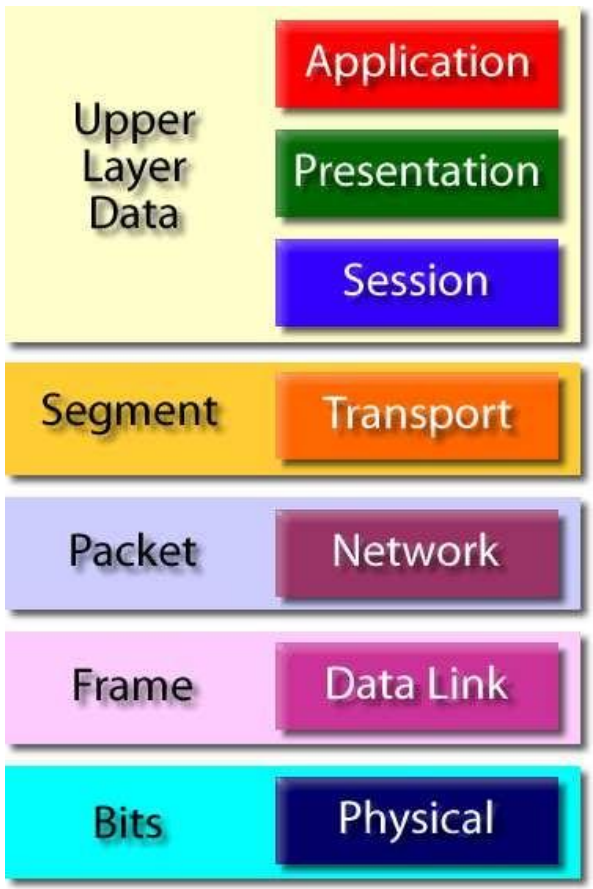
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:

Data – Application layer data PDU
Segment – Transport layer data PDU Packet – Network interface layer data PDU

Reference:
CISA review manual 2014 page number 272

QUESTION 474
Which of the following INCORRECTLY describes the layer functions of the LAN or WAN Layer of the TCP/IP model?

A. Combines packets into bytes and bytes into frame
B. Providers logical addressing which routers use for path determination
C. Provide address to media using MAC address
D. Performs only error detection

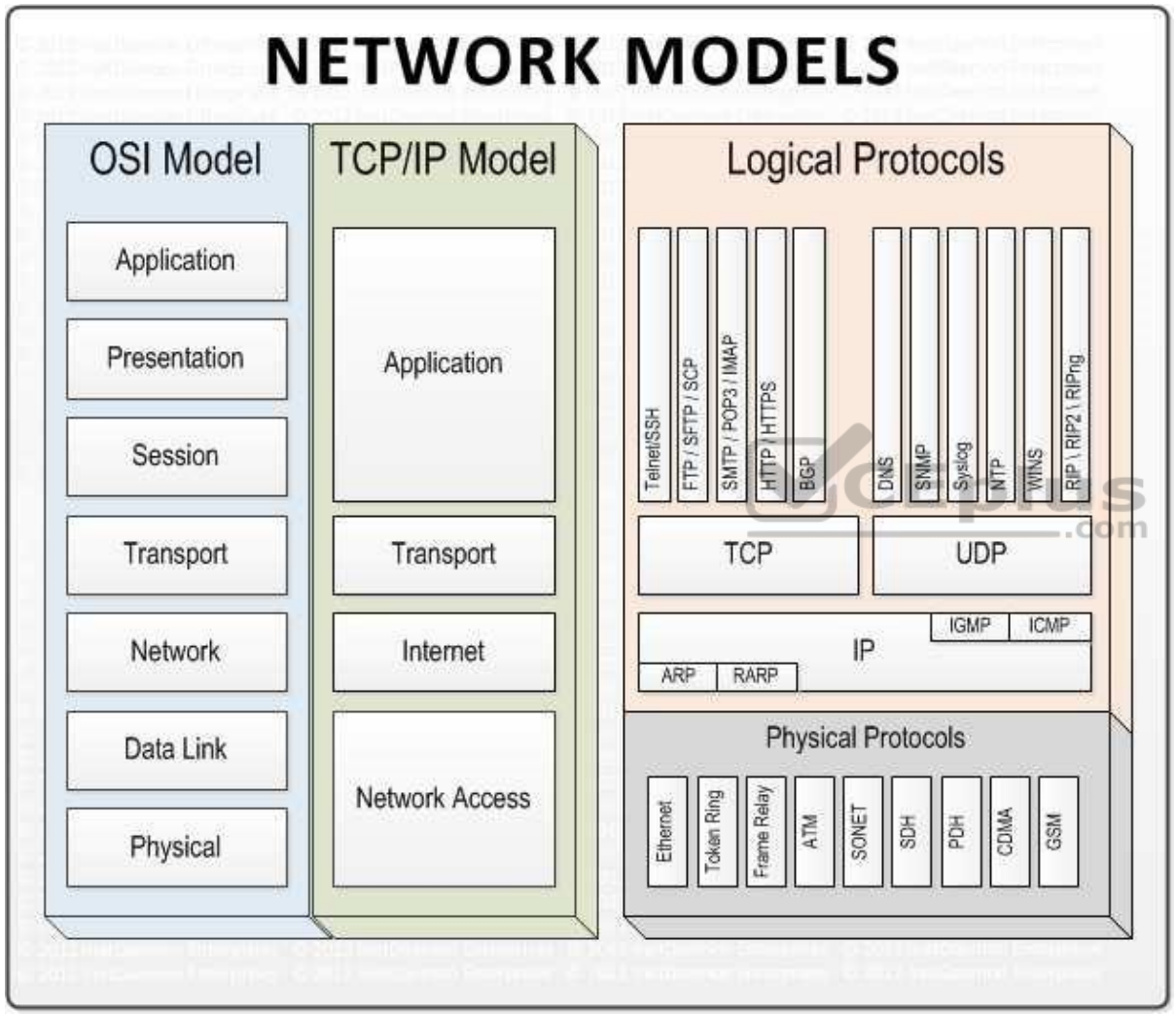
Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference: Explanation:

The word INCORRECTLY is the keyword used in the question. You need to find out the functionality that is not performed by LAN or WAN layer in TCP/IP model.

The Network layer of a TCP/IP model provides logical addressing which routers use for path determination.

For your exam you should know below information about TCP/IP model:
Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer
Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

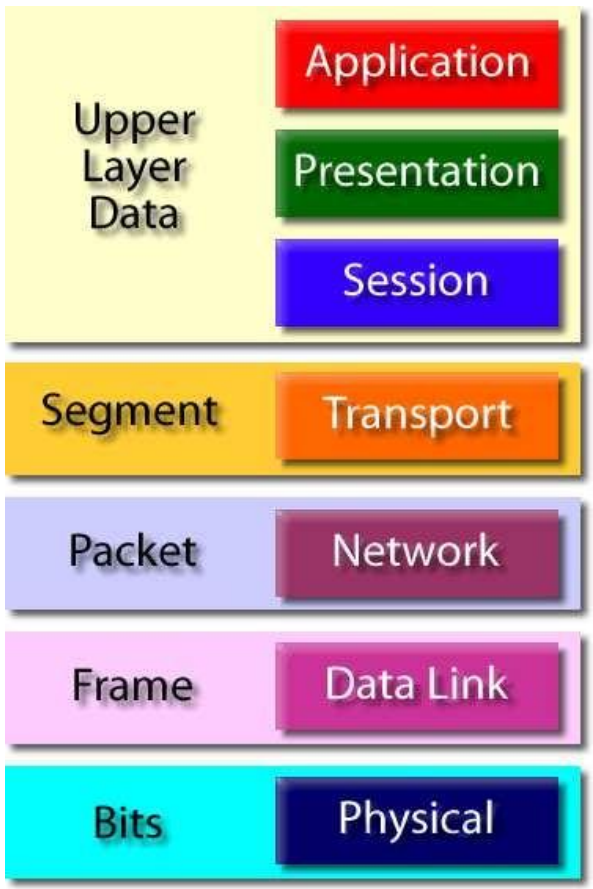
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:
The other options correctly describe functionalities of application layer in TCP/IP model.

Reference:
CISA review manual 2014 page number 272

QUESTION 475
Which of the following functionality is NOT performed by the application layer of a TCP/IP model?

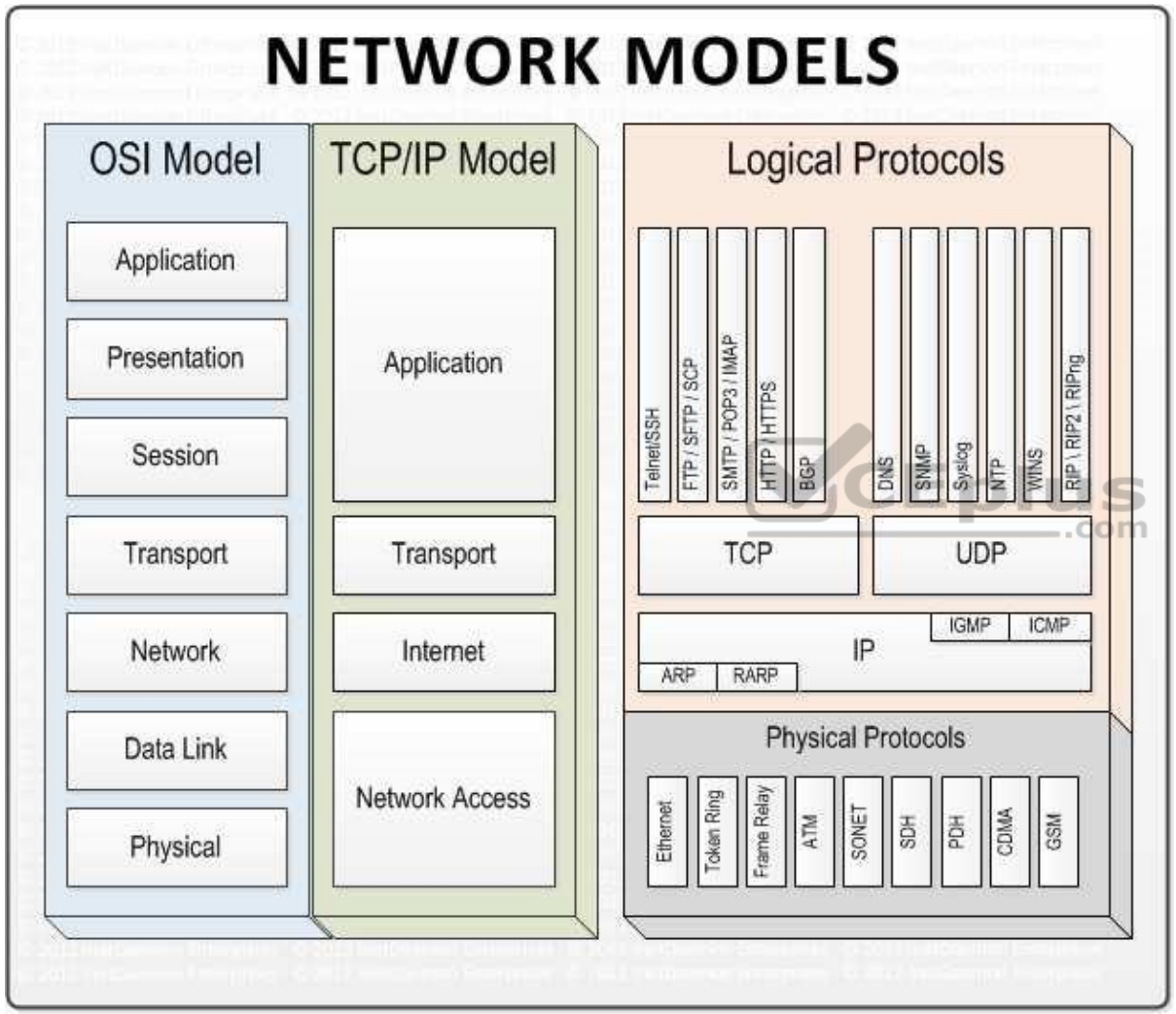
A. Print service, application services
B. Data encryption and compression
C. Dialog management
D. End-to-end connection

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
The word NOT is the keyword used in the question. You need to find out a functionality which is not performed by application layer of a TCP/IP model.

End-to-end connection is the Transport layer functionality in TCP/IP model.

For your exam you should know below information about TCP/IP model:
Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer
Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

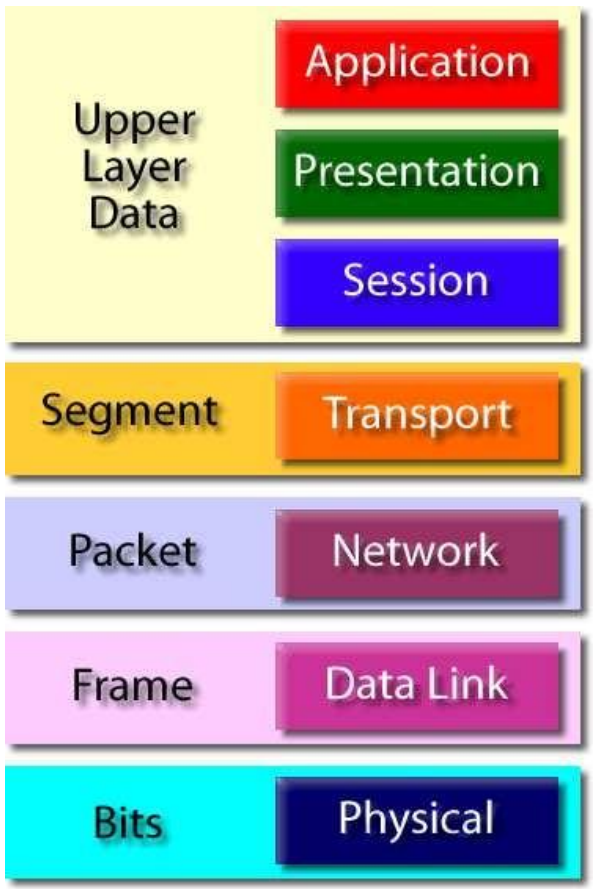
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:
The other functionalities described in the options are performed by application layer in TCP/IP model.

Reference:
CISA review manual 2014 page number 272

QUESTION 476
Which of the following service is a distributed database that translate host name to IP address to IP address to host name?

A. DNS
B. FTP
C. SSH
D. SMTP

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Network access point -Internet service providers access internet using net access point. A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

The following answers are incorrect:
SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/ server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Reference:
CISA review manual 2014 page number 273 and 274

QUESTION 477
Which of the following term related to network performance refers to the maximum rate that information can be transferred over a network?

A. Bandwidth
B. Throughput
C. Latency
D. Jitter

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:
Explanation:
In computer networks, bandwidth is often used as a synonym for data transfer rate - it is the amount of data that can be carried from one point to another in a given time period (usually a second).

This kind of bandwidth is usually expressed in bits (of data) per second (bps). Occasionally, it's expressed as bytes per second (Bps). A modem that works at 57,600 bps has twice the bandwidth of a modem that works at 28,800 bps. In general, a link with a high bandwidth is one that may be able to carry enough information to sustain the succession of images in a video presentation.

It should be remembered that a real communications path usually consists of a succession of links, each with its own bandwidth. If one of these is much slower than the rest, it is said to be a bandwidth bottleneck.

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Reference:
CISA review manual 2014 page number 275

QUESTION 478
Which of the following term related to network performance refers to the delay that packet may experience on their way to reach the destination from the source?

A. Bandwidth
B. Throughput

C. Latency
D. Jitter

Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:
Latency the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses.

In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. In some usages (for example, AT&T), latency is measured by sending a packet that is returned to the sender and the round-trip time is considered the latency.

The latency assumption seems to be that data should be transmitted instantly between one point and another (that is, with no delay at all). The contributors to network latency include:

Propagation: This is simply the time it takes for a packet to travel between one place and another at the speed of light.
Transmission: The medium itself (whether optical fiber, wireless, or some other) introduces some delay. The size of the packet introduces delay in a round trip since a larger packet will take longer to receive and return than a short one.
Router and other processing: Each gateway node takes time to examine and possibly change the header in a packet (for example, changing the hop count in the time-to-live field).
Other computer and storage delays: Within networks at each end of the journey, a packet may be subject to storage and hard disk access delays at intermediate devices such as switches and bridges. (In backbone statistics, however, this kind of latency is probably not considered.)

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred Jitter -
Jitter is the variation in the time of arrival at the receiver of the information

Reference:
CISA review manual 2014 page number 275

QUESTION 479
Which of the following term related to network performance refers to the variation in the time of arrival of packets on the receiver of the information?

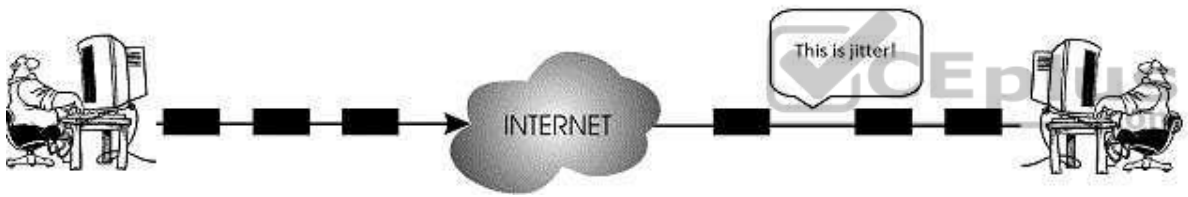
A. Bandwidth
B. Throughput
C. Latency
D. Jitter

Correct Answer: D

Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:
Simply said, the time difference in packet inter-arrival time to their destination can be called jitter. Jitter is specific issue that normally exists in packet switched networks and this phenomenon is usually not causing any communication problems. TCP/IP is responsible for dealing with the jitter impact on communication.

On the other hand, in VoIP network environment, or better say in any bigger environment today where we use IP phones on our network this can be a bigger problem. When someone is sending VoIP communication at a normal interval (let's say one frame every 10 ms) those packets can stuck somewhere in between inside the packet network and not arrive at expected regular peace to the destined station. That's the whole jitter phenomenon all about so we can say that the anomaly in tempo with which packet is expected and when it is in reality received is jitter.
jitter



In this image above, you can notice that the time it takes for packets to be send is not the same as the period in which the will arrive on the receiver side. One of the packets encounters some delay on his way and it is received little later than it was asumed. Here are the jitter buffers entering the story. They will mitigate packet delay if required. VoIP packets in networks have very changeable packet inter-arrival intervals because they are usually smaller than normal data packets and are therefore more numerous with bigger chance to get some delay along the way.

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Reference:

CISA review manual 2014 page number 275 and
http://howdoesinternetwork.com/2013/jitter

QUESTION 480
Which of the following term related to network performance refers to the number of corrupted bits expressed as a percentage or fraction of the total sent?

A. Bandwidth
B. Throughput
C. Latency

D. Error Rate

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sent

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Reference:
CISA review manual 2014 page number 275

QUESTION 481
Which of the following term in business continuity determines the maximum acceptable amount of data loss measured in time?

A. RPO
B. RTO
C. WRT
D. MTD

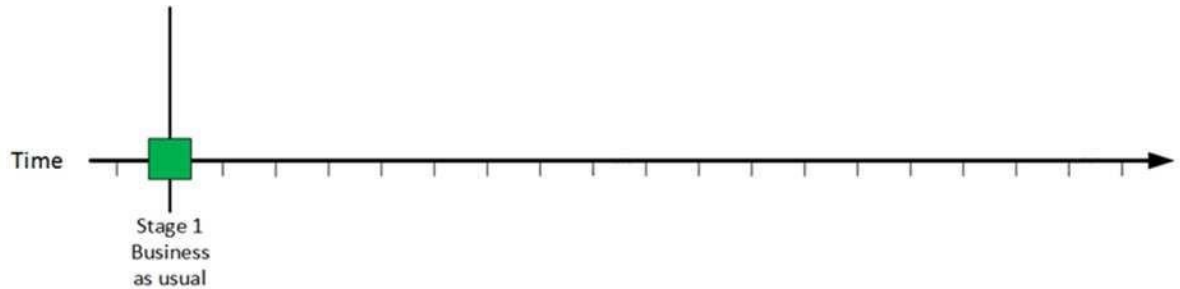
Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:

A recovery point objective, or “RPO”, is defined by business continuity planning. It is the maximum tolerable period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit to work to. For instance, if the RPO is set to four hours, then in practice, off-site mirrored backups must be continuously maintained – a daily off-site backup on tape will not suffice. Care must be taken to avoid two common mistakes around the use and definition of RPO. Firstly, BC staff use business impact analysis to determine RPO for each service – RPO is not determined by the existent backup regime. Secondly, when any level of preparation of off-site data is required, rather than at the time the backups are offsite, the period during which data is lost very often starts near the time of the beginning of the work to prepare backups which are eventually offsite.

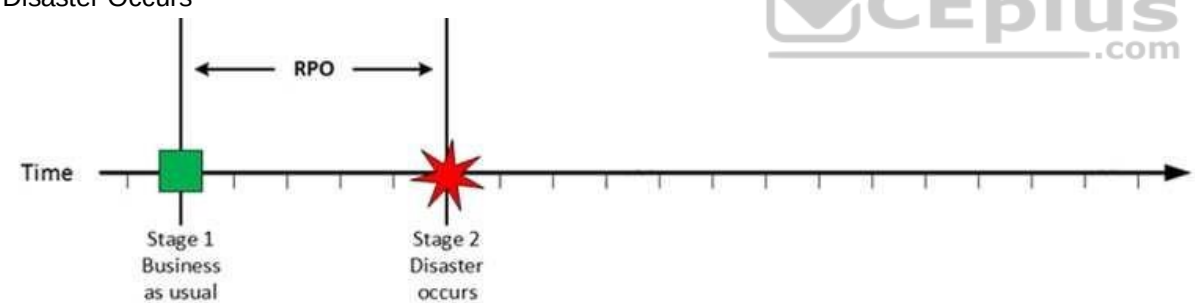
For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual
Business as usual



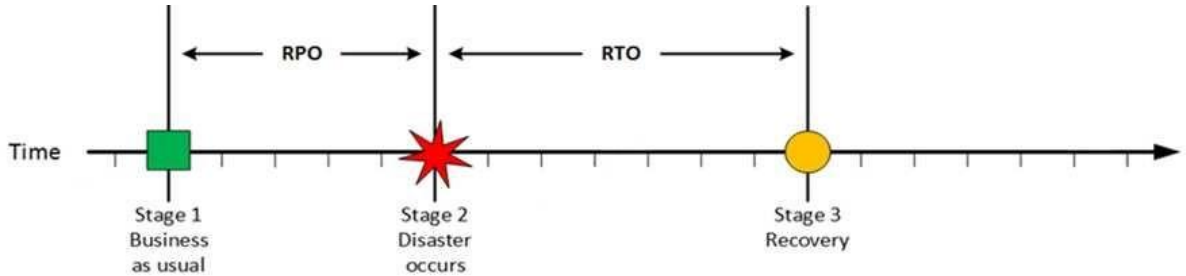
At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs



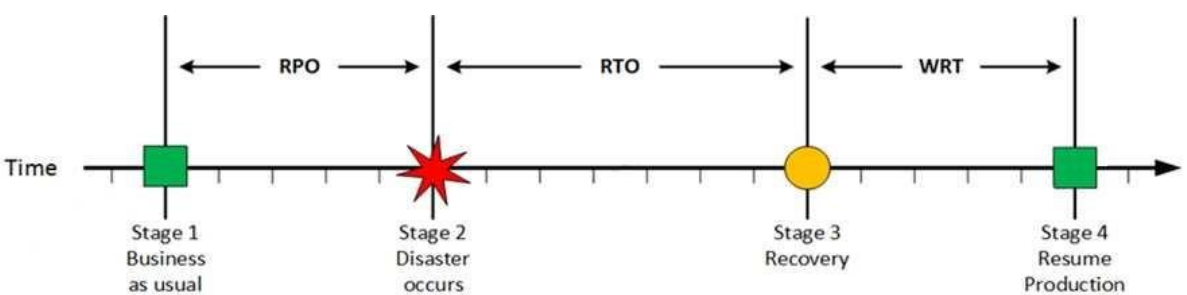
On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery
Recovery



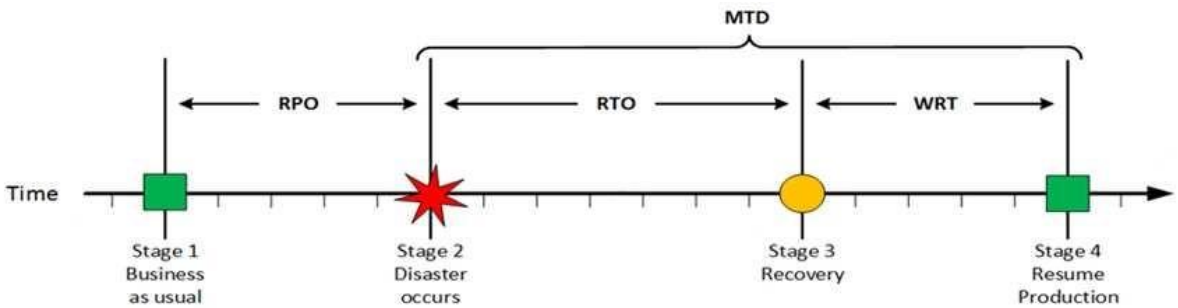
At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production
Resume Production



At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

Reference:
CISA review manual 2014 page number 284
http://en.wikipedia.org/wiki/Recovery_point_objective
http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

QUESTION 482
Which of the following term in business continuity determines the maximum tolerable amount of time needed to bring all critical systems back online after disaster occurs?

A. RPO
B. RTO
C. WRT
D. MTD

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

It can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users. Decision time for users representative is not included.

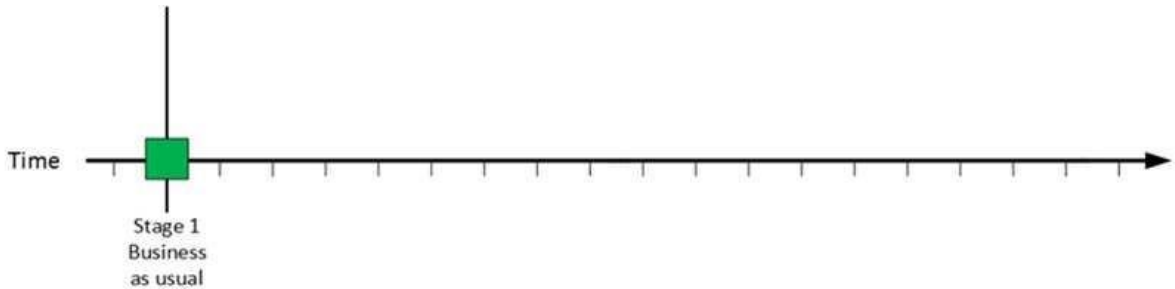
The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points.

In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance.

The RTO attaches to the business process and not the resources required to support the process.
The RTO and the results of the BIA in its entirety provide the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs.

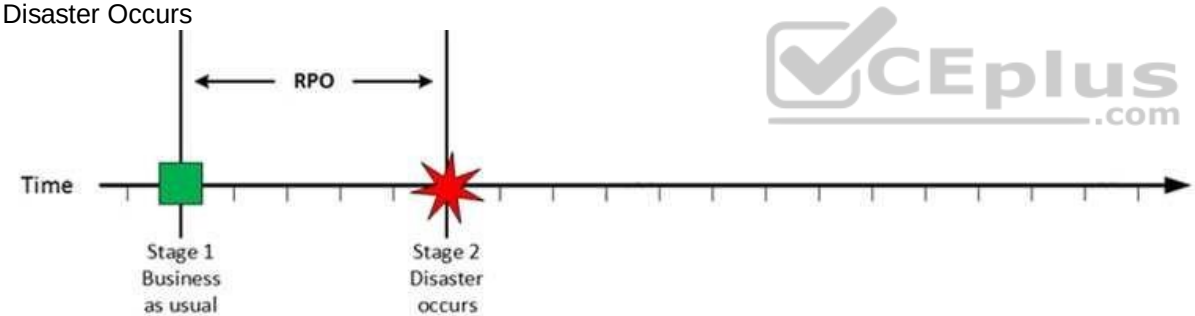
For your exam you should know below information about RPO, RTO, WRT and MTD :

Stage 1: Business as usual
Business as usual



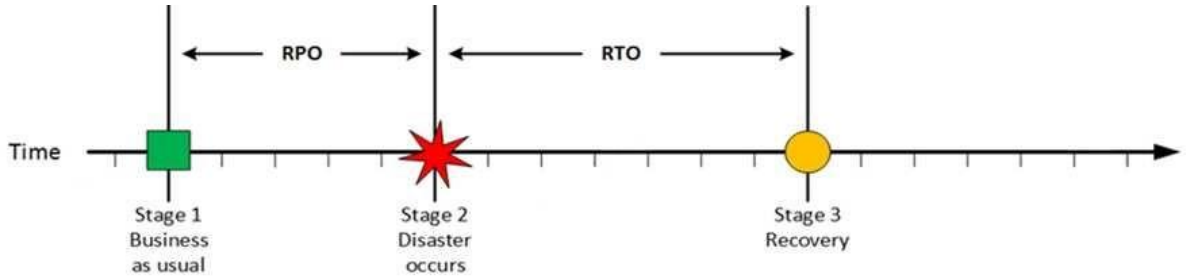
At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs



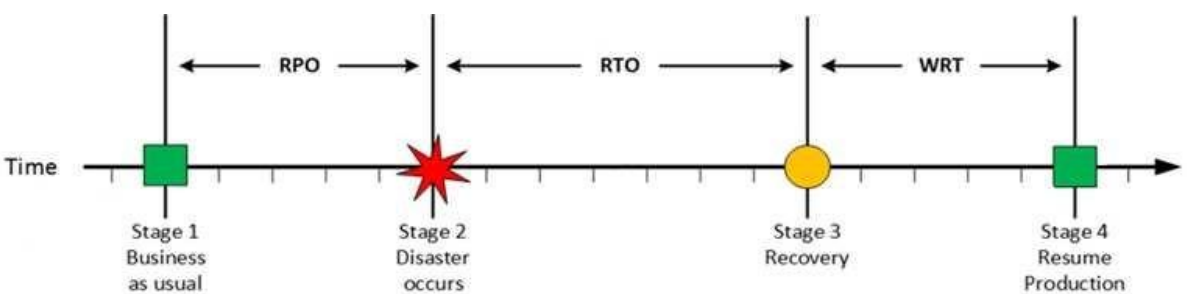
On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery
Recovery



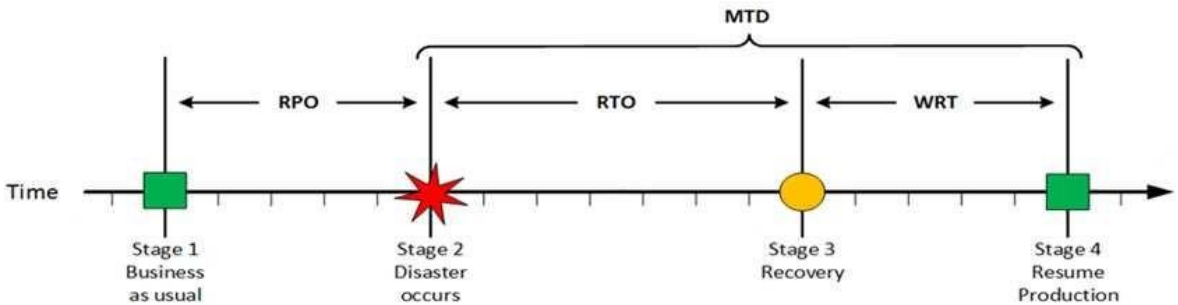
At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production
Resume Production



At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

Reference:
CISA review manual 2014 page number 284
http://en.wikipedia.org/wiki/Recovery_time_objective
http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

QUESTION 483
Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?

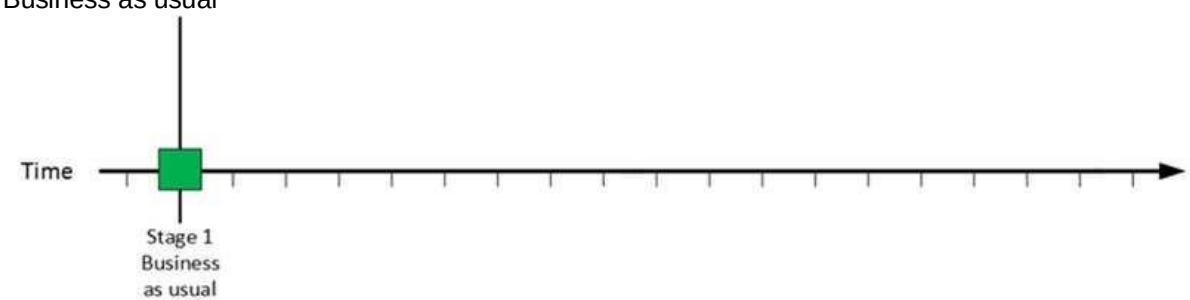
A. RPO
B. RTO
C. WRT
D. MTD

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Explanation:
The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

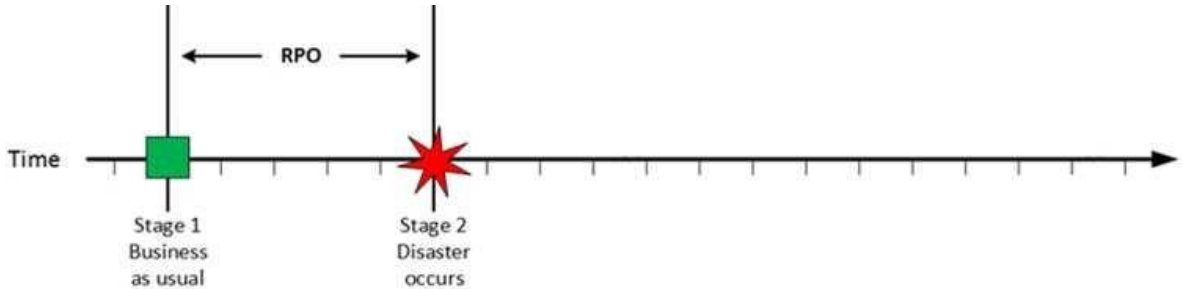
For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual
Business as usual



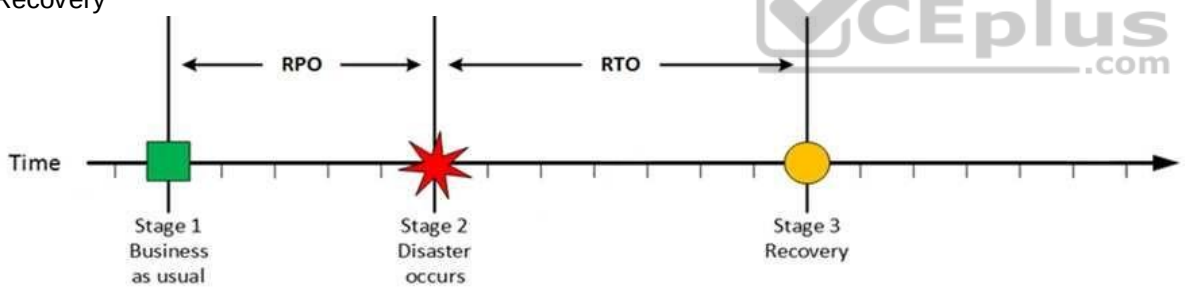
At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs



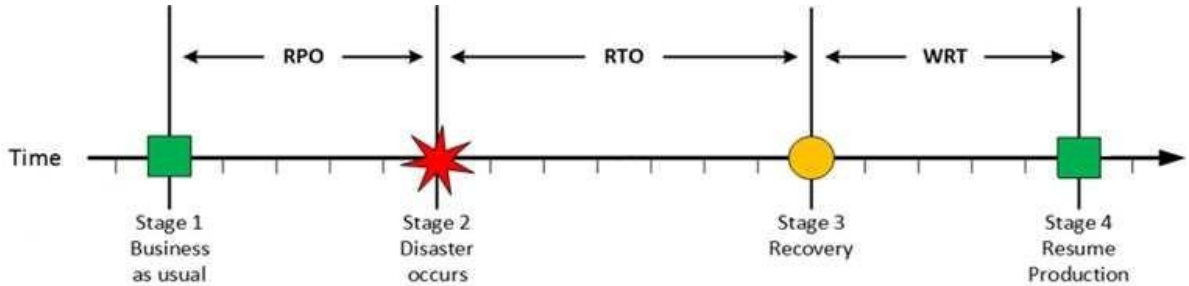
On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery
Recovery



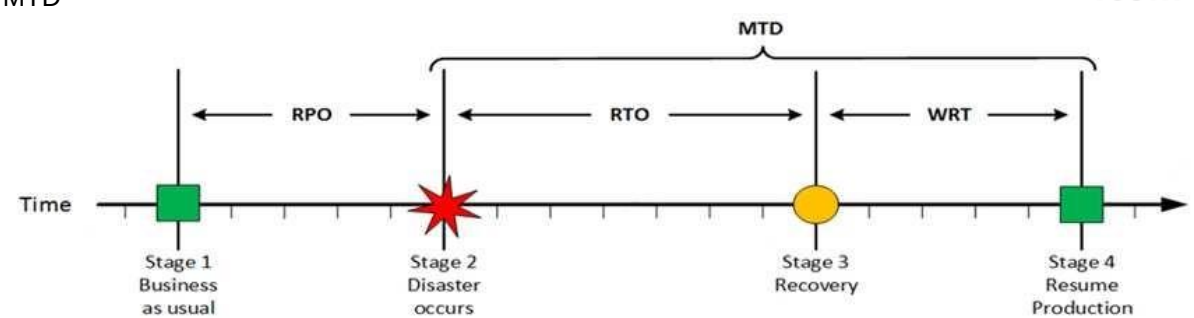
At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production
Resume Production



At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

Reference:
CISA review manual 2014 page number 284
http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

QUESTION 484
As an IS auditor it is very important to understand the importance of job scheduling. Which of the following statement is NOT true about job scheduler or job scheduling software?

A. Job information is set up only once, which increase the probability of an error.
B. Records are maintained of all job success and failures.
C. Reliance on operator is reduced.
D. Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:
The NOT keyword is used in this question. You need to find out an option which is not true about job scheduling.

Below are some advantages of job scheduling or using job scheduling software.

Job information is set up only once, reduce the probability of an error.
Records are maintained of all job success and failures.
Reliance on operator is reduced.
Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

For your exam you should know the information below:

A job scheduler is a computer application for controlling unattended background program execution (commonly called batch processing).

Synonyms are batch system, Distributed Resource Management System (DRMS), and Distributed Resource Manager (DRM). Today's job schedulers, often termed workload automation, typically provide a graphical user interface and a single point of control for definition and monitoring of background executions in a distributed network of computers. Increasingly, job schedulers are required to orchestrate the integration of real-time business activities with traditional background IT processing across different operating system platforms and business application environments.

Job scheduling should not be confused with process scheduling, which is the assignment of currently running processes to CPUs by the operating system.

Basic features expected of job scheduler software include:

interfaces which help to define workflows and/or job dependencies
automatic submission of executions interfaces to monitor the
executions priorities and/or queues to control the execution order of
unrelated jobs

If software from a completely different area includes all or some of those features, this software is consider to have job scheduling capabilities.

Most operating systems (such as Unix and Windows) provide basic job scheduling capabilities, for example: croon. Web hosting services provide job scheduling capabilities through a control panel or a webcron solution. Many programs such as DBMS, backup, ERPs, and BPM also include relevant job-scheduling capabilities. Operating system ("OS") or point program supplied job-scheduling will not usually provide the ability to schedule beyond a single OS instance or outside the remit of the specific program. Organizations needing to automate unrelated IT workload may also leverage further advanced features from a job scheduler, such as:

real-time scheduling based on external, unpredictable
events automatic restart and recovery in event of failures
alerting and notification to operations personnel generation
of incident reports audit trails for regulatory compliance
purposes

The following answers are incorrect:
The other options are correctly defined about job scheduling

Reference:

CISA review manual 2014 page number 242
http://en.wikipedia.org/wiki/Job_scheduler

QUESTION 485
In RFID technology which of the following risk could represent a threat to non-RFID networked or collocated systems, assets, and people?

A. Business Process Risk
B. Business Intelligence Risk
C. Privacy Risk
D. Externality Risk

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:
RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

RFID systems typically are not isolated from other systems and assets in the enterprise. Every connection point between the RFID system and something outside the RFID system represents a potential vulnerability for the entity on the other side of the connection, whether that is an application process, a valued asset, or a person.

Externality risks are present for both the RF and enterprise subsystems of an RFID system.
The main externality risk for the RF subsystem is hazards resulting from electromagnetic radiation, which could possibly range from adverse human health effects to ignition of combustible material, such as fuel or ordnance.

The main externality risk for the enterprise subsystem is successful computer network attacks on networked devices and applications. Computer network attacks can involve malware (e.g., worms and viruses) or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage.

The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application. Because the externality risk by definition involves risks outside of the RFID system, it is distinct from both the business process and business intelligence risks; externality risks can be realized without having any effect on RFID-supported business processes or without revealing any information to adversaries.

For your exam you should know the information below:

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal.

RFID RISKS

RFID technology enables an organization to significantly change its business processes to:

Increase its efficiency, which results in lower costs, Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk.

For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics. This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments.

The risks are as follows:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people. An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users.

The following answers are incorrect:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Reference:
CISA review manual 2014 page number 248

QUESTION 486
John has been hired to fill a new position in one of the well-known financial institute. The position is for IS auditor. He has been assigned to complete IS audit of one of critical financial system. Which of the following should be the first step for John to be perform during IS audit planning?

A. Perform risk assessment
B. Determine the objective of the audit
C. Gain an understanding of the business process
D. Assign the personnel resource to audit

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Explanation:
Determine the objective of audit should be the first step in the audit planning process. Depending upon the objective of an audit, auditor can gather the information about business process.
For CISA exam you should know the information below:

Steps to perform audit planning

Gain an understanding of the business mission, objectives, purpose and processes which includes information and processing requirement such as availability, integrity, security and business technology and information confidentiality.
Understand changes in the business environment audited.
Review prior work papers
Identify stated contents such as policies, standards and required guidelines, procedure and organization structures.
Perform a risk analysis to help in designing the audit plan.
Set the audit scope and audit objectives.
Develop the audit approach or audit strategy
Assign personnel resources to audit
Address engagement logistics.

The following answers are incorrect:
The other options specified should be completed once we finalize on the objective of audit.

Reference:
CISA review manual 2014 page number 30 (The process of auditing information system)

QUESTION 487
A reduction in which of the following would indicate improved performance in the administration of information security?

Explanation

Explanation/Reference:

IT security awareness training days

B. Number of staff involved in security administration
C. Systems subject to an intrusion detection process
D. Turnaround time for requests for new user access

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 488
Senior management has allocated funding to each of the organization's divisions to address information security vulnerabilities. The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of **GREATEST** concern to the information security manager?

A. Redundant controls may be implemented across divisions
B. Information security governance could be decentralized by divisions
C. Areas of highest risk may not be adequately prioritized for treatment
D. Return on investment may be inconsistently reported to senior management

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 489
Which of the following provides the **BEST** assurance that security policies are applied across business operations?

A. Organizational standards are required to be formally accepted.
B. Organizational standards are enforced by technical controls.
C. Organizational standards are included in awareness training.

A.
D. Organizational standards are documented in operational procedures.

D

QUESTION 490
Management has decided to include a compliance manager in the approval process for a new business that may require changes to the IT infrastructure. Which of the following is the **GREATEST** benefit of this approach?

A. Security breach incidents can be identified in early stages.
B. Regulatory risk exposures can be identified before they materialize.
C. Fewer reviews are needed when updating the IT compliance process.
D. Process accountabilities to external stakeholders are improved.

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 491
The prioritization of incident response actions should be **PRIMARILY** based on which of the following?

A. Scope of disaster
B. Business impact
C. Availability of personnel
D. Escalation process

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Correct Answer:
Section: Information System Operations, Maintenance and Support

Explanation

Explanation/Reference:
Explanation/Reference:

QUESTION 492
Which of the following is a passive attack on a network?
Message service interruption
B. Message modification
C. Traffic analysis
D. Sequence analysis

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 493
Which of the following would be **MOST** useful to an information security manager when conducting a post-incident review of an attack?

A. Details from intrusion detection system logs
B. Method of operation used by the attacker
C. Cost of the attack to the organization
D. Location of the attacker

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 494

A.

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the **MOST** important action of the security manager?

A. Follow the outsourcer's response plan
B. Refer to the organization's response plan
C. Notify the outsourcer of the privacy breach
D. Alert the appropriate law enforcement authorities

C

QUESTION 495

An external penetration test identified a serious security vulnerability in a critical business application. Before reporting the vulnerability to senior management, the information security manager's **BEST** course of action should be to:

A. determine the potential impact with the business owner
B. initiate the incident response process
C. block access to the vulnerable business application
D. report the vulnerability to IT for remediation

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 496

When conducting a post-incident review, the **GREATEST** benefit of collecting mean time to resolution (MTTR) data is the ability to:

A. reduce the costs of future preventive controls
B. provide metrics for reporting to senior management
C. verify compliance with the service level agreement (SLA)

Correct Answer:
Section: Information System Operations, Maintenance and Support

Explanation

Explanation/Reference:
D. learn of potential areas of improvement

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 497
Which of the following should be done **FIRST** when handling multiple confirmed incidents raised at the same time?
Categorize incidents by the value of the affected asset. B. Inform senior management.
C. Update the business impact assessment.
D. Activate the business continuity plan.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 498
An IS auditor observes that an organization's critical IT systems have experienced several failures throughout the year. Which of the following is the **BEST** recommendation?

A. Perform a disaster recovery test.
B. Perform a root cause analysis.
C. Contract for a hot site.
D. Implement redundant systems.

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

A.

Explanation/Reference:

QUESTION 499

Of the following procedures for testing a disaster recovery plan (DRP), which should be used **MOST** frequently?

A. Unannounced shutdown of the primary computing facility.
B. Review of documented backup and recovery procedures
C. Testing at a secondary site using offsite data backups
D. Preplanned shutdown of the computing facility during an off-peak period

B

QUESTION 500

When reviewing a disaster recovery plan (DRP), an IS auditor should examine the:

A. access to the computer site by backup staff.
B. offsite data file storage.
C. uninterruptible power supply (UPS).
D. fire-fighting equipment.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 501

Since data storage of a critical business application is on a redundant array of inexpensive disks (RAID), backups are not considered essential. The IS auditor should recommend proper backups because RAID:

Correct Answer:
Section: Information System Operations, Maintenance and Support

Explanation

Explanation/Reference:

A. relies on proper maintenance.
B. cannot offer protection against disk corruption.
C. cannot recover from a natural disaster.
D. disks cannot be hot-swapped for quick recovery.

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 502
Which of the following would be **MOST** helpful in ensuring security procedures are followed by employees in a multinational organization?

A.

Security architecture review

B. Regular clean desk reviews
C. Comprehensive end-user training
D. Regular policy updates by management

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 503
Which of the following would be the **PRIMARY** benefit of replacing physical keys with an electronic badge system for access to a data center?

A. Increasing accountability
B. Maintaining compliance
C. Tracking employee work hours
D. Increasing reliability

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 504
Outsourcing the development of business systems is **MOST** likely to result in the loss of:

A. control over strategic direction.
B. accountability for end products.
C. in-house competencies.
D. responsibility for IT security.

Correct Answer: A

Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:

QUESTION 505
Overall responsibility for approving logical access rights to information assets should reside with the:

A. data and systems owners.
B. systems delivery and operations group.
C. security administrator.
D. systems administrator.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 506
In a complex IS environment, which of the following tasks should be performed by the data owner?

A. Perform technical database maintenance.
B. Perform data restoration when necessary.
C. Review data classifications periodically.
D. Test the validity of backup data.

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 507
Which of the following is the **GREATEST** risk posed by denial-of-service attacks?

A. Confidential information leakage
B. Loss of integrity and corruption of databases
C. Loss of reputation and business
D. Unauthorized access to the systems

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 508
Which of the following would **BEST** indicate the effectiveness of a security awareness training program?

A. Increased number of employees completing training
B. Employee satisfaction with training
C. Reduced unintentional violations
D. Results of third-party social engineering tests.

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 509
Which of the following is the **BEST** approach to verify that internal help desk procedures are executed in compliance with policies?

A. Benchmark help desk procedures.
B. Interview end users.
C. Test a sample of closed tickets.
D. Evaluate help desk call metrics.

Correct Answer: C

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 510

When replacing a critical software application, which of the following provides for the **LOWEST** risk of interruption to business processes?

A. Parallel implementation
B. Pilot implementation
C. Incremental implementation
D. Big-bang implementation

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 511

Which of the following is the **BEST** indicator of an effective employee information security program?

A. Increased management support for security
B. More efficient and effective incident handling
C. Increased detection and reporting of incidents
D. Reduced operational cost of security

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 512

Of the following, who should the security manager consult **FIRST** when determining the severity level of a security incident involving a third-party vendor?

A. IT process owners
B. Business partners
C. Risk manager
D. Business process owners

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 513
When developing an escalation process for an incident response plan, the information security manager should **PRIMARLY** consider the:

A. affected stakeholders
B. availability of technical resources
C. incident response team
D. media coverage

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 514
Which of the following is **MOST** likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?

A. The activities being monitored deviate from what is considered normal.
B. The environment is complex.
C. The pattern of normal behavior changes quickly and dramatically.
D. The information regarding monitored activities becomes state.

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 515
What should be the **MAIN** goal of an organization's incident response plan?

A. Keep stakeholders notified of incident status.
B. Enable appropriate response according to criticality.
C. Correlate incidents from different systems.
D. Identify the root cause of the incident.

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 516
An organization has purchased a security information and event management (SIEM) tool. Which of the following would be **MOST** important to consider before implementation?

A. The contract with the SIEM vendor
B. Controls to be monitored
C. Available technical support
D. Reporting capabilities

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 517
A client/server configuration will:

A. optimize system performance by having a server on a front-end and clients on a host
B. enhance system performance through the separation of front-end and back-end processes
C. keep track of all the clients using the IS facilities of a service organization
D. limit the clients and servers' relationship by limiting the IS facilities to a single hardware system

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 518
Which of the following is the **GREATEST** risk of cloud computing?

A. Reduced performance
B. Disclosure of data
C. Lack of scalability
D. Inflexibility

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 519
In an IT organization where many responsibilities are shared, which of the following would be the **BEST** control for detecting unauthorized data changes?

A. Data changes are independently reviewed by another group.
B. Users are required to periodically rotate responsibilities.

C. Segregation of duties conflicts are periodically reviewed.
D. Data changes are logged in an outside application.

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 520
Which of the following is a substantive test procedure?
A. Using audit software to verify the total of an accounts receivable file
B. Observing that user IDs and passwords are required to sign on to the online system
C. Test of invoice calculation process
D. Verifying that appropriate approvals are documented in a sample of program changes

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 521
For an organization which uses a VoIP telephony system exclusively, the **GREATEST** concern associated with leaving a connected telephone in an unmonitored public area is the possibility of:

A. connectivity issues when used with an analog local exchange carrier
B. unauthorized use leading to theft of services and financial loss
C. network compromise due to the introduction of malware
D. theft or destruction of an expensive piece of electronic equipment

Correct Answer: B

Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 522
When responding to an ongoing denial of service (DoS) attack, an organization's **FIRST** course of action should be to:

A. restore service
B. minimize impact
C. analyze the attack path
D. investigate damage

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 523
Which of the following is the **GREATEST** risk when relying on reports generated by end-user computing?

A. Data may be inaccurate
B. Reports may not work efficiently
C. Reports may not be timely
D. Historical data may not be available

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 524

The **MOST** effective control to detect fraud inside an organization's network, is to:

A. implement an intrusion detection system (IDS)
B. apply two-factor authentication
C. review access logs
D. segregate duties

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 525
Which of the following is the **GREATEST** risk of single sign-on?

Password carelessness by one user may render the entire infrastructure vulnerable

B. Integration of single sign-on with the rest of the infrastructure is complicated
C. It is a single point of failure for an enterprise access control process
D. One administrator maintains the single sign-on solutions without segregation of duty

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 526
Which of the following is the **BEST** defense against a brute force attack?

A. Discretionary access control
B. Intruder detection lockout
C. Mandatory access control
D. Time-of-day restrictions

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 527
An employee uses a personal mobile device to access corporate data and email, but also allows friends to use it as a mobile hotspot for Internet access when not at work. The information security manager is concerned this situation may expose confidential data. The manager's **FIRST** step should be to:

A. update the mobile device usage standards to address the issue and communicate to all employees
B. activate the incident response plan to mitigate the impact and stop the compromise
C. review the associated risks to determine if additional controls are needed
D. implement additional security controls that will mitigate the situation and then reassess risks

A.

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 528
Senior management has approved employees working off-site by using a virtual private network (VPN) connection. It is **MOST** important for the information security manager to periodically:

A. review firewall configuration
B. review the security policy
C. perform a cost-benefit analysis
D. perform a risk assessment

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 529
The **BEST** way to avoid session hijacking is to use:

A. a reverse lookup
B. a secure protocol
C. a firewall
D. strong password controls

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 530
Performance monitoring tools report that servers are significantly below their planned utilization. Which of the following would be the **BEST** recommendation?

Consolidate physical servers. B.
Review the capacity plan.

C. Deploy load balancing.
D. Reconfigure server settings.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 531
A security administrator should have read-only access for which of the following?

A. Router configuration
B. Password policy
C. Security logs
D. Services/daemons configuration

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 532
Which of the following should be the **PRIMARY** consideration for IT management when selecting a new information security tool that monitors suspicious file access patterns?

A. Integration with existing architecture

A.

B. Ease of support and troubleshooting
C. Data correlation and visualization capabilities
D. Ability to contribute to key performance indicator data

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 533
Which of the following will **BEST** ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

A. Maintaining system console logs in electronic format
B. Ensuring bisynchronous capabilities on all transmission lines
C. Using a database management system (DBMS) to dynamically back-out partially processed transactions
D. Rotating backup copies of transaction files offsite

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 534
Which of the following is the **GREATEST** concern with conducting penetration testing on an internally developed application in the production environment?

A. The testing could create application availability issues.
B. The testing may identify only known operating system vulnerabilities.
C. The issues identified during the testing may require significant remediation efforts.
D. Internal security staff may not be qualified to conduct application penetration testing.

Correct Answer: D

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 535
What is the **MOST** important business concern when an organization is about to migrate a mission-critical application to a virtual environment?
The organization's experience with virtual applications
B. Adequacy of the fallback procedures
C. Confidentiality of network traffic
D. Adequacy of the virtual architecture

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 536
Which of the following is the **PRIMARY** advantage of single sign-on (SSO)?

A. Improves system performance
B. Ensures good password practices
C. Improves security
D. Reduces administrative workload.

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 537
Which of the following **BEST** ensures that only authorized software is moved into a production environment?

A.

A. Restricting read/write access to production code to computer programmers only
B. Assigning programming managers to transfer tested programs to production
C. A librarian compiling source code into production after independent testing
D. Requiring programming staff to move tested code into production

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:

QUESTION 538
Which of the following is the **BEST** way to help ensure the security of privacy-related data stored by an organization?

A. Encrypt personally identifiable information (PII).
B. Publish the data classification scheme.
C. Inform data owners of the purpose of collecting information.
D. Classify privacy-related data as confidential.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 539
Which of the following controls is **MOST** appropriate against brute force attacks at login?

A. Storing password files using one-way encryption
B. Locking the account after three invalid passwords
C. Storing passwords under a one-way hash function
D. Increasing the minimum password length to 10 characters

Correct Answer: B

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 540
An organization has performance metrics to track how well IT resources are being used, but there has been little progress on meeting the organization's goals. Which of the following would be **MOST** helpful to determine the underlying reason?

A. Conducting a root cause analysis

B. Re-evaluating organizational goals
C. Re-evaluating key performance indicators (KPIs)
D. Conducting a business impact analysis (BIA)

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 541
Which of the following concerns is **BEST** addressed by securing production source libraries?

A. Production source and object libraries may not be synchronized.
B. Unauthorized changes can be moved into production.
C. Programs are not approved before production source libraries are updated.
D. Changes are applied to the wrong version of production source libraries.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 542
Which of the following security testing techniques is **MOST** effective in discovering unknown malicious attacks?

A. Vulnerability testing
B. Reverse engineering
C. Penetration testing
D. Sandboxing

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 543

An organization has recently converted its infrastructure to a virtualized environment. The **GREATEST** benefit related to disaster recovery is that virtualized servers:

A. reduce the time it takes to successfully create backups.
B. decrease the recovery time objective (RTO).
C. eliminate the manpower necessary to restore the server.
D. can be recreated on similar hardware faster than restoring from backups.

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 544

Which of the following is used in providing logical access control to restrict updating or deleting business information in a relational database?

A. Trigger
B. View
C. Join
D. Primary key

Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 545

Which of the following is the **MOST** reliable control to prevent double payments made as a result of payment system batch jobs restarting after processing errors?

A. Database rollback in case of processing errors
B. Review of batch job competition logs
C. Duplicate verification at the last possible point in processing
D. Restart procedures integrated in job controls

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 546
Which cloud deployment model is **MOST** likely to be limited in scalability?

A. Public
B. Private
C. Hybrid
D. Community

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 547
During a computer forensics investigation, what is the **PRIMARY** reason for obtaining a bit-for-bit copy of data in storage?

A. To document findings
B. To obtain residual data
C. To obtain data as well as source code details
D. To transfer the data into a controlled location

Correct Answer: B

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 548

Controls related to authorized modifications to production programs are **BEST** tested by:

A. testing only the authorizations to implement the new program.
B. tracing modifications from the executable program back to the original request for change.
C. reviewing only the actual lines of source code changed in the program.
D. tracing modifications from the original request for change forward to the executable program.

Correct Answer: D

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 549

IS management has decided to replace the current single-server-based local area network (LAN) with three interconnected servers running different operating systems. Existing applications and data on the old server have been exclusively distributed on the new servers. This will **MOST** likely result in:

A. disclosure of information.
B. multiple authentication.
C. data incompleteness.
D. data unavailability.

Correct Answer: B

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 550

A retailer normally uses a scanner to read product labels and input product codes and prices. The unit is not functioning and staff are keying information manually. With respect to the accuracy of the input, it is likely that:

A. audit risk has increased.
B. control risk has increased.
C. inherent risk has decreased.
D. detection risk has decreased.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 551
When reviewing an end-user computing (EUC) application, which of the following techniques is **MOST** appropriate for testing program logic?

A. Integrated testing facility
B. Test decking
C. Re-performance
D. Key calculation inspection

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 552
For a company that outsources payroll processing, which of the following is the **BEST** way to ensure that only authorized employees are paid?

A. The company's bank reconciliations should be independently prepared and checked.
B. Employees should receive pay statements showing gross pay, net pay, and deductions.
C. Only payroll employees should be given the password for data entry and report retrieval.
D. Electronic payroll reports should be independently reviewed.

Correct Answer: A

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 553

Which of the following strategies **BEST** optimizes data storage without compromising data retention practices?

A. Limiting the size of the file attachments being sent via email
B. Automatically deleting emails older than one year
C. Moving emails to a virtual email vault after 30 days
D. Allowing employees to store large emails on flash drives

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 554

A database administrator should be prevented from:

A. using an emergency user ID.
B. accessing sensitive information.
C. having end user responsibilities.
D. having access to production files.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 555

Which of the following does a lack of adequate security controls represent?

A. Threat
B. Asset
C. Impact
D. Vulnerability

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers. This could result in a loss of sensitive information and lead to the loss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the 'potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.' The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionality in this context is a vulnerability.

QUESTION 556
Assessing IT risks is BEST achieved by:

A. evaluating threats associated with existing IT assets and IT projects.
B. using the firm's past actual loss experience to determine current exposure.
C. reviewing published loss statistics from comparable organizations.
D. reviewing IT control weaknesses identified in audit reports.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient. Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to be assessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure

and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

QUESTION 557
Which of the following terms refers to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders?

A. ILD&P
B. ICT&P
C. ILP&C
D. ILR&D
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Information Leakage Detection and Prevention (ILD&P) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Network ILD&P are gateway-based systems installed on the organization's internet network connection and analyze network traffic to search for unauthorized information transmissions. Host Based ILD&P systems run on end-user workstations to monitor and control access to physical devices and access information before it has been encrypted.

QUESTION 558
To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

A. avoidance
B. transference
C. mitigation
D. acceptance

Correct Answer: C
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation:
Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

QUESTION 559
A poor choice of passwords and transmission over unprotected communications lines are examples of:

A. vulnerabilities.
B. threats.
C. probabilities.
D. impacts.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Vulnerabilities represent characteristics of information resources that may be exploited by a threat. Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat, while impacts represent the outcome or result of a threat exploiting a vulnerability.

QUESTION 560
Which of the following should be considered FIRST when implementing a risk management program?

A. An understanding of the organization's threat, vulnerability and risk profile
B. An understanding of the risk exposures and the potential consequences of compromise
C. A determination of risk management priorities based on potential consequences
D. A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
Implementing risk management, as one of the outcomes of effective information security governance, would require a collective understanding of the organization's threat, vulnerability and risk profile as a first step. Based on this, an understanding of risk exposure and potential consequences of compromise could be determined. Risk management priorities based on potential consequences could then be developed. This would provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

QUESTION 561
As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

A. performance measurement.
B. strategic alignment.
C. value delivery.
D. resource management.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Performance measurement includes setting and monitoring measurable objectives of what the IT processes need to deliver {process outcome) and how they deliver it (process capability and performance). Strategic alignment primarily focuses on ensuring linkage of business and IT plans. Value delivery is about executing the value proposition throughout the delivery cycle. Resource management is about the optimal investment in and proper management of critical IT resources. Transparency is primarily achieved through performance measurement as it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.

QUESTION 562
Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

A. Process maturity
B. Performance indicators
C. Business risk
D. Assurance reports

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.

QUESTION 563
The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

A. alignment of the IT activities with IS audit recommendations.
B. enforcement of the management of security risks.
C. implementation of the chief information security officer's (CISO) recommendations.
D. reduction of the cost for IT security.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The major benefit of implementing a security program is management's assessment of risk and its mitigation to an appropriate level of risk, and the monitoring of the remaining residual risks. Recommendations, visions and objectives of the auditor and the chief information security officer (CISO) are usually included within a security program, but they would not be the major benefit. The cost of IT security may or may not be reduced.

QUESTION 564
Which of the following is the PRIMARY objective of an IT performance measurement process?

A. Minimize errors
B. Gather performance data
C. Establish performance baselines
D. Optimize performance

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of IT measurement process and would be used to evaluate the performance against previously established performance baselines.

QUESTION 565
Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

A. Function point analysis
B. PERT chart
C. Rapid application development
D. Object-oriented system development

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A PERT chart will help determine project duration once all the activities and the work involved with those activities are known. Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many overlapping tasks. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality, while object-oriented system development is the process of solution specification and modeling.

QUESTION 566
The reason for establishing a stop or freezing point on the design of a new system is to:

A. prevent further changes to a project in process.
B. indicate the point at which the design is to be completed.

C. require that changes after that point be evaluated for cost-effectiveness.
D. provide the project management team with more control over the project design.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs, it is recommended that the project be stopped or frozen to allow a review of all of the cost- benefits and the payback period.

QUESTION 567
At the completion of a system development project, a post project review should include which of the following?

A. Assessing risks that may lead to downtime after the production release
B. Identifying lessons learned that may be applicable to future projects
C. Verifying the controls in the delivered system are working
D. Ensuring that test data are deleted

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects. An assessment of potential downtime should be made with the operations group and other specialists before implementing a system. Verifying that controls are working should be covered during the acceptance test phase and possibly, again, in the post implementation review. Test data should be retained for future regression testing.

QUESTION 568
An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

A. complexity and risks associated with the project have been analyzed.
B. resources needed throughout the project have been determined.
C. project deliverables have been identified.
D. a contract for external parties involved in the project has been completed.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Understanding complexity and risk, and actively managing these throughout a project are critical to a successful outcome. The other choices, while important during the course of the project, cannot be fully determined at the time the project is initiated, and are often contingent upon the risk and complexity of the project.

QUESTION 569
An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

A. stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.
B. accept the project manager's position as the project manager is accountable for the outcome of the project.
C. offer to work with the risk manager when one is appointed.
D. inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: the majority of project risks can typically be identified before a project begins, allowing mitigation/avoidance plans to be put in place to deal with the risks. A project should have a clear link back to corporate strategy and tactical plans to support this strategy. The process of setting corporate strategy, setting objectives and developing tactical plans should include the consideration of risks. Appointing a risk manager is a good practice but waiting until the project has been impacted by risks is misguided. Risk management needs to be forward looking; allowing risks to evolve into issues that adversely impact the project represents a failure of risk management. With or without a risk manager, persons within and outside of the project team need to be consulted and encouraged to comment when they believe new risks have emerged or risk priorities have changed. The IS auditor has an obligation to the project sponsor and the organization

to advise on appropriate project manage me practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

QUESTION 570
While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

A. effectiveness of the QA function because it should interact between project management and user management
B. efficiency of the QA function because it should interact with the project implementation team.
C. effectiveness of the project manager because the project manager should interact with the QA function.
D. efficiency of the project manager because the QA function will need to communicate with the project implementation team.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To be effective the quality assurance (QA) function should be independent of project management. The QA function should never interact with the project implementation team since this can impact effectiveness. The project manager does not interact with the QA function, which should not impact the effectiveness of the project manager. The QA function does not interact with the project implementation team, which should not impact the efficiency of the project manager.

QUESTION 571
An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

A. Project sponsor
B. System development project team (SPDT)
C. Project steering committee
D. User project team (UPT)

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support. The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics for the project. The project sponsor is not responsible for reviewing the progress of the project. A system development project team (SDPT) completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for reviewing the progress of the project. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

QUESTION 572
A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor
B. Database administrator
C. Project manager
D. Data owner

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
During the data conversion stage of a project, the data owner is primarily responsible for reviewing and signing-off that the data are migrated completely, accurately and are valid. An IS auditor is not responsible for reviewing and signing-off on the accuracy of the converted data. However, an IS auditor should ensure that there is a review and sign-off by the data owner during the data conversion stage of the project. A database administrator's primary responsibility is to maintain the integrity of the database and make the database available to users. A database administrator is not responsible for reviewing migrated data. A project manager provides day-to- day management and leadership of the project, but is not responsible for the accuracy and integrity of the data.

QUESTION 573
A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

A. what amount of progress against schedule has been achieved.
B. if the project budget can be reduced.
C. if the project could be brought in ahead of schedule.
D. if the budget savings can be applied to increase the project scope.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Cost performance of a project cannot be properly assessed in isolation of schedule performance. Cost cannot be assessed simply in terms of elapsed time on a project. To properly assess the project budget position, it is necessary to know how much progress has actually been made and, given this, what level of expenditure would be expected. It is possible that project expenditure appears to be low because actual progress has been slow. Until the analysis of project against schedule has been completed, it is impossible to know whether there is any reason to reduce budget, if the project has slipped behind schedule, then not only may there be no spare budget but it is possible that extra expenditure may be needed to retrieve the slippage. The low expenditure could actually be representative of a situation where the project is likely to miss deadlines rather than potentially come in ahead of time. If the project is found to be ahead of budget after adjusting for actual progress, this is not necessarily a good outcome because it points to flaws in the original budgeting process; and, as said above, until further analysis is undertaken, it cannot be determined whether any spare funds actually exist. Further, if the project is behind schedule, then adding scope may be the wrong thing to do.

QUESTION 574
A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

A. recommend that the project be halted until the issues are resolved.
B. recommend that compensating controls be implemented.
C. evaluate risks associated with the unresolved issues.
D. recommend that the project manager reallocate test resources to resolve the issues.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

It is important to evaluate what the exposure would be when audit recommendations have not been completed by the target date. Based on the evaluation, management can accordingly consider compensating controls, risk acceptance, etc. All other choices might be appropriate only after the risks have been assessed.

QUESTION 575
Which of the following techniques would BEST help an IS auditor gain reasonable assurance that a project can meet its target date?

A. Estimation of the actual end date based on the completion percentages and estimated time to complete, taken from status reports
B. Confirmation of the target date based on interviews with experienced managers and staff involved in the completion of the project deliverables.
C. Extrapolation of the overall end date based on completed work packages and current resources
D. Calculation of the expected end date based on current resources and remaining available project budget **Correct Answer:** C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Direct observation of results is better than estimations and qualitative information gained from interviews or status reports. Project managers and involved staff tend to underestimate the time needed for completion and the necessary time buffers for dependencies between tasks, while overestimating the completion percentage for tasks underway (80:20 rule). The calculation based on remaining budget does not take into account the speed at which the project has been progressing.

QUESTION 576
Which of the following situations would increase the likelihood of fraud?

A. Application programmers are implementing changes to production programs.
B. Application programmers are implementing changes to test programs.
C. Operations support staff are implementing changes to batch schedules.
D. Database administrators are implementing changes to data structures.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Production programs are used for processing an enterprise's data. It is imperative that controls on changes to production programs are stringent. Lack of control in this area could result in application programs being modified to manipulate the data. Application programmers are required to implement changes to test programs. These are used only in development and do not directly impact the live processing of data. The implementation of changes to batch schedules by operations support staff will affect the scheduling of the batches only; it does not impact the live data. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.

QUESTION 577
Before implementing controls, management should FIRST ensure that the controls:

A. satisfy a requirement in addressing a risk issue.
B. do not reduce productivity.
C. are based on a cost-benefit analysis.
D. are detective or corrective.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventive controls that attack the cause of a threat.

QUESTION 578
Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printout.
B. transaction journal.
C. automated suspense file listing.
D. user error report.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, while the user error report would only list input that resulted in an edit error.

QUESTION 579
The editing/validation of data entered at a remote site would be performed MOST effectively at the:

A. central processing site after running the application system.
B. central processing sire during the running of the application system.
C. remote processing site after transmission of the data to the central processing site.
D. remote processing site prior to transmission of the data to the central processing site.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.
QUESTION 580
Functional acknowledgements are used:

A. as an audit trail for EDI transactions.
B. to functionally describe the IS department.
C. to document user roles and responsibilities.
D. as a functional description of application software.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

QUESTION 581
Which of the following will BEST ensure the successful offshore development of business applications?

A. Stringent contract management practices
B. Detailed and correctly applied specifications
C. Awareness of cultural and political differences
D. Post implementation reviews

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When dealing with offshore operations, it is essential that detailed specifications be created. Language differences and a lack of interaction between developers and physically remote end users could create gaps in communication in which assumptions and modifications may not be adequately communicated. Contract management practices, cultural and political differences, and post implementation reviews, although important, are not as pivotal to the success of the project.

QUESTION 582
Which of the following is the GREATEST risk to the effectiveness of application system controls?

A. Removal of manual processing steps
B. inadequate procedure manuals
C. Collusion between employees
D. Unresolved regulatory compliance issues

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Collusion is an active attack that can be sustained and is difficult to identify since even well-thought-out application controls may be circumvented. The other choices do not impact well-designed application controls.

QUESTION 583
A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies
B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
D. Reengineering the existing processing and redesigning the existing system

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
EDI is the best answer. Properly implemented (e.g., agreements with trading partner's transaction standards, controls over network security mechanisms in conjunction with application controls), EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

QUESTION 584
During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

A. test the software for compatibility with existing hardware.
B. perform a gap analysis.
C. review the licensing policy.
D. ensure that the procedure had been approved.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions an IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

QUESTION 585
An organization has an integrated development environment (IDE) on which the program libraries reside on the server, but modification/development and testing are done from PC workstations.
Which of the following would be a strength of an IDE?

A. Controls the proliferation of multiple versions of programs
B. Expands the programming resources and aids available
C. Increases program and processing integrity
D. Prevents valid changes from being overwritten by other changes

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A strength of an IDE is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

QUESTION 586
Which of the following is the most important element in the design of a data warehouse?

A. Quality of the metadata
B. Speed of the transactions
C. Volatility of the data
D. Vulnerability of the system

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for query and analysis. Metadata aim to provide a table of contents to the information stored in the data warehouse. Companies that have built warehouses believe that metadata are the most important component of the warehouse.

QUESTION 587
Which of the following is an advantage of prototyping?

A. The finished system normally has strong internal controls.
B. Prototype systems can provide significant time and cost savings.
C. Change control is often less complicated with prototype systems.
D. it ensures that functions or extras are not added to the intended system.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 588
A decision support system (DSS):

A. is aimed at solving highly structured problems.
B. combines the use of models with nontraditional data access and retrieval functions.

C. emphasizes flexibility in the decision making approach of users.
D. supports only structured decision making tasks.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
DSS emphasizes flexibility in the decision making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semi structured decision making tasks.

QUESTION 589
The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

A. rules.
B. decision trees.C. semantic nets.
D. dataflow diagrams.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a dataflow diagram and make use of an inheritance mechanism to prevent duplication of data.

QUESTION 590
An advantage in using a bottom-up vs. a top-down approach to software testing is that:

A. interface errors are detected earlier.
B. confidence in the system is achieved earlier.
C. errors in critical modules are detected earlier.

D. major functions and processing are tested earlier.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upward until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices in this question all refer to advantages of a top-down approach, which follows the opposite path, either in depthfirst or breadth-first search order.

QUESTION 591
The MOST likely explanation for the use of applets in an Internet application is that:

A. it is sent over the network from the server.
B. the server does not run the program and the output is not sent over the network.
C. they improve the performance of the web server and network.
D. it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An applet is a JAVA program that is sent over the network from the web server, through a web browser and to the client machine; the code is then run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on the web server and network-over which the server and client are connected-drastically improves through the use of applets. Performance improvement is more important than the reasons offered in choices A and B. Since JAVA virtual machine (JVM) is embedded in most web browsers, the applet download through the web browser runs on the client machine from the web browser, not from the web server, making choice D incorrect.

QUESTION 592
The waterfall life cycle model of software development is most appropriately used when:

A. requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.
B. requirements are well understood and the project is subject to time pressures.
C. the project intends to apply an object-oriented design and programming approach.
D. the project will involve the use of new technology.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Historically, the waterfall model has been best suited to the stable conditions described in choice
A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative development life cycle gives the advantage of breaking down the scope of the overall system to be delivered, making the requirements gathering and design activities more manageable. The ability to deliver working software earlier also acts to alleviate uncertainty and may allow an earlier realization of benefits. The choice of a design and programming approach is not itself a determining factor of the type of software development life cycle that is appropriate. The use of new technology in a project introduces a significant element of risk. An iterative form of development, particularly one of the agile methods that focuses on early development of actual working software, is likely to be the better option to manage this uncertainty.

QUESTION 593
During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:

A. buffer overflow.
B. brute force attack.
C. distributed denial-of-service attack.
D. war dialing attack.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Poorly written code, especially in web-based applications, is often exploited by hackers using buffer overflow techniques. A brute force attack is used to crack passwords. A distributed denial- of-service attack floods its target with numerous packets, to prevent it from responding to legitimate requests. War dialing uses modem-scanning tools to hack PBXs.

QUESTION 594
Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

A. increase the time allocated for system testing
B. implement formal software inspections
C. increase the development staff
D. Require the sign-off of all project deliverables

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: inspections of code and design are a proven software quality technique. An advantage of this approach is that defects are identified before they propagate through the development life cycle. This reduces the cost of correction as less rework is involved. Allowing more time for testing may discover more defects; however, little is revealed as to why the quality problems are occurring and the cost of the extra testing, and the cost of rectifying the defects found will be greater than if they had been discovered earlier in the development process. The ability of the development staff can have a bearing on the quality of what is produced; however, replacing staff can be expensive and disruptive, and the presence of a competent staff cannot guarantee quality in the absence of effective quality management processes. Sign-off of deliverables may help detect defects if signatories are diligent about reviewing deliverable content; however, this is difficult to enforce.
Deliverable reviews normally do not go down to the same level of detail as software inspections.

QUESTION 595
The MAJOR advantage of a component-based development approach is the:

A. ability to manage an unrestricted variety of data types.
B. provision for modeling complex relationships.
C. capacity to meet the demands of a changing environment.
D. support of multiple development environments.

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic. The other choices are not the most significant advantages of a component-based development approach.

QUESTION 596
The specific advantage of white box testing is that it:

A. verifies a program can operate successfully with other parts of the system.
B. ensures a program's functional operating effectiveness without regard to the internal program structure.
C. determines procedural accuracy or conditions of a program's specific logic paths.
D. examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths. Verifying the program can operate successfully with other parts of the system is sociability testing. Testing the program's functionality without knowledge of internal structures is black box testing. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

QUESTION 597
Following best practices, formal plans for implementation of new information systems are developed during the:

A. development phase.
B. design phase.C. testing phase.
D. deployment phase.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Planning for implementation should begin well in advance of the actual implementation date. A formal implementation plan should be constructed in the design phase and revised as the development progresses.

QUESTION 598
At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

A. report the error as a finding and leave further exploration to the auditee's discretion.
B. attempt to resolve the error.
C. recommend that problem resolution be escalated.
D. ignore the error, as it is not possible to get objective evidence for the software error.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

QUESTION 599
An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

A. Pilot
B. Parallel
C. Direct cutover
D. Phased

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Direct cutover implies switching to the new system immediately, usually without the ability to revert to the old system in the event of problems. All other alternatives are done gradually and thus provide greater recoverability and are therefore less risky.

QUESTION 600
During a postimplementation review of an enterprise resource management system, an IS auditor would MOST likely:

A. review access control configuration
B. evaluate interface testing.
C. review detailed design documentation.
D. evaluate system testing.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Reviewing access control configuration would be the first task performed to determine whether security has been appropriately mapped in the system. Since a postimplementation review is done after user acceptance testing and actual implementation, one would not engage in interface testing or detailed design documentation. Evaluating interface testing would be part of the implementation process. The issue of reviewing detailed design documentation is not generally relevant to an enterprise resource management system, since these are usually vendor packages with user manuals. System testing should be performed before final user signoff.

QUESTION 601
In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

A. isolation.
B. consistency.

C. atomicity.D. durability.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the database be maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions; hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that, when a transaction has been reported back to a user as complete, the resultant changes to the database will survive subsequent hardware or software failures.

QUESTION 602
Business units are concerned about the performance of a newly implemented system. Which of the following should an IS auditor recommend?

A. Develop a baseline and monitor system usage.
B. Define alternate processing procedures.
C. Prepare the maintenance manual.
D. implement the changes users have suggested.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor should recommend the development of a performance baseline and monitor the system's performance, against the baseline, to develop empirical data upon which decisions for modifying the system can be made. Alternate processing procedures and a maintenance manual will not alter a system's performance. Implementing changes without knowledge of the cause(s) for the perceived poor performance may not result in a more efficient system.

QUESTION 603
An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:

A. check to ensure that the type of transaction is valid for the card type.
B. verify the format of the number entered then locate it on the database.
C. ensure that the transaction entered is within the cardholder's credit limit.
D. confirm that the card is not shown as lost or stolen on the master file.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed. A validation control in data capture will ensure that the data entered is valid (i.e., it can be processed by the system). If the data captured in the initial validation is not valid (if the card number or PIN do not match with the database), then the card will be rejected or captured per the controls in place. Once initial validation is completed, then other validations specific to the card and cardholder would be performed.

QUESTION 604
A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

A. Key verification
B. One-for-one checking
C. Manual recalculations
D. Functional acknowledgements

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. All the other choices are manual input controls, whereas data mapping deals with automatic integration of data in the receiving company.

B.

QUESTION 605

A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy: A. payroll reports should be compared to input forms.

gross payroll should be recalculated manually.

C. checks (cheques) should be compared to input forms.

D. checks (cheques) should be reconciled with output reports.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports. Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques)have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

QUESTION 606

Which of the following represents the GREATEST potential risk in an EDI environment?

A. Transaction authorization

B. Loss or duplication of EDI transmissions

C. Transmission delay

D. Deletion or manipulation of transactions prior to or after establishment of application controls

Correct Answer: A
Section: Protection of Information Assets
Explanation

C.

Explanation/Reference:

Explanation:

Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk. Choices B and D are examples of risks, but the impact is not as great as that of unauthorized transactions. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed; however, there will be no loss of data.

QUESTION 607

When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

A. Use of a cryptographic hashing algorithm
B. Enciphering the message digest
   Deciphering the message digest
D. A sequence number and time stamp

Correct Answer: D

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

When transmitting data, a sequence number and/or time stamp built into the message to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed. This is known as replay protection, and could be used to verify that a payment instruction was not duplicated. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the transaction. When the message is deciphered by the receiver using the sender's public key, it ensures that the message could only have come from the sender. This process of sender authentication achieves nonrepudiation.

QUESTION 608

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

A. not be concerned since there may be other compensating controls to mitigate the risks.
B. ensure that overrides are automatically logged and subject to review.
C. verify whether all such overrides are referred to senior management for approval.
D. recommend that overrides not be permitted.

D.
Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log. An IS auditor should not assume that compensating controls exist. As long as the overrides are policy- compliant, there is no need for senior management approval or a blanket prohibition.

QUESTION 609
The GREATEST advantage of using web services for the exchange of information between two systems is:

A. secure communications.
B. improved performance.

C. efficient interfacing.
D. enhanced documentation.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

QUESTION 610
An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

A. reverse engineering.
B. prototyping.
C. software reuse.
D. reengineering.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

QUESTION 611
An IS auditor performing an application maintenance audit would review the log of program changes for the:

A. authorization of program changes.
B. creation date of a current object module.
C. number of program changes actually made.
D. creation date of a current source program.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a changelog would most likely contain date information for the source and executable modules.

QUESTION 612
After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?

A. Stress
B. Black box
C. Interface
D. System

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.

QUESTION 613

When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?

A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.
B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
C. A single implementation is planned, immediately decommissioning the legacy system.
D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risks. Decommissioning or disposing of the old hardware would complicate any fallback strategy, should the new system not operate correctly. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

QUESTION 614
Which of the following reports should an IS auditor use to check compliance with a service level agreements (SLA) requirement for uptime?

A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

QUESTION 615
A benefit of quality of service (QoS) is that the:

A. entire network's availability and performance will be significantly improved.
B. telecom carrier will provide the company with accurate service-level compliance reports.
C. participating applications will have guaranteed service levels.
D. communications link will be supported by security controls to perform secure online transactions.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The main function of QoS is to optimize network performance by assigning priority to business applications and end users, through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

QUESTION 616
An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

A. Overall number of users supported
B. Percentage of incidents solved in the first call
C. Number of incidents reported to the help desk
D. Number of agents answering the phones

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since it is about service level (performance) indicators, the percentage of incidents solved on the first call is the only option that is relevant. Choices A, C and D are not quality measures of the help desk service.

QUESTION 617
During a human resources (HR) audit, an IS auditor is informed that there is a verbal agreement between the IT and HR departments as to the level of IT services expected. In this situation, what should the IS auditor do FIRST?

A. Postpone the audit until the agreement is documented
B. Report the existence of the undocumented agreement to senior management
C. Confirm the content of the agreement with both departments
D. Draft a service level agreement (SLA) for the two departments

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor should first confirm and understand the current practice before making any recommendations. The agreement can be documented after it has been established that there is an agreement in place. The fact that there is not a written agreement does not justify postponing the audit, and reporting to senior management is not necessary at this stage of the audit. Drafting a service level agreement (SLA) is not the IS auditor's responsibility.

QUESTION 618
Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

A. The use of diskless workstations
B. Periodic checking of hard drives
C. The use of current antivirus software
D. policies that result in instant dismissal if violated

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software, unless the software contains a virus. Diskless workstations act as a preventive control and are not effective, since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

QUESTION 619
Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

A. A system downtime log
B. Vendors' reliability figures
C. Regularly scheduled maintenance log
D. A written preventive maintenance schedule

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

QUESTION 620
Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

A. Sensitive data can be read by operators.
B. Data can be amended without authorization.
C. Unauthorized report copies can be printed.
D. Output can be lost in the event of system failure.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operations. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

QUESTION 621
Which of the following is a network diagnostic tool that monitors and records network information?

A. Online monitor
B. Downtime report
C. Help desk report
D. Protocol analyzer

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

QUESTION 622
An intruder accesses an application server and makes changes to the system log. Which of the following would enable the identification of the changes?

A. Mirroring the system log on another server
B. Simultaneously duplicating the system log on a write-once disk
C. Write-protecting the directory containing the system log
D. Storing the backup of the system log offsite

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write-protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

QUESTION 623
The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:

A. compression software to minimize transmission duration.
B. functional or message acknowledgments.
C. a packet-filtering firewall to reroute messages.
D. leased asynchronous transfer mode lines.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Leased asynchronous transfer mode lines are a way to avoid using public and shared infrastructures from the carrier or Internet service provider that have a greater number of communication failures. Choice A, compression software, is a valid way to reduce the problem, but is not as good as leased asynchronous transfer mode lines. Choice B is a control based on higher protocol layers and helps if communication lines are introducing noise, but not if a link is down. Choice C, a packetfiltering firewall, does not reroute messages.

QUESTION 624
Which of the following BEST limits the impact of server failures in a distributed environment?
A. Redundant pathways
B. Clustering
C. Dial backup lines
D. Standby power

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Clustering allows two or more servers to work as a unit, so that when one of them fails, the other takes over. Choices A and C are intended to minimize the impact of channel communications failures, but not a server failure. Choice D provides an alternative power source in the event of an energy failure.

QUESTION 625
An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?

A. Staging and job set up
B. Supervisory review of logs
C. Regular back-up of tapes
D. Offsite storage of tapes

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If the IS auditor finds that there are effective staging and job set up processes, this can be accepted as a compensating control. Choice B is a detective control while choices C and D are corrective controls, none of which would serve as good compensating controls.

QUESTION 626
To verify that the correct version of a data file was used for a production run, an IS auditor should review:

A. operator problem reports.
B. operator work schedules.
C. system logs.
D. output distribution reports.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
System logs are automated reports which identify most of the activities performed on the computer. Programs that analyze the system log have been developed to report on specifically defined items. The auditor can then carry out tests to ensure that the correct file version was used for a production run. Operator problem reports are used by operators to log computer operation problems. Operator work schedules are maintained to assist in human resources planning. Output distribution reports identify all application reports generated and their distribution.

QUESTION 627
Doing which of the following during peak production hours could result in unexpected downtime?

A. Performing data migration or tape backup
B. Performing preventive maintenance on electrical systems
C. Promoting applications from development to the staging environment
D. Replacing a failed power supply in the core router of the data center

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choices A and C are processing events which may impact performance, but would not cause downtime. Enterprise-class routers have redundant hot-swappable power supplies, so replacing a failed power supply should not be an issue. Preventive maintenance activities should be scheduled for non-peak times of the day, and preferably during a maintenance window time period. A mishap or incident caused by a maintenance worker could result in unplanned downtime.

QUESTION 628
An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

A. Consistency
B. Isolation
C. Durability
D. Atomicity

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Atomicity guarantees that either the entire transaction is processed or none of it is. Consistency ensures that the database is in a legal state when the transaction begins and ends, isolation means that, while in an intermediate state, the transaction data is invisible to external operations. Durability guarantees that a successful transaction will persist, and cannot be undone.

QUESTION 629
During maintenance of a relational database, several values of the foreign key in a transaction table of a relational database have been corrupted. The consequence is that:

A. the detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processed.
B. there is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transactions.
C. the database will immediately stop execution and lose more information.
D. the database will no longer accept input data.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When the external key of a transaction is corrupted or lost, the application system will normally be incapable of directly attaching the master data to the transaction data. This will normally cause the system to undertake a sequential search and slow down the processing. If the concerned files are big, this slowdown will be unacceptable. Choice B is incorrect, since a system can recover the corrupted external key by reindexing the table. Choices C and D would not result from a corrupted foreign key.

QUESTION 630
In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

Correct Answer:
Section: Protection of Information Assets

Explanation

Explanation/Reference:

A. Foreign key
B. Primary key
C. Secondary key
D. Public key

A

Explanation:
In a relational database with referential integrity, the use of foreign keys would prevent events such as primary key changes and record deletions, resulting in orphaned relations within the database. It should not be possible to delete a row from a customer table when the customer number (primary key) of that row is stored with live orders on the orders table (the foreign key to the customer table). A primary key works in one table, so it is not able to provide/ensure referential integrity by itself. Secondary keys that are not foreign keys are not subject to referential integrity checks. Public key is related to encryption and not linked in any way to referential integrity.

QUESTION 631
A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

A. concurrent access.
B. deadlocks.
C. unauthorized access to data.
D. a loss of data integrity.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity. Deadlocks are not caused by denormalization. Access to data is controlled by defining user rights to information, and is not affected by denormalization.

Correct Answer:
Section: Protection of Information Assets

Explanation

Explanation/Reference:

QUESTION 632

An IS auditor finds that, at certain times of the day, the data warehouse query performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?

A. Permanent table-space allocation
B. Commitment and rollback controls
C. User spool and database limit controls
D. Read/write access log controls

C

Explanation:

User spool limits restrict the space available for running user queries. This prevents poorly formed queries from consuming excessive system resources and impacting general query performance. Limiting the space available to users in their own databases prevents them from building excessively large tables. This helps to control space utilization which itself acts to help performance by maintaining a buffer between the actual data volume stored and the physical device capacity. Additionally, it prevents users from consuming excessive resources in ad hoc table builds (as opposed to scheduled production loads that often can run overnight and are optimized for performance purposes), in a data warehouse, since you are not running online transactions, commitment and rollback does not have an impact on performance. The other choices are not as likely to be the root cause of this performance issue.

QUESTION 633

Which of the following is MOST directly affected by network performance monitoring tools?

A. Integrity
B. Availability
C. Completeness
D. Confidentiality

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Correct Answer:
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation:
In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

QUESTION 634
A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:

A. analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.
B. WAN capacity is adequate for the maximum traffic demands since saturation has not been reached.
C. the line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.
D. users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.

A

Correct Answer:
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation:
The peak at 96 percent could be the result of a one-off incident, e.g., a user downloading a large amount of data; therefore, analysis to establish whether this is a regular pattern and what causes this behavior should be carried out before expenditure on a larger line capacity is recommended. Since the link provides for a standby database, a short loss of this service should be acceptable. If the peak is established to be a regular occurrence without any other opportunities for mitigation (usage of bandwidth reservation protocol, or other types of prioritizing network traffic), the line should be replaced as there is the risk of loss of service as the traffic approaches 100 percent. If, however, the peak is a one-off or can be put in other time frames, then user education may be an option.

QUESTION 635
While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:

A. recommend the use of disk mirroring.
B. review the adequacy of offsite storage.
C. review the capacity management process.
D. recommend the use of a compression algorithm.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Capacity management is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively. Business criticality must be considered before recommending a disk mirroring solution and offsite storage is unrelated to the problem. Though data compression may save disk space, it could affect system performance.

QUESTION 636
Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

A. Assess the impact of patches prior to installation.
B. Ask the vendors for a new software version with all fixes included.
C. install the security patch immediately.
D. Decline to deal with these vendors in the future.

Correct Answer: A

Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. To install the patch without knowing what it might affect could easily cause problems. New software versions withal fixes included are not always available and a full installation could be time consuming. Declining to deal with vendors does not take care of the flaw.

QUESTION 637
Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

A. Review software migration records and verify approvals.
B. identify changes that have occurred and verify approvals.
C. Review change control documentation and verify approvals.
D. Ensure that only appropriate staff can migrate changes into production.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most effective method is to determine through code comparisons what changes have been made and then verify that they have been approved. Change control records and software migration records may not have all changes listed. Ensuring that only appropriate staff can migrate changes into production is a key control process, but in itself does not verify compliance.

QUESTION 638
An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

A. Analyze the need for the structural change.
B. Recommend restoration to the originally designed structure.
C. Recommend the implementation of a change control process.
D. Determine if the modifications were properly approved.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the IS auditor find that the structural modification had not been approved.

QUESTION 639
A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

A. Comparing source code
B. Reviewing system log files
C. Comparing object code
D. Reviewing executable and source code integrity

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Reviewing system log files is the only trail that may provide information about the unauthorized activities in the production library. Source and object code comparisons are ineffective, because the original programs were restored and do not exist. Reviewing executable and source code integrity is an ineffective control, because integrity between the executable and source code is automatically maintained.

QUESTION 640
The purpose of code signing is to provide assurance that:

A. the software has not been subsequently modified.
B. the application can safely interface with another signed application.
C. the signer of the application is trusted.
D. the private key of the signer has not been compromised.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Code signing can only ensure that the executable code has not been modified after being signed. The other choices are incorrect and actually represent potential and exploitable weaknesses of code signing.

QUESTION 641
To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

A. examine the change control system records and trace them forward to object code files.
B. review access control permissions operating within the production program libraries.
C. examine object code to find instances of changes and trace them back to change control records.
D. review change approved designations established within the change control system.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The procedure of examining object code files to establish instances of code changes and tracing these back to change control system records is a substantive test that directly addresses the risk of unauthorized code changes. The other choices are valid procedures to apply in a change control audit but they do not directly address the risk of unauthorized code changes.

QUESTION 642
After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

A. Differential reporting
B. False-positive reporting
C. False-negative reporting
D. Less-detail reporting

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
False-negative reporting on weaknesses means the control weaknesses in the network are not identified and therefore may not be addressed, leaving the network vulnerable to attack. False- positive reporting is one in which the controls are in place, but are evaluated as weak, which should prompt a rechecking of the controls. Less-detail reporting and differential reporting functions provided by these tools compare scan results over a period of time.

QUESTION 643
Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

A. Install the vendor's security fix for the vulnerability.

B. Block the protocol traffic in the perimeter firewall.
C. Block the protocol traffic between internal network segments.
D. Stop the service until an appropriate security fix is installed.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Stopping the service and installing the security fix is the safest way to prevent the worm from spreading, if the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits any software that utilizes it from working between segments.

QUESTION 644
Which of the following would be an indicator of the effectiveness of a computer security incident response team?

A. Financial impact per security incident
B. Number of security vulnerabilities that were patched

C. Percentage of business applications that are being protected
D. Number of successful penetration tests

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most important indicator is the financial impact per security incident. Choices B, C and D could be measures of effectiveness of security, but would not be a measure of the effectiveness of a response team.

QUESTION 645
Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

A. Firewalls
B. Routers
C. Layer 2 switches
D. VLANs

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Firewall systems are the primary tool that enable an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls. Routers can filter packets based on parameters, such as source address, but are not primarily a security tool. Based on Media Access Control (MAC) addresses, layer 2 switches separate traffic in a port as different segments and without determining if it is authorized or unauthorized traffic. A virtual LAN (VLAN) is a functionality of some switches that allows them to switch the traffic between different ports as if they are in the same LAN. Nevertheless, they do not deal with authorized vs. unauthorized traffic.

QUESTION 646

An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

A. compromises the Wireless Application Protocol (WAP) gateway.
B. installs a sniffing program in front of the server.
C. steals a customer's PDA.
D. listens to the wireless transmission.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In a WAP gateway, the encrypted messages from customers must be decrypted to transmit over the Internet and vice versa. Therefore, if the gateway is compromised, all of the messages would be exposed. SSL protects the messages from sniffing on the Internet, limiting disclosure of the customer's information. WTLS provides authentication, privacy and integrity and prevents messages from eavesdropping.

QUESTION 647
Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

A. Filters
B. Switches
C. Routers
D. Firewalls

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Switches are at the lowest level of network security and transmit a packet to the device to which it is addressed. This reduces the ability of one device to capture the packets that are meant for another device. Filters allow for some basic isolation of network traffic based on the destination addresses. Routers allow packets to

be given or denied access based on the addresses of the sender and receiver and the type of packet. Firewalls are a collection of computer and network equipment used to allow communications to flow out of the organization and restrict communications flowing into the organization.

QUESTION 648
In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

A. Diskless workstations
B. Data encryption techniques
C. Network monitoring devices
D. Authentication systems

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Network monitoring devices may be used to inspect activities from known or unknown users and can identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a detective control. Diskless workstations prevent access control software from being bypassed. Data encryption techniques can help protect sensitive or propriety data from unauthorized access, thereby serving as a preventive control. Authentication systems may provide environment wide, logical facilities that can differentiate among users, before providing access to systems.

QUESTION 649
Which of the following is a control over component communication failure/errors?

A. Restricting operator access and maintaining audit trails
B. Monitoring and reviewing system engineering activity
C. Providing network redundancy
D. Establishing physical barriers to the data transmitted over the network

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Redundancy by building some form of duplication into the network components, such as a link, router or switch to prevent loss, delays or data duplication is a control over component communication failure or error. Other related controls are loop/echochecks to detect line errors, parity checks, error correction codes and sequence checks. Choices A, B and D are communication network controls.

QUESTION 650
An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

A. Electromagnetic interference (EMI)
B. Cross-talk
C. Dispersion
D. Attenuation

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around 100 meters. Electromagnetic interference (EMl) is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross-talk has nothing to do with the length of the UTP cable.

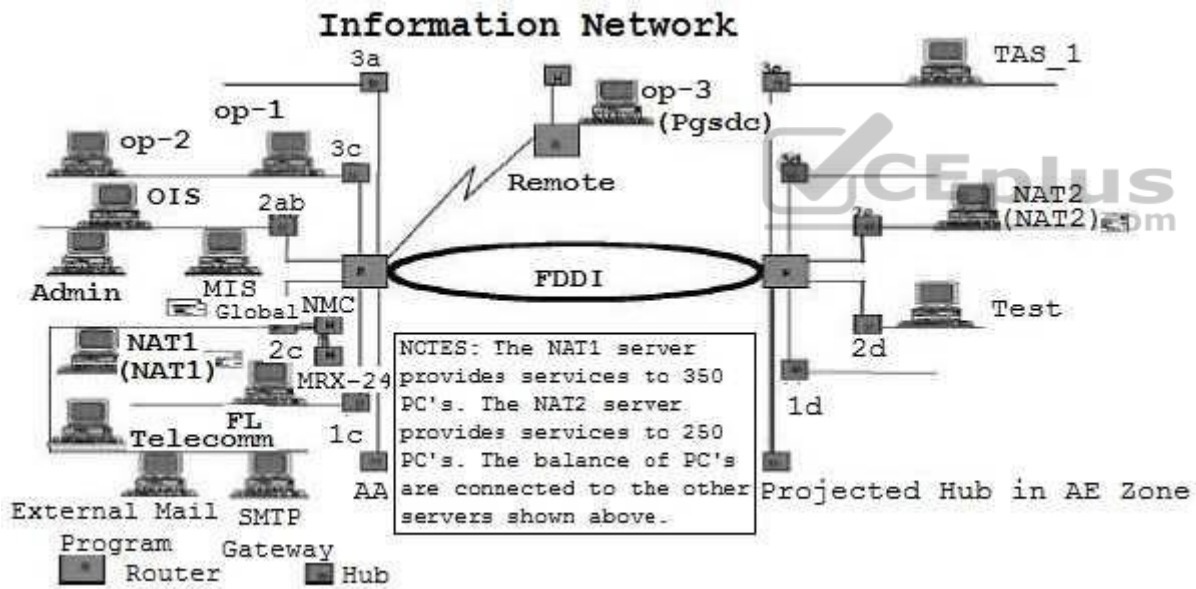
QUESTION 651
Neural networks are effective in detecting fraud because they can:

A. discover new trends since they are inherently linear.
B. solve problems where large and general sets of training data are not obtainable.
C. attack problems that require consideration of a large number of input variables.
D. make assumptions about the shape of any curve relating variables to the output.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, but they will not discover new trends. Neural networks are inherently nonlinear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.

QUESTION 652
For locations 3a, 1d and 3d, the diagram indicates hubs with lines that appear to be open and active. Assuming that is true, what control, if any, should be recommended to mitigate this weakness?



A. Intelligent hub
B. Physical security over the hubs
C. Physical security and an intelligent hub
D. No controls are necessary since this is not a weakness

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Open hubs represent a significant control weakness because of the potential to access a network connection easily. An intelligent hub would allow the deactivation of a single port while leaving the remaining ports active. Additionally, physical security would also provide reasonable protection over hubs with active ports.

QUESTION 653
In what way is a common gateway interface (CGI) MOST often used on a webserver?

A. Consistent way for transferring data to the application program and back to the user
B. Computer graphics imaging method for movies and TV
C. Graphic user interface for web design
D. interface to access the private gateway domain

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word orienteering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

QUESTION 654
The most likely error to occur when implementing a firewall is:

A. incorrectly configuring the access lists.
B. compromising the passwords due to social engineering.
C. connecting a modem to the computers in the network.

D. inadequately protecting the network and server from virus attacks.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An updated and flawless access list is a significant challenge and, therefore, has the greatest chance for errors at the time of the initial installation. Passwords do not apply to firewalls, a modem bypasses a firewall and a virus attack is not an element in implementing a firewall.

QUESTION 655
Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

A. Simple Network Management Protocol
B. File Transfer Protocol
C. Simple Mail Transfer Protocol
D. Telnet

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The Simple Network Management Protocol provides a means to monitor and control network devices and to manage configurations and performance. The File Transfer Protocol (FTP) transfers files from a computer on the Internet to the user's computer and does not have any functionality related to monitoring network devices. Simple Mail Transfer Protocol (SMTP) is a protocol for sending and receiving e-mail messages and does not provide any monitoring or management for network devices. Telnet is a standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were connected to a local system; it does not provide any monitoring or management of network devices.

QUESTION 656
Which of the following types of transmission media provide the BEST security against unauthorized access?

A. Copper wire

B. Twisted pair
C. Fiberoptic cables
D. Coaxial cables

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Fiberoptic cables have proven to be more secure than the other media. Satellite transmission and copper wire can be violated with inexpensive equipment. Coaxial cable can also be violated more easily than other transmission media.

QUESTION 657
When auditing a proxy-based firewall, an IS auditor should:

A. verify that the firewall is not dropping any forwarded packets.
B. review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresses.
C. verify that the filters applied to services such as HTTP are effective.
D. test whether routing information is forwarded by the firewall.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A proxy-based firewall works as an intermediary (proxy) between the service or application and the client, it makes a connection with the client and opens a different connection with the server and, based on specific filters and rules, analyzes all the traffic between the two connections.
Unlike a packet-filtering gateway, a proxy-based firewall does not forward any packets. Mapping between media access control (MAC) and IP addresses is a task for protocols such as Address Resolution Protocol/Reverse Address Resolution Protocol (ARP/RARP).

QUESTION 658
An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

A. Simple Object Access Protocol (SOAP)
B. Address Resolution Protocol (ARP)
C. Routing Information Protocol (RIP)
D. Transmission Control Protocol (TCP)

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Address Resolution Protocol (ARP) provides dynamic address mapping between an IP address and hardware address. Simple Object Access Protocol (SOAP) is a platform- independent XML- based protocol, enabling applications to communicate with each other over the Internet, and does not deal with media access control (MAC) addresses. Routing Information Protocol (RIP) specifies how routers exchange routing table information. Transmission Control Protocol (TCP) enables two hosts to establish a connection and exchange streams of data.

QUESTION 659
The MAIN reason for requiring that all computer clocks across an organization be synchronized is to:

A. prevent omission or duplication of transactions.
B. ensure smooth data transition from client machines to servers.
C. ensure that e-mail messages have accurate time stamps.
D. support the incident investigation process.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
During an investigation of incidents, audit logs are used as evidence, and the time stamp information in them is useful. If the clocks are not synchronized, investigations will be more difficult because a time line of events might not be easily established. Time-stamping a transaction has nothing to do with the update itself. Therefore, the possibility of omission or duplication of transactions does not exist. Data transfer has nothing to do with the time stamp. While the time stamp on an e-mail may not be accurate, this is not a significant issue.

QUESTION 660

When reviewing the configuration of network devices, an IS auditor should FIRST identify:

A. the best practices for the type of network devices deployed.
B. whether components of the network are missing.
C. the importance of the network device in the topology.
D. whether subcomponents of the network are being used appropriately.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The first step is to understand the importance and role of the network device within the organization's network topology. After understanding the devices in the network, the best practice for using the device should be reviewed to ensure that there are no anomalies within the configuration. Identification of which component or subcomponent is missing or being used inappropriately can only be known upon reviewing and understanding the topology and the best practice for deployment of the device in the network.

QUESTION 661
Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?
A. System analysis
B. Authorization of access to data
C. Application programming
D. Data administration

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The application owner is responsible for authorizing access to data. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

QUESTION 662
To determine who has been given permission to use a particular system resource, an IS auditor should review:

A. activity lists.
B. access control lists.
C. logon ID lists.
D. password lists.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Access control lists are the authorization tables that document the users who have been given permission to use a particular system resource and the types of access they have been granted. The other choices would not document who has been given permission to use (access) specific system resources.

QUESTION 663
What is the MOST effective method of preventing unauthorized use of data files?

A. Automated file entry
B. Tape librarian
C. Access control software
D. Locked library

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Access control software is an active control designed to prevent unauthorized access to data.

QUESTION 664

Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:

A. change the company's security policy.
B. educate users about the risk of weak passwords.
C. build in validations to prevent this during user creation and password change.
D. require a periodic review of matching user ID and passwords for detection and correction.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risks of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

QUESTION 665
Which of the following exposures could be caused by a line grabbing technique?

A. Unauthorized data access
B. Excessive CPU cycle usage
C. Lockout of terminal polling
D. Multiplexor control dysfunction

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Line grabbing will enable eavesdropping, thus allowing unauthorized data access, it will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

QUESTION 666
With the help of a security officer, granting access to data is the responsibility of:

A. data owners.
B. programmers.
C. system analysts.
D. librarians.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners' approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (e.g., read or update).

QUESTION 667
The FIRST step in data classification is to:

A. establish ownership.
B. perform a criticality analysis.
C. define access rules.
D. create a data dictionary.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data classification is necessary to define access rules based on a need-to-do and need-to- know basis. The data owner is responsible for defining the access rules; therefore, establishing ownership is the first step in data classification. The other choices are incorrect. A criticality analysis is required for protection of data, which

takes input from data classification. Access definition is complete after data classification and input for a data dictionary is prepared from the data classification process.

QUESTION 668
A hacker could obtain passwords without the use of computer tools or programs through the technique of:

A. social engineering.
B. sniffers.
C. back doors.
D. Trojan horses.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Social engineering is based on the divulgence of private information through dialogues, interviews, inquiries, etc., in which a user may be indiscreet regarding their or someone else's personal data. A sniffer is a computer tool to monitor the traffic in networks. Back doors are computer programs left by hackers to exploit vulnerabilities. Trojan horses are computer programs that pretend to supplant a real program; thus, the functionality of the program is not authorized and is usually malicious in nature.

QUESTION 669
Which of the following is an example of the defense in-depth security principle?

A. Using two firewalls of different vendors to consecutively check the incoming network traffic
B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic
C. Having no physical signs on the outside of a computer center building
D. Using two firewalls in parallel to check different types of incoming traffic

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Defense in-depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

QUESTION 670
An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

A. Piggybacking
B. Dumpster diving
C. Shoulder surfing
D. Impersonation

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If a password is displayed on a monitor, any person nearby could look over the shoulder of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to 'the display of passwords.' If the policy referred to 'the display and printing of passwords' then it would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information), impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

QUESTION 671
To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

A. the company policy be changed.
B. passwords are periodically changed.
C. an automated password management tool be used.
D. security awareness training is delivered.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing their old password for a designated period of time. Choices A, B and D do not enforce compliance.

QUESTION 672
An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

A. more than one individual can claim to be a specific user.
B. there is no way to limit the functions assigned to users.
C. user accounts can be shared.
D. users have a need-to-know privilege.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Without an appropriate authorization process, it will be impossible to establish functional limits and accountability. The risk that more than one individual can claim to be a specific user is associated with the authentication processes, rather than with authorization. The risk that user accounts can be shared is associated with identification processes, rather than with authorization. The need-to-know basis is the best approach to assigning privileges during the authorization process.

QUESTION 673
An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

A. Digitalized signatures
B. Hashing
C. Parsing
D. Steganography

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Steganography is a technique for concealing the existence of messages or information. An increasingly important stenographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes, and is widely applied in the design of programming languages or in data entry editing.

QUESTION 674
The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

A. Piggybacking
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have their badge read at every controlled door no unauthorized person could enter the sensitive area. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

QUESTION 675

Which of the following presents an inherent risk with no distinct identifiable preventive controls?

A. Piggybacking
B. Viruses
C. Data diddling
D. Unauthorized application shutdown

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses, because it requires limited technical knowledge and occurs before computer security can protect the data. There are only compensating controls for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-re plicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdown of an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which is effective if there are proper access controls.

QUESTION 676
Which of the following is a general operating system access control function?

A. Creating database profiles
B. Verifying user authorization at a field level
C. Creating individual accountability
D. Logging database access activities for monitoring access violation

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Creating individual accountability is the function of the general operating system. Creating database profiles, verifying user authorization at a field level and logging database access activities for monitoring access violations are all database-level access control functions.

QUESTION 677
For a discretionary access control to be effective, it must:

A. operate within the context of mandatory access controls.
B. operate independently of mandatory access controls.
C. enable users to override mandatory access controls when necessary.
D. be specifically permitted by the security policy.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Mandatory access controls are prohibitive; anything that is not expressly permitted is forbidden. Only within this context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. When systems enforce mandatory access control policies, they must distinguish between these and the mandatory access policies that offer more flexibility.
Discretionary controls do not override access controls and they do not have to be permitted in the security policy to be effective.

QUESTION 678
An organization has been recently downsized, in light of this, an IS auditor decides to test logical access controls. The IS auditor's PRIMARY concern should be that:

A. all system access is authorized and appropriate for an individual's role and responsibilities.
B. management has authorized appropriate access for all newly-hired individuals.
C. only the system administrator has authority to grant or modify access to individuals.
D. access authorization forms are used to grant or modify access to individuals.

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The downsizing of an organization implies a large number of personnel actions over a relatively short period of time. Employees can be assigned new duties while retaining some or all of their former duties. Numerous employees may be laid off. The auditor should be concerned that an appropriate segregation of duties is maintained, that access is limited to what is required for an employee's role and responsibilities, and that access is revoked for those that are no longer employed by the organization. Choices B, C and D are all potential concerns of an IS auditor, but in light of the particular risks associated with a downsizing, should not be the primary concern.

QUESTION 679
The logical exposure associated with the use of a checkpoint restart procedure is:

A. denial of service.
B. an asynchronous attack
C. wire tapping.
D. computer shutdown.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Asynchronous attacks are operating system-based attacks. A checkpoint restart is a feature that stops a program at specified intermediate points for later restart in an orderly manner without losing data at the checkpoint. The operating system saves a copy of the computer programs and data in their current state as well as several system parameters describing the mode and security level of the program at the time of stoppage. An asynchronous attack occurs when an individual with access to this information is able to gain access to the checkpoint restart copy of the system parameters and change those parameters such that upon restart the program would function at a higher-priority security level.

QUESTION 680
Which of the following would prevent unauthorized changes to information stored in a server's log?

A. Write-protecting the directory containing the system log
B. Writing a duplicate log to another server

C. Daily printing of the system log
D. Storing the system log in write-once media

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Storing the system log in write-once media ensures the log cannot be modified. Write- protecting the system log does not prevent deletion or modification, since the superuser or users that have special permission can override the write protection. Writing a duplicate log to another server or daily printing of the system log cannot prevent unauthorized changes.

QUESTION 681
After reviewing its business processes, a large organization is deploying a new web application based on a VoIP technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

A. Fine-grained access control
B. Role-based access control (RBAC)
C. Access control lists
D. Network/service access control

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Authorization in this VoIP case can best be addressed by role-based access control (RBAC) technology. RBAC is easy to manage and can enforce strong and efficient access controls in large-scale web environments including VoIP implementation. Access control lists and fine- grained access control on VoIP web applications do not scale to enterprise wide systems, because they are primarily based on individual user identities and their specific technical privileges. Network/ service addresses VoIP availability but does not address application-level access or authorization.

QUESTION 682
In an online banking application, which of the following would BEST protect against identity theft?

A. Encryption of personal password
B. Restricting the user to a specific terminal
C. Two-factor authentication
D. Periodic review of access logs

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Two-factor authentication requires two independent methods for establishing identity and privileges. Factors include something you know, such as a password; something you have, such as a token; and something you are, which is biometric. Requiring two of these factors makes identity theft more difficult. A password could be guessed or broken. Restricting the user to a specific terminal is not a practical alternative for an online application. Periodic review of access logs is a detective control and does not protect against identity theft.

QUESTION 683
The responsibility for authorizing access to application data should be with the:

A. data custodian.
B. database administrator (DBA).
C. data owner.
D. security administrator.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data owners should have the authority and responsibility for granting access to the data and applications for which they are responsible. Data custodians are responsible only for storing and safeguarding the data. The database administrator (DBA) is responsible for managing the database and the security administrator is responsible for implementing and maintaining IS security. The ultimate responsibility for data resides with the data owner.

QUESTION 684

During an audit of the logical access control of an ERP financial system an IS auditor found some user accounts shared by multiple individuals. The user IDs were based on roles rather than individual identities. These accounts allow access to financial transactions on the ERP. What should the IS auditor do next?

A. Look for compensating controls.
B. Review financial transactions logs.
C. Review the scope of the audit.
D. Ask the administrator to disable these accounts.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The best logical access control practice is to create user IDs for each individual to define accountability. This is possible only by establishing a one-to-one relationship between IDs and individuals. However, if the user IDs are created based on role designations, an IS auditor should first understand the reasons and then evaluate the effectiveness and efficiency of compensating controls. Reviewing transactions logs is not relevant to an audit of logical access control nor is reviewing the scope of the audit relevant. Asking the administrator to disable the shared accounts should not be recommended by an IS auditor before understanding the reasons and evaluating the compensating controls. It is not an IS auditor's responsibility to ask for disabling accounts during an audit.

QUESTION 685
An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:

A. accept the DBA access as a common practice.
B. assess the controls relevant to the DBA function.
C. recommend the immediate revocation of the DBA access to production data.
D. review user access authorizations approved by the DBA.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is good practice when finding a potential exposure to look for the best controls. Though granting the database administrator (DBA) access to production data might be a common practice, the IS auditor should evaluate the relevant controls. The DBA should have access based on a need-to- know and need-to-do basis;

therefore, revocation may remove the access required. The DBA, typically, may need to have access to some production data. Granting user authorizations is the responsibility of the data owner and not the DBA.

QUESTION 686
A technical lead who was working on a major project has left the organization. The project manager reports suspicious system activities on one of the servers that is accessible to the whole team. What would be of GREATEST concern if discovered during a forensic investigation?

A. Audit logs are not enabled for the system
B. A logon ID for the technical lead still exists
C. Spyware is installed on the system
D. A Trojan is installed on the system

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Audit logs are critical to the investigation of the event; however, if not enabled, misuse of the logon ID of the technical lead and the guest account could not be established. The logon ID of the technical lead should have been deleted as soon as the employee left the organization but, without audit logs, misuse of the ID is difficult to prove. Spyware installed on the system is a concern but could have been installed by any user and, again, without the presence of logs, discovering who installed the spyware is difficult. A Trojan installed on the system is a concern, but it can be done by any user as it is accessible to the whole group and, without the presence of logs, investigation would be difficult.

QUESTION 687
An IS auditor should expect the responsibility for authorizing access rights to production data and systems to be entrusted to the:

A. process owners.
B. system administrators.
C. security administrator.
D. data owners.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data owners are primarily responsible for safeguarding the data and authorizing access to production data on a need-to-know basis.

QUESTION 688
Which of the following would MOST effectively enhance the security of a challenge- response based authentication system?

A. Selecting a more robust algorithm to generate challenge strings
B. implementing measures to prevent session hijacking attacks
C. increasing the frequency of associated password changes
D. increasing the length of authentication strings

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Challenge response-based authentication is prone to session hijacking or man-in-the- middle attacks. Security management should be aware of this and engage in risk assessment and control design when they employ this technology. Selecting a more robust algorithm will enhance the security; however, this may not be as important in terms of risk when compared to man-in- the-middle attacks. Choices C and D are good security practices; however, they are not as effective a preventive measure. Frequently changing passwords is a good security practice; however, the exposures lurking in communication pathways may pose a greater risk.

QUESTION 689
Which of the following should an IS auditor recommend for the protection of specific sensitive information stored in the data warehouse?

A. implement column- and row-level permissions
B. Enhance user authentication via strong passwords
C. Organize the data warehouse into subject matter-specific databases
D. Log user access to the data warehouse

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choice A specifically addresses the question of sensitive data by controlling what information users can access. Column-level security prevents users from seeing one or more attributes on a table. With row-level security a certain grouping of information on a table is restricted; e.g., if a table held details of employee salaries, then a restriction could be put in place to ensure that, unless specifically authorized, users could not view the salaries of executive staff. Column- and row-level security can be achieved in a relational database by allowing users to access logical representations of data rather than physical tables. This 'fine-grained' security model is likely to offer the best balance between information protection while still supporting a wide range of analytical and reporting uses. Enhancing user authentication via strong passwords is a security control that should apply to all users of the data warehouse and does not specifically address protection of sensitive data. Organizing a data warehouse into subject-specific databases is a potentially useful practice but, in itself, does not adequately protect sensitive data. Database-level security is normally too 'coarse' a level to efficiently and effectively protect information. For example, one database may hold information that needs to be restricted such as employee salary and customer profitability details while other information such as employee department may need to be legitimately a accessed by a large number of users. Organizing the data warehouse into subject matter-specific databases is similar to user access in that this control should generally apply. Extra attention could be devoted to reviewing access to tables with sensitive data, but this control is not sufficient without strong preventive controls at the column and row level. For choice D, logging user access is important, but it is only a detective control that will not provide adequate protection to sensitive information.

QUESTION 690
What would be the MOST effective control for enforcing accountability among database users accessing sensitive information?

A. implement a log management process
B. implement a two-factor authentication
C. Use table views to access sensitive data
D. Separate database and application servers

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Accountability means knowing what is being done by whom. The best way to enforce the principle is to implement a log management process that would create and store logs with pertinent information such as user name, type of transaction and hour. Choice B, implementing a two- factor authentication, and choice C, using table views to access sensitive data, are controls that would limit access to the database to authorized users but would not resolve the accountability problem. Choice D may help in a better administration or even in implementing access controls but, again, does not address the accountability issues.

QUESTION 691

Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

A. Signature-based
B. Neural networks-based
C. Statistical-based
D. Host-based

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The neural networks-based IDS monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but has the added function of self-learning. Signature-based systems are a type of IDS in which the intrusive patterns identified are stored in the form of signatures. These IDS systems protect against detected intrusion patterns. Statistical-based systems need a comprehensive definition of the known and expected behavior of systems. Host-based systems are not a type of IDS, but a category of IDS, and are configured for a specific environment. They will monitor various internal resources of the operating system to warn of a possible attack.

QUESTION 692
Which of the following cryptography options would increase overhead/cost?

A. The encryption is symmetric rather than asymmetric.
B. A long asymmetric encryption key is used.
C. The hash is encrypted rather than the message.
D. A secret key is used.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Computer processing time is increased for longer asymmetric encryption keys, and the increase may be disproportionate. For example, one benchmark showed that doubling the length of an RSA key from 512 bits to 1,024 bits caused the decrypt time to increase nearly six-fold. An asymmetric algorithm requires more

processing time than symmetric algorithms. A hash is shorter than the original message; therefore, a smaller overhead is required if the hash is encrypted rather than the message. Use of a secret key, as a symmetric encryption key, is generally small and used for the purpose of encrypting user data.

QUESTION 693
Which of the following append themselves to files as a protection against viruses?

A. Behavior blockers
B. Cyclical redundancy checkers (CRCs)
C. Immunizers
D. Active monitors

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Immunizers defend against viruses by appending sections of themselves to files. They continuously check the file for changes and report changes as possible viral behavior. Behavior blockers focus on detecting potentially abnormal behavior, such as writing to the boot sector or the master boot record, or making changes to executable files. Cyclical redundancy checkers compute a binary number on a known virus-free program that is then stored in a database file. When that program is subsequently called to be executed, the checkers look for changes to the files, compare it to the database and report possible infection if changes have occurred. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions.

QUESTION 694
Which of the following acts as a decoy to detect active internet attacks?

A. Honeypots
B. Firewalls
C. Trapdoors
D. Traffic analysis

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Honeypots are computer systems that are expressly set up to attract and trap individuals who attempt to penetrate other individuals' computer systems. The concept of a honeypot is to learn from intruder's actions. A properly designed and configured honeypot provides data on methods used to attack systems. The data are then used to improve measures that could curb future attacks. A firewall is basically a preventive measure. Trapdoors create a vulnerability that provides an opportunity for the insertion of unauthorized code into a system. Traffic analysis is a type of passive attack.

QUESTION 695
Which of the following results in a denial-of-service attack?

A. Brute force attack
B. Ping of death
C. Leapfrog attack
D. Negative acknowledgement (NAK) attack

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of Ping with a packet size higher than 65 KB and no fragmentation flag on will cause a denial of service. A brute force attack is typically a text attack that exhausts all possible key combinations. A leapfrog attack, the act of tenting through one or more hosts to preclude a trace, makes use of user ID and password information obtained illicitly from one host to compromise another host. A negative acknowledgement attack is a penetration technique that capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly, leaving the system in an unprotected state during such interrupts.

QUESTION 696
Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

A. Computation speed
B. Ability to support digital signatures
C. Simpler key distribution
D. Greater strength for a given key length

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The main advantage of elliptic curve encryption over RSA encryption is its computation speed. This method was first independently suggested by Neal Koblitz and Victor S. Miller. Both encryption methods support digital signatures and are used for public key encryption and distribution. However, a stronger key per se does not necessarily guarantee better performance, but rather the actual algorithm employed.

QUESTION 697
Which of the following would be the BEST overall control for an Internet business looking for confidentiality, reliability and integrity of data?

A. Secure Sockets Layer (SSL)
B. Intrusion detection system (IDS)
C. Public key infrastructure (PKI)
D. Virtual private network (VPN)

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
PKI would be the best overall technology because cryptography provides for encryption, digital signatures and non-repudiation controls for confidentiality and reliability. SSL can provide confidentiality. IDS is a detective control. A VPN would provide confidentiality and authentication (reliability).

QUESTION 698
Which of the following would be of MOST concern to an IS auditor reviewing a virtual private network (VPN) implementation? Computers on the network that are located:

A. on the enterprise's internal network.
B. at the backup site.
C. in employees' homes.
D. at the enterprise's remote offices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
One risk of a virtual private network (VPN) implementation is the chance of allowing high- risk computers onto the enterprise's network. All machines that are allowed onto the virtual network should be subject to the same security policy. Home computers are least subject to the corporate security policies, and therefore are high-risk computers. Once a computer is hacked and 'owned/ any network that trusts that computer is at risk. Implementation and adherence to corporate security policy is easier when all computers on the network are on the enterprise's campus. On an enterprise's internal network, there should be security policies in place to detect and halt an outside attack that uses an internal machine as a staging platform. Computers at the backup site are subject to the corporate security policy, and therefore are not high-risk computers. Computers on the network that are at the enterprise's remote offices, perhaps with different IS and security employees who have different ideas about security, are more risky than choices A and B, but obviously less risky than home computers.

QUESTION 699
Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called a:

A. feedback error control.
B. block sum check.
C. forward error control.
D. cyclic redundancy check.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Forward error control involves transmitting additional redundant information with each character or frame to facilitate detection and correction of errors, in feedback error control, only enough additional information is transmitted so the receiver can identify that an error has occurred.
Choices B and D are both error detection methods but not error correction methods. Block sum check is an extension of parity check wherein an additional set of parity bits is computed for a block of characters. A cyclic redundancy check is a technique wherein a single set of check digits is generated, based on the contents of the frame, for each frame transmitted.

QUESTION 700

The security level of a private key system depends on the number of:

A. encryption key bits.
B. messages sent.
C. keys.
D. channels used.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, the algorithm and its complexity make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

QUESTION 701
During what process should router access control lists be reviewed?

A. Environmental review
B. Network security review
C. Business continuity review
D. Data integrity review

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Network security reviews include reviewing router access control lists, port scanning, internal and external connections to the system, etc. Environmental reviews, business continuity reviews and data integrity reviews do not require a review of the router access control lists.

QUESTION 702
Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

A. Analyzer
B. Administration console
C. User interface
D. Sensor

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Sensors are responsible for collecting data. Analyzers receive input from sensors and determine intrusive activity. An administration console and a user interface are components of an IDS.

QUESTION 703
Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

A. Unauthorized access from outside the organization
B. Unauthorized access from within the organization
C. A delay in Internet connectivity
D. A delay in downloading using File Transfer Protocol (FTP)

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Firewalls are meant to prevent outsiders from gaining access to an organization's computer systems through the internet gateway. They form a barrier with the outside world, but are not intended to address access by internal users; they are more likely to cause delays than address such concerns.

QUESTION 704
A digital signature contains a message digest to:

A. show if the message has been altered after transmission.

B. define the encryption algorithm.
C. confirm the identity of the originator.
D. enable message transmission in a digital format.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
The message digest is calculated and included in a digital signature to prove that the message has not been altered. It should be the same value as a recalculation performed upon receipt. It does not define the algorithm or enable the transmission in digital format and has no effect on the identity of the user; it is there to ensure integrity rather than identity.

QUESTION 705
Digital signatures require the:

A. signer to have a public key and the receiver to have a private key.
B. signer to have a private key and the receiver to have a public key.
C. signer and receiver to have a public key.
D. signer and receiver to have a private key.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Digital signatures are intended to verify to a recipient the integrity of the data and the identity of the sender. The digital signature standard is a public key algorithm. This requires the signer to have a private key and the receiver to have a public key.

QUESTION 706
The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is called:

A. data integrity.
B. authentication.

C. non repudiation.
D. replay protection.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
All of the above are features of a digital signature. Non repudiation ensures that the claimed sender cannot later deny generating and sending the message. Data integrity refers to changes in the plaintext message that would result in the recipient failing to compute the same message hash. Since only the claimed sender has the key, authentication ensures that the message has been sent by the claimed sender. Replay protection is a method that a recipient can use to check that the message was not intercepted and replayed.

QUESTION 707
An IS auditor doing penetration testing during an audit of internet connections would:

A. evaluate configurations.
B. examine security settings.
C. ensure virus-scanning software is in use.
D. use tools and techniques available to a hacker.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Penetration testing is a technique used to mimic an experienced hacker attacking a live site by using tools and techniques available to a hacker. The other choices are procedures that an IS auditor would consider undertaking during an audit of Internet connections, but are not aspects of penetration testing techniques.

QUESTION 708
Which of the following controls would BEST detect intrusion?

A. User IDs and user privileges are granted through authorized procedures.

B. Automatic logoff is used when a workstation is inactive for a particular period of time.
C. Automatic logoff of the system occurs after a specified number of unsuccessful attempts.
D. Unsuccessful logon attempts are monitored by the security administrator.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Intrusion is detected by the active monitoring and review of unsuccessful logons. User IDs and the granting of user privileges define a policy, not a control. Automatic logoff is a method of preventing access on inactive terminals and is not a detective control. Unsuccessful attempts to log on are a method for preventing intrusion, not detecting.

QUESTION 709
Which of the following is the MOST effective type of antivirus software?
A. Scanners
B. Active monitors
C. integrity checkers
D. Vaccines

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Integrity checkers compute a binary number on a known virus-free program that is then stored in a database file. This number is called a cyclical redundancy check (CRC). When that program is called to execute, the checker computes the CRC on the program about to be executed and compares it to the number in the database. A match means no infection; a mismatch means that a change in the program has occurred. A change in the program could mean a virus. Scanners look for sequences of bits called signatures that are typical of virus programs. They examine memory, disk boot sectors, executables and command files for bit patterns that match a known virus. Therefore, scanners need to be updated periodically to remain effective. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions.

Active monitors can be misleading, because they cannot distinguish between a user request and a program or virus request. As a result, users are asked to confirm actions like formatting a disk or deleting a file or set of files. Vaccines are known to be good antivirus software. However, they also need to be updated periodically to remain effective.

QUESTION 710
When using public key encryption to secure data being transmitted across a network:

A. both the key used to encrypt and decrypt the data are public.
B. the key used to encrypt is private, but the key used to decrypt the data is public.
C. the key used to encrypt is public, but the key used to decrypt the data is private.
D. both the key used to encrypt and decrypt the data are private.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Public key encryption, also known as asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.

QUESTION 711
The technique used to ensure security in virtual private networks (VPNs) is:
A. encapsulation.
B. wrapping.
C. transform.
D. encryption

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Encapsulation, or tunneling, is a technique used to carry the traffic of one protocol over a network that does not support that protocol directly. The original packet is wrapped in another packet. The other choices are not security techniques specific to VPNs.

QUESTION 712
An internet-based attack using password sniffing can:

A. enable one party to act as if they are another party.
B. cause modification to the contents of certain transactions.
C. be used to gain access to systems containing proprietary information.
D. result in major problems with billing systems and transaction processing agreements.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Password sniffing attacks can be used to gain access to systems on which proprietary information is stored. Spoofing attacks can be used to enable one party to act as if they are another party. Data modification attacks can be used to modify the contents of certain transactions. Repudiation of transactions can cause major problems with billing systems and transaction processing agreements.

QUESTION 713
Which of the following controls would be the MOST comprehensive in a remote access network with multiple and diverse subsystems?

A. Proxy server
B. Firewall installation
C. Network administrator
D. Password implementation and administration

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most comprehensive control in this situation is password implementation and administration. While firewall installations are the primary line of defense, they cannot protect all access and, therefore, an element of risk remains. A proxy server is a type of firewall installation; thus, the same rules apply. The network administrator may serve as a control, but typically this would not be comprehensive enough to serve on multiple and diverse systems.

QUESTION 714
Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity and nonrepudiation by either sender or recipient?

A. The recipient uses their private key to decrypt the secret key.
B. The encrypted prehash code and the message are encrypted using a secret key.
C. The encrypted prehash code is derived mathematically from the message to be sent.
D. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Most encrypted transactions use a combination of private keys, public keys, secret keys, hash functions and digital certificates to achieve confidentiality, message integrity and nonrepudiation by either sender or recipient. The recipient uses the sender's public key to decrypt the prehash code into a posthash code, which when equaling the prehash code, verifies the identity of the sender and that the message has not been changed in route; this would provide the greatest assurance. Each sender and recipient has a private key known only to themselves and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key, and both must be from the same party. A single, secret key is used to encrypt the message, because secret key encryption requires less processing power than using public and private keys. A digital certificate, signed by a certificate authority, validates senders' and recipients' public keys.

QUESTION 715
E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

A. sender's private key and encrypting the message using the receiver's public key.
B. sender's public key and encrypting the message using the receiver's private key.
C. receiver's private key and encrypting the message using the sender's public key.
D. receiver's public key and encrypting the message using the sender's private key.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
By signing the message with the sender's private key, the receiver can verify its authenticity using the sender's public key. By encrypting the message with the receiver's public key, only the receiver can decrypt the message using their own private key. The receiver's private key is confidential and, therefore, unknown to the sender. Messages encrypted using the sender's private key can be read by anyone with the sender's public key.

QUESTION 716
An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the BEST protection against hacking?

A. An application-level gateway
B. A remote access server
C. A proxy server
D. Port scanning

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An application-level gateway is the best way to protect against hacking because it can define with detail rules that describe the type of user or connection that is or is not permitted, it analyzes in detail each package, not only in layers one through four of the OSI model but also layers five through seven, which means that it reviews the commands of each higher-level protocol (HTTP, FTP, SNMP, etc.). For a remote access server, there is a device (server) that asks for a username and password before entering the network. This is good when accessing private networks, but it can be mapped or scanned from the Internet creating security exposure. Proxy servers can provide protection based on the IP address and ports. However, an individual is needed who really knows how to do this, and applications can use different ports for the different sections of the program. Port scanning works when there is a very specific task to complete, but not when trying to control what comes from the Internet, or when all the ports available need to be controlled. For example, the port for Ping (echo request) could be blocked and the IP addresses would be available for the application and browsing, but would not respond to Ping.

QUESTION 717
Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

A. Virtual private network
B. Dedicated line
C. Leased line

D. integrated services digital network

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most secure method is a virtual private network (VPN), using encryption, authentication and tunneling to allow data to travel securely from a private network to the internet. Choices B, C and D are network connectivity options that are normally too expensive to be practical for small- to medium-sized organizations.

QUESTION 718
The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

A. connecting points are available in the facility to connect laptops to the network.
B. users take precautions to keep their passwords confidential.
C. terminals with password protection are located in insecure locations.
D. terminals are located within the facility in small clusters under the supervision of an administrator.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Any person with wrongful intentions can connect a laptop to the network. The insecure connecting points, make unauthorized access possible if the individual has knowledge of a valid user ID and password. The other choices are controls for preventing unauthorized network access. If system passwords are not readily available for intruders to use, they must guess, introducing an additional factor and requires time. System passwords provide protection against unauthorized use of terminals located in insecure locations. Supervision is a very effective control when used to monitor access to a small operating unit or production resources.

QUESTION 719
Which of the following functions is performed by a virtual private network (VPN)?

A. Hiding information from sniffers on the net
B. Enforcing security policies

C. Detecting misuse or mistakes
D. Regulating access

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A VPN hides information from sniffers on the net using encryption. It works based on tunneling. A VPN does not analyze information packets and, therefore, cannot enforce security policies, it also does not check the content of packets, so it cannot detect misuse or mistakes. A VPN also does not perform an authentication function and, therefore, cannot regulate access.

QUESTION 720
Applying a digital signature to data traveling in a network provides:

A. confidentiality and integrity.
B. security and nonrepudiation.
C. integrity and nonrepudiation.
D. confidentiality and nonrepudiation.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The process of applying a mathematical algorithm to the data that travel in the network and placing the results of this operation with the hash data is used for controlling data integrity, since any unauthorized modification to this data would result in a different hash. The application of a digital signature would accomplish the non-repudiation of the delivery of the message. The term security is a broad concept and not a specific one. In addition to a hash and a digital signature, confidentiality is applied when an encryption process exists.

QUESTION 721
Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital certificates for its business-to- consumer transactions via the internet?

A. Customers are widely dispersed geographically, but the certificate authorities are not.
B. Customers can make their transactions from any computer or mobile device.
C. The certificate authority has several data processing subcenters to administer certificates.
D. The organization is the owner of the certificate authority.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: If the certificate authority belongs to the same organization, this would generate a conflict of interest. That is, if a customer wanted to repudiate a transaction, they could allege that because of the shared interests, an unlawful agreement exists between the parties generating the certificates, if a customer wanted to repudiate a transaction, they could argue that there exists a bribery between the parties to generate the certificates, as shared interests exist. The other options are not weaknesses.

QUESTION 722
Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

A. Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
B. Secure Sockets Layer (SSL) mode
C. Tunnel mode with AH plus ESP
D. Triple-DES encryption mode

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Tunnel mode provides protection to the entire IP package. To accomplish this, AH and ESP services can be nested. The transport mode provides primary protection for the higher layers of the protocols by extending protection to the data fields (payload) of an IP package. The SSL mode provides security to the higher communication layers (transport layer). The triple-DES encryption mode is an algorithm that provides confidentiality.

QUESTION 723
Which of the following internet security threats could compromise integrity?

A. Theft of data from the client
B. Exposure of network configuration information
C. A Trojan horse browser
D. Eavesdropping on the net

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Internet security threats/vulnerabilities to integrity include a Trojan horse, which could modify user data, memory and messages found in client-browser software. The other options compromise confidentiality.

QUESTION 724
If inadequate, which of the following would be the MOST likely contributor to a denial-of- service attack?

A. Router configuration and rules
B. Design of the internal network
C. Updates to the router system software
D. Audit testing and review techniques

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Inadequate router configuration and rules would lead to an exposure to denial-of-service attacks. Choices B and C would be lesser contributors. Choice D is incorrect because audit testing and review techniques are applied after the fact.

QUESTION 725
The PRIMARY goal of a web site certificate is:

A. authentication of the web site that will be surfed.

B. authentication of the user who surfs through that site.
C. preventing surfing of the web site by hackers.
D. the same purpose as that of a digital certificate.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Authenticating the site to be surfed is the primary goal of a web certificate. Authentication of a user is achieved through passwords and not by a web site certificate. The site certificate does not prevent hacking nor does it authenticate a person.

QUESTION 726
The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:
A. searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.
B. and penetration tests are different names for the same activity.
C. is executed by automated tools, whereas penetration testing is a totally manual process.
D. is executed by commercial tools, whereas penetration testing is executed by public processes.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The objective of a vulnerability assessment is to find the security holds in the computers and elements analyzed; its intent is not to damage the infrastructure. The intent of penetration testing is to imitate a hacker's activities and determine how far they could go into the network. They are not the same; they have different approaches. Vulnerability assessments and penetration testing can be executed by automated or manual tools or processes and can be executed by commercial or free tools.

QUESTION 727
The role of the certificate authority (CA) as a third party is to:

A. provide secured communication and networking services based on certificates.
B. host a repository of certificates with the corresponding public and secret keys issued by that CA.
C. act as a trusted intermediary between two communication partners.
D. confirm the identity of the entity owning a certificate issued by that CA.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary activity of a CA is to issue certificates. The primary role of the CA is to check the identity of the entity owning a certificate and to confirm the integrity of any certificate it issued. Providing a communication infrastructure is not a CA activity. The secret keys belonging to the certificates would not be archived at the CA. The CA can contribute to authenticating the communicating partners to each other, but the CA is not involved in the communication stream itself.

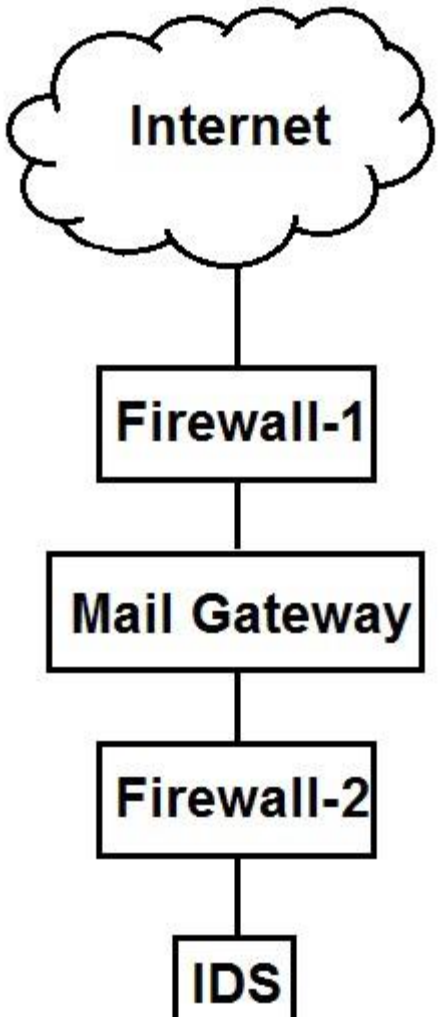
QUESTION 728
Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?
A. The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
B. All personal SET certificates are stored securely in the buyer's computer.
C. The buyer is liable for any transaction involving his/her personal SET certificates.
D. The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The usual agreement between the credit card issuer and the cardholder stipulates that the cardholder assumes responsibility for any use of their personal SET certificates for e- commerce transactions. Depending upon the agreement between the merchant and the buyer's credit card issuer, the merchant will have access to the credit card number and expiration date. Secure data storage in the buyer's computer (local computer security) is not part of the SET standard. Although the buyer is not required to enter their credit card data, they will have to handle the wallet software.

QUESTION 729

E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



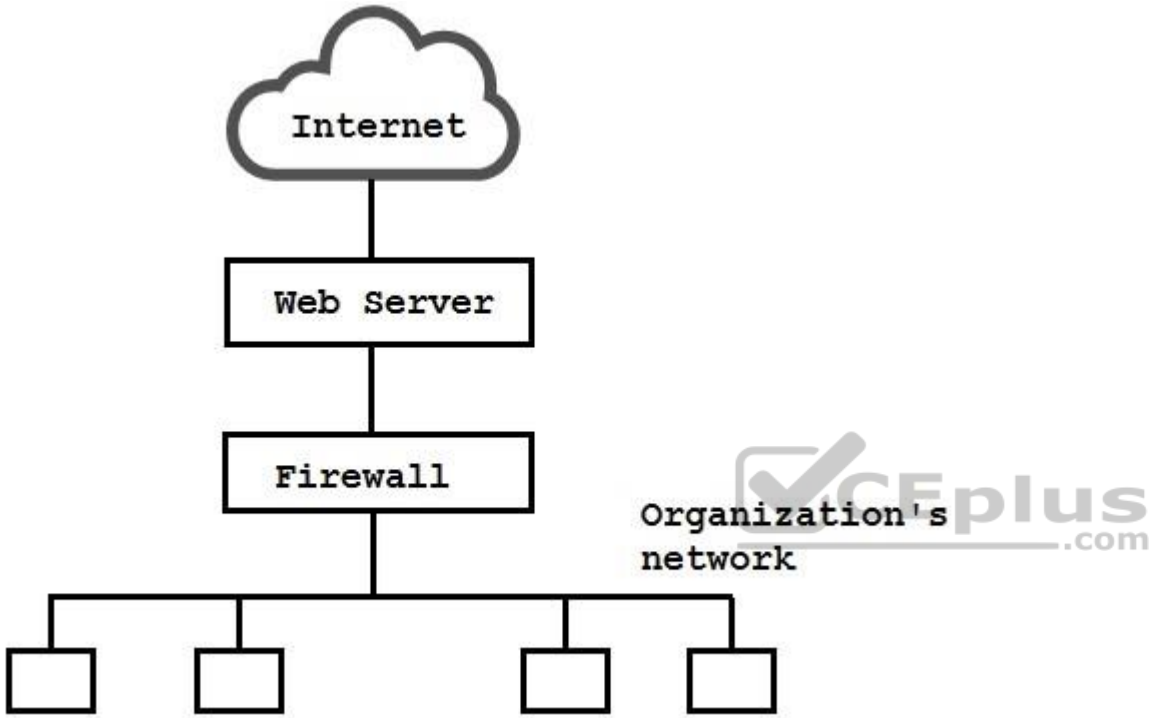
The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

A. alert the appropriate staff.
B. create an entry in the log.
C. close firewall-2.
D. close firewall-1.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Traffic for the internal network that did not originate from the mail gateway is a sign that firewall-1 is not functioning properly. This may have been caused by an attack from a hacker. Closing firewall-2 is the first thing that should be done, thus preventing damage to the internal network.
After closing firewall-2, the malfunctioning of firewall-1 can be investigated. The IDS should trigger the closing of firewall-2 either automatically or by manual intervention. Between the detection by the IDS and a response from the system administrator valuable time can be lost, in which a hacker could also compromise firewall-2. An entry in the log is valuable for later analysis, but before that, the IDS should close firewall-2. If firewall-1 has already been compromised by a hacker, it might not be possible for the IDS to close it.

QUESTION 730
To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



A. Firewall and the organization's network.
B. Internet and the firewall.
C. Internet and the web server.
D. Web server and the firewall.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Attack attempts that could not be recognized by the firewall will be detected if a network- based intrusion detection system is placed between the firewall and the organization's network. A network-based intrusion detection system placed between the internet and the firewall will detect attack attempts, whether they do or do not enter the firewall.

QUESTION 731
Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

A. Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
B. The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
C. Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
D. Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To ensure authenticity and confidentiality, a message must be encrypted twice: first with the sender's private key, and then with the receiver's public key. The receiver can decrypt the message, thus ensuring confidentiality of the message. Thereafter, the decrypted message can be decrypted with the public key of the sender, ensuring authenticity of the message. Encrypting the message with the sender's private key enables anyone to decrypt it.

QUESTION 732
Disabling which of the following would make wireless local area networks more secure against unauthorized access?

A. MAC (Media Access Control) address filtering
B. WPA (Wi-Fi Protected Access Protocol)
C. LEAP (Lightweight Extensible Authentication Protocol)
D. SSID (service set identifier) broadcasting

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Disabling SSID broadcasting adds security by making it more difficult for unauthorized users to find the name of the access point. Disabling MAC address filtering would reduce security. Using MAC filtering makes it more difficult to access a WLAN, because it would be necessary to catch traffic and forge the MAC address. Disabling WPA reduces security. Using WPA adds security by encrypting the traffic. Disabling LEAP reduces security. Using LEAP adds security by encrypting the wireless traffic.

QUESTION 733
Which of the following is BEST suited for secure communications within a small group?
A. Key distribution center
B. Certification authority
C. Web of trust
D. Kerberos Authentication System

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Web of trust is a key distribution method suitable for communication in a small group. It ensures pretty good privacy (PGP) and distributes the public keys of users within a group. Key distribution center is a distribution method suitable for internal communication for a large group within an institution, and it will distribute symmetric keys for each session. Certification authority is a trusted third party that ensures the authenticity of the owner of the certificate. This is necessary for large groups and formal communication. A Kerberos Authentication System extends the function of a key distribution center, by generating 'tickets' to define the facilities on networked machines which are accessible to each user.

QUESTION 734
Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is:

A. restricted to predefined MAC addresses.
B. encrypted using static keys.
C. encrypted using dynamic keys.
D. initiated from devices that have encrypted storage.

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When using dynamic keys, the encryption key is changed frequently, thus reducing the risk of the key being compromised and the message being decrypted. Limiting the number of devices that can access the network does not address the issue of encrypting the session. Encryption with static keys-using the same key for a long period of time-risks that the key would be compromised. Encryption of the data on the connected device (laptop, PDA, etc.) addresses the confidentiality of the data on the device, not the wireless session.

QUESTION 735
When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

A. Number of nonthreatening events identified as threatening
B. Attacks not being identified by the system
C. Reports/logs being produced by an automated tool
D. Legitimate traffic being blocked by the system

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Attacks not being identified by the system present a higher risk, because they are unknown and no action will be taken to address the attack. Although the number of false-positives is a serious issue, the problem will be known and can be corrected. Often, IDS reports are first analyzed by an automated tool to eliminate known false-positives, which generally are not a problem. An IDS does not block any traffic.

QUESTION 736
Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

A. Logic bombs
B. Phishing
C. Spyware
D. Trojan horses

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Trojan horses are malicious or damaging code hidden within an authorized computer program. Hackers use Trojans to mastermind DDOS attacks that affect computers that access the same Internet site at the same moment, resulting in overloaded site servers that may no longer be able to process legitimate requests. Logic bombs are programs designed to destroy or modify data at a specific time in the future. Phishing is an attack, normally via e-mail, pretending to be an authorized person or organization requesting information. Spyware is a program that picks up information from PC drives by making copies of their contents.

QUESTION 737
In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

A. connectionless integrity.
B. data origin authentication.
C. antireplay service.
D. confidentiality.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Both protocols support choices A, B and C, but only the ESP protocol provides confidentiality via encryption.

QUESTION 738
IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

A. Port scanning
B. Back door
C. Man-in-the-middle

D. War driving

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A war driving attack uses a wireless Ethernet card, set in promiscuous mode, and a powerful antenna to penetrate wireless systems from outside. Port scanning will often target the external firewall of the organization. A back door is an opening left in software that enables an unknown entry into a system. Man-in-the-middle attacks intercept a message and either replace or modify it.

QUESTION 739
Which of the following encryption techniques will BEST protect a wireless network from a man-in-the-middle attack?

A. 128-bit wired equivalent privacy (WEP)
B. MAC-based pre-shared key(PSK)
C. Randomly generated pre-shared key (PSKJ
D. Alphanumeric service set identifier (SSID)

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A randomly generated PSK is stronger than a MAC-based PSK, because the MAC address of a computer is fixed and often accessible. WEP has been shown to be a very weak encryption technique and can be cracked within minutes. The SSID is broadcast on the wireless network in plaintext.

QUESTION 740
An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

A. digitally signing all e-mail messages.
B. encrypting all e-mail messages.
C. compressing all e-mail messages.

D. password protecting all e-mail messages.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity. Password protecting all e-mail messages would ensure that only those who have the password would be able to open the message; however, it would not ensure the authenticity of the sender.

QUESTION 741
Sending a message and a message hash encrypted by the sender's private key will ensure:

A. authenticity and integrity.
B. authenticity and privacy.
C. integrity and privacy.
D. privacy and nonrepudiation.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If the sender sends both a message and a message hash encrypted by its private key, then the receiver can apply the sender's public key to the hash and get the message hash. The receiver can apply the hashing algorithm to the message received and generate a hash. By matching the generated hash with the one received, the receiver is ensured that the message has been sent by the specific sender, i.e., authenticity, and that the message has not been changed enroute. Authenticity and privacy will be ensured by first using the sender's private key and then the receiver's public key to encrypt the message. Privacy and integrity can be ensured by using the receiver's public key to encrypt the message and sending a message hash/digest. Only nonrepudiation can be ensured by using the sender's private key to encrypt the message. The sender's public key, available to anyone, can decrypt a message; thus, it does not ensure privacy.

QUESTION 742

An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. An IS auditor recommends replacing the non-upgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

A. The new access points with stronger security are affordable.
B. The old access points are poorer in terms of performance.
C. The organization's security would be as strong as its weakest points.
D. The new access points are easier to manage.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The old access points should be discarded and replaced with products having strong security; otherwise, they will leave security holes open for attackers and thus make the entire network as weak as they are. Affordability is not the auditor's major concern. Performance is not as important as security in this situation. Product manageability is not the IS auditor's concern.

QUESTION 743
An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

A. encrypting the hash of the newsletter using the advisor's private key.
B. encrypting the hash of the newsletter using the advisor's public key.
C. digitally signing the document using the advisor's private key.
D. encrypting the newsletter using the advisor's private key.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
There is no attempt on the part of the investment advisor to prove their identity or to keep the newsletter confidential. The objective is to assure the receivers that it came to them without any modification, i.e., it has message integrity. Choice A is correct because the hash is encrypted using the advisor's private key. The recipients can open the newsletter, recompute the hash and decrypt the received hash using the advisor’s public key. If the two hashes are equal, the newsletter

was not modified in transit. Choice B is not feasible, for no one other than the investment advisor can open it. Choice C addresses sender authentication but not message integrity. Choice D addresses confidentiality, but not message integrity, because anyone can obtain the investment advisor's public key, decrypt the newsletter, modify it and send it to others. The interceptor will not be able to use the advisor's private key, because they do not have it. Anything encrypted using the interceptor's private key can be decrypted by the receiver only by using their public key.

QUESTION 744
An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol is disabled at all wireless access points. This practice:

A. reduces the risk of unauthorized access to the network.
B. is not suitable for small networks.
C. automatically provides an IP address to anyone.
D. increases the risks associated with Wireless Encryption Protocol (WEP).

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to anyone connected to the network. With DHCP disabled, static IP addresses must be used and represent less risk due to the potential for address contention between an unauthorized device and existing devices on the network. Choice B is incorrect because DHCP is suitable for small networks.
Choice C is incorrect because DHCP does not provide IP addresses when disabled. Choice D is incorrect because disabling of the DHCP makes it more difficult to exploit the well-known weaknesses in WEP.

QUESTION 745
In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

A. common gateway interface (CGI) scripts.
B. enterprise Java beans (EJBs).
C. applets.
D. web services.

Correct Answer: A
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation: Common gateway interface (CGI) scripts are executable machine independent software programs on the server that can be called and executed by a web server page. CGI performs specific tasks such as processing inputs received from clients. The use of CGI scripts needs to be evaluated, because as they run in the server, a bug in them may allow a user to gain unauthorized access to the server and from there gain access to the organization's network.
Applets are programs downloaded from a web server and executed on web browsers on client machines to run any web-based applications. Enterprise java beans (EJBs) and web services have to be deployed by the web server administrator and are controlled by the application server. Their execution requires knowledge of the parameters and expected return values.

QUESTION 746
An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

A. IDS sensors are placed outside of the firewall.
B. a behavior-based IDS is causing many false alarms.
C. a signature-based IDS is weak against new types of attacks.
D. the IDS is used to detect encrypted traffic.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An intrusion detection system (IDS) cannot detect attacks within encrypted traffic, and it would be a concern if someone was misinformed and thought that the IDS could detect attacks in encrypted traffic. An organization can place sensors outside of the firewall to detect attacks.
These sensors are placed in highly sensitive areas and on extranets. Causing many false alarms is normal for a behavior-based IDS, and should not be a matter of concern. Being weak against new types of attacks is also expected from a signature- based IDS, because it can only recognize attacks that have been previously identified.

QUESTION 747
Which of the following ensures confidentiality of information sent over the internet?

A. Digital signature
B. Digital certificate

C. Online Certificate Status Protocol
D. Private key cryptosystem

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Confidentiality is assured by a private key cryptosystem. Digital signatures assure data integrity, authentication and nonrepudiation, but not confidentially. A digital certificate is a certificate that uses a digital signature to bind together a public key with an identity; therefore, it does not address confidentiality. Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of a digital certificate.

QUESTION 748
To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:

A. access control servers. B.
session border controllers.

C. backbone gateways.
D. intrusion detection system (IDS).

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Session border controllers enhance the security in the access network and in the core. In the access network, they hide a user's real address and provide a managed public address. This public address can be monitored, minimizing the opportunities for scanning and denial-of-service (DoS) attacks. Session border controllers permit access to clients behind firewalls while maintaining the firewall's effectiveness. In the core, session border controllers protect the users and the network. They hide network topology and users' real addresses. They can also monitor bandwidth and quality of service. Securing the access control server, backbone gateways and intrusion detection systems (IDSs) does not effectively protect against DoS attacks.

QUESTION 749
Which of the following attacks targets the Secure Sockets Layer (SSL)?

A. Man-in-the middle
B. Dictionary
C. Password sniffing
D. Phishing

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Attackers can establish a fake Secure Sockets Layer (SSL) server to accept user's SSL traffic and then route to the real SSL server, so that sensitive information can be discovered. A dictionary attack that has been launched to discover passwords would not attack SSL since SSL does not rely on passwords. SSL traffic is encrypted; thus it is not possible to sniff the password. A phishing attack targets a user and not SSL Phishing attacks attempt to have the user surrender private information by falsely claiming to be a trusted person or enterprise.

QUESTION 750
Which of the following potentially blocks hacking attempts?

A. intrusion detection system
B. Honeypot system
C. Intrusion prevention system
D. Network security scanner

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An intrusion prevention system (IPS) is deployed as an in-line device that can detect and block hacking attempts. An intrusion detection system (IDS) normally is deployed in sniffing mode and can detect intrusion attempts, but cannot effectively stop them. A honeypot solution traps the intruders to explore a simulated target. A network security scanner scans for the vulnerabilities, but it will not stop the intrusion.

QUESTION 751
What is the BEST approach to mitigate the risk of a phishing attack?

A. implement an intrusion detection system (IDS)
B. Assess web site security
C. Strong authentication
D. User education

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Phishing attacks can be mounted in various ways; intrusion detection systems (IDSs) and strong authentication cannot mitigate most types of phishing attacks. Assessing web site security does not mitigate the risk. Phishing uses a server masquerading as a legitimate server. The best way to mitigate the risk of phishing is to educate users to take caution with suspicious internet communications and not to trust them until verified. Users require adequate training to recognize suspicious web pages and e-mail.

QUESTION 752
The BEST filter rule for protecting a network from being used as an amplifier in a denial of service (DoS) attack is to deny all:

A. outgoing traffic with IP source addresses externa! to the network.
B. incoming traffic with discernible spoofed IP source addresses.
C. incoming traffic with IP options set.
D. incoming traffic to critical hosts.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Outgoing traffic with an IP source address different than the IP range in the network is invalid, in most of the cases, it signals a DoS attack originated by an internal user or by a previously compromised internal machine; in both cases, applying this filter will stop the attack.

QUESTION 753
A company has decided to implement an electronic signature scheme based on public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The MOST significant risk of this approach is:

A. use of the user's electronic signature by another person if the password is compromised.
B. forgery by using another user's private key to sign a message with an electronic signature.
C. impersonation of a user by substitution of the user's public key with another person's public key.
D. forgery by substitution of another person's private key on the computer.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The user's digital signature is only protected by a password. Compromise of the password would enable access to the signature. This is the most significant risk.
Choice B would require subversion of the public key infrastructure mechanism, which is very difficult and least likely.
Choice C would require that the message appear to have come from a different person and therefore the true user's credentials would not be forged. Choice D has the same consequence as choice C.

QUESTION 754
A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?

A. Reviewing logs frequently
B. Testing and validating the rules
C. Training a local administrator at the new location

D. Sharing firewall administrative duties

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A mistake in the rule set can render a firewall insecure. Therefore, testing and validating the rules is the most important factor in ensuring a successful deployment. A regular review of log files would not start until the deployment has been completed. Training a local administrator may not be necessary if the firewalls are managed from a central location. Having multiple administrators is a good idea, but not the most important.

QUESTION 755
What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

A. Malicious code could be spread across the network
B. VPN logon could be spoofed
C. Traffic could be sniffed and decrypted
D. VPN gateway could be compromised

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
VPN is a mature technology; VPN devices are hard to break. However, when remote access is enabled, malicious code in a remote client could spread to the organization's network. Though choices B, C and D are security risks, VPN technology largely mitigates these risks.

QUESTION 756
The FIRST step in a successful attack to a system would be:

A. gathering information.
B. gaining access.
C. denying services.

D. evading detection.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Successful attacks start by gathering information about the target system. This is done in advance so that the attacker gets to know the target systems and their vulnerabilities. All of the other choices are based on the information gathered.

QUESTION 757
An organization is planning to replace its wired networks with wireless networks. Which of the following would BEST secure the wireless network from unauthorized access?

A. Implement Wired Equivalent Privacy (WEP)
B. Permit access to only authorized Media Access Control (MAC) addresses
C. Disable open broadcast of service set identifiers (SSID)
D. Implement Wi-Fi Protected Access (WPA) 2

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Wi-Fi Protected Access (WPA) 2 implements most of the requirements of the IEEE 802.11i standard. The Advanced Encryption Standard (AESJ used in WPA2 provides better security. Also, WPA2 supports both the Extensible Authentication Protocol and the preshared secret key authentication model. Implementing Wired Equivalent Privacy (WEP) is incorrect since it can be cracked within minutes. WEP uses a static key which has to be communicated to all authorized users, thus management is difficult. Also, there is a greater vulnerability if the static key is not changed at regular intervals. The practice of allowing access based on Media Access Control (MAC) is not a solution since MAC addresses can be spoofed by attackers to gain access to the network. Disabling open broadcast of service set identifiers (SSID) is not the correct answer as they cannot handle access control.

QUESTION 758
An IS auditor is reviewing a software-based configuration. Which of the following represents the GREATEST vulnerability? The firewall software:

A. is configured with an implicit deny rule as the last rule in the rule base.
B. is installed on an operating system with default settings.
C. has been configured with rules permitting or denying access to systems or networks.
D. is configured as a virtual private network (VPN) endpoint.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Default settings are often published and provide an intruder with predictable configuration information, which allows easier system compromise. To mitigate this risk, firewall software should be installed on a system using a hardened operating system that has limited functionality, providing only the services necessary to support the firewall software. Choices A, C and D are normal or best practices for firewall configurations.

QUESTION 759
The GREATEST risk posed by an improperly implemented intrusion prevention system (IPS) is:

A. that there will be too many alerts for system administrators to verify.
B. decreased network performance due to IPS traffic.
C. the blocking of critical systems or services due to false triggers.
D. reliance on specialized expertise within the IT organization.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
An intrusion prevention system (IPS) prevents a connection or service based on how it is programmed to react to specific incidents. If the packets are coming from a spoofed address and the IPS is triggered based on previously defined behavior, it may block the service or connection of a critical internal system. The other choices are risks that are not as severe as blocking critical systems or services due to false triggers.

QUESTION 760
When reviewing a digital certificate verification process, which of the following findings represents the MOST significant risk?

A. There is no registration authority (RA) for reporting key compromises
B. The certificate revocation list(CRL) is not current.
C. Digital certificates contain a public key that is used to encrypt messages and verify digital signatures.
D. Subscribers report key compromises to the certificate authority (CA).

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If the certificate revocation list (CRL) is not current, there could be a digital certificate that is not revoked that could be used for unauthorized or fraudulent activities. The certificate authority (CA) can assume the responsibility if there is no registration authority (RA). Digital certificates containing a public key that is used to encrypt messages and verifying digital signatures is not a risk. Subscribers reporting key compromises to the CA is not a risk since reporting this to the CA enables the CA to take appropriate action.

QUESTION 761
Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the:

A. registration authority (RA).
B. certificate authority (CA).
C. certificate repository.
D. receiver.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. As a part of the public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate. The CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will decrypt the certificate with the CA's public key.

QUESTION 762
IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

A. Review and, where necessary, upgrade firewall capabilities
B. Install modems to allow remote maintenance support access
C. Create a physically distinct network to handle VoIP traffic
D. Redirect all VoIP traffic to allow clear text logging of authentication credentials

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Firewalls used as entry points to a Voice-over Internet Protocol (VoIP) network should be VoIP- capable. VoIP network services such as H.323 introduce complexities that are likely to strain the capabilities of older firewalls. Allowing for remote support access is an important consideration. However, a virtual private network (VPN) would offer a more secure means of enabling this access than reliance on modems. Logically separating the VoIP and data network is a good idea. Options such as virtual LANS (VLA.NS), traffic shaping, firewalls and network address translation (NAT) combined with private IP addressing can be used; however, physically separating the networks will increase both cost and administrative complexity. Transmitting or storing clear text information, particularly sensitive information such as authentication credentials, will increase network vulnerability. When designing a VoIP network, it is important to avoid introducing any processing that will unnecessarily increase latency since this will adversely impact VoIP quality.

QUESTION 763
Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

A. Statistical-based
B. Signature-based
C. Neural network
D. Host-based

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal network activity may at times include unexpected behavior (e.g., a sudden massive download by multiple users), these activities will be flagged as suspicious. A signature-based IDS is limited to its predefined set of detection rules, just like a virus scanner. A neural network combines the previous two IDSs to create a hybrid and better system. Host-based is another classification of IDS. Any of the three IDSs above may be host- or network-based.

QUESTION 764
Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

A. Power line conditioners
B. Surge protective devices
C. Alternative power supplies
D. Interruptible power supplies

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Power line conditioners are used to compensate for peaks and valleys in the power supply and reduce peaks in the power flow to what is needed by the machine. Any valleys are removed by power stored in the equipment. Surge protection devices protect against high- voltage bursts. Alternative power supplies are intended for computer equipment running for longer periods and are normally coupled with other devices such as an uninterruptible power supply (UPS) to compensate for the power loss until the alternate power supply becomes available. An interruptible power supply would cause the equipment to come down whenever there was a power failure.

QUESTION 765
A penetration test performed as part of evaluating network security:

A. provides assurance that all vulnerabilities are discovered.
B. should be performed without warning the organization's management.
C. exploits the existing vulnerabilities to gain unauthorized access.
D. would not damage the information assets when performed at network perimeters.

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Penetration tests are an effective method of identifying real-time risks to an information processing environment. They attempt to break into a live site in order to gain unauthorized access to a system. They do have the potential for damaging information assets or misusing information because they mimic an experienced hacker attacking a live system. On the other hand, penetration tests do not provide assurance that all vulnerabilities are discovered because they are based on a limited number of procedures. Management should provide consent for the test to avoid false alarms to IT personnel or to law enforcement bodies.

QUESTION 766
An accuracy measure for a biometric system is:
A. system response time.
B. registration time.
C. input file size.
D. false-acceptance rate.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
For a biometric solution three main accuracy measures are used: false-rejection rate (FRR), cross-error rate (CER) and false-acceptance rate (FAR). FRR is a measure of how often valid individuals are rejected. FAR is a measure of how often invalid individuals are accepted. CER is a measure of when the false-rejection rate equals the false-acceptance rate. Choices A and B are performance measures.

QUESTION 767
The BEST overall quantitative measure of the performance of biometric control devices is:

A. false-rejection rate.
B. false-acceptance rate.
C. equal-error rate.
D. estimated-error rate.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A low equal-error rate (EER) is a combination of a low false-rejection rate and a low false- acceptance rate. EER, expressed as a percentage, is a measure of the number of times that the false-rejection and false-acceptance rates are equal. A low EER is the measure of the more effective biometrics control device. Low falserejection rates or low false- acceptance rates alone do not measure the efficiency of the device. Estimated-error rate is nonexistent and therefore irrelevant.

QUESTION 768
The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

A. Replay
B. Brute force
C. Cryptographic
D. Mimic

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Residual biometric characteristics, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access. A brute force attack involves feeding the biometric capture device numerous different biometric samples. A cryptographic attack targets the algorithm or the encrypted data, in a mimic attack, the attacker reproduces characteristics similar to those of the enrolled user, such as forging a signature or imitating a voice.

QUESTION 769
The MOST likely explanation for a successful social engineering attack is:

A. that computers make logic errors.
B. that people make judgment errors.
C. the computer knowledge of the attackers.
D. the technological sophistication of the attack method.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Humans make errors in judging others; they may trust someone when, in fact, the person is untrustworthy. Driven by logic, computers make the same error every time they execute the erroneous logic; however, this is not the basic argument in designing a social engineering attack. Generally, social engineering attacks do not require technological expertise; often, the attacker is not proficient in information technology or systems. Social engineering attacks are human-based and generally do not involve complicated technology.

QUESTION 770
Which of the following physical access controls effectively reduces the risk of piggybacking?

A. Biometric door locks
B. Combination door locks
C. Deadman doors
D. Bolting door locks

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Deadman doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding areA. This effectively reduces the risk of piggybacking. An individual's unique body features such as voice, retina, fingerprint or signature activate biometric door locks; however, they do not prevent or reduce the risk of piggybacking. Combination door locks, also known as cipher locks, use a numeric key pad or dial to gain entry. They do not prevent or reduce the risk of piggybacking since unauthorized individuals may still gain access to the processing center. Bolting door locks require the traditional metal key to gain entry. Unauthorized individuals could still gain access to the processing center along with an authorized individual.

QUESTION 771
The MOST effective biometric control system is the one:

A. which has the highest equal-error rate (EER).
B. which has the lowest EER.

C. for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
D. for which the FRR is equal to the failure-to-enroll rate (FER).

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The equal-error rate (EER) of a biometric system denotes the percent at which the false- acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of FRR.

QUESTION 772
Which of the following is the BEST way to satisfy a two-factor user authentication?

A. A smart card requiring the user's PIN
B. User ID along with password
C. Iris scanning plus fingerprint scanning
D. A magnetic card requiring the user's PIN

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). An ID and password, what the user knows, is a single-factor user authentication. Choice C is not a two- factor user authentication because it is only biometric. Choice D is similar to choice A, but the magnetic card may be copied; therefore, choice A is the best way to satisfy a two-factor user authentication.

QUESTION 773
Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

A. Overwriting the tapes
B. initializing the tape labels
C. Degaussing the tapes
D. Erasing the tapes

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

QUESTION 774
Which of the following is the MOST important objective of data protection?

A. identifying persons who need access to information
B. Ensuring the integrity of information
C. Denying or authorizing access to the IS system
D. Monitoring logical accesses

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

QUESTION 775
A hard disk containing confidential data was damaged beyond repair. What should be done to the hard disk to prevent access to the data residing on it?

A. Rewrite the hard disk with random Os and Is.

B. Low-level format the hard disk.
C. Demagnetize the hard disk.
D. Physically destroy the hard disk.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Physically destroying the hard disk is the most economical and practical way to ensure that the data cannot be recovered. Rewriting data and low-level formatting are impractical, because the hard disk is damaged. Demagnetizing is an inefficient procedure, because it requires specialized and expensive equipment to be fully effective.

QUESTION 776
Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

A. Policies that require instant dismissal if such devices are found
B. Software for tracking and managing USB storage devices
C. Administratively disabling the USB port
D. Searching personnel for USB storage devices at the facility's entrance

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Software for centralized tracking and monitoring would allow a USB usage policy to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management. A policy requiring dismissal may result in increased employee attrition and business requirements would not be properly addressed. Disabling ports would be complex to manage and might not allow for new business needs. Searching of personnel for USB storage devices at the entrance to a facility is not a practical solution since these devices are small and could be easily hidden.

QUESTION 777
To ensure authentication, confidentiality and integrity of a message, the sender should encrypt the hash of the message with the sender's:

A. public key and then encrypt the message with the receiver's private key.
B. private key and then encrypt the message with the receiver's public key.
C. public key and then encrypt the message with the receiver's public key.
D. private key and then encrypt the message with the receiver's private key.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Obtaining the hash of the message ensures integrity; signing the hash of the message with the sender's private key ensures the authenticity of the origin, and encrypting the resulting message with the receiver's public key ensures confidentiality. The other choices are incorrect.

QUESTION 778
At a hospital, medical personal carry handheld computers which contain patient health data. These handheld computers are synchronized with PCs which transfer data from a hospital database. Which of the following would be of the most importance?

A. The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss.
B. The employee who deletes temporary files from the local PC, after usage, is authorized to maintain PCs.
C. Timely synchronization is ensured by policies and procedures.
D. The usage of the handheld computers is allowed by the hospital policy.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data confidentiality is a major requirement of privacy regulations. Choices B, C and D relate to internal security requirements, and are secondary when compared to compliance with data privacy laws.

QUESTION 779
The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:
A. achieve performance improvement.

B. provide user authentication.
C. ensure availability of data.
D. ensure the confidentiality of data.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk; if disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication and does nothing to provide for data confidentiality.

QUESTION 780
Which of the following is the MOST important criterion when selecting a location for an offsite storage facility for IS backup files? The offsite facility must be:

A. physically separated from the data center and not subject to the same risks.
B. given the same level of protection as that of the computer data center.
C. outsourced to a reliable third party.
D. equipped with surveillance capabilities.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

QUESTION 781
As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following is necessary to restore these files?

A. The previous day's backup file and the current transaction tape
B. The previous day's transaction file and the current transaction tape
C. The current transaction tape and the current hard copy transaction log
D. The current hard copy transaction log and the previous day's transaction file

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The previous day's backup file will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

QUESTION 782
An offsite information processing facility:

A. should have the same amount of physical access restrictions as the primary processing site.
B. should be easily identified from the outside so that, in the event of an emergency, it can be easily found.
C. should be located in proximity to the originating site, so it can quickly be made operational.
D. need not have the same level of environmental monitoring as the originating site.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity of the original site. The offsite facility should possess the same level of environmental monitoring and control as the originating site.

QUESTION 783
Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

A. Reviewing program code
B. Reviewing operations documentation
C. Turning off the UPS, then the power
D. Reviewing program documentation

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

QUESTION 784
Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

A. database integrity checks.
B. validation checks.
C. input controls.
D. database commits and rollbacks.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

QUESTION 785

Which of the following ensures the availability of transactions in the event of a disaster?

A. Send tapes hourly containing transactions offsite,
B. Send tapes daily containing transactions offsite.
C. Capture transactions to multiple storage devices.
D. Transmit transactions offsite in real time.

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
The only way to ensure availability of all transactions is to perform a real-time transmission to an offsite facility. Choices A and B are not in real time and, therefore, would not include all the transactions. Choice C does not ensure availability at an offsite location.

QUESTION 786
In which of the following situations is it MOST appropriate to implement data mirroring as the recovery strategy?

A. Disaster tolerance is high.
B. Recovery time objective is high.
C. Recovery point objective is low.
D. Recovery point objective is high.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A recovery point objective (RPO) indicates the latest point in time at which it is acceptable to recover the data. If the RPO is low, data mirroring should be implemented as the data recovery strategy. The recovery time objective (RTO) is an indicator of the disaster tolerance. The lower the RTO, the lower the disaster tolerance. Therefore, choice C is the correct answer.

QUESTION 787
Network Data Management Protocol (NDMP) technology should be used for backup if:

A. a network attached storage (NAS) appliance is required.
B. the use of TCP/I P must be avoided.
C. file permissions that can not be handled by legacy backup systems must be backed up.
D. backup consistency over several related data volumes must be ensured.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
NDMP defines three kinds of services: a data service that interfaces with the primary storage to be backed up or restored, a tape service that interfaces with the secondary storage (primarily a tape device), and a translator service performing translations including multiplexing multiple data streams into one data stream and vice versa. NDMP services interact with each other. The result of this interaction is the establishment of an NDMP control session if the session is being used to achieve control for the backup or restore operation. It would result in an NDMP data session if the session is being used to transfer actual file system or volume data (including metadata). Control sessions are always TCP/IP-based, but data streams can be TCP/IP-or SAN-based. NDMP is more or less NAS-centric and defines a way to back up and restore data from a device, such as a NAS appliance, on which it is difficult to install a backup software agent, in the absence of NDMP, this data must be backed up as a shared drive on the LAN, which is accessed via network file protocols, such as Common Internet File System (CIFS) or Network File System (NFS), degrading backup performance. NDMP works on a block level for transferring payload data (file content) but metadata and traditional file system information needs to be handled by legacy backup systems that initiate NDMP data movement. NDMP does not know about nor takes care of consistency issues regarding related volumes (e.g., a volume to store database files, a volume to store application server data and a volume to store web server data). NDMP can be used to do backups in such an environment (e.g., SAP) but the logic required either must be put into a dedicated piece of software or must be scripted into the legacy backup software.

QUESTION 788
An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to- disk solution. This is appropriate because:

A. fast synthetic backups for offsite storage are supported.
B. backup to disk is always significantly faster than backup to tape.
C. tape libraries are no longer needed.
D. data storage on disks is more reliable than on tapes.

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Disk-to-disk (D2D) backup should not be seen as a direct replacement for backup to tape; rather, it should be viewed as part of a multitier backup architecture that takes advantage of the best features of both tape and disk technologies. Backups to disks are not dramatically faster than backups to tapes in a balanced environment. Most often than not there is hardly a difference, since the limiting components are not tape or disk drives but the overall sustained bandwidth of the backup server's backplane. The advantage in terms of speed is in restoring performance, since all data are on hand and can be accessed randomly, resulting in a dramatic enhancement in throughput. This makes fast synthetic backups (making a full back up without touching the host's data only by using the existing incremental backups) efficient and easy. Although the cost of disks has been reduced, tape-based backup can offer an overall cost advantage over disk-only solutions. Even if RAID arrays are used for D2Dstorage, a failed drive must be swapped out and the RAID set rebuilt before another disk drive fails, thus making this kind of backup more risky and not suitable as a solution of last resort. In contrast, a single tape drive failure does not produce any data loss since the data resides on the tape media. In a multidrive library, the loss of the use of a single tape drive has no impact on the overall level of data protection. Conversely, the loss of a disk drive in an array can put all data at risk. This in itself reinforces the benefits of a disk-to-disk-to-any storage hierarchy, as data could be protected by a tertiary stage of disk storage and ultimately tape. Beyond the drive failure issue, tape has an inherent reliability advantage over any disk drive as it has no boot sector or file allocation table that can be infected or manipulated by a virus.

QUESTION 789
Which of the following should be the MOST important criterion in evaluating a backup solution for sensitive data that must be retained for a long period of time due to regulatory requirements?

A. Full backup window
B. Media costs
C. Restore window
D. Media reliability

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To comply with regulatory requirements, the media should be reliable enough to ensure an organization's ability to recovery the data should they be required for any reason. Media price is a consideration, but should not be more important than the ability to provide the required reliability. Choices A and C are less critical than reliability.

QUESTION 790
Which of the following backup techniques is the MOST appropriate when an organization requires extremely granular data restore points, as defined in the recovery point objective (RPO)?

A. Virtual tape libraries
B. Disk-based snapshots
C. Continuous data backup
D. Disk-to-tape backup

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The recovery point objective (RPO) is based on the acceptable data loss in the case of a disruption. In this scenario the organization needs a short RPO. Virtual tape libraries, disk- based snapshots and disk-to-tape backup would require time to complete the backup, while continuous data backup happens online (in real time).

QUESTION 791
During an audit, an IS auditor notes that an organization's business continuity plan (BCP) does not adequately address information confidentiality during a recovery process. The IS auditor should recommend that the plan be modified to include:
A. the level of information security required when business recovery procedures are invoked.
B. information security roles and responsibilities in the crisis management structure.
C. information security resource requirements.
D. change management procedures for information security that could affect business continuity arrangements.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Business should consider whether information security levels required during recovery should be the same, lower or higher than when business is operating normally. In particular, any special rules for access to confidential data during a crisis need to be identified. The other choices do not directly address the information confidentiality issue.

QUESTION 792
Which of the following is the GREATEST risk when storage growth in a critical file server is not managed properly?

A. Backup time would steadily increase
B. Backup operational cost would significantly increase
C. Storage operational cost would significantly increase
D. Server recovery work may not meet the recovery time objective (RTO)

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In case of a crash, recovering a server with an extensive amount of data could require a significant amount of time. If the recovery cannot meet the recovery time objective (RTO), there will be a discrepancy in IT strategies. It's important to ensure that server restoration can meet the RTO. Incremental backup would only take the backup of the daily differential, thus a steady increase in backup time is not always true. The backup and storage costs issues are not as significant as not meeting the RTO.

QUESTION 793
Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?

A. Minimum operating requirements
B. Acceptable data loss
C. Mean time between failures
D. Acceptable time for recovery

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Recovery time objectives (RTOs) are the acceptable time delay in availability of business operations, while recovery point objectives (RPOs) are the level of data loss/reworking an organization is willing to accept. Mean time between failures and minimum operating requirements help in defining recovery strategies.

QUESTION 794
Which of the following is the GREATEST concern when an organization's backup facility is at a warm site?

A. Timely availability of hardware
B. Availability of heat, humidity and air conditioning equipment
C. Adequacy of electrical power connections
D. Effectiveness of the telecommunications network

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A warm site has the basic infrastructure facilities implemented, such as power, air conditioning and networking, but is normally lacking computing equipment. Therefore, the availability of hardware becomes a primary concern.

QUESTION 795
The PRIMARY purpose of a business impact analysis (BIA) is to:

A. provide a plan for resuming operations after a disaster.
B. identify the events that could impact the continuity of an organization's operations.
C. publicize the commitment of the organization to physical and logical security.
D. provide the framework for an effective disaster recovery plan.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
A business impact analysis (BIA) is one of the key steps in the development of a business continuity plan (BCP). A BIA will identify the diverse events that could impact the continuity of the operations of an organization.

QUESTION 796
After implementation of a disaster recovery plan, pre-disaster and post-disaster operational costs for an organization will:

A. decrease.
B. not change (remain the same).
C. increase.
D. increase or decrease depending upon the nature of the business.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
There are costs associated with all activities and disaster recovery planning (DRP) is not an exception. Although there are costs associated with a disaster recovery plan, there are unknown costs that are incurred if a disaster recovery plan is not implemented.

QUESTION 797
An organization's disaster recovery plan should address early recovery of:

A. all information systems processes.
B. all financial processing applications.
C. only those applications designated by the IS manager.
D. processing in priority order, as defined by business management.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Business management should know which systems are critical and when they need to process well in advance of a disaster. It is management's responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organizations that exist for the purpose of assisting the general user management in successfully performing their jobs.

QUESTION 798
Am advantage of the use of hot sites as a backup alternative is that:

A. the costs associated with hot sites are low.
B. hot sites can be used for an extended amount of time.
C. hot sites can be made ready for operation within a short period of time.
D. they do not require that equipment and systems software be compatible with the primary site.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Hot sites can be made ready for operation normally within hours. However, the use of hot sites is expensive, should not be considered as a long-term solution, and requires that equipment and systems software be compatible with the primary installation being backed up.

QUESTION 799
Disaster recovery planning (DRP) addresses the:

A. technological aspect of business continuity planning.
B. operational piece of business continuity planning.
C. functional aspect of business continuity planning.
D. overall coordination of business continuity planning.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Disaster recovery planning (DRP) is the technological aspect of business continuity planning. Business resumption planning addresses the operational part of business continuity planning.

QUESTION 800
The MAIN purpose for periodically testing offsite facilities is to:
A. protect the integrity of the data in the database.
B. eliminate the need to develop detailed contingency plans.
C. ensure the continued compatibility of the contingency facilities.
D. ensure that program and system documentation remains current.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The main purpose of offsite hardware testing is to ensure the continued compatibility of the contingency facilities. Specific software tools are available to protect the ongoing integrity of the database. Contingency plans should not be eliminated and program and system documentation should be reviewed continuously for currency.

QUESTION 801
A large chain of shops with electronic funds transfer (EFT) at point-of-sale devices has a central communications processor for connecting to the banking network. Which of the following is the BEST disaster recovery plan for the communications processor?

A. Offsite storage of daily backups
B. Alternative standby processor onsite
C. installation of duplex communication links
D. Alternative standby processor at another network node

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Having an alternative standby processor at another network node would be the best solution. The unavailability of the central communications processor would disrupt all access to the banking network, resulting in the disruption of operations for all of the shops. This could be caused by failure of equipment, power or communications. Offsite storage of backups would not help, since EFT tends to be an online process and offsite storage will not replace the dysfunctional processor. The provision of an alternate processor onsite would be fine if it were an equipment problem, but would not help in the case of a power outage, installation of duplex communication links would be most appropriate if it were only the communication link that failed.

QUESTION 802
Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

A. Developments may result in hardware and software incompatibility.
B. Resources may not be available when needed.
C. The recovery plan cannot be tested.
D. The security infrastructures in each company may be different.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If one organization updates its hardware and software configuration, it may mean that it is no longer compatible with the systems of the other party in the agreement. This may mean that each company is unable to use the facilities at the other company to recover their processing following a disaster. Resources being unavailable when needed are an intrinsic risk in any reciprocal agreement, but this is a contractual matter and is not the greatest risk. The plan can be tested by paper-based walkthroughs, and possibly by agreement between the companies. The difference in security infrastructures, while a risk, is not insurmountable.

QUESTION 803
An IS auditor reviewing an organization's IS disaster recovery plan should verify that it is:

A. tested every six months.
B. regularly reviewed and updated.
C. approved by the chief executive officer (CEO).
D. communicated to every department head in the organization.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The plan should be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel. Otherwise, it may become out of date and may no longer be effective. The plan must be subjected to regular testing, but the period between tests will again depend on the nature of the organization and the relative importance of IS. Three months or even annually may be appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally or more appropriate. For a purely ISrelated plan, the executive responsible for technology may have approved the plan. Similarly, although a business continuity plan is likely to be circulated throughout an organization, the IS disaster recovery plan will usually be a technical document and only relevant to IS and communications staff.

QUESTION 804
While reviewing the business continuity plan of an organization, an IS auditor observed that the organization's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?

A. Deterrence
B. Mitigation
C. Recovery
D. Response

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An effective business continuity plan includes steps to mitigate the effects of a disaster. Files must be restored on a timely basis for a backup plan to be effective. An example of deterrence is when a plan includes installation of firewalls for information systems. An example of recovery is when a plan includes an organization's hot site to restore normal business operations.

QUESTION 805
An offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment, is a:

A. cold site.
B. warm site.
C. dial-up site.
D. duplicate processing facility.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A cold site is ready to receive equipment but does not offer any components at the site in advance of the need. A warm site is an offsite backup facility that is partially configured with network connections and selected peripheral equipment-such as disk and tape units, controllers and CPUs-to operate an information processing facility. A duplicate information processing facility is a dedicated, self-developed recovery site that can back up critical applications.

QUESTION 806
A disaster recovery plan for an organization should:

A. reduce the length of the recovery time and the cost of recovery.
B. increase the length of the recovery time and the cost of recovery.
C. reduce the duration of the recovery time and increase the cost of recovery.
D. affect neither the recovery time nor the cost of recovery.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
One of the objectives of a disaster recovery plan is to reduce the duration and cost of recovering from a disaster. A disaster recovery plan would increase the cost of operations before and after the disaster occurs, but should reduce the time to return to normal operations and the cost that could result from a disaster.

QUESTION 807
A financial institution that processes millions of transactions each day has a central communications processor (switch) for connecting to automated teller machines (ATMs). Which of the following would be the BEST contingency plan for the communications processor?

A. Reciprocal agreement with another organization
B. Alternate processor in the same location
C. Alternate processor at another network node
D. Installation of duplex communication links

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The unavailability of the central communications processor would disrupt all access to the banking network. This could be caused by an equipment, power or communications failure. Reciprocal agreements make an organization dependent on the other organization and raise privacy, competition and regulatory issues. Having an alternate processor in the same location resolves the equipment problem, but would not be effective if the failure was caused by environmental conditions (i.e., power disruption). The installation of duplex communication links would only be appropriate if the failure were limited to the communication link.

QUESTION 808
Which of the following tasks should be performed FIRST when preparing a disaster recovery plan?

A. Develop a recovery strategy.
B. Perform a business impact analysis.
C. Map software systems, hardware and network components.
D. Appoint recovery teams with defined personnel, roles and hierarchy.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The first step in any disaster recovery plan is to perform a business impact analysis. All other tasks come afterwards.

QUESTION 809
An organization has implemented a disaster recovery plan. Which of the following steps should be carried out next?

A. Obtain senior management sponsorship.
B. Identify business needs.
C. Conduct a paper test.
D. Perform a system restore test.

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A best practice would be to conduct a paper test. Senior management sponsorship and business needs identification should have been obtained prior to implementing the plan. A paper test should be conducted first, followed by system or full testing.

QUESTION 810
When auditing a disaster recovery plan for a critical business area, an IS auditor finds that it does not cover all the systems. Which of the following is the MOST appropriate action for the IS auditor?

A. Alert management and evaluate the impact of not covering all systems.
B. Cancel the audit.
C. Complete the audit of the systems covered by the existing disaster recovery plan.
D. Postpone the audit until the systems are added to the disaster recovery plan.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
An IS auditor should make management aware that some systems are omitted from the disaster recovery plan. An IS auditor should continue the audit and include an evaluation of the impact of not including all systems in the disaster recovery plan. Cancelling the audit, ignoring the fact that some systems are not covered or postponing the audit are inappropriate actions to take.

QUESTION 811
Which of the following should be of MOST concern to an IS auditor reviewing the BCP?

A. The disaster levels are based on scopes of damaged functions, but not on duration.
B. The difference between low-level disaster and software incidents is not clear.
C. The overall BCP is documented, but detailed recovery steps are not specified.
D. The responsibility for declaring a disaster is not identified.

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
If nobody declares the disaster, the response and recovery plan would not be invoked, making all other concerns mute. Although failure to consider duration could be a problem, it is not as significant as scope, and neither is as critical as the need to have someone invoke the plan. The difference between incidents and lowlevel disasters is always unclear and frequently revolves around the amount of time required to correct the damage. The lack of detailed steps should be documented, but their absence does not mean a lack of recovery, if in fact someone has invoked the plan.

QUESTION 812
Of the following alternatives, the FIRST approach to developing a disaster recovery strategy would be to assess whether:

A. all threats can be completely removed.
B. a cost-effective, built-in resilience can be implemented.
C. the recovery time objective can be optimized.
D. the cost of recovery can be minimized.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is critical to initially identify information assets that can be made more resilient to disasters, e.g., diverse routing, alternate paths or multiple communication carriers. It is impossible to remove all existing and future threats. The optimization of the recovery time objective and efforts to minimize the cost of recovery come later in the development of the disaster recovery strategy.

QUESTION 813
An organization has a number of branches across a wide geographical area. To ensure that all aspects of the disaster recovery plan are evaluated in a cost effective manner, an IS auditor should recommend the use of a:

A. data recovery test.
B. full operational test.
C. posttest.
D. preparedness test.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A preparedness test should be performed by each local office/area to test the adequacy of the preparedness of local operations in the event of a disaster. This test should be performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence of the plan's adequacy. A data recovery test is a partial test and will not ensure that all aspects are evaluated. A full operational test is not the most cost effective test in light of the geographical dispersion of the branches, and a posttest is a phase of the test execution process.

QUESTION 814
A lower recovery time objective (RTO) results in:

A. higher disaster tolerance.
B. higher cost.
C. wider interruption windows.
D. more permissive data loss.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A recovery time objective (RTO) is based on the acceptable downtime in case of a disruption of operations. The lower the RTO, the higher the cost of recovery strategies. The lower the disaster tolerance, the narrower the interruption windows, and the lesser the permissive data loss.

QUESTION 815
Regarding a disaster recovery plan, the role of an IS auditor should include:

A. identifying critical applications.
B. determining the external service providers involved in a recovery test.
C. observing the tests of the disaster recovery plan. determining the criteria for
D. establishing a recovery time objective (RTO).

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The IS auditor should be present when disaster recovery plans are tested, to ensure that the test meets the targets for restoration, and the recovery procedures are effective and efficient. As appropriate, the auditor should provide a report of the test results. All other choices are a responsibility of management.

QUESTION 816
During a disaster recovery test, an IS auditor observes that the performance of the disaster recovery site's server is slow. To find the root cause of this, the IS auditor should FIRST review the:

A. event error log generated at the disaster recovery site.
B. disaster recovery test plan.
C. disaster recovery plan (DRP).
D. configurations and alignment of the primary and disaster recovery sites.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since the configuration of the system is the most probable cause, the IS auditor should review that first. If the issue cannot be clarified, the IS auditor should then review the event error log. The disaster recovery test plan and the disaster recovery plan (DRP) would not contain information about the system configuration.

QUESTION 817
An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:
A. a data loss of up to 1 minute, but the processing must be continuous.
B. a 1-minute processing interruption but cannot tolerate any data loss.
C. a processing interruption of 1 minute or more.
D. both a data less and processing interruption longer than 1 minute.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery point objective (RPO) measures how much data loss can be accepted. Choices B, C and D are incorrect since they exceed the RTO limits set by the scenario.

QUESTION 818
A live test of a mutual agreement for IT system recovery has been carried out, including a four- hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:

A. system and the IT operations team can sustain operations in the emergency environment.
B. resources and the environment could sustain the transaction load.
C. connectivity to the applications at the remote site meets response time requirements.
D. workflow of actual business operations can use the emergency system in case of a disaster.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The applications have been intensively operated, therefore choices B, C and D have been actually tested, but the capability of the system and the IT operations team to sustain and support this environment (ancillary operations, batch closing, error corrections, output distribution, etc.) is only partially tested.

QUESTION 819
After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?

A. Test and maintain the plan.
B. Develop a specific plan.
C. Develop recovery strategies.
D. implement the plan.

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster. After selecting a strategy, a specific plan can be developed, tested and implemented.

QUESTION 820
Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?

A. Pilot
B. Paper
C. Unit
D. System

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A paper test is appropriate for testing a BCP. it is a walkthrough of the entire plan, or part of the plan, involving major players in the plan's execution, who reason out what may happen in a particular disaster. Choices A, C and D are not appropriate for a BCP.

QUESTION 821
An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?

A. Nonavailability of an alternate private branch exchange (PBX) system
B. Absence of a backup for the network backbone
C. Lack of backup systems for the users' PCs
D. Failure of the access card system

Correct Answer: B
Section: Protection of Information Assets

Explanation
Explanation/Reference:
Explanation:
Failure of a network backbone will result in the failure of the complete network and impact the ability of all users to access information on the network. The nonavailability of an alternate PBX system will result in users not being able to make or receive telephone calls or faxes; however, users may have alternate means of communication, such as a mobile phone or e-mail. Lack of backup systems for user PCs will impact only the specific users, not all users. Failure of the access card system impacts the ability to maintain records of the users who are entering the specified work areas; however, this could be mitigated by manual monitoring controls.

QUESTION 822
As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

A. Organizational risks, such as single point-of-failure and infrastructure risk
B. Threats to critical business processes
C. Critical business processes for ascertaining the priority for recovery
D. Resources required for resumption of business

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The identification of the priority for recovering critical business processes should be addressed first. Organizational risks should be identified next, followed by the identification of threats to critical business processes. Identification of resources for business resumption will occur after the tasks mentioned.

QUESTION 823
Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?

A. verify compatibility with the hot site.
B. Review the implementation report.
C. Perform a walk-through of the disaster recovery plan.
D. Update the IS assets inventory.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS assets inventory is the basic input for the business continuity/disaster recovery plan, and the plan must be updated to reflect changes in the IS infrastructure. The other choices are procedures required to update the disaster recovery plan after having updated the required assets inventory.

QUESTION 824
Which of the following would contribute MOST to an effective business continuity plan (BCP)?

A. Document is circulated to all interested parties
B. Planning involves all user departments
C. Approval by senior management
D. Audit by an external IS auditor

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The involvement of user departments in the BCP is crucial for the identification of the business processing priorities. The BCP circulation will ensure that the BCP document is received by all users. Though essential, this does not contribute significantly to the success of the BCP. A BCP approved by senior management would not ensure the quality of the BCP, nor would an audit necessarily improve the quality of the BCP.

QUESTION 825
To develop a successful business continuity plan, end user involvement is critical during which of the following phases?

A. Business recovery strategy
B. Detailed plan development
C. Business impact analysis (BIA)
D. Testing and maintenance

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
End user involvement is critical in the BIA phase. During this phase the current operations of the business needs to be understood and the impact on the business of various disasters must be evaluated. End users are the appropriate persons to provide relevant information for these tasks, inadequate end user involvement in this stage could result in an inadequate understanding of business priorities and the plan not meeting the requirements of the organization.

QUESTION 826
While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/backup at an offsite location would be:

A. shadow file processing.
B. electronic vaulting.
C. hard-disk mirroring.
D. hot-site provisioning.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In shadow file processing, exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently. This is used for critical data files, such as airline booking systems. Electronic vaulting electronically transmits data either to direct access storage, an optical disc or another storage medium; this is a method used by banks. Hard-disk mirroring provides redundancy in case the primary hard disk fails. All transactions and operations occur on two hard disks in the same server. A hot site is an alternate site ready to take over business operations within a few hours of any business interruption and is not a method for backing up data.

QUESTION 827
Depending on the complexity of an organization's business continuity plan (BCP), the plan may be developed as a set of more than one plan to address various aspects of business continuity and disaster recovery, in such an environment, it is essential that:

A. each plan is consistent with one another.
B. all plans are integrated into a single plan.
C. each plan is dependent on one another.
D. the sequence for implementation of all plans is defined.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Depending on the complexity of an organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan. However, each plan has to be consistent with other plans to have a viable business continuity planning strategy. It may not be possible to define a sequence in which plans have to be implemented, as it may be dependent on the nature of disaster, criticality, recovery time, etc.

QUESTION 828
During a business continuity audit, an IS auditor found that the business continuity plan (BCP) covers only critical processes. The IS auditor should::

A. recommend that the BCP cover all business processes.
B. assess the impact of the processes not covered.
C. report the findings to the IT manager.
D. redefine the critical processes.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The business impact analysis needs to be either updated or revisited to assess the risk of not covering all processes in the plan. It is possible that the cost of including all processes might exceed the value of those processes; therefore, they should not be covered. An IS auditor should substantiate this by analyzing the risk.

QUESTION 829
The PRIMARY objective of testing a business continuity plan is to:

A. familiarize employees with the business continuity plan.
B. ensure that all residual risks are addressed.
C. exercise all possible disaster scenarios.
D. identify limitations of the business continuity plan.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Testing the business continuity plan provides the best evidence of any limitations that may exist. Familiarizing employees with the business continuity plan is a secondary benefit of a test. It is not cost effective to address residual risks in a business continuity plan, and it is not practical to test all possible disaster scenarios.

QUESTION 830
In determining the acceptable time period for the resumption of critical business processes: A.

only downtime costs need to be considered.

B. recovery operations should be analyzed.
C. both downtime costs and recovery costs need to be evaluated.
D. indirect downtime costs should be ignored.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Both downtime costs and recovery costs need to be evaluated in determining the acceptable time period before the resumption of critical business processes. The outcome of the business impact analysis (BIA) should be a recovery strategy that represents the optimal balance. Downtime costs cannot be looked at in isolation. The quicker information assets can be restored and business processing resumed, the smaller the downtime costs. However, the expenditure needed to have the redundant capability required to recover information resources might be prohibitive for nonessential business processes. Recovery operations do not determine the acceptable time period for the resumption of critical business processes, and indirect downtime costs should be considered in addition to the direct cash outflows

incurred due to business disruption. The indirect costs of a serious disruption to normal business activity, e.g., loss of customer and supplier goodwill and loss of market share, may actually be more significant than direct costs over time, thus reaching the point where business viability is threatened.

QUESTION 831
In the event of a disruption or disaster, which of the following technologies provides for continuous operations?

A. Load balancing
B. Fault-tolerant hardware
C. Distributed backups
D. High-availability computing

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Fault-tolerant hardware is the only technology that currently supports continuous, uninterrupted service. Load balancing is used to improve the performance of the server by splitting the work between several servers based on workloads. High-availability (HA) computing facilities provide a quick but not continuous recovery, while distributed backups require longer recovery times.

QUESTION 832
Which of the following would be MOST important for an IS auditor to verify when conducting a business continuity audit?

A. Data backups are performed on a timely basis
B. A recovery site is contracted for and available as needed
C. Human safety procedures are in place
D. insurance coverage is adequate and premiums are current

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

The most important element in any business continuity process is the protection of human life. This takes precedence over all other aspects of the plan.

QUESTION 833
Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

A. Business interruption
B. Fidelity coverage
C. Errors and omissions
D. Extra expense

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees. Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization. Errors and omissions insurance provides legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client. Extra expense insurance is designed to cover the extra costs of continuing operations following a disaster/ disruption within an organization.

QUESTION 834
The BEST method for assessing the effectiveness of a business continuity plan is to review the:

A. plans and compare them to appropriate standards.
B. results from previous tests.
C. emergency procedures and employee training.
D. offsite storage and environmental controls.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:

Previous test results will provide evidence of the effectiveness of the business continuity plan. Comparisons to standards will give some assurance that the plan addresses the critical aspects of a business continuity plan but will not reveal anything about its effectiveness. Reviewing emergency procedures, offsite storage and environmental controls would provide insight into some aspects of the plan but would fall short of providing assurance of the plan's overall effectiveness.

QUESTION 835
With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:

A. clarity and simplicity of the business continuity plans.
B. adequacy of the business continuity plans.
C. effectiveness of the business continuity plans.
D. ability of IS and end-user personnel to respond effectively in emergencies.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The IS auditor should interview key stakeholders to evaluate how well they understand their roles and responsibilities. When all stakeholders have a detailed understanding of their roles and responsibilities in the event of a disaster, an IS auditor can deem the business continuity plan to be clear and simple. To evaluate adequacy, the IS auditor should review the plans and compare them to appropriate standards. To evaluate effectiveness, the IS auditor should review the results from previous tests. This is the best determination for the evaluation of effectiveness. An understanding of roles and responsibilities by key stakeholders will assist in ensuring the business continuity plan is effective. To evaluate the response, the IS auditor should review results of continuity tests. This will provide the IS auditor with assurance that target and recovery times are met. Emergency procedures and employee training need to be reviewed to determine whether the organization had implemented plans to allow for the effective response.

QUESTION 836
During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:

A. responsibility for maintaining the business continuity plan.
B. criteria for selecting a recovery site provider.
C. recovery strategy.
D. responsibilities of key personnel.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most appropriate strategy is selected based on the relative risk level and criticality identified in the business impact analysis (BIA.) The other choices are made after the selection or design of the appropriate recovery strategy.

QUESTION 837
During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:

A. assessment of the situation may be delayed.
B. execution of the disaster recovery plan could be impacted.
C. notification of the teams might not occur.
D. potential crisis recognition might be ineffective.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Execution of the business continuity plan would be impacted if the organization does not know when to declare a crisis. Choices A, C and D are steps that must be performed to know whether to declare a crisis. Problem and severity assessment would provide information necessary in declaring a disaster. Once a potential crisis is recognized, the teams responsible for crisis management need to be notified. Delaying this step until a disaster has been declared would negate the effect of having response teams. Potential crisis recognition is the first step in responding to a disaster.

QUESTION 838
An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?

A. Review and evaluate the business continuity plan for adequacy
B. Perform a full simulation of the business continuity plan
C. Train and educate employees regarding the business continuity plan

D. Notify critical contacts in the business continuity plan

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The business continuity plan should be reviewed every time a risk assessment is completed for the organization. Training of the employees and a simulation should be performed after the business continuity plan has been deemed adequate for the organization. There is no reason to notify the business continuity plan contacts at this time.

QUESTION 839
The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:

A. duration of the outage.
B. type of outage.
C. probability of the outage.
D. cause of the outage.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The initiation of a business continuity plan (action) should primarily be based on the maximum period for which a business function can be disrupted before the disruption threatens the achievement of organizational objectives.

QUESTION 840
An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

A. alignment of the BCP with industry best practices.
B. results of business continuity tests performed by IS and end-user personnel.
C. off-site facility, its contents, security and environmental controls.
D. annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:

The effectiveness of the business continuity plan (BCP) can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives. All other choices do not provide the assurance of the effectiveness of the BCP.

QUESTION 841
To optimize an organization's business contingency plan (BCP), an IS auditor should recommend conducting a business impact analysis (BlA) in order to determine:

A. the business processes that generate the most financial value for the organization and therefore must be recovered first.
B. the priorities and order for recovery to ensure alignment with the organization's business strategy.
C. the business processes that must be recovered following a disaster to ensure the organization's survival.
D. he priorities and order of recovery which will recover the greatest number of systems in the shortest time frame.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To ensure the organization's survival following a disaster, it is important to recover the most critical business processes first, it is a common mistake to overemphasize value (A) rather than urgency. For example, while the processing of incoming mortgage loan payments is important from a financial perspective, it could be delayed for a few days in the event of a disaster. On the other hand, wiring funds to close on a loan, while not generating direct revenue, is far more critical because of the possibility of regulatory problems, customer complaints and reputation issues. Choices B and D are not correct because neither the long-term business strategy nor the mere number of recovered systems has a direct impact at this point in time.

QUESTION 842
A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?

A. Full-scale test with relocation of all departments, including IT, to the contingency site
B. Walk-through test of a series of predefined scenarios with all critical personnel involved
C. IT disaster recovery test with business departments involved in testing the critical applications
D. Functional test of a scenario with limited IT involvement

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
After a tabletop exercise has been performed, the next step would be a functional test, which includes the mobilization of staff to exercise the administrative and organizational functions of a recovery. Since the IT part of the recovery has been tested for years, it would be more efficient to verify and optimize the business continuity plan (BCP) before actually involving IT in a full-scale test. The full-scale test would be the last step of the verification process before entering into a regular annual testing schedule. A full-scale test in the situation described might fail because it would be the first time that the plan is actually exercised, and a number of resources (including IT) and time would be wasted. The walk- through test is the most basic type of testing. Its intention is to make key staff familiar with the plan and discuss critical plan elements, rather than verifying its adequacy. The recovery of applications should always be verified and approved by the business instead of being purely IT-driven. A disaster recovery test would not help in verifying the administrative and organizational parts of the BCP which are not IT-related.

QUESTION 843
Talking about the different approaches to security in computing, the principle of regarding the computer system itself as largely an untrusted system emphasizes:

A. most privilege
B. full privilege
C. least privilege
D. null privilege
E. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

There are two different approaches to security in computing. One focuses mainly on external threats, and generally treats the computer system itself as a trusted system. The other regards the computer system itself as largely an untrusted system, and redesigns it to make it more secure in a number of ways. This technique enforces the principle of least privilege to great extent, where an entity has only the privileges that are needed for its function.

QUESTION 844
Which of the following refers to the proving of mathematical theorems by a computer program?

A. Analytical theorem proving
B. Automated technology proving
C. Automated theorem processing
D. Automated theorem proving
E. None of the choices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Automated theorem proving (ATP) is the proving of mathematical theorems by a computer program. Depending on the underlying logic, the problem of deciding the validity of a theorem varies from trivial to impossible. Commercial use of automated theorem proving is mostly concentrated in integrated circuit design and verification.

QUESTION 845
"Under the concept of ""defense in depth"", subsystems should be designed to:"

A. ""fail insecure"""
B. ""fail secure"""
C. ""react to attack"""
D. ""react to failure"""
E. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"With 0""defense in depth"", more than one subsystem needs to be compromised to compromise the security of the system and the information it holds. Subsystems should default to secure settings, and wherever possible should be designed to ""fail secure"" rather than ""fail insecure"".

QUESTION 846
The 'trusted systems' approach has been predominant in the design of:

A. many earlier Microsoft OS products
B. the IBM AS/400 series
C. the SUN Solaris series
D. most OS products in the market
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The 'trusted systems' approach has been predominant in the design of many Microsoft OS products, due to the long-standing Microsoft policy of emphasizing functionality and 'ease of use'.

QUESTION 847
Human error is being HEAVILY relied upon on by which of the following types of attack?

A. Eavedropping
B. DoS
C. DDoS
D. ATP
E. Social Engineering
F. None of the choices.

Correct Answer: E

Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 848
Which of the following will replace system binaries and/or hook into the function calls of the operating system to hide the presence of other programs (choose the most precise answer)?

A. rootkits
B. virus
C. trojan
D. tripwire
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"A backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing ""legitimate"" program, or executable file. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports."

QUESTION 849
Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?

A. key pair
B. Oakley
C. certificate
D. 3-DES
E. one-time pad
F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad --has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

QUESTION 850
Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

A. Blowfish
B. Tripwire
C. certificate
D. DES
E. one-time pad
F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad - has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

QUESTION 851
You may reduce a cracker's chances of success by: (Choose
all that apply.)

A. keeping your systems up to date using a security scanner.
B. hiring competent people responsible for security to scan and update your systems.

C. using multiple firewalls.
D. using multiple firewalls and IDS.
E. None of the choices.

Correct Answer: AB
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Only a small fraction of computer program code is mathematically proven, or even goes through comprehensive information technology audits or inexpensive but extremely valuable computer security audits, so it is quite possible for a determined cracker to read, copy, alter or destroy data in well secured computers, albeit at the cost of great time and resources. You may reduce a cracker's chances by keeping your systems up to date, using a security scanner or/and hiring competent people responsible for security.

QUESTION 852
"Nowadays, computer security comprises mainly "preventive"" measures."

A. True
B. True only for trusted networks
C. True only for untrusted networks
D. False
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
"Nowadays, computer security comprises mainly ""preventive"" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network and is normally implemented as software running on the machine or as physical integrated hardware."

QUESTION 853
ALL computer programming languages are vulnerable to command injection attack.

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The majority of software vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. Some common languages such as C and C++ are vulnerable to all of these defects. Languages such as Java are immune to some of these defects but are still prone to code/ command injection and other software defects which lead to software vulnerabilities.

QUESTION 854
Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer?

A. buffer overflow
B. format string vulnerabilities
C. integer misappropriation
D. code injection
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

QUESTION 855
Buffer overflow aims primarily at corrupting:

A. system processor
B. network firewall

C. system memory
D. disk storage
E. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

QUESTION 856
Which of the following measures can effectively minimize the possibility of buffer overflows?

A. Sufficient bounds checking
B. Sufficient memory
C. Sufficient processing capability
D. Sufficient code injection
E. None of the choices

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Buffer overflows may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits. Sufficient bounds checking by either the programmer or the compiler can prevent buffer overflows.

QUESTION 857
Integer overflow occurs primarily with:
A. string formatting

B. debug operations
C. output formatting
D. input verificationsE. arithmetic operations
F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An integer overflow occurs when an arithmetic operation attempts to create a numeric value that is larger than can be represented within the available storage space. On some processors the result saturates - once the maximum value is reached attempts to make it larger simply return the maximum result.

QUESTION 858
Which of the following types of attack works by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs?

A. format string vulnerabilities
B. integer overflow
C. code injection
D. command injection
E. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Code injection is a technique to introduce code into a computer program or system by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs.

QUESTION 859
Which of the following is MOST likely to result from a business process reengineering (BPR) project?

A. An increased number of people using technology
B. Significant cost savings, through a reduction in the complexity of information technology
C. A weaker organizational structures and less accountability
D. Increased information protection (IP) risk will increase

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:
B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area.
D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

QUESTION 860
A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

A. Identify high-risk areas that might need a detailed review later
B. Reduce audit costs
C. Reduce audit time
D. Increase audit accuracy

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can identify high-risk areas that might need a detailed review later.

QUESTION 861
Host Based ILD&P primarily addresses the issue of:

A. information integrity
B. information accuracy
C. information validity
D. information leakage
E. None of the choices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Information Leakage Detection and Prevention (ILD&P) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Network ILD&P are gateway-based systems installed on the organization's internet network connection and analyze network traffic to search for unauthorized information transmissions. Host Based ILD&P systems run on end-user workstations to monitor and control access to physical devices and access information before it has been encrypted.

QUESTION 862
Which of the following are valid examples of Malware:

A. viruses
B. worms
C. trojan horses
D. spyware
E. All of the above

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Software is considered malware based on the intent of the creator rather than any particular features. It includes computer viruses, worms, trojan horses, spyware, adware, and other malicious and unwanted software.

QUESTION 863
Which of the following refers to any program that invites the user to run it but conceals a harmful or malicious payload?

A. virus
B. worm
C. trojan horse
D. spyware
E. rootkits
F. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 864
A Trojan horse's payload would almost always take damaging effect immediately.

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Broadly speaking, a Trojan horse is any program that invites the user to run it, but conceals a harmful or malicious payload. The payload may take effect immediately and can lead to immediate yet undesirable effects, or more commonly it may install further harmful software into the user's system to serve the creator's longer-term goals.

QUESTION 865
Which of the following terms is used more generally for describing concealment routines in a malicious program?

A. virus
B. worm
C. trojan horse
D. spyware
E. rootkits
F. backdoor
G. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Rootkits can prevent a malicious process from being reported in the process table, or keep its files from being read. Originally, a rootkit was a set of tools installed by a human attacker on a Unix system where the attacker had gained administrator access. Today, the term is used more generally for concealment routines in a malicious program.

QUESTION 866
To install backdoors, hackers generally prefer to use:

A. either Trojan horse or computer worm.
B. either Tripwire or computer virus.
C. either eavedropper or computer worm.
D. either Trojan horse or eavedropper.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A backdoor is a method of bypassing normal authentication procedures.

Many computer manufacturers used to preinstall backdoors on their systems to provide technical support for customers. Hackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors, hackers prefer to use either Trojan horse or computer worm.

QUESTION 867
Which of the following may be deployed in a network as lower cost surveillance and early-warning tools?

A. Honeypots
B. Hardware IPSs
C. Hardware IDSs
D. Botnets
E. Stateful inspection firewalls
F. Stateful logging facilities
G. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques.

QUESTION 868
Relatively speaking, firewalls operated at the application level of the seven layer OSI model are:

A. almost always less efficient.
B. almost always less effective.
C. almost always less secure.
D. almost always less costly to setup.
E. None of the choices.

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Early attempts at producing firewalls operated at the application level of the seven-layer OSI model but this required too much CPU processing power. Packet filters operate at the network layer and function more efficiently because they only look at the header part of a packet.

QUESTION 869
Relatively speaking, firewalls operated at the physical level of the seven-layer OSI model are:

A. almost always less efficient.
B. almost always less effective.
C. almost always less secure.
D. almost always less costly to setup.
E. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Early attempts at producing firewalls operated at the application level of the seven-layer OSI model but this required too much CPU processing power. Packet filters operate at the network layer and function more efficiently because they only look at the header part of a packet. NO FIREWALL operates at the physical level.

QUESTION 870
Which of the following refers to the act of creating and using an invented scenario to persuade a target to perform an action?

A. Pretexting
B. Backgrounding
C. Check making
D. Bounce checking
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
Pretexting is the act of creating and using an invented scenario to persuade a target to release information or perform an action and is usually done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information.

QUESTION 871
Pretexting is an act of:

A. DoS
B. social engineering
C. eavedropping
D. soft coding
E. hard coding
F. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Pretexting is the act of creating and using an invented scenario to persuade a target to release information or perform an action and is usually done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information.

QUESTION 872
With Deep packet inspection, which of the following OSI layers are involved?

A. Layer 2 through Layer 7
B. Layer 3 through Layer 7
C. Layer 2 through Layer 6
D. Layer 3 through Layer 6

E. Layer 2 through Layer 5
F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Deep packet inspection (DPI) is a form of computer network packet filtering that examines the data part of a through-passing packet, searching for non- protocol compliance or predefined criteria to decide if the packet can pass.
DPI devices have the ability to look at Layer 2 through Layer 7 of the OSI model.

QUESTION 873
Which of the following types of firewall treats each network frame or packet in isolation?

A. statefull firewall
B. hardware firewall
C. combination firewall
D. packet filtering firewall
E. stateless firewall
F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A stateless firewall treats each network frame or packet in isolation.
Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

QUESTION 874
Which of the following types of attack involves a program that creates an infinite loop, makes lots of copies of itself, and continues to open lots of files?

A. Local DoS attacks
B. Remote DoS attacks
C. Distributed DoS attacks
D. Local Virus attacks
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Local DoS attacks can be a program that creates an infinite loop, makes lots of copies of itself, and continues to open lots of files. The best defense is to find this program and kill it.

QUESTION 875
Which of the following are often considered as the first defensive line in protecting a typical data and information environment?

A. certificates
B. security token
C. password
D. biometrics
E. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password.

QUESTION 876
Which of the following are the characteristics of a good password?

A. It has mixed-case alphabetic characters, numbers, and symbols.
B. It has mixed-case alphabetic characters and numbers.
C. It has mixed-case alphabetic characters and symbols.
D. It has mixed-case alphabetic characters, numbers, and binary codes.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixedcase alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters.

QUESTION 877
Which of the following is a good tool to use to help enforcing the deployment of good passwords?

A. password cracker
B. local DoS attacker
C. network hackerD. remote windowing tool
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixedcase alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters. You may want to run a "password cracker" program periodically, and require users to immediately change any easily cracked passwords. In any case ask them to change their passwords every 90 to 120 days."

QUESTION 878
A virus typically consists of what major parts (Choose three.):

A. a mechanism that allows them to infect other files and reproduce" a trigger that activates delivery of a "payload""
B. a payload
C. a signature
D. None of the choices.

Correct Answer: ABC
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"A virus typically consist of three parts, which are a mechanism that allows them to infect other files and reproduce a trigger that activates delivery of a "payload" and the payload from which the virus often gets its name. The payload is what the virus does to the victim file."

QUESTION 879
Within a virus, which component is responsible for what the virus does to the victim file?

A. the payload
B. the signature
C. the trigger
D. the premium
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"A virus typically consist of three parts, which are a mechanism that allows them to infect other files and reproduce a trigger that activates delivery of a "payload" and the payload from which the virus often gets its name. The payload is what the virus does to the victim file."

QUESTION 880
Why is it not preferable for a firewall to treat each network frame or packet in isolation?
A. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
B. Such a firewall is costly to setup.
C. Such a firewall is too complicated to maintain.
D. Such a firewall is CPU hungry.
E. Such a firewall offers poor compatibility.
F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A stateless firewall treats each network frame or packet in isolation.
Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

QUESTION 881
Phishing attack works primarily through:

A. email and hyperlinks
B. SMS
C. chat
D. email attachment
E. news
F. file download
G. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
"Phishing applies to email appearing to come from a legitimate business, requesting "verification"" of information and warning of some dire consequence if it is not done. The letter usually contains a link to a fradulent web page that looks legitimate and has a form requesting everything from a home address to an ATM card's PIN."

QUESTION 882
Gimmes often work through:

A. SMS
B. IRC chat
C. email attachment
D. news
E. file download
F. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Gimmes take advantage of curiosity or greed to deliver malware. Also known as a Trojan Horse, gimmes can arrive as an email attachment promising anything. The recipient is expected to give in to the need to the program and open the attachment. In addition, many users will blindly click on any attachments they receive that seem even mildly legitimate.

QUESTION 883
Performance of a biometric measure is usually referred to in terms of (Choose three.):

A. failure to reject rate
B. false accept rate
C. false reject rate
D. failure to enroll rate
E. None of the choices.

Correct Answer: BCD
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false non match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted in, while the FRR measures the percent of valid users who are wrongly rejected.

QUESTION 884
Talking about biometric measurement, which of the following measures the percent of invalid users who are incorrectly accepted in?

A. failure to reject rate
B. false accept rate
C. false reject rate
D. failure to enroll rate
E. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false non match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted in, while the FRR measures the percent of valid users who are wrongly rejected.

QUESTION 885
An accurate biometric system usually exhibits (Choose two.):

A. low EER
B. low CER
C. high EER

D. high CER
E. None of the choices.

Correct Answer: AB
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
One most commonly used measure of real-world biometric systems is the rate at which both accept and reject errors are equal: the equal error rate (EER), also known as the cross-over error rate (CER). The lower the EER or CER, the more accurate the system is considered to be.

QUESTION 886
Wi-Fi Protected Access implements the majority of which IEEE standard?
A. 802.11i B.
802.11g
C. 802.11x
D. 802.11v
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Wi-Fi Protected Access (WPA / WPA2) is a class of systems to secure wireless computer networks. It implements the majority of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards (but not necessarily with first generation wireless access points). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used.

QUESTION 887
One major improvement in WPA over WEP is the use of a protocol which dynamically changes keys as the system is used. What protocol is this?

A. SKIP
B. RKIP

C. OKIP
D. EKIPE. TKIP
F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Wi-Fi Protected Access (WPA / WPA2) is a class of systems to secure wireless computer networks. It implements the majority of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards (but not necessarily with first generation wireless access points). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used.

QUESTION 888
Which of the following typically consists of a computer, some real looking data and/or a network site that appears to be part of a production network but which is in fact isolated and well prepared?

A. honeypot
B. superpot
C. IDS
D. IPS
E. firewall
F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
You may use a honeypot to detect and deflect unauthorized use of your information systems. A typical honeypot consists of a computer, some real looking data and/or a network site that appears to be part of a production network but which is in fact isolated and well prepared for trapping hackers.

QUESTION 889
Which of the following are valid choices for the Apache/SSL combination (Choose three.):

A. the Apache-SSL project
B. third-party SSL patches
C. the mod_ssl module
D. the mod_css module
E. None of the choices.

Correct Answer: ABC
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
On Linux you have Apache which is supposed to be a safer choice of web service. In fact you have several choices for the Apache/SSL combination, such as the Apache-SSL project (www.apache-ssl.org) using third-party SSL patches, or have Apache compiled with the mod_ssl module.

QUESTION 890
Most trojan horse programs are spread through: A.

e-mails.

B. MP3.
C. MS Office.
D. Word template.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"Most trojan horse programs are spread through e-mails. Some earlier trojan horse programs were bundled in "Root Kits". For example, the Linux Root Kit version 3 (lrk3) which was released in December 96 had tcp wrapper trojans included and enhanced in the kit. Portable devices that run Linux can also be affected by trojan horse. The Trojan.Linux.JBellz Trojan horse runs as a malformed .mp3 file."

QUESTION 891
Cisco IOS based routers perform basic traffic filtering via which of the following mechanisms?

A. datagram scanning
B. access lists
C. stateful inspection
D. state checking
E. link progressing
F. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In addition to deploying stateful firewall, you may setup basic traffic filtering on a more sophisticated router. As an example, on a Cisco IOS based router you may use ip access lists (ACL) to perform basic filtering on the network edge. Note that if they have denied too much traffic, something is obviously being too restrictive and you may want to reconfigure them.

QUESTION 892
The Federal Information Processing Standards (FIPS) are primarily for use by (Choose two.):

A. all non-military government agencies
B. US government contractors
C. all military government agenciesD. all private and public colleges in the US
E. None of the choices.

Correct Answer: AB
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal government for use by all nonmilitary government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community.

QUESTION 893
Which of the following refers to an important procedure when evaluating database security?

A. performing vulnerability assessments against the database.
B. performing data check against the database.
C. performing dictionary check against the database.
D. performing capacity check against the database system.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Databases provide many layers and types of security, including Access control, Auditing, Authentication, Encryption and Integrity controls. An important procedure when evaluating database security is performing vulnerability assessments against the database. Database administrators or Information security administrators run vulnerability scans on databases to discover misconfiguration of controls within the layers mentioned above along with known vulnerabilities within the database software.

QUESTION 894
Which of the following refers to any authentication protocol that requires two independent ways to establish identity and privileges?

A. Strong-factor authentication
B. Two-factor authentication
C. Dual-password authentication
D. Two-passphrases authentication
E. Dual-keys authentication
F. Rich-factor authentication

Correct Answer: B

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Two-factor authentication (T-FA) refers to any authentication protocol that requires two independent ways to establish identity and privileges. Common implementations of two-factor authentication use 'something you know' as one of the two factors, and use either 'something you have' or 'something you are' as the other factor. In fact, using more than one factor is also called strong authentication. On the other hand, using just one factor is considered by some weak authentication.

QUESTION 895
Common implementations of strong authentication may use which of the following factors in their authentication efforts (Choose three.):

A. 'something you know'
B. 'something you have'
C. 'something you are'
D. 'something you have done in the past on this same system'
E. 'something you have installed on this same system'
F. None of the choices.

Correct Answer: ABC
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Two-factor authentication (T-FA) refers to any authentication protocol that requires two independent ways to establish identity and privileges. Common implementations of two-factor authentication use 'something you know' as one of the two factors, and use either 'something you have' or 'something you are' as the other factor. In fact, using more than one factor is also called strong authentication. On the other hand, using just one factor is considered by some weak authentication.

QUESTION 896
Fault-tolerance is a feature particularly sought-after in which of the following kinds of computer systems:
A. desktop systems
B. laptop systems

C. handheld PDAs
D. business-critical systems
E. None of the choices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Fault-tolerance enables a system to continue operating properly in the event of the failure of some parts of it. It avoids total breakdown, and is particularly soughtafter in high-availability environment full of business critical systems.

QUESTION 897
The purpose of a mainframe audit is to provide assurance that processes are being implemented as required, the mainframe is operating as it should, security is strong, and that procedures in place are working and are updated as needed. The auditor may accordingly make recommendations for improvement. Which of the following types of audit always takes high priority over the others? (Choose five.)

A. System audit
B. Application audit
C. Software audit
D. License audit
E. Security server audit
F. None of the choices.

Correct Answer: ABCDE
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 898

A successful risk-based IT audit program should be based on: A.

an effective scoring system.

B. an effective PERT diagram.
C. an effective departmental brainstorm session.
D. an effective organization-wide brainstorm session.
E. an effective yearly budget.
F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A successful risk-based IT audit program could be based on an effective scoring system. In establishing a scoring system, management should consider all relevant risk factors and avoid subjectivity. Auditors should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee.

QUESTION 899
Your final audit report should be issued:

A. after an agreement on the observations is reached.
B. before an agreement on the observations is reached.
C. if an agreement on the observations cannot reached.
D. without mentioning the observations.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Reporting can take the forms of verbal presentation, an issue paper or a written audit report summarizing observations and management's responses. After agreement is reached on the observations, a final report can be issued.

QUESTION 900
In-house personnel performing IS audits should possess which of the following knowledge and/or skills (Choose two.):

A. information systems knowledge commensurate with the scope of the IT environment in question
B. sufficient analytical skills to determine root cause of deficiencies in question
C. sufficient knowledge on secure system coding
D. sufficient knowledge on secure platform development
E. information systems knowledge commensurate outside of the scope of the IT environment in question

Correct Answer: AB
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Personnel performing IT audits should have information systems knowledge commensurate with the scope of the institution's IT environment. They should also possess sufficient analytical skills to determine the root cause of deficiencies.

QUESTION 901
For application acquisitions with significant impacts, participation of your IS audit team should be encouraged:

A. early in the due diligence stage.
B. at the testing stage.
C. at the final approval stage.
D. at the budget preparation stage.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
For acquisitions with significant IT impacts, participation of IS audit is often necessary early in the due diligence stage as defined in the audit policy.

QUESTION 902
Which of the following is not a good tactic to use against hackers?

A. Enticement
B. Entrapment

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Enticement occurs after somebody has gained unlawful access to a system and then subsequently lured to a honey pot. Entrapment encourages the commitment of unlawful access. The latter is not a good tactic to use as it involves encouraging someone to commit a crime.

QUESTION 903
Which of the following is the **GREATEST** concern when an organization allows personal devices to connect to its network?

A. It is difficult to enforce the security policy on personal devices
B. Help desk employees will require additional training to support devices.
C. IT infrastructure costs will increase.
D. It is difficult to maintain employee privacy.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 904
Which of the following **BEST** ensures that effective change management is in place in an IS environment?

A. User authorization procedures for application access are well established. B.
User-prepared detailed test criteria for acceptance testing of the software.
C. Adequate testing was carried out by the development team.
D. Access to production source and object programs is well controlled.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 905
The **MOST** appropriate person to chair the steering committee for an enterprise-wide system development should normally be the:
A. project manager
B. IS director
C. executive level manager.
D. business analyst

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 906
Which of the following activities is **MOST** important to consider when conducting IS audit planning?

A. Results from previous audits are reviewed.
B. Audit scheduling is based on skill set of audit team.
C. Resources are allocated to areas of high risk.
D. The audit committee agrees on risk rankings.

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 907
A small startup organization does not have the resources to implement segregation of duties. Which of the following would be the **MOST** effective compensating control?

A. Rotation of log monitoring and analysis responsibilities
B. Additional management reviews and reconciliations
C. Third-party assessments
D. Mandatory vacations

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Reference:https://www.computerweekly.com/tip/Segregation-of-duties-Small-business-best-practices

QUESTION 908
Which of the following **BEST** facilitates compliance with requirements mandating the security of confidential data?

A. Classification of data
B. Security awareness training
C. Encryption of external data transmissions
D. Standardized escalation protocols for breaches

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 909
An IS auditor is performing an audit of a large organization's operating system maintenance procedures. Which of the following findings presents the **GREATEST** risk?

A. Some internal servers cannot be patched due to software incompatibility.
B. The configuration management database is not up-to-date.
C. Vulnerability testing is not performed on the development servers.
D. Critical patches are applied immediately while others follow quarterly release cycles.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 910
Which of the following should occur **EARLIEST** in a business continuity management lifecycle?
A. Defining business continuity procedures
B. Identifying critical business processes
C. Developing a training and awareness program
D. Carrying out a threat and risk assessment

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 911
While performing a risk-based audit, which of the following would **BEST** enable an IS auditor to identify and categorize risk?

A. Understanding the control framework
B. Developing a comprehensive risk model
C. Understanding the business environment

D. Adopting qualitative risk analysis

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 912
Which of the following is a **MAJOR** benefit of using a wireless network?

A. Faster network speed
B. Stronger authentication
C. Protection against eavesdropping
D. Lower installation cost

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:

QUESTION 913
Which of the following is appropriate when an IS auditor is conducting an exit meeting with senior management?

A. Eliminate significant findings where audit and management agree on risk acceptance.
B. Agree with senior management on the risk grading of the audit report.
C. Document written responses from management along with an implementation plan.
D. Escalate disputed recommendations to the audit committee.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 914
A new system development project is running late against a critical implementation deadline. Which of the following is the **MOST** important activity?

A. Document last-minute enhancements.
B. Perform user acceptance testing.
C. Perform a pre-implementation audit.
D. Ensure that code has been reviewed.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 915
Which of the following actions should an organization's security policy require an employee to take upon finding a security breach?

A. Report the incident to the manager immediately.
B. Inform IS audit management immediately.
C. Confirm the breach can be exploited.
D. Devise appropriate countermeasures.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 916
The performance of an order-processing system can be measured **MOST** reliably by monitoring:

A. input/request queue length.
B. turnaround time of completed transactions.
C. application and database servers' CPU load.
D. heartbeats between server systems.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 917
An IS auditor considering use of another auditor's workpapers should:

A. rarely rely on the work of another auditor.
B. determine that the workpapers were completed within the past month.
C. determine that then auditee agrees with key issues in these workpapers.
D. consider the appropriateness and sufficiency of the workpapers.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 918
Which of the following is the **MOST** important issue for an IS auditor to consider with regard to VoIP communications?

A. Continuity of service
B. Homogeneity of the network
C. Nonrepudiation
D. Identity management

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 919
The business case for an IS project has changed during the course of the project due to new requirements being added. What should be done **NEXT**?

A. The project should go through the formal reapproval process.
B. The changes to the business case should be documented in the project plan.
C. Additional resources should be allocated to the project due to the new requirements.
D. Project stakeholders should be notified of the changes.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 920
When planning an audit, it is acceptable for an IS auditor to rely on a third-party provider's external audit report on service level management when the:

A. report was released within the last 12 months.
B. scope and methodology meet audit requirements.
C. service provider is independently certified and accredited.
D. report confirms that service levels were not violated.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 921
When auditing a software development project, a review of which of the following will **BEST** verify that project work is adequately subdivided?

A. Work breakdown structure
B. Statement of work
C. Scope statement
D. Functional and technical design documents

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 922
An organization's business continuity plan should be:

A. updated based on changes to personnel and environments.
B. updated only after independent audit review by a third party.
C. tested whenever new applications are implemented.
D. tested after successful intrusions into the organization's hot site.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 923
Due to a recent business divesture, an organization has limited IT resources to deliver critical projects. Reviewing the IT staffing plan against which of the following would **BEST** guide IT management when estimating resource requirements for future projects?

A. Peer organizational staffing benchmarks
B. Budgeted forecast for the next financial year
C. Human resources sourcing strategy
D. Records of actual time spent on projects

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 924
During audit follow-up, an IS auditor finds that a control has been implemented differently than recommended. The auditor should:

A. verify whether the control objectives are adequately addressed.
B. compare the control to the action plan.
C. report as a repeat finding.
D. inform management about incorrect implementation.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 925
A source code repository should be designed to:

A. provide automatic incorporation and distribution of modified code.
B. prevent changes from being incorporated into existing code.
C. provide secure versioning and backup capabilities for existing code.
D. prevent developers from accessing secure source code.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 926
Which of the following could be determined by an entity-relationship diagram?

A. Links between data objects
B. How the system behaves as a consequence of external events
C. How data are transformed as they move through the system

D. Modes of behavior of data objects

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 927
To restore service at a large processing facility after a disaster, which of the following tasks should be performed **FIRST**?

A. Launch the emergency action team.
B. Inform insurance company agents.
C. Contact equipment vendors.
D. Activate the reciprocal agreement.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 928
A database is denormalized in order to:
A. prevent loss of data.
B. increase processing efficiency.
C. ensure data integrity.
D. save storage space.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 929
Electrical surge protectors **BEST** protect from the impact of:

A. electromagnetic interference.
B. power outages.
C. sags and spikes
D. reduced voltage.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 930
When planning an audit to assess application controls of a cloud-based system, it is **MOST** important for the IS auditor to understand the:

A. policies and procedures of the business area being audited.
B. business process supported by the system.
C. availability reports associated with the cloud-based system.
D. architecture and cloud environment of the system.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 931
An IS auditor is reviewing a contract for the outsourcing of IT facilities. If missing, which of the following should present the **GREATEST** concern to the auditor?

A. Access control requirements
B. Hardware configurations
C. Perimeter network security diagram

D. Help desk availability

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 932
Which of the following would be the **BEST** performance indicator for the effectiveness of an incident management program?

A. Incident alert meantime
B. Average time between incidents
C. Number of incidents reported
D. Incident resolution meantime

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 933
An IS auditor is reviewing the performance outcomes of controls in an agile development project. Which of the following would provide the **MOST** relevant evidence for the auditor to consider?

A. Progress report of outstanding work
B. Product backlog
C. Number of failed builds
D. Composition of the scrum team

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 934
An IS auditor performing an audit of backup procedures observes that backup tapes are picked up weekly and stored offsite at a third-party hosting facility. Which of the following recommendations would be the **BEST** way to protect the data on the backup tapes?

A. Ensure that data is encrypted before leaving the facility.
B. Ensure that the transport company obtains signatures for all shipments.
C. Confirm that data is transported in locked tamper-evident containers.
D. Confirm that data transfers are logged and recorded.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 935
During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's **NEXT** step?

A. Perform a review of terminated users' account activity.
B. Conclude that IT general controls are ineffective.
C. Communicate risks to the application owner.
D. Perform substantive testing of terminated users' access rights.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 936

In an organization that has a staff-rotation policy, the **MOST** appropriate access control model is:

A. role based.
B. discretionary.
C. mandatory.
D. lattice based.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 937
When protecting the confidentiality of information assets, the **MOST** effective control practice is the:

A. awareness training of personnel on regulatory requirements.
B. enforcement of a need-to-know access control philosophy.
C. utilization of a dual-factor authentication mechanism.
D. configuration of read-only access to all users.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 938
When designing metrics for information security, the **MOST** important consideration is that the metrics:
A. provide actionable data.
B. apply to all business units.
C. are easy to understand.
D. track trends over time.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Reference: https://m.isaca.org/Journal/archives/2016/volume-6/Documents/Journal-volume-6-2016.pdf

QUESTION 939
In a high-volume, real-time system, the **MOST** effective technique by which to continuously monitor and analyze transaction processing is:

A. integrated test facility (ITF).
B. embedded audit modules.
C. parallel simulation.
D. transaction tagging.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 940
Which of the following would **MOST** likely impact the integrity of a database backup?

A. Record fields contain null information
B. Open database files during backup
C. Relational database model used
D. Backing up the database to an optical disk

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:

QUESTION 941

Reviewing project plans and status reports throughout the development life cycle will:

A. eliminate the need to perform a risk assessment.
B. postpone documenting the project's progress until the final phase.
C. guarantee that the project will meet its intended deliverables.
D. facilitate the optimal use of resources over the life of the project.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 942
The final acceptance testing of a new application system should be the responsibility of the:

A. IS audit team.
B. user group
C. IS management
D. quality assurance team

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 943
Which of the following is **MOST** important when an organization contracts for the long-term use of a custom-developed application?

A. Documented coding standards
B. Error correction management
C. Contract renewal provisions
D. Escrow clause

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 944
An IS auditor has just completed a physical access review of the organization's primary data center. Which of the following weaknesses should be of **MOST** concern?

A. Metal keys are used for access.
B. Backups of video cameras are corrupt.
C. There is no mantrap at the main door.
D. There is no manual logging for visitors.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 945
An IS auditor's **PRIMARY** concern about a business partner agreement for the exchange of electronic information should be to determine whether there is:

A. a clause that addresses the audit of shared systems.
B. evidence of review and approval by each partner's legal department.
C. an information classification framework.
D. appropriate control and responsibility defined for each partner.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The overall purpose of using a formal information classification scheme is to ensure proper handling based on the information content and context. Context refers to the usage of information.
Two major risks are present in the absence of an information classification scheme. The first major risk is that information will be mishandled. The second major risk is that without an information classification scheme, all of the organization's data may be subject to scrutiny during legal proceedings. The information classification scheme safeguards knowledge. Failure to implement a records and data classification scheme leads to disaster

QUESTION 946
The **BEST** reason for implementing a virtual private network (VPN) is that it:

A. eases the implementation of data encryption.
B. allows for public use of private networks.
C. enables use of existing hardware platforms.
D. allows for private use of public networks.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Virtual private networks (VPNs) connect remote users over an insecure public network such as the Internet. The connection is virtual because it is temporary with no physical presence. VPN technology is cost-effective and highly flexible. A VPN creates an encrypted tunnel to securely pass data as follows: ▪ Between two machines (host-host)
▪ From a machine to a network (host-gateway)
▪ From one network to another network (gateway-gateway)

QUESTION 947
Which of the following would be the **PRIMARY** benefit of replacing physical keys with an electronic entry system for a data center?

A. Creates an audit trail
B. Enables data mining
C. Ensures compliance
D. Reduces cost

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 948
Which of the following would be the **BEST** way to address segregation of duties issues in an organization with budget constraints?

A. Perform an independent audit.
B. Rotate job duties periodically.
C. Implement compensating controls.
D. Hire temporary staff.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 949
In a large organization, IT deadlines on important projects have been missed because IT resources are not prioritized properly. Which of the following is the **BEST** recommendation to address this problem?

A. Implement project portfolio management.
B. Implement an integrated resource management system.
C. Implement a comprehensive project scorecard.
D. Revisit the IT strategic plan.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 950

C.

D.

A recent audit identified duplicate software licenses and technologies. Which of the following would be **MOST** helpful to prevent this type of duplication in the future?

A. Centralizing IT procurement and approval practices
B. Updating IT procurement policies and procedures
Conducting periodic inventory reviews
Establishing a project management office

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 951
An IS auditor finds multiple situations where the help desk resolved security incidents without notifying IT security as required by policy. Which of the following is the **BEST** audit recommendation?

A. Display the incident response hotline in common areas.
B. Have IT security review problem management policy.
C. Reinforce the incident escalation process.
D. Redesign the help desk reporting process.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 952
Organization A has a Software as a Service Agreement (SaaS) with Organization B. The software is vital to Organization A. Which of the following would provide the **GREATEST** assurance that the application can be recovered in the event of a disaster?

A. Organization B is responsible for disaster recovery and held accountable for interruption of service.
B. Organization A has a source code escrow agreement and hardware procurement provisions for disaster recovery purposes.
C. Organization B has a disaster recovery plan included in its contract and allows oversight by Organization A.
D. Organization A buys disaster insurance to recuperate losses in the event of a disaster.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
QUESTION 953
Which of the following should be of **MOST** concern to an IS auditor during the review of a quality management system?

A. The quality management system includes training records for IT personnel.
B. There are no records to document actions for minor business processes.
C. Important quality checklists are maintained outside the quality management system.
D. Indicators are not fully represented in the quality management system.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 954
An organization has begun using social media to communicate with current and potential clients. Which of the following should be of **PRIMARY** concern to the auditor?

A. Using a third-party provider to host and manage content
B. Lack of guidance on appropriate social media usage and monitoring
C. Negative posts by customers affecting the organization's image

C.

D.

D. Reduced productivity of stuff using social media

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 955
Which of the following is the **FIRST** step in initiating a data classification program?

A. Risk appetite assessment
B. Inventory of data assetsAssignment of data ownership Assignment of sensitivity levels

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The data classification process starts with the process of establishing ownership of data. This process also helps to prepare data dictionary

QUESTION 956
Which of the following is the **MOST** important difference between end-user computing (EUC) applications and traditional applications?

A. Traditional application documentation is typically less comprehensive than EUC application documentation.
B. Traditional applications require roll-back procedures whereas EUC applications do not.
C. Traditional applications require periodic patching whereas EUC applications do not.
D. Traditional application input controls are typically more robust than EUC application input controls.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 957
Which of the following is the **MOST** significant risk when an application uses individual end user accounts to access the underlying database?

A. User accounts may remain active after a termination.
B. Multiple connects to the database are used and slow the process.
C. Application may not capture a complete audit trail.
D. Users may be able to circumvent application controls.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 958
Which of the following is the **MOST** effective way to maintain network integrity when using mobile devices?

A. Perform network reviews.
B. Implement network access control.
C. Implement outbound firewall rules.
D. Review access control lists.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 959
Which of the following should be an IS auditor's **PRIMARY** focus when developing a risk-based IS audit program?

A. Business plans
B. Business processes

C.

D.

C. IT strategic plans
D. Portfolio management

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 960
During a follow-up audit, an IS auditor discovers that a recommendation has not been implemented. However, the auditee has implemented a manual workaround that addresses the identified risk, through far less efficiency than the recommended action would. Which of the following would be the auditor's **BEST** course of action?

A. Notify management that the risk has been addressed and take no further action.
B. Escalate the remaining issue for further discussion and resolution.
Note that the risk has been addressed and notify management of the inefficiency.
Insist to management that the original recommendation be implemented.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 961
Which of the following methods would be **MOST** effective in verifying that all changes have been authorized?

A. Reconciling problem tickets with authorized change control entries
B. Reconciling reports of changes in production libraries to authorized change log entries
C. Validating authorized change log entries with individual(s) who promoted into production
D. Reconciling reports of changes in development libraries to supporting documentation

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 962
During the evaluation of a firm's newly established whistleblower system, an auditor notes several findings. Which of the following should be the auditor's **GREATEST** concern?

A. New employees have not been informed of the whistleblower policy.
B. The whistleblower's privacy is not protected.
C. The whistleblower system does not track the time and date of submission.
D. The whistleblower system is only available during business hours.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

C.

D.

QUESTION 963
An organization allows its employees to use personal mobile devices for work. Which of the following would **BEST** maintain information security without compromising employee privacy?

A. Partitioning the work environment from personal space on devices
B. Preventing users from adding applications
C. Restricting the use of devices for personal purposes during working hours
D. Installing security software on the devices

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 964
Which of the following is a reason for implementing a decentralized IT governance model?

A. Standardized controls and economies of scale
B. IT synergy among business units
C. Greater consistency among business units
D. Greater responsiveness to business needs

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 965
A purpose of project closure is to determine the:

A. potential risks affecting the quality of deliverables.

B. lessons learned for use in future projects.
C. project feasibility requirements
professional expertise of the project manager.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 966
When providing a vendor with data containing personally identifiable information (PII) for offsite testing, the data should be:

A. current
B. encrypted.
C. sanitized.
D. backed up.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 967
An IS auditor is reviewing the results of a business process improvement project. Which of the following should be performed **FIRST**?

A. Evaluate control gaps between the old and the new processes.
B. Develop compensating controls.
C. Document the impact of control weaknesses in the process.
D. Ensure that lessons learned during the change process are documented.

Correct Answer: A

D.

Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 968
Which of the following must be in place before an IS auditor initiates audit follow-up activities?

A. A heat map with the gaps and recommendations displayed in terms of risk
B. A management response in the final report with a committed implementation date
C. Supporting evidence for the gaps and recommendations mentioned in the audit report
D. Available resources for the activities included in the action plan

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 969
To maintain the confidentiality of information moved between office and home on removable media, which of the following is the **MOST** effective control?

A. Mandatory file passwords
B. Security awareness training
C. Digitally signed media
D. Data encryption

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 970

An IS auditor intends to accept a management position in the data processing department within the same organization. However, the auditor is currently working on an audit of a major application and has not yet finished the report. Which of the following would be the **BEST** step for the IS auditor to take?

A. Start in the position and inform the application owner of the job change.
B. Start in the position immediately.
C. Disclose this issue to the appropriate parties.
D. Complete the audit without disclosure and then start in the position.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 971
Which of the following would **BEST** describe an audit risk?

A. The company is being sued for false accusations.
B. The financial report may contain undetected material errors.
C. Key employees have not taken vacation for 2 years.
D. Employees have been misappropriating funds.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 972
During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be **MOST** concerned with the:

A. allocation of resources during an emergency.
B. maintenance of hardware and software compatibility.
C. differences in IS policies and procedures.
D. frequency of system testing.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 973
While planning a review of IT governance, the IS auditor is **MOST** likely to:

A. examine audit committee minutes for IS-related matters and their control.
B. obtain information about the framework of control adopted by management.
C. assess whether business process owner responsibilities are consistent across the organization.
D. review compliance with policies and procedures issued by the board of directors.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 974
What is the **MOST** difficult aspect of access control in a multiplatform, multiple-site client/server environment?

A. Creating new user IDs valid only on a few hosts
B. Maintaining consistency throughout all platforms
C. Restricting a local user to necessary resources on a local platform
D. Restricting a local user to necessary resources on the host server

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 975
An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the **MOST** significant risk from this situation?

A. Developer access to production
B. Lack of system integrity
C. Outdated system documentation
D. Loss of application support

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 976
Which of the following would **BEST** help ensure information security is effective following the outsourcing of network operations?

A. Test security controls periodically.
B. Review security key performance indicators (KPIs).
C. Establish security service level agreements (SLAs).
D. Appoint a security service delivery monitoring manager.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 977
As part of a mergers and acquisitions activity, an acquiring organization wants to consolidate data and system from the organization being acquired into existing systems. To ensure the data is relevant, the acquiring organization should:

A. obtain data quality software.
B. define data quality requirements based on business needs.
C. automate the process of data collection and cleaning.
D. implement a data warehouse solution.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 978
A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items to the inventory system. Which control would have **BEST** prevented this type of fraud in a retail environment?

A. An edit check for the validity of the inventory transaction
B. Separate authorization for input of transactions
C. Unscheduled audits of lost stock lines
D. Statistical sampling of adjustment transactions

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 979
Which of the following controls will **MOST** effectively detect inconsistent records resulting from the lack of referential integrity in a database management system?

A. Concurrent access controls
B. Incremental data backups
C. Performance monitoring tools
D. Periodic table link checks

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 980
Which of the following is **MOST** appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

A. Apply single sign-on for access control.
B. Enforce an internal data access policy.
C. Enforce the use of digital signatures.
D. Implement segregation of duties.
Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 981
Which of the following is the **MOST** effective way for an organization to protect against data leakage?

A. Conduct periodic security awareness training.
B. Limit employee Internet access.
C. Review firewall logs for anomalies.
D. Develop a comprehensive data loss prevention policy.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 982
Disaster recovery planning for network connectivity to a hot site over a public-switched network would be **MOST** likely to include:

A. minimizing the number of points of presence
B. contracts for acquiring new leased lines
C. reciprocal agreements with customers of that network
D. redirecting private virtual circuits

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 983
An organization's software develops need access to personally identifiable information (PII) stored in a particular data format. Which of the following would be the **BEST** way to protect this sensitive information while allowing the developers to use it in development and test environments?

A. Data masking
B. Data encryption
C. Data tokenization
D. Data abstraction

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 984
When developing a business continuity plan (BCP), which of the following should be performed **FIRST**?

A. Develop business continuity training
B. Classify operations
C. Conduct a business impact analysis (BIA)
D. Establish a disaster recovery plan (DRP)

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 985
Which of the following activities is **MOST** important in determining whether a test of a disaster recovery plan (DRP) has been successful?

A. Evaluating participation by key personnel
B. Testing at the backup data center
C. Analyzing whether predetermined test objectives were met
D. Testing with offsite backup files

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 986
Which of the following should be the **FIRST** step when conducting an IT risk assessment?

A. Assess vulnerabilities
B. Identify assets to be protected
C. Evaluate controls in place
D. Identify potential threats

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 987
To develop a robust data security program, the **FIRST** course of action should be to:

A. implement monitoring controls
B. implement data loss prevention controls
C. perform an inventory of assets

D. interview IT senior management

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 988
When is the **BEST** time to commence continuity planning for a new application system?

A. Immediately after implementation
B. Just prior to the handover to the system maintenance group
C. During the design phase
D. Following successful user testing

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 989
An IS auditor is performing a consulting engagement and needs to make a recommendation for securing all doors to a data center to prevent unauthorized access. Which of the following access control techniques would be **MOST** difficult for an intruder to compromise?

A. Dead-man door and swipe card
B. Smart card and numeric keypad
C. USB token and password
D. Biometrics and PIN

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 990
When using digital signatures, a sender transmits an encrypted message digest. This ensures that the:

A. message is not intercepted during transmission
B. message is not altered during transmission
C. message sender obtains acknowledgement of delivery
D. message remains confidential during transmission

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 991
An information security risk analysis **BEST** assists an organization in ensuring that:

A. cost-effective decisions are made with regard to which assets need protection
B. the organization implements appropriate security technologies
C. the infrastructure has the appropriate level of access control
D. an appropriate level of funding is applied to security processes

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 992
When building a corporate-wide business continuity plan, it is discovered there are two separate lines of business systems that could be impacted by the same threat. Which of the following is the **BEST** method to determine the priority of systems recovery in the event of a disaster?

A. Reviewing the business plans of each department
B. Evaluating the cost associated with each system's outage
C. Reviewing each system's key performance indicators (KPIs)
D. Comparing the recovery point objectives (RPOs)

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:

QUESTION 993
Business applications should be selected for disaster recovery testing on the basis of:

A. the results of contingency desktop checks
B. the number of failure points that are being tested
C. recovery time objectives (RTOs)
C. criticality to the enterprise

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 994
When performing a data classification project, an information security manager should:

A. assign information critically and sensitivity
B. identify information owners
C. identify information custodians
D. assign information access privileges

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 995
A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following **MUST** be in place for this solution to be relevant to the organization?

A. An adequate data testing environment
B. Senior management support
C. A business case
D. A data classification

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 996
Which of the following needs be established **FIRST** in order to categorize data properly?

A. A data protection policy
B. A data classification framework
C. A data asset inventory
D. A data asset protection standard

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 997
Which of the following is **MOST** likely to prevent social engineering attacks?

A. Security awareness program
B. Employee background checks
C. Implementing positive identification policies
D. Enforcing stronger hiring policies

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 998
The recovery point objective (RPO) is required in which of the following?

A. Information security plan
B. Incident response plan
C. Disaster recovery plan
D. Business continuity plan

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 999
Which of the following is the **PRIMARY** purpose of data classification?

A. To determine access rights to data
B. To provide a basis for protecting data
C. To select encryption technologies
D. To ensure integrity of data

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1000
Which of the following is the **MOST** important reason for performing vulnerability assessments periodically?

A. Technology risks must be mitigated.
B. Management requires regular reports.
C. The environment changes constantly.
D. The current threat levels are being assessed.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1001
Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:

A. the likelihood of a given threat attempting to exploit a vulnerability
B. a function of the cost and effectiveness of controls over a vulnerability
C. the magnitude of the impact should a threat exploit a vulnerability
D. a function of the likelihood and impact, should a threat exploit a vulnerability

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1002
Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

A. Alternative routing
B. Diverse routing
C. Long haul network diversity
D. Last mile circuit protection

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Diverse routing routes traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. This type of access is time-consuming and costly. Long haul network diversity is a diverse long-distance network utilizing T1 circuits among the

major long-distance carriers. It ensures long-distance access should any one carrier experience a network failure. Last mile circuit protection is a redundant combination of local carrier T1s microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also utilized.
Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 259).

QUESTION 1003
Which of the following would be the FIRST step to help ensure the necessary regulatory requirements are addressed in an organization's cross-border data protection policy?

A. Conduct a risk assessment
B. Perform a gap analysis
C. Conduct stakeholder interviews
D. Perform a business impact analysis

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1004
Which of the following should an IS auditor recommend be done FIRST upon learning that new data protection legislation may affect the organization?

A. Implement data protection best practices
B. Implement a new security baseline for achieving compliance
C. Restrict system access for noncompliant business processes
D. Perform a gap analysis of data protection practices

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 1005
Data confidentiality is a requirement for an organization's new web service. Which of the following would provide the BEST protection?

A. Telnet
B. Secure Sockets Layer (SSL)
C. Transport Layer Security (TLS)
D. Secure File Transfer Protocol (SFTP)

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1006
The BEST way to assure an organization's board of directors that IT strategies support business objectives is to:

A. provide regular assessments of emerging technologies
B. identify and report on the achievement of critical success factors (CSFs)
C. confirm that IT strategies have been fully documented and disseminated
D. ensure that senior business managers review IT budgets

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1007

Which of the following is the **MOST** effective way to reduce risk to an organization from widespread use of web-based communication technologies?

A. Publish an enterprise-wide policy outlining acceptance use of web-based communication technologies.
B. Incorporate risk awareness training for web-based communications into the IT security program.
C. Monitor staff usage of web-based communication and notify the IT security department of violations.
D. Block access from user devices to unauthorized pages that allow web-based communication.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1008
Which of the following will enable a customer to authenticate an online Internet vendor?

A. Vendor signs a reply using a hash function and the customer's public key.
B. Customer encrypts an order using the vendor's public key.
C. Customer verifies the vendor's certificate with a certificate authority (CA).
D. Vendor decrypts incoming orders using its own private key.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1009
Which of the following is **MOST** likely to enable a hacker to successfully penetrate a system?

A. Lack of virus protection
B. Unpatched software
C. Decentralized dialup access
D. Lack of DoS protection

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1010
A stockbroker accepts orders over the Internet. Which of the following is the **MOST** appropriate control to ensure confidentiality of the orders?

A. Virtual private network
B. Public key encryption
C. Data Encryption Standard (DES)
D. Digital signature

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1011
Which of the following is the **GREATEST** advantage of application penetration testing over vulnerability scanning?

A. Penetration testing does not require a special skill set to be executed.

B. Penetration testing provides a more accurate picture of gaps in application controls.
C. Penetration testing can be conducted in a relatively short time period.
D. Penetration testing creates relatively smaller risks to application availability and integrity.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1012
A bank is relocating its servers to a vendor that provides data center hosting services to multiple clients. Which of the following controls would restrict other clients from physical access to the bank's servers?

A. Closed-circuit television cameras
B. Locking server cages
C. Biometric access at all data center entrances
D. 24-hour security guards
Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1013
Which of the following validation techniques would **BEST** prevent duplicate electronic vouchers?

A. Cyclic redundancy check
B. Edit check
C. Reasonableness check
D. Sequence check

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1014
On a daily basis, an in-house development team moves duplicate copies of production data containing personally identifiable information (PII) to the test environment. Which of the following is the **BEST** way to mitigate the privacy risk involved?

A. Require data owners to sign off on production data.
B. Encrypt the data file.
C. Obtain customer opt-in acceptances.
D. Sanitize the data in the test environment.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1015
Which of the following would **BEST** detect logic bombs in the new programs?

A. Final acceptance testing by users
B. Parallel/pilot testing
C. Regression testing
D. Independent program review

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1016
The **FIRST** course of action an investigator should take when a computer is being attacked is to:

A. terminate all active processes.
B. copy the contents of the hard drive.
C. disconnect it from the network.
D. disconnect the power source.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1017
Which of the following would be the **MOST** likely reason for an intrusion prevention system (IPS) being unable to block an ongoing web attack?

A. The firewall is not configured properly.
B. The network design contains flaws.
C. Monitoring personnel are not proactive.
D. Signatures are outdated.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1018
Due to the increasing size of a database, user access times and daily backups continue to increase. Which of the following would be the **BEST** way to address this situation?

A. Data modeling
B. Data visualization
C. Data mining
D. Data purging

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1019
Documentation of workaround processes to keep a business function operational during recovery of IT systems is a core part of a:

A. business impact analysis (BIA).
B. threat and risk assessment.
C. business continuity plan (BCP).
D. disaster recovery plan (DRP).

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1020
Which of the following protects against the impact of temporary and rapid decreases or increases in electricity?
A. Redundant power supply
B. Emergency power-off switch
C. Stand-by generator
D. Uninterruptible power supply (UPS)

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1021
An organization using instant messaging to communicate with customers can prevent legitimate customers from being impersonated by:

A. using call monitoring.
B. using firewalls to limit network traffic to authorized ports.
C. logging conversations.
D. authenticating users before conversations are initiated.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1022
As described at security policy, the CSO implemented an e-mail package solution that allows for ensuring integrity of messages sent using SMIME. Which of the options below BEST describes how it implements the environment to suite policy´s requirement?

A. Implementing PGP and allowing for recipient to receive the private key used to sign e-mail message.
B. Implementing RSA standard for messages envelope and instructing users to sign all messages using their private key from their PKI digital certificate.
C. Implementing RSA standard for messages envelope and instructing users to sign all messages using their public key from their PKI digital certificate.
D. Implementing MIME solutions and providing a footer within each message sent, referencing to policy constraints related to e-mail usage.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
RSA e-mail standers stands for SMIME envelope. Using tm's private key to sign messages, users will ensure recipients of message integrity by using sender´s public key for hash decryption and content comparison.

Exam candidates should be aware of e-mail solutions and technologies that addresses confidentiality, integrity and non-repudiation.

The following answers are incorrect:

Implementing PGP and allowing for recipient to receive the private key used to sign e-mail message.

Implementing RSA standard for messages envelope and instructing users to sign all messages using their public key from the PKI digital certificate.

Implementing MIME solutions and providing a footer within each message sent, referencing to policy constraints related to e-mail usage.

Reference:
CISA Review Manual 2010 - Chapter 5 - 5.4.5-Encryption - Digital Envelope

QUESTION 1023
Which of the following attack involves slicing small amount of money from a computerize transaction or account?

A. Eavesdropping
B. Traffic Analysis
C. Salami
D. Masquerading

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Salami slicing or Salami attack refers to a series of many small actions, often performed by clandestine means, that as an accumulated whole produces a much larger action or result that would be difficult or unlawful to perform all at once. The term is typically used pejoratively. Although salami slicing is often used to carry out illegal activities, it is only a strategy for gaining an advantage over time by accumulating it in small increments, so it can be used in perfectly legal ways as well. An example of salami slicing, also known as penny shaving, is the fraudulent practice of stealing money repeatedly in extremely small quantities, usually by taking advantage of rounding to the nearest cent (or other monetary unit) in financial transactions. It would be done by always rounding down, and putting the fractions of a cent into another account. The idea is to make the change small enough that any single transaction will go undetected.

In information security, a salami attack is a series of minor attacks that together results in a larger attack. Computers are ideally suited to automating this type of attack.

The following answers are incorrect:

Eavesdropping – is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis – is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Masquerading – A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Reference:

http://searchfinancialsecurity.techtarget.com/definition/eavesdropping http://en.wikipedia.org/wiki/Salami_slicing
http://en.wikipedia.org/wiki/Eavesdropping http://en.wikipedia.org/wiki/Traffic_analysis http://www.techopedia.com/definition/4020/masquerade-attack

QUESTION 1024
Which of the following is NOT a disadvantage of Single Sign On (SSO)?

A. Support for all major operating system environment is difficult
B. The cost associated with SSO development can be significant
C. SSO could be single point of failure and total compromise of an organization asset
D. SSO improves an administrator's ability to manage user's account and authorization to all associated system

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Single sign-on (SSO)is a Session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

SSO Advantages include
Multiple passwords are no longer required

It improves an administrator's ability to manage user's accounts and authorization to all associated systems
It reduces administrative overhead in resetting forgotten password over multiple platforms and applications It reduces time taken by users to logon into multiple application and platform

SSO Disadvantages include
Support for all major operating system is difficult

The cost associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary
The centralize nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information asset.

Reference:
CISA review manual 2014 Page number 332

QUESTION 1025
As an IS auditor, it is very important to make sure all storage media are well protected. Which of the following is the LEAST important factor for protecting CDs and DVDs?

A. Handle by edges or by the hole in the middle
B. Store in anti-static bag
C. Avoid long term exposure to bright light
D. Store in a hard jewel case, not in soft sleeves

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
CDs and DVDs are least affected by static current so it is not as important to store them into anti-static bags.

CDs and DVDs Storage protection recommendations:

Handle by edges or by hole in the middle
Be careful not to bend the CD or DVD
Avoid long term exposure to bright light
Store in a hard jewel case, not is soft sleeves

Also, you should know the media storage precautions listed below in preparation for the CISA exam:

USB and portable hard drive

Avoid high temperature, humidity extremes and strong magnetic field

Tape Cartridges
Store Cartridges vertically
Store cartridges in a protective container for transport

Write-protect cartridges immediately

Hard Drive
Store hard drives in anti-static bags, and be sure that person removing them from bag is static free If the original box and padding for the hard drive is available, use it for shipping
If the hard drive has been in a cold environment, bring it to room temperature prior to installing and using it

Reference:

Reference used - CISA review manual 2014. Page number 338

QUESTION 1026
As an auditor it is very important to ensure confidentiality, integrity, authenticity and availability are implemented appropriately in an information system. Which of the following definitions incorrectly describes these parameters?

1. Authenticity – A third party must be able to verify that the content of a message has been sent by a specific entity and nobody else.

2. Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party. A person cannot deny having sent a message if the message is signed by the originator.

3. Accountability – The action of an entity must be uniquely traceable to different entities
4. Availability – The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

A. All of the options presented

B. None of the options presented
C. Options number 1 and 2
D. Option number 3

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
It is important to read carefully the question. The word "incorrectly" was the key word. You had to find which one of the definitions presented is incorrect. The definition of Accountability was NOT properly described. Below you have the proper definition.

The correct definitions are as follows

Authenticity – A third party must be able to verify that the content of a message is from a specific entity and nobody else.

Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party. A person cannot deny having sent a message if the message is signed by the originator.

Accountability – The action of an entity must be uniquely traceable to that entity

Network availability – The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

Reference:

CISA review manual 2014 Page number 34

QUESTION 1027
There are many known weaknesses within an Intrusion Detection System (IDS). Which of the following is NOT a limitation of an IDS?

A. Weakness in the identification and authentication scheme.
B. Application level vulnerability.
C. Backdoor into application
D. Detect zero day attack.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Detecting zero day attack is an advantage of IDS system making use of behavior or heuristic detection.

It is important to read carefully the question. The word "NOT" was the key word.

Intrusion Detection System are somewhat limited in scope, they do not address the following:

Weakness in the policy definition
Application-level vulnerability
Backdoor within application
Weakness in identification and authentication schemes

Also, you should know the information below for your CISA exam:

An IDS works in conjunction with routers and firewall by monitoring network usage anomalies.

Broad category of IDS includes:

1. Network Based IDS
2. Host Based IDS

Network Based IDS
They identify attack within the monitored network and issue a warning to the operator.

If a network based IDS is placed between the Internet and the firewall, it will detect all the attack attempts whether or not they enter the firewall Network Based IDS are blinded when dealing with encrypted traffic

Host Based IDS
They are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack.
They can detect the modification of executable programs, detect the detection of files and issue a warning when an attempt is made to use a privilege account. They can monitor traffic after it is decrypted and they supplement the Network Based IDS.

Types of IDS includes:
Statistical Based IDS – This system needs a comprehensive definition of the known and expected behavior of system

Neural Network – An IDS with this feature monitors the general patterns of activity and traffic on the network, and create a database. This is similar to statistical model but with added self-learning functionality.

Signature Based IDS – These IDS system protect against detected intrusion patterns. The intrusive pattern they can identify are stored in the form of signature.
The following were incorrect answers:

The other options mentioned are all limitations of an IDS.

Reference:

CISA review manual 2014 Page number 346 and 347

QUESTION 1028
Which of the following is a software application that pretend to be a server on the Internet and is not set up purposely to actively protect against break-ins?

A. Bastion host
B. Honey pot
C. Dual Homed
D. Demilitarize Zone (DMZ)

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A Honey pot is a software application or system that pretends to be a normal server on the internet and it is not set up actively protect against all break-ins. In purpose, some of the updates, patches, or upgrades are missing.

You then monitor the honey pot to learn from the offensive side. There are two types of honey pot:

High-interaction Honey pots – Essentially gives hacker a real environment to attack. High-interaction honey pots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time. According to recent research into high-interaction honey pot technology, by employing virtual machines, multiple honey pots can be hosted on a single physical machine. Therefore, even if the honey pot is compromised, it can be restored more quickly. In general, high-interaction honey pots provide more security by being difficult to detect, but they are highly expensive to maintain. If virtual machines are not available, one honey pot must be maintained for each physical computer, which can be exorbitantly expensive. Example: Honey net.

Low interaction – Emulate production environment and therefore, provide more limited information. Low-interaction honey pots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Example: Honeyed.

The following were incorrect answers:

Bastion host - On the Internet, a bastion host is the only host computer that a company allows to be addressed directly from the public network and that is designed to screen the rest of its network from security exposure. DMZ or Demilitarize Zone In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Dual Homed - Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures for implementing preventive security.

Dual-Homed - An example of dual-homed devices are enthusiast computing motherboards that incorporate dual Ethernet network interface cards or a firewall with two network interface cards. One facing the external network and one facing the internal network.

Reference:

CISA review manual 2014 Page number 348

http://searchsecurity.techtarget.com/definition/bastion-host http://searchsecurity.techtarget.com/definition/DMZ http://en.wikipedia.org/wiki/Honeypot_%28computing%29
http://en.wikipedia.org/wiki/Dual-homed

QUESTION 1029
An IS auditor needs to consider many factors while evaluating an encryption system. Which of the following is LEAST important factor to be considered while evaluating an encryption system?

A. Encryption algorithm
B. Encryption keys
C. Key length
D. Implementation language

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Implementation language is LEAST important as compare to other options. Encryption algorithm, encryption keys and key length are key elements of an Encryption system.

It is important to read carefully the question. The word "LEAST" was the key word. You had to find which one was LEAST important.

The following were incorrect answers:

Other options mentioned are key elements of an Encryption system

Encryption Algorithm – A mathematically based function or calculation that encrypts/decrypts data
Encryption keys – A piece of information that is used within an encryption algorithm (calculation) to make encryption or decryption process unique. Similar to passwords, a user needs to use the correct key to access or decipher the message into an unreadable form.

Key length – A predetermined length for the key. The longer the key, the more difficult it is to compromise in brute-force attack where all possible key combinations are tried.

Reference:

CISA review manual 2014 Page number 348

QUESTION 1030
Which of the following comparisons are used for identification and authentication in a biometric system?

A. One-to-many for identification and authentication
B. One-to-one for identification and authentication
C. One-to-many for identification and one-to-one for authentication
D. One-to-one for identification and one-to-many for authentication

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
In identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual.
The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.
Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be"

In verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.

Management of Biometrics

Management of biometrics should address effective security for the collection, distribution and processing of biometrics data encompassing:
Data integrity, authenticity and non-repudiation
Management of biometric data across its life cycle – compromised of the enrollment, transmission and storage, verification, identification, and termination process Usage of biometric technology, including one-to-one and one-to-many matching, for identification and authentication Application of biometric technology for internal and external, as well as logical and physical access control Encapsulation of biometric data
Security of the physical hardware used throughout the biometric data life cycle Techniques for integrity and privacy protection of biometric data.

The following were incorrect answers:

All other choices presented were incorrectly describing identification and authentication mapping.

Reference:

CISA review manual 2014 Page number 331 http://en.wikipedia.org/wiki/Biometrics

QUESTION 1031
Which of the following is an advantage of asymmetric crypto system over symmetric key crypto system?

A. Performance and Speed
B. Key Management is built in
C. Adequate for Bulk encryption
D. Number of keys grows very quickly

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Key management is better in asymmetric key encryption as compare to symmetric key encryption. In fact, there is no key management built within Symmetric Crypto systems. You must use the sneaker net or a trusted courier to exchange the key securely with the person you wish to communicate with.

Key management is the major issue and challenge in symmetric key encryption.

In symmetric key encryption, a symmetric key is shared between two users who wish to communicate together. As the number of users grows, the number of keys required also increases very rapidly.

For example, if a user wants to communicate with 5 different users then total number of different keys required by the user are 10. The formula for calculating total number of key required is n(n-1)/2Or total number of users times total of users minus one divided by 2.

Where n is number of users communicating with each others securely.

In an asymmetric key encryption, every user will have only two keys, also referred to as a Key Pair. Private Key – Only known to the user who initially generated the key pair
Public key – Known to everyone, can be distributed at large

The following were incorrect answers:

Performance – Symmetric key encryption performance is better than asymmetric key encryption
Bulk encryption – As symmetric key encryption gives better performance, symmetric key should be used for bulk data encryption

Number of keys grows very quickly - The number of keys under asymmetric grows very nicely.1000 users would need a total of only 2000 keys, or a private and a public key for each user. Under symmetric encryption, one thousand users would need 495,000 keys to communicate securely with each others.

Reference:

CISA review manual 2014 Page number 348

QUESTION 1032
Which of the following is a form of Hybrid Cryptography where the sender encrypts the bulk of the data using Symmetric Key cryptography and then communicates securely a copy of the session key to the receiver?

A. Digital Envelope
B. Digital Signature
C. Symmetric key encryption
D. Asymmetric

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A Digital Envelope is used to send encrypted information using symmetric keys, and the relevant session key along with it. It is a secure method to send electronic document without compromising the data integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.

A Digital envelope mechanism works as follows:

The symmetric key, which is used to encrypt the bulk of the date or message can be referred to as session key. It is simply a symmetric key picked randomly in the key space.
In order for the receiver to have the ability to decrypt the message, the session key must be sent to the receiver.
This session key cannot be sent in clear text to the receiver, it must be protected while in transit, else anyone who have access to the network could have access to the key and confidentiality can easily be compromised.
Therefore, it is critical to encrypt and protect the session key before sending it to the receiver. The session key is encrypted using receiver's public key. Thus providing confidentiality of the key.
The encrypted message and the encrypted session key are bundled together and then sent to the receiver who, in turn opens the session key with the receiver matching private key.
The session key is then applied to the message to get it in plain text.

The process of encrypting bulk data using symmetric key cryptography and encrypting the session key with a public key algorithm is referred as a digital envelope. Sometimes people refer to it as Hybrid Cryptography as well.

The following were incorrect answers:

Digital-signature – A digital signature is an electronic identification of a person or entity created by using public key algorithm and intended to verify to recipient the integrity of the data and the identity of the sender. Applying a digital signature consist of two simple steps, first you create a message digest, then you encrypt the message digest with the sender's private key. Encrypting the message digest with the private key is the act of signing the message.

Symmetric Key Encryption - Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Asymmetric Key Encryption - The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both. Public-key algorithms are based on mathematical problems which currently admit no efficient solution that are inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to generate their own public and private key-pair and to use them for encryption and decryption. The strength lies in the fact that it is
"impossible" (computationally unfeasible) for a properly generated private key to be determined from its corresponding public key. Thus the public key may be published without compromising security, whereas the private key must not be revealed to anyone not authorized to read messages or perform digital signatures.
Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of one (or more) secret keys between the parties.

Reference:

CISA review manual 2014 Page number 350 and 351 http://en.wikipedia.org/wiki/Public-key_cryptography

QUESTION 1033
How does the digital envelop work? What are the correct steps to follow?

A. You encrypt the data using a session key and then encrypt session key using private key of a sender
B. You encrypt the data using the session key and then you encrypt the session key using sender's public key
C. You encrypt the data using the session key and then you encrypt the session key using the receiver's public key
D. You encrypt the data using the session key and then you encrypt the session key using the receiver's private key

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The process of encrypting bulk data using symmetric key cryptography and then encrypting the session key using public key algorithm is referred as a digital envelope.

A Digital Envelope is used to send encrypted information using symmetric crypto cipher and then key session along with it. It is secure method to send electronic document without compromising the data integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.

A Digital envelope mechanism works as follows:

The symmetric key used to encrypt the message can be referred to as session key. The bulk of the message would take advantage of the high speed provided by Symmetric Cipher.
The session key must then be communicated to the receiver in a secure way to allow the receiver to decrypt the message.
If the session key is sent to receiver in the plain text, it could be captured in clear text over the network and anyone could access the session key which would lead to confidentiality being compromised.
Therefore it is critical to encrypt the session key with the receiver public key before sending it to the receiver. The receiver's will use their matching private key to decrypt the session key which then allow them to decrypt the message using the session key.

The encrypted message and the encrypted session key are sent to the receiver who, in turn decrypts the session key with the receiver's private key. The session key is then applied to the message cipher text to get the plain text.

The following were incorrect answers:

You encrypt the data using a session key and then encrypt session key using private key of a sender - If the session key is encrypted using sender's private key, it can be decrypted only using sender's public key. The sender's public key is known to everyone so anyone can decrypt session key and message.

You encrypt the data using the session key and then you encrypt the session key using sender's public key - If the session key is encrypted by using sender's public key then only sender can decrypt the session key using his/her own private key and receiver will not be able to decrypt the same.

You encrypt the data using the session key and then you encrypt the session key using the receiver's private key - Sender should not have access to receiver's private key. This is not a valid option.

Reference:
CISA review manual 2014 Page number 350 and 351

QUESTION 1034
Which of the following is NOT a true statement about public key infrastructure (PKI)?

A. The Registration authority role is to validate and issue digital certificates to end users
B. The Certificate authority role is to issue digital certificates to end users
C. The Registration authority (RA) acts as a verifier for Certificate Authority (CA)
D. Root certificate authority's certificate is always self-signed

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The word NOT is the keyword used in the question. We need to find out the invalid statement from the options.

A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)

A public key infrastructure consists of:

A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requester A Subscriber is the end user who wish to get digital certificate from certificate authority.

The following were incorrect answers:

The Certificate authority role is to issue digital certificates to end users - This is a valid statement as the job of a certificate authority is to issue a digital certificate to end user.

The Registration authority (RA) acts as a verifier for Certificate Authority (CA) - This is a valid statement as registration authority acts as a verifier for certificate authority

Root certificate authority's certificate is always self-signed - This is a valid statement as the root certificate authority's certificate is always self-signed.

Reference:
http://searchsecurity.techtarget.com/definition/PKI
QUESTION 1035
Which of the following statement correctly describes one way SSL authentication between a client (e.g. browser) and a server (e.g. web server)?

A. Only the server is authenticated while client remains unauthenticated
B. Only the client is authenticated while server remains authenticated
C. Client and server are authenticated
D. Client and server are unauthenticated

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

Explanation:
In one way authentication only server needs to be authenticated where as in mutual authentication both the client and the server needs to be authenticated.

For CISA exam you should know the information below about Secure Socket Layer (SSL) and Transport Layer Security (TLS)

These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.

SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases
Peer negotiation for algorithm support
Public-key, encryption based key exchange and certificate based authentication Symmetric cipher based traffic encryption.

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.
The following were incorrect answers:

The other choices presented in the options are not valid as in one way authentication only server needs to be authenticated where as client will remain unauthenticated.

Reference:
CISA review manual 2014 Page number 352

QUESTION 1036
Which of the following statement correctly describes difference between SSL and S/HTTP?

A. Both works at application layer of OSI model
B. SSL works at transport layer where as S/HTTP works at application layer of OSI model
C. Both works at transport layer
D. S/HTTP works at transport layer where as SSL works at the application layer of OSI model

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
For your exam you should know below information about S/HTTP and SSL protocol:

Secure Hypertext Transfer Protocol (S/HTTP) -As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

Secure Socket Layer (SSL) and Transport Layer Security (TLS) - These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.
SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases
Peer negotiation for algorithm support
Public-key, encryption based key exchange and certificate based authentication Symmetric cipher based traffic encryption.
SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.

The following were incorrect answers:

The other choices presented in the options are not valid asSSL works at transport layer where as S/HTTP works at application layer of OSI model.

Reference:

CISA review manual 2014 Page number 352

QUESTION 1037
Which of the following statement correctly describes the differences between tunnel mode and transport mode of the IPSec protocol?

A. In transport mode the ESP is encrypted where as in tunnel mode the ESP and its header's are encrypted
B. In tunnel mode the ESP is encrypted where as in transport mode the ESP and its header's are encrypted
C. In both modes (tunnel and transport mode) the ESP and its header's are encrypted
D. There is no encryption provided when using ESP or AH

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology. For your exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.
In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.
In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/ Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

The other options presented are invalid as the transport mode encrypts ESP and the tunnel mode encrypts ESP and its header's.

Reference:
CISA review manual 2014 Page number 353

QUESTION 1038
Which of the following is the unique identifier within and IPSec packet that enables the sending host to reference the security parameter to apply?

A. SPI
B. SA
C. ESP
D. AH

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The Security Parameter Index (SPI) is the unique identifier that enables the sending host to reference the security parameter to apply in order to decrypt the packet.

For your exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.
In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.
In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/ Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

SA – Security Association (SA) defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc.
ESP – Encapsulation Security Payload (ESP) is used to support authentication of sender and encryption of data AH – Authentication Header allows authentication of a sender of a data.

Reference:
CISA review manual 2014 Page number 353

QUESTION 1039
Within IPSEC which of the following defines security parameters which should be applied between communicating parties such as encryption algorithms, key initialization vector, life span of keys, etc?

A. Security Parameter Index (SPI)
B. Security Association (SA)
C. Encapsulation Security Payload (ESP)
D. Authentication Header (AH)

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Security Association (SA)s defines which security parameters should be applied between communication parties as encryption algorithms, key initialization vector, life span of keys, etc.

For your exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.
For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.

In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/ Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

Security Parameter Index (SPI) – A Security Parameter Index (SPI) is an unique identifier that enables the sending host to reference the security parameters to apply.

Encapsulation Security Payload (ESP) – Encapsulation Security Payload (ESP) is used support authentication of sender and encryption of data.

Authentication Header(AH) – Authentication Header allows authentication of a sender of a data.

Reference:

CISA review manual 2014 Page number 353

QUESTION 1040
Which of the following malware technical fool's malware by appending section of themselves to files – somewhat in the same way that file malware appends themselves?

A. Scanners
B. Active Monitors
C. Immunizer
D. Behavior blocker

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Immunizers defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

For your exam you should know below mentioned different kinds of malware Controls

A. Scanners – Look for sequences of bit called signature that are typical malware programs.
The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.
2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)
Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker – Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker – Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.
E. Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.
The following were incorrect answers:

Scanners – Look for sequences of bit called signature that are typical malware programs.
Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

Behavior Blocker – Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

Reference:
CISA review manual 2014 Page number 354 and 355

QUESTION 1041
Which of the following security risks can be reduced by a properly configured network firewall?

A. Insider attacks
B. SQL injection attacks
C. Denial of service (DoS) attacks

D. Phishing attacks

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1042
Which of the following is a sophisticated computer based switch that can be thought of as essentially a small in-house phone company for the organization?

A. Private Branch Exchange
B. Virtual Local Area Network
C. Voice over IP
D. Dial-up connection

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A Private Branch Exchange(PBX) is a sophisticated computer based switch that can be thought of as essentially a small in-house phone company for the organization that operates it. Protection of PBX is thus a height priority. Failure to secure PBX can result in exposing the organization to toll fraud, theft of proprietary or confidential information, loss of revenue or legal entanglements.
PBX environment involves many security risks, presented by people both internal and external to an organization. The threat of the PBX telephone system is many, depending on the goals of these attackers, and include:

Theft of service – Toll fraud, probably the most common of motives for attacker.

Disclosure of Information – Data disclosed without authorization, either by deliberate actionably accident. Examples includes eavesdropping on conversation and unauthorized access to routing and address data.

Data Modification – Data altered in some meaningful way by recording, deleting or modifying it. For example, an intruder may change billing information or modify system table to gain additional services.

Unauthorized access – Actions that permit an unauthorized user to gain access to system resources or privileges.

Denial of service – Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

Traffic Analysis – A form of passive attack in which an intruder observes information about calls and make inferences, e.g. from the source and destination number or frequency and length of messages. For example, an intruder observes a high volume of calls between a company's legal department and patent office, and conclude that a patent is being filed.

The following were incorrect answers:

Virtual Local Area Network – A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to change in network requirements and relocation of workstations and server nodes.

Voice over IP – VoIP is a technology where voice traffic is carried on top of existing data infrastructure. Sounds are digitalized into IP packets and transferred through the network layer before being decode back into the original voice.

Dial-up connection – Dial-up refers to an Internet connection that is established using a modem. The modem connects the computer to standard phone lines, which serve as the data transfer medium. When a user initiates a dial-up connection, the modem dials a phone number of an Internet Service Provider (ISP) that is designated to receive dial-up calls. The ISP then establishes the connection, which usually takes about ten seconds and is accompanied by several beeping an buzzing sounds.

Reference:
CISA review manual 2014 Page number 356

QUESTION 1043
Which of the following PBX feature provides the possibility to break into a busy line to inform another user of an important message?

A. Account Codes
B. Access Codes
C. Override
D. Tenanting

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Override feature of PBS provides for the possibility to break into a busy line to inform another user an important message.

For CISA exam you should know below mentioned PBS features and Risks

System Features
Description
Risk
Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic
Call forwarding
Allow specifying an alternate number to which calls will be forwarded based on certain condition User tracking Account codes

Used to:
Track calls made by certain people or for certain projects for appropriate billing
Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes
Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features
Silent Monitoring
Silently monitors other calls
Eavesdropping
Conferencing

Allows for conversation among several users

Eavesdropping, by adding unwanted/unknown parties to a conference override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message Eavesdropping
Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting
Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail
Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release
Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension
Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress
Diagnostics
Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage

Camp-on or call waiting
When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections
Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility Eavesdropping on a line

The following were incorrect answers:

Account Codes – that are used to:
Track calls made by certain people or for certain projects for appropriate billing
Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Access Codes – Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Tenanting – Limits system user access to only those users who belong to the same tenant group useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Reference:

CISA review manual 2014 Page number 358

QUESTION 1044
Which of the following PBX feature supports shared extensions among several devices, ensuring that only one device at a time can use an extension?

A. Call forwarding
B. Privacy release
C. Tenanting
D. Voice mail

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Privacy release supports shared extensions among several devices, ensuring that only one device at a time can use an extension.

For your exam you should know below mentioned PBX features and Risks:

System Features
Description
Risk

Automatic Call distribution
Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding
Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking Account codes

Used to:
Track calls made by certain people or for certain projects for appropriate billing
Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes
Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features
Silent Monitoring

Silently monitors other calls
Eavesdropping Conferencing Allows for conversation among several users
Eavesdropping, by adding unwanted/unknown parties to a conference override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping
Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting
Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail
Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release
Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension
Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics
Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage
Camp-on or call waiting
When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections

Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:

Call forwarding - Allow specifying an alternate number to which calls will be forwarded based on certain condition

Tenanting -Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Voice Mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Reference:

CISA review manual 2014 Page number358

QUESTION 1045
Which of the following option INCORRECTLY describes PBX feature?

A. Voice mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
B. Tenanting-Provides for the possibility to break into a busy line to inform another user an important message
C. Automatic Call Distribution - Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available
D. Diagnostics -Allows for bypassing normal call restriction procedures

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The word INCORRECTLY was the keyword used in the question. You need to find out the incorrectly described PBX feature from given options. The Tenanting feature is incorrectly described.

Tenanting limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

For your exam you should know below mentioned PBX features and Risks:

System Features
Description
Risk

Automatic Call distribution
Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding
Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking Account codes

Used to:

Track calls made by certain people or for certain projects for appropriate billing

Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes
Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features Silent Monitoring

Silently monitors other calls

Eavesdropping
Conferencing
Allows for conversation among several users
Eavesdropping, by adding unwanted/unknown parties to a conference override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping

Auto-answer
Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting
Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail
Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release
Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension
Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics
Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage
Camp-on or call waiting
When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections
Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:
The other options presented correctly describes PBX features thus not the right choice.

Reference:
CISA review manual 2014 Page number358

QUESTION 1046
Who is responsible for providing adequate physical and logical security for IS program, data and equipment?

A. Data Owner
B. Data User
C. Data Custodian
D. Security Administrator

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Security administrator are responsible for providing adequate physical and logical security for IS programs, data and equipment.

For CISA exam you should know below roles in an organization

Data Owners – These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.
Data Custodian or Data Steward – These people are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:
Data Owner- These peoples are generally managers and directors responsible for using information for running and controlling the business.
Data Users – Data users, including internal and external user community, are the actual user of computerized data.
Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

Reference:
CISA review manual 2014 Page number 361

QUESTION 1047
Who is responsible for authorizing access level of a data user?

A. Data Owner
B. Data User
C. Data Custodian
D. Security Administrator

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Data owners are responsible for authorizing access level of a data user. These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

For your exam you should know below roles in an organization

Data Owners – Data Owners are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.
Data Custodian or Data Steward –are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Security Administrator -Security administrator is responsible for providing adequate and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.
Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

Reference:
CISA review manual 2014 Page number 361

QUESTION 1048
In computer forensics, which of the following is the process that allows bit-for-bit copy of a data to avoid damage of original data or information when multiple analysis may be performed?

A. Imaging
B. Extraction
C. Data Protection
D. Data Acquisition

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Imaging is the process that allows one to obtain a bit-for bit copy of a data to avoid damage to the original data or information when multiple analysis may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

For CISA exam you should know below mentioned key elements of computer forensics during audit planning.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.
Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Imaging -The Imaging is a process that allows one to obtain bit-for bit copy of a data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Reporting- The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis. The report should achieve the following goals

Accurately describes the details of an incident.

Be understandable to decision makers.
Be able to withstand a barrage of legal security Be unambiguous and not open to misinterpretation.
Be easily referenced
Contains all information required to explain conclusions reached Offer valid conclusions, opinions or recommendations when needed Be created in
timely manner.

The following were incorrect answers:

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Reference:
CISA review manual 2014 Page number367 and 368

QUESTION 1049
In computer forensic which of the following describe the process that converts the information extracted into a format that can be understood by investigator?

A. Investigation
B. Interrogation
C. Reporting
D. Extraction

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Investigation is the process that converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

For CISA exam you should know below mentioned key elements of computer forensics during audit planning.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Imaging -The Imaging is a process that allows one to obtain bit-for bit copy of a data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Reporting- The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis. The report should achieve the following goals

Accurately describes the details of an incident.

Be understandable to decision makers.
Be able to withstand a barrage of legal security Be unambiguous and not open to misinterpretation.
Be easily referenced
Contains all information required to explain conclusions reached Offer valid conclusions, opinions or recommendations when needed Be created in
timely manner.

The following were incorrect answers:

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.
Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability.

Reporting -The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis.

Reference:
CISA review manual 2014 Page number 367 and 368

QUESTION 1050

There are several types of penetration tests depending upon the scope, objective and nature of a test. Which of the following describes a penetration test where you attack and attempt to circumvent the controls of the targeted network from the outside, usually the Internet?

A. External Testing
B. Internal Testing
C. Blind Testing
D. Targeted Testing

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
External testing refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system, usually the Internet.

For the CISA exam you should know penetration test types listed below:

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system, usually the Internet

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Blind Testing -Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Double Blind Testing -It is an extension of blind testing, since the administrator and security staff at the target are also not aware of test. Such a testing can effectively evaluate the incident handling and response capability of the target and how well managed the environment is.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

The following were incorrect answers:

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Blind Testing -Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such a testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

Reference:
CISA review manual 2014 Page number 369

QUESTION 1051
Which of the following is penetration test where the penetration tester is provided with limited or no knowledge of the target's information systems?

A. External Testing
B. Internal Testing
C. Blind Testing
D. Targeted Testing

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Blind Testing refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target. Such a testing is expensive, since the penetration tester has to research the target and profile it based on publicly available information.

For your exam you should know below mentioned penetration types

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system is usually the Internet

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Blind Testing -Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such a testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Double Blind Testing -It is an extension of blind testing, since the administrator and security staff at the target are also not aware of test. Such a testing can effectively evaluate the incident handling and response capability of the target.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

The following were incorrect answers:

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system is usually the Internet

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

Reference:
CISA review manual 2014 Page number 369

QUESTION 1052

Which of the following term describes a failure of an electric utility company to supply power within acceptable range?

A. Sag
B. Blackout
C. Brownout
D. EMI

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

For CISA exam you should know below information about power failure

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Sags, spike and surge – Temporary and rapid decreases (sag) or increases (spike and surges) in a voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices.

Electromagnetic interference (EMI) - The electromagnetic interference (EMI) caused by electrical storms or noisy electrical equipments. The interference may cause computer system to hang or crash as well as damages similar to those caused by sags, spike and surges.

The following were incorrect answers:

Sag – Temporarily rapid decrease in a voltage.
Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Reference:
CISA review manual 2014 Page number372

QUESTION 1053
COBIT 5 separates information goals into three sub-dimensions of quality. Which of the following sub-dimension of COBIT 5 describes the extent to which data values are in conformance with the actual true value?

A. Intrinsic quality
B. Contextual and representational quality
C. Security quality
D. Accessibility quality

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Three sub-dimensions of quality in COBIT 5 are as follows:

1. Intrinsic quality – The extent to which data values are in conformance with the actual or true values. It includes

Accuracy – The extent to which information is correct or accurate and reliable
Objectivity – The extent to which information is unbiased, unprejudiced and impartial.
Believability – The extent to which information is regarded as true and credible.
Reputation – The extent to which information is highly regarded in terms of its source or content.

2. Contextual and Representational Quality – The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, reorganizing that information quality depends on the context of use. It includes

Relevancy – The extent to which information is applicable and helpful for the task at hand.
Completeness – The extent to which information is not missing and is of sufficient depth and breadth for the task at hand Currency – The extent to which information is sufficiently up to date for task at hand.
Appropriate amount of information – The extent to which the volume of information is appropriate for the task at hand Consistent Representation – The extent to which information is presented in the same format.
Interpretability – The extent to which information is in appropriate languages, symbols and units, with clear definitions.
Understandability - The extent to which information is easily comprehended.
Ease of manipulation – The extent to which information is easy to manipulate and apply to different tasks.

3. Security/accessibility quality – The extent to which information is available or obtainable. It includes:
Availability/timeliness – The extent to which information is available when required, or easily available when required, or easily and quickly retrievable.

Restricted Access – The extent to which access to information is restricted appropriately to authorize parties.

The following were incorrect answers:

Contextual and representational quality - The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, reorganizing that information quality depends on the context of use.

Security Quality or Accessibility quality -The extent to which information is available or obtainable.

Reference:
CISA review manual 2014 Page number 310

QUESTION 1054
During an IS audit, auditor has observed that authentication and authorization steps are split into two functions and there is a possibility to force the authorization step to be completed before the authentication step. Which of the following technique an attacker could user to force authorization step before authentication?

A. Eavesdropping
B. Traffic analysis
C. Masquerading
D. Race Condition

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A race condition is when processes carry out their tasks on a shared resource in an incorrect order. A race condition is possible when two or more processes use a shared resource, as in data within a variable. It is important that the processes carry out their functionality in the correct sequence. If process 2 carried out its task on the data before process 1, the result will be much different than if process1 carried out its tasks on the data before process 2.

In software, when the authentication and authorization steps are split into two functions, there is a possibility an attacker could use a race condition to force the authorization step to be completed before the authentication step. This would be a flaw in the software that the attacker has figured out how to exploit. A race condition occurs when two or more processes use the same resource and the sequences of steps within the software can be carried out in an improper order, something that can drastically affect the output. So, an attacker can force the authorization step to take place before the authentication step and gain unauthorized access to a resource.

The following answers are incorrect:
Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cyber crime opportunities if they’ve gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Reference:

CISA review manual 2014 Page number 324
Official ISC2 guide to CISSP CBK 3rd Edition Page number 66 CISSP All-In-One Exam guide 6th Edition Page Number 161

QUESTION 1055
Which of the following attack is also known as Time of Check(TOC)/Time of Use(TOU)?

A. Eavesdropping
B. Traffic analysis
C. Masquerading
D. Race Condition

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A Race Condition attack is also known as Time of Check(TOC)/Time of Use(TOU).

A race condition is when processes carry out their tasks on a shared resource in an incorrect order. A race condition is possible when two or more processes use a shared resource, as in data within a variable. It is important that the processes carry out their functionality in the correct sequence. If process 2 carried out its task on the data before process 1, the result will be much different than if process1 carried out its tasks on the data before process 2.
In software, when the authentication and authorization steps are split into two functions, there is a possibility an attacker could use a race condition to force the authorization step to be completed before the authentication step. This would be a flaw in the software that the attacker has figured out how to exploit. A race condition occurs when two or more processes use the same resource and the sequences of steps within the software can be carried out in an improper order, something that can drastically affect the output. So, an attacker can force the authorization step to take place before the authentication step and gain unauthorized access to a resource.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've

managed to attain. As such, masquerade attackers can have a full smorgasbord of cyber crime opportunities if they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Reference:
CISA review manual 2014 Page number 324
Official ISC2 guide to CISSP CBK 3rd Edition Page number 66
CISSP All-In-One Exam guide 6th Edition Page Number 161

QUESTION 1056
Which of the following attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call?

A. Eavesdropping
B. Traffic analysis
C. Masquerading
D. Interrupt attack

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
An Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Example: A boot sector virus typically issues an interrupt to execute a write to the boot sector.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cyber crime opportunities if they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Reference:
CISA review manual 2014 Page number 322

QUESTION 1057
Which of the following attack includes social engineering, link manipulation or web site forgery techniques?

A. surf attack
B. Traffic analysis
C. Phishing
D. Interrupt attack

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Phishing technique include social engineering, link manipulation or web site forgery techniques.

For your exam you should know the information below:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

Link manipulation
Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishes. In the following example URL, http:// www.yourbank.example.com/, it appears as though the URL will take you to the example section of the your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the tags) suggest a reliable destination, when the link actually goes to the phishes' site. The following example link, //en.wikipedia.org/wiki/Genuine, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phishes through the HTML tooltip tag.

Website forgery
Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

The following answers are incorrect:

Smurf Attack – Occurs when mix-configured network device allow packet to be sent to all hosts on a particular network via the broadcast address of the network

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Interrupt attack- Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Reference:

CISA review manual 2014 Page number 323
Official ISC2 guide to CISSP CBK 3rd Edition Page number 493 http://en.wikipedia.org/wiki/Phishing

QUESTION 1058
Which of the following attack is MOSTLY performed by an attacker to steal the identity information of a user such as credit card number, passwords, etc?

A. Smurf attack
B. Traffic analysis
C. Harming
D. Interrupt attack

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Harming is a cyber attack intended to redirect a website's traffic to another, bogus site. Harming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Harming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

The term "phrasing" is a neologism based on the words "farming" and "phishing". Phishing is a type of social-engineering attack to obtain access credentials, such as user names and passwords. In recent years, both phrasing and phishing have been used to gain information for online identity theft. Phrasing has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-harming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against harming.

For your exam you should know the information below:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

Link manipulation
Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishes. In the following example URL, http:// www.yourbank.example.com/, it appears as though the URL will take you to the example section of your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the are tags) suggest a reliable destination, when the link actually goes to the phishes' site. The following example link, //en.wikipedia.org/wiki/Genuine, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phishes through the HTML tooltip tag.

Website forgery
Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

The following answers are incorrect:

Smurf Attack – Occurs when mix-configured network device allow packet to be sent to all hosts on a particular network via the broadcast address of the network

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Interrupt attack- Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Reference:
CISA review manual 2014 Page number 323
Official ISC2 guide to CISSP CBK 3rd Edition Page number326 http://en.wikipedia.org/wiki/Phishing http://en.wikipedia.org/wiki/Pharming

QUESTION 1059
Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?
A. Palm Scan
B. Hand Geometry
C. Fingerprint
D. Retina scan

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Retina based biometric involves analyzing the layer of blood vessels situated at the back of the eye.
An established technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device. For these reasons, retinal scanning is not warmly accepted by all users, even though the technology itself can work well.

For your exam you should know the information below:

Biometrics
Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification and not well received by society. Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual's behavior, as in signature dynamics, but these can change over time and possibly be forged. Biometric systems that base authentication decisions on physical attributes (such as iris, retina, or fingerprint) provide more accuracy because physical attributes typically don't change, absent some disfiguring injury, and are harder to impersonate

Biometrics is typically broken up into two different categories. The first is the physiological. These are traits that are physical attributes unique to a specific individual. Fingerprints are a common example of a physiological trait used in biometric systems. The second category of biometrics is known as behavioral. The behavioral authentication is also known as continuous authentication. The behavioral/continuous authentication prevents session hijacking attack. This is based on a characteristic of an individual to confirm his identity. An example is signature Dynamics. Physiological is “what you are” and behavioral is “what you do.”

When a biometric system rejects an authorized individual, it is called a Type I error (false rejection rate). When the system accepts impostors who should be rejected, it is called a Type II error (false acceptance rate). The goal is to obtain low numbers for each type of error, but Type II errors are the most dangerous and thus the most important to avoid.
When comparing different biometric systems, many different variables are used, but one of the most important metrics is the crossover error rate (CER). This rating is stated as a percentage and represents the point at which the false rejection rate equals the false acceptance rate. This rating is the most important measurement when determining the system’s accuracy. A biometric system that delivers a CER of 3 will be more accurate than a system that delivers a CER of 4.
Crossover error rate (CER) is also called equal error rate (EER).

Throughput describes the process of authenticating to a biometric system. This is also referred to as the biometric system response time. The primary consideration that should be put into the purchasing and implementation of biometric access control are user acceptance, accuracy and processing speed.

Biometric Considerations
In addition to the access control elements of a biometric system, there are several other considerations that are important to the integrity of the control environment. These are:
Resistance to counterfeiting
Data storage requirements
User acceptance
Reliability and
Target User and approach

Fingerprint
Fingerprints are made up of ridge endings and bifurcations exhibited by friction ridges and other detailed characteristics called minutiae. It is the distinctiveness of these minutiae that gives each individual a unique fingerprint. An individual places his finger on a device that reads the details of the fingerprint and compares this to a reference file. If the two match, the individual’s identity has been verified.

Palm Scan
The palm holds a wealth of information and has many aspects that are used to identify an individual. The palm has creases, ridges, and grooves throughout that are unique to a specific person. The palm scan also includes the fingerprints of each finger. An individual places his hand on the biometric device, which scans and captures this information. This information is compared to a reference file, and the identity is either verified or rejected.

Hand Geometry
The shape of a person’s hand (the shape, length, and width of the hand and fingers) defines hand geometry. This trait differs significantly between people and is used in some biometric systems to verify identity. A person places her hand on a device that has grooves for each finger. The system compares the geometry of each finger, and the hand as a whole, to the information in a reference file to verify that person’s identity.

Retina Scan
A system that reads a person’s retina scans the blood-vessel pattern of the retina on the backside of the eyeball. This pattern has shown to be extremely unique between different people. A camera is used to project a beam inside the eye and capture the pattern and compare it to a reference file recorded previously.

Iris Scan
An iris scan is a passive biometric control
The iris is the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas, and furrows. The uniqueness of each of these characteristics within the iris is captured by a camera and compared with the information gathered during the enrollment phase.
When using an iris pattern biometric system, the optical unit must be positioned so the sun does not shine into the aperture; thus, when implemented, it must have proper placement within the facility.

Signature Dynamics
When a person signs a signature, usually they do so in the same manner and speed each time. Signing a signature produces electrical signals that can be captured by a biometric system. The physical motions performed when someone is signing a document create these electrical signals. The signals provide unique characteristics that can be used to distinguish one individual from another. Signature dynamics provides more information than a static signature, so there are more variables to verify when confirming an individual’s identity and more assurance that this person is who he claims to be.
Keystroke Dynamics
Whereas signature dynamics is a method that captures the electrical signals when a person signs a name, keystroke dynamics captures electrical signals when a person types a certain phrase. As a person types a specified phrase, the biometric system captures the speed and motions of this action. Each individual has a certain style and speed, which translate into unique signals. This type of authentication is more effective than typing in a password, because a password is easily obtainable. It is much harder to repeat a person’s typing style than it is to acquire a password.

Voice Print
People’s speech sounds and patterns have many subtle distinguishing differences. A biometric system that is programmed to capture a voice print and compare it to the information held in a reference file can differentiate one individual from another. During the enrollment process, an individual is asked to say several different words.

Facial Scan
A system that scans a person’s face takes many attributes and characteristics into account. People have different bone structures, nose ridges, eye widths, forehead sizes, and chin shapes. These are all captured during a facial scan and compared to an earlier captured scan held within a reference record. If the information is a match, the person is positively identified.

Hand Topography

Whereas hand geometry looks at the size and width of an individual's hand and fingers, hand topology looks at the different peaks and valleys of the hand, along with its overall shape and curvature. When an individual wants to be authenticated, she places her hand on the system. Off to one side of the system, a camera snaps a side-view picture of the hand from a different view and angle than that of systems that target hand geometry, and thus captures different data. This attribute is not unique enough to authenticate individuals by itself and is commonly used in conjunction with hand geometry.

Vascular Scan
Vascular Scan uses the blood vessel under the first layer of skin.

The following answers are incorrect:

Fingerprint - Fingerprints are made up of ridge endings and bifurcations exhibited by friction ridges and other detailed characteristics called minutiae. It is the distinctiveness of these minutiae that gives each individual a unique fingerprint. An individual places his finger on a device that reads the details of the fingerprint and compares this to a reference file. If the two match, the individual's identity has been verified.

Hand Geometry - The shape of a person's hand (the shape, length, and width of the hand and fingers) defines hand geometry. This trait differs significantly between people and is used in some biometric systems to verify identity. A person places her hand on a device that has grooves for each finger. The system compares the geometry of each finger, and the hand as a whole, to the information in a reference file to verify that person's identity.

Palm Scan - The palm holds a wealth of information and has many aspects that are used to identify an individual. The palm has creases, ridges, and grooves throughout that are unique to a specific person. The palm scan also includes the fingerprints of each finger. An individual places his hand on the biometric device, which scans and captures this information. This information is compared to a reference file, and the identity is either verified or rejected.

Reference:
CISA review manual 2014 Page number 330 and 331
Official ISC2 guide to CISSP CBK 3rd Edition Page number 924

QUESTION 1060
Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?

A. Confidentiality
B. Integrity
C. Availability
D. Accuracy

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis.

The level of access that an authorized individual should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information.

Identity theft is the act of assuming one's identity through knowledge of confidential information obtained from various sources.

An important measure to ensure confidentiality of information is data classification. This helps to determine who should have access to the information (public, internal use only, or confidential). Identification, authentication, and authorization through access controls are practices that support maintaining the confidentiality of information.

A sample control for protecting confidentiality is to encrypt information. Encryption of information limits the usability of the information in the event it is accessible to an unauthorized person.

For your exam you should know the information below:

Integrity
Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Information stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making. Controls are put in place to ensure that information is modified through accepted practices.

Sample controls include management controls such as segregation of duties, approval checkpoints in the systems development life cycle, and implementation of testing practices that assist in providing information integrity. Well-formed transactions and security of the update programs provide consistent methods of applying changes to systems. Limiting update access to those individuals with a need to access limits the exposure to intentional and unintentional modification.

Availability
Availability is the principle that ensures that information is available and accessible to users when needed.

The two primary areas affecting the availability of systems are:
1. Denial-of-Service attacks and
2. Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (e.g., earthquake, tornado, blackout, hurricane, fire, and flood).

In either case, the end user does not have access to information needed to conduct business. The criticality of the system to the user and its importance to the survival of the organization will determine how significant the impact of the extended downtime becomes. The lack of appropriate security controls can increase the risk of viruses, destruction of data, external penetrations, or denial-of-service (DOS) attacks. Such events can prevent the system from being used by normal users.
CIA

The following answers are incorrect:

Integrity- Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Availability - Availability is the principle that ensures that information is available and accessible to users when needed. Accuracy – Accuracy is not a valid CIA attribute.

Reference:
CISA review manual 2014 Page number 314
Official ISC2 guide to CISSP CBK 3rd Edition Page number 350

QUESTION 1061
Which of the following method should be recommended by security professional to erase the data on the magnetic media that would be reused by another employee?

A. Degaussing
B. Overwrite every sector of magnetic media with pattern of 1's and 0's
C. Format magnetic media
D. Delete File allocation table

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Software tools can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media.

For your exam you should know the information below:

When media is to be reassigned (a form of object reuse), it is important that all residual data is carefully removed. Simply deleting files or formatting media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information. Providing assurance for object reuse requires specialized tools and techniques according to the type of media on which the data resides. Specialized hardware devices known as degausses can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degasser is of sufficient strength to meet object reuse requirements when erasing data. If a degasser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.
Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There exists a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. To provide higher assurance in this case, it is necessary to overwrite each sector multiple times. Security practitioners should keep in mind that a one-time pass may be acceptable for noncritical information, but sensitive data should be overwritten with multiple passes.

Overwrite software can also be used to clear the sectors within solid-state media such as USB thumb drives. It is suggested that physical destruction methods such as incineration or secure recycling should be considered for solid-state media that is no longer used.
The last form of preventing unauthorized access to sensitive data is media destruction. Shredding, burning, grinding, and pulverizing are common methods of physically destroying media. Degaussing can also be a form of media destruction. High-power degausses are so strong in some cases that they can literally bend and warp the platters in a hard drive. Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine. However, the residue size might be too large for media containing sensitive information. Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media. Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal.

The following answers are incorrect:

Degaussing -Erasing data by applying magnetic field around magnetic media. Degausses device is used to erase the data. Sometime degausses can make magnetic media unusable. So degaussing is not recommended way if magnetic media needs to be reused.
Format magnetic media – Formatting magnetic media does not erase all data. Data can be recoverable after formatting using software tools.
Delete File allocation table-It will not erase all data. Data can be recoverable using software tools.

Reference:
CISA review manual 2014 Page number 338

QUESTION 1062
Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?

A. SSL
B. FTP
C. SSH
D. S/MIME

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The Secure Socket Layer (SSL) Protocol is primarily used to provide confidentiality to the information sent across clients and servers.

For your exam you should know the information below:

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmitted over a public network such as the Internet.

SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

SSL is included as part of both the Microsoft and Netscape browsers and most Web server products.

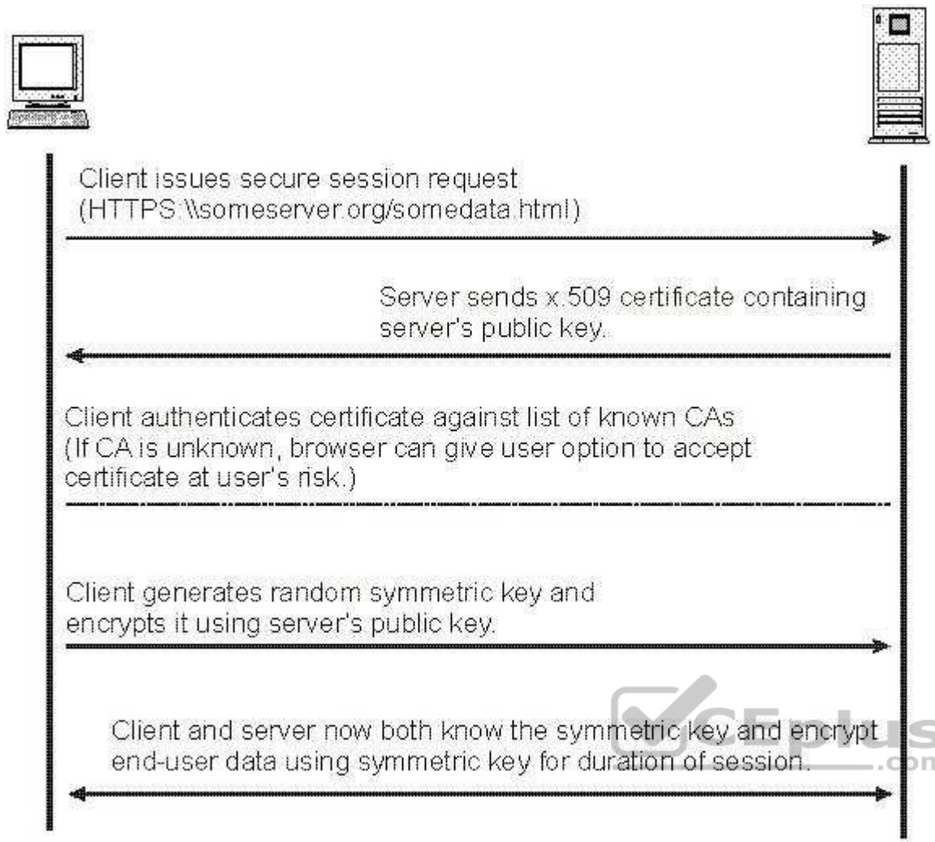
Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. Later on SSL uses a Session Key along a Symmetric Cipher for the bulk of the data.

TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Any Web server can be enabled by using Netscape's SSLRef program library which can be downloaded for noncommercial use or licensed for commercial use.

TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.

The SSL handshake
A HTTP-based SSL connection is always initiated by the client using a URL starting with https:// instead of with http://. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session. A simplified overview of how the SSL handshake is processed is shown in the diagram below.

SSL Handshake



The client sends a client "hello" message that lists the cryptographic capabilities of the client (sorted in client preference order), such as the version of SSL, the cipher suites supported by the client, and the data compression methods supported by the client. The message also contains a 28-byte random number.

The server responds with a server "hello" message that contains the cryptographic method (cipher suite) and the data compression method selected by the server, the session ID, and another random number.

Note:
The client and the server must support at least one common cipher suite, or else the handshake fails. The server generally chooses the strongest common cipher suite.

The server sends its digital certificate. (In this example, the server uses X.509 V3 digital certificates with SSL.)

If the server uses SSL V3, and if the server application (for example, the Web server) requires a digital certificate for client authentication, the server sends a "digital certificate request" message. In the "digital certificate request" message, the server sends a list of the types of digital certificates supported and the distinguished names of acceptable certificate authorities.

The server sends a server "hello done" message and waits for a client response. Upon receipt of the server "hello done" message, the client (the Web browser) verifies the validity of the server's digital certificate and checks that the server's "hello" parameters are acceptable.

If the server requested a client digital certificate, the client sends a digital certificate, or if no suitable digital certificate is available, the client sends a "no digital certificate" alert. This alert is only a warning, but the server application can fail the session if client authentication is mandatory.

The client sends a "client key exchange" message. This message contains the pre-master secret, a 46-byte random number used in the generation of the symmetric encryption keys and the message authentication code (MAC) keys, encrypted with the public key of the server.

If the client sent a digital certificate to the server, the client sends a "digital certificate verify" message signed with the client's private key. By verifying the signature of this message, the server can explicitly verify the ownership of the client digital certificate.

Note:
An additional process to verify the server digital certificate is not necessary. If the server does not have the private key that belongs to the digital certificate, it cannot decrypt the pre-master secret and create the correct keys for the symmetric encryption algorithm, and the handshake fails.

The client uses a series of cryptographic operations to convert the pre-master secret into a master secret, from which all key material required for encryption and message authentication is derived. Then the client sends a "change cipher spec" message to make the server switch to the newly negotiated cipher suite. The next message sent by the client (the "finished" message) is the first message encrypted with this cipher method and keys.

The server responds with a "change cipher spec" and a "finished" message of its own. The SSL handshake ends, and encrypted application data can be sent.

The following answers are incorrect:

FTP - File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

SSH - Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively.

S/MIME - S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail that uses the Rivets-Shamir-Adelman encryption system. S/MIME is included in the latest versions of the Web browsers from Microsoft and Netscape and has also been endorsed by other vendors that make messaging products. RSA has proposed S/MIME as a standard to the Internet Engineering Task Force (IETF).

Reference:
CISA review manual 2014 Page number 352
Official ISC2 guide to CISSP CBK 3rd Edition Page number 256 http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/ss7aumst18.htm

QUESTION 1063
IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

A. Inadequate screen/report design facilities
B. Complex programming language subsets
C. Lack of portability across operating systems
D. Inability to perform data intensive operations

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
4GLs are usually not suitable for data intensive operations. Instead, they are used mainly for graphic user interface (GUI) design or as simple query/report generators.

QUESTION 1064
Which of the following is MOST likely to result from a business process reengineering (BPR) Project?

A. An increased number of people using technology
B. Significant cost saving, through a reduction the complexity of information technology
C. A weaker organizational structures and less accountability
D. Increased information protection (IP) risk will increase

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:
B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area.
D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

QUESTION 1065
Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check
B. Check digit
C. Validity check

D. Duplicate check

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteria. In a duplicate check, newer fresh transactions are matched to those previously entered to ensure that they are not already in the system.

QUESTION 1066
A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

A. Unit testing
B. Integration testing
C. Design walk-throughs
D. Configuration management

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight), units are tested by the programmer, and then transferred to the acceptance test area. This often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

QUESTION 1067
The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

A. testing stage.
B. evaluation stage.
C. maintenance stage.
D. early stages of planning.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Company.com in the early stages of a BCP will incur the most significant level of program development effort, which will level out as the BCP moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

QUESTION 1068
Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

A. Check digit
B. Existence check
C. Completeness check
D. Reasonableness check

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A completeness check is used to determine if a field contains data and not zeros or blanks.

QUESTION 1069
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls
B. A compliance test of program library controls
C. A compliance test of the program compiler controls D. A substantive test of the program compiler controls

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

QUESTION 1070
A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

A. digest signature.
B. electronic signature.
C. digital signature.
D. hash signature.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

QUESTION 1071
Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?
A. Spool
B. Cluster controller
C. Protocol converter
D. Front end processor

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A front-end processor is a hardware device that connects all communication lines to a central computer to relieve the central computer.

QUESTION 1072
The use of a GANTT chart can:

A. aid in scheduling project tasks. B. determine project checkpoints.
C. ensure documentation standards.
D. direct the post-implementation review.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

QUESTION 1073
Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

A. Gateway
B. Protocol converter
C. Front-end communication processor
D. Concentrator/multiplexor

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
A gateway performs the job of translating e-mail formats from one network to another so messages can make their way through all the networks.

QUESTION 1074
Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

A. Specific developments only
B. Business requirements only
C. All phases of the installation must be documented
D. No need to develop a customer specific documentation

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

QUESTION 1075
A LAN administrator normally would be restricted from:

A. having end-user responsibilities.
B. reporting to the end-user manager.
C. having programming responsibilities.
D. being responsible for LAN security administration.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A LAN administrator should not have programming responsibilities but may have end- user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator also may be responsible for security administration over the LAN.

QUESTION 1076
For which of the following applications would rapid recovery be MOST crucial?

A. Point-of-sale system B. Corporate planning
C. Regulatory reporting
D. Departmental chargeback

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly.

QUESTION 1077
A malicious code that changes itself with each file it infects is called a:

A. logic bomb.
B. stealth virus.
C. trojan horse.
D. polymorphic virus.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

QUESTION 1078
Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

A. Paper test
B. Post test
C. Preparedness test
D. Walk-through

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments. A paper test is a walkthrough of the plan, involving major players, who attempt to determine what might happen in a particular type of service disruption in the plan's execution. A paper test usually precedes the preparedness test. A post-test is actually a test phase and is comprised of a group of activities, such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third- party systems. A walkthrough is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

QUESTION 1079
Which of the following is a data validation edit and control?

A. Hash totals
B. Reasonableness checks
C. Online access controls
D. Before and after image reporting

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A reasonableness check is a data validation edit and control, used to ensure that data conforms to predetermined criteria.

QUESTION 1080
A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:
A. reasonableness check.
B. parity check.
C. redundancy check.

D. check digits.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data.

QUESTION 1081
IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

QUESTION 1082
Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Proper segregation of duties prohibits a system analyst from performing quality-assurance functions.

QUESTION 1083
What should an IS auditor do if he or she observes that project-approval procedures do not exist?

A. Advise senior management to invest in project-management training for the staff
B. Create project-approval procedures for future project implementations
C. Assign project leaders
D. Recommend to management that formal approval procedures be adopted and documented

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
If an IS auditor observes that project-approval procedures do not exist, the IS auditor should recommend to management that formal approval procedures be adopted and documented.

QUESTION 1084
Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Proper segregation of duties normally prohibits a LAN administrator from also having programming responsibilities.

QUESTION 1085
Batch control reconciliation is a _____ (fill the blank) control for mitigating risk of inadequate segregation of duties. A. Detective

B. Corrective
C. Preventative
D. Compensatory

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Batch control reconciliations is a compensatory control for mitigating risk of inadequate segregation of duties.

QUESTION 1086
Key verification is one of the best controls for ensuring that:

A. Data is entered correctly
B. Only authorized cryptographic keys are used
C. Input is authorized
D. Database indexing is performed properly

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Key verification is one of the best controls for ensuring that data is entered correctly.

QUESTION 1087
What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

A. A star network topology
B. A mesh network topology with packet forwarding enabled at each host
C. A bus network topology
D. A ring network topology

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A mesh network topology provides a point-to-point link between every network host. If each host is configured to route and forward communication, this topology provides the greatest redundancy of routes and the greatest network fault tolerance.

QUESTION 1088
What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

A. Nonconnection-oriented protocols
B. Connection-oriented protocols
C. Session-oriented protocols
D. Nonsession-oriented protocols

Correct Answer: B

Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
The transport layer of the TCP/IP protocol suite provides for connection- oriented protocols to ensure reliable communication.

QUESTION 1089
How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

A. EDI usually decreases the time necessary for review.
B. EDI usually increases the time necessary for review.
C. Cannot be determined.
D. EDI does not affect the time necessary for review.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Electronic data interface (EDI) supports intervendor communication while decreasing the time necessary for review because it is usually configured to readily identify errors requiring follow-up.

QUESTION 1090
What would an IS auditor expect to find in the console log?

A. Evidence of password spoofing
B. System errors
C. Evidence of data copy activities
D. Evidence of password sharing

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An IS auditor can expect to find system errors to be detailed in the console log.

QUESTION 1091
Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing.

QUESTION 1092
What is essential for the IS auditor to obtain a clear understanding of network management?

A. Security administrator access to systems
B. Systems logs of all hosts providing application services
C. A graphical map of the network topology
D. Administrator access to systems

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A graphical interface to the map of the network topology is essential for the IS auditor to obtain a clear understanding of network management.

QUESTION 1093
What is the most common purpose of a virtual private network implementation?

A. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.
B. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a dedicated T1 connection.
C. A virtual private network (VPN) helps to secure access within an enterprise when communicating over a dedicated T1 connection between network segments within the same facility.
D. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a wireless connection.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.

QUESTION 1094
What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management?

A. The software can dynamically readjust network traffic capabilities based upon current usage.
B. The software produces nice reports that really impress management.
C. It allows users to properly allocate resources and ensure continuous efficiency of operations.
D. It allows management to properly allocate resources and ensure continuous efficiency of operations.

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Using capacity-monitoring software to monitor usage patterns and trends enables management to properly allocate resources and ensure continuous efficiency of operations.

QUESTION 1095
Which of the following best characterizes “worms”?

A. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email.
B. Programming code errors that cause a program to repeatedly dump data
C. Malicious programs that require the aid of a carrier program such as email
D. Malicious programs that masquerade as common applications such as screensavers or macro- enabled Word documents

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Worms are malicious programs that can run independently and can propagate without the aid of a carrier program such as email.

QUESTION 1096
What is an initial step in creating a proper firewall policy?

A. Assigning access to users according to the principle of least privilege
B. Determining appropriate firewall hardware and software
C. Identifying network applications such as mail, web, or FTP servers
D. Configuring firewall access rules

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Identifying network applications such as mail, web, or FTP servers to be externally accessed is an initial step in creating a proper firewall policy.

QUESTION 1097
What are used as the framework for developing logical access controls?
A. Information systems security policies
B. Organizational security policies
C. Access Control Lists (ACL)
D. Organizational charts for identifying roles and responsibilities

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Information systems security policies are used as the framework for developing logical access controls.

QUESTION 1098
Which of the following is a guiding best practice for implementing logical access controls?

A. Implementing the Biba Integrity Model
B. Access is granted on a least-privilege basis, per the organization's data owners
C. Implementing the Take-Grant access control model
D. Classifying data according to the subject's requirements

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners.

QUESTION 1099
Regarding digital signature implementation, which of the following answers is correct?

A. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
B. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
C. A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
D. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

QUESTION 1100
What are often the primary safeguards for systems software and data?

A. Administrative access controls
B. Logical access controls
C. Physical access controls
D. Detective access controls

Correct Answer: B

Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Logical access controls are often the primary safeguards for systems software and datA.

QUESTION 1101
Which of the following is an effective method for controlling downloading of files via FTP?

A. An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
B. An application-layer gateway, or proxy firewall
C. A circuit-level gateway
D. A first-generation packet-filtering firewall

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

QUESTION 1102
Which of the following provides the strongest authentication for physical access control?

A. Sign-in logs
B. Dynamic passwords
C. Key verification
D. Biometrics

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Biometrics can be used to provide excellent physical access control.

QUESTION 1103
What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off?

A. Employee security awareness training
B. Administrator alerts
C. Screensaver passwords
D. Close supervision

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off.
QUESTION 1104
What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources?

A. OSI Layer 2 switches with packet filtering enabled
B. Virtual Private Networks
C. Access Control Lists (ACL)

D. Point-to-Point Tunneling Protocol

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
ISPs can use access control lists to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources.

QUESTION 1105
What is the key distinction between encryption and hashing algorithms?

A. Hashing algorithms ensure data confidentiality.
B. Hashing algorithms are irreversible.
C. Encryption algorithms ensure data integrity.
D. Encryption algorithms are not irreversible.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A key distinction between encryption and hashing algorithms is that hashing algorithms are irreversible.

QUESTION 1106
Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

A. Data diddling
B. Skimming
C. Data corruption
D. Salami attack

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Data diddling involves modifying data before or during systems data entry.

QUESTION 1107
Who is ultimately responsible and accountable for reviewing user access to systems?

A. Systems security administrators
B. Data custodians
C. Data owners
D. Information systems auditors

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data owners are ultimately responsible and accountable for reviewing user access to systems.

QUESTION 1108
Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

A. End-user involvement

B. Senior management involvement
C. Security administration involvement
D. IS auditing involvement

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
End-user involvement is critical during the business impact assessment phase of business continuity planning.

QUESTION 1109
What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

A. Paper
B. Preparedness
C. Walk-through
D. Parallel

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Of the three major types of BCP tests (paper, walk-through, and preparedness), only the preparedness test uses actual resources to simulate a system crash and validate the plan's effectiveness.

QUESTION 1110
Which of the following typically focuses on making alternative processes and resources available for transaction processing?

A. Cold-site facilities
B. Disaster recovery for networks
C. Diverse processing
D. Disaster recovery for systems

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Disaster recovery for systems typically focuses on making alternative processes and resources available for transaction processing.

QUESTION 1111
What influences decisions regarding criticality of assets?

A. The business criticality of the data to be protected
B. Internal corporate politics
C. The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
D. The business impact analysis

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

QUESTION 1112

With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
With the objective of mitigating the risk and impact of a major business interruption, a disaster- recovery plan should endeavor to reduce the length of recovery time necessary and the costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs.

QUESTION 1113
Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Obtaining user approval of program changes is very effective for controlling application changes and maintenance.

QUESTION 1114
Library control software restricts source code to:

A. Read-only access
B. Write-only access
C. Full access
D. Read-write access

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Library control software restricts source code to read-only access.

QUESTION 1115
When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

A. In program development and change management
B. In program feasibility studies
C. In program development
D. In change management

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Regression testing is used in program development and change management to determine whether new changes have introduced any errors in the remaining unchanged code.

QUESTION 1116
What is often the most difficult part of initial efforts in application development?

A. Configuring software
B. Planning security
C. Determining time and resource requirements
D. Configuring hardware

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Determining time and resource requirements for an application-development project is often the most difficult part of initial efforts in application development.

QUESTION 1117
Whenever an application is modified, what should be tested to determine the full impact of the change?

A. Interface systems with other applications or systems
B. The entire program, including any interface systems with other applications or systems
C. All programs, including interface systems with other applications or systems
D. Mission-critical functions and any interface systems with other applications or systems

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change.

QUESTION 1118
The quality of the metadata produced from a data warehouse is _____ in the warehouse's design.

A. Often hard to determine because the data is derived from a heterogeneous data environment
B. The most important consideration
C. Independent of the quality of the warehoused databases
D. Of secondary importance to data warehouse content

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

QUESTION 1119
Who assumes ownership of a systems-development project and the resulting system?

A. User management
B. Project steering committee
C. IT management
D. Systems developers

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
User management assumes ownership of a systems-development project and the resulting system.

QUESTION 1120
If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

A. Documentation development
B. Comprehensive integration testing
C. Full unit testing
D. Full regression testing

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
If an IS auditor observes individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further comprehensive integration testing.

QUESTION 1121
When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
When participating in a systems-development project, an IS auditor should also strive to ensure that adequate and complete documentation exists for all projects.

QUESTION 1122
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

A. Function Point Analysis (FPA)
B. GANTT
C. Rapid Application Development (RAD)
D. PERT

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
PERT is a program-evaluation review technique that considers different scenarios for planning and control projects.

QUESTION 1123
An e-commerce enterprise's disaster recovery (DR) site has 30% less processing capability than the primary site. Based on this information, which of the following presents the **GREATEST** risk?

A. Network firewalls and database firewalls at the DR site do not provide high availability.
B. No disaster recovery plan (DRP) testing has been performed during the last six months.
C. The DR site is in a shared location that hosts multiple other enterprises.
D. The DR site has not undergone testing to confirm its effectiveness.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1124
Which of the following is the **MOST** important prerequisite to performing an information security assessment?

A. Reviewing the business impact analysis (BIA)
B. Assessing threats and vulnerabilities

C. Determining risk tolerance
D. Classifying assets

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1125
To ensure appropriate control of information processed in IT systems, security safeguards should be based **PRIMARILY** on:

A. established guidelines.
B. overall IT capacity and operational constraints.
C. efficient technical processing considerations.
D. criteria consistent with classification levels.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 1126
Which of the following is the **MOST** important factor when determining the frequency of information security risk reassessment?

A. Audit findings
B. Risk priority
C. Mitigating controls
D. Risk metrics

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1127
Utilizing external resources for highly technical information security tasks allows an information security manager to:

A. transfer business risk.
B. distribute technology risk.
C. outsource responsibility.
D. leverage limited resources.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1128
The **GREATEST** benefit of choosing a private cloud over a public cloud would be:

A. server protection.
B. online service availability.
C. containment of customer data.
D. collection of data forensics.
Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1129
Which is **MOST** important when contracting an external party to perform a penetration test?

A. Obtain approval from IT management.
B. Define the project scope.
C. Increase the frequency of log reviews.
D. Provide network documentation.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1130
The selection of security controls is **PRIMARILY** linked to:

A. risk appetite of the organization.
B. regulatory requirements.
C. business impact assessment.
D. best practices of similar organizations.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1131
When an operating system is being hardened, it is **MOST** important for an information security manager to ensure that:

A. default passwords are changed.
B. anonymous access is removed.
C. file access is restricted.
D. system logs are activated.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1132
What should be the **PRIMARY** objective of conducting interviews with business unit managers when developing an information security strategy?

A. Obtain information on department goals.
B. Classify information assets.
C. Identify data and system ownership.
D. Determine information types.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1133
Which of the following is **MOST** effective against system intrusions?

A. Continuous monitoring
B. Layered protection
C. Penetration testing
D. Two-factor authentication

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1134
Which of the following is **MOST** important to consider when developing a disaster recovery plan?

A. Business continuity plan (BCP) B. Feasibility assessment
C. Business impact analysis (BIA)
D. Cost-benefit analysis

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1135
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities **BEST** supports the concept of integrity?

A. Ensuring encryption for data in transit
B. Implementing a data classification schema
C. Utilizing a formal change management process
D. Enforcing service level agreements (SLAs)

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1136
Which of the following tools **BEST** demonstrate the effectiveness of the information security program?
A. A security balanced scorecard
B. Management satisfaction surveys
C. Risk heat map
D. Key risk indicators (KRIs)

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1137
Following a malicious security incident, an organization has decided to prosecute those responsible. Which of the following will **BEST** facilitate the forensic investigation?

A. Identifying the affected environment
B. Performing a backup of affected systems

C. Determining the degree of loss
D. Maintaining chain of custody

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1138
Calculation of the recovery time objective (RTO) is necessary to determine the:

A. time required to restore files.
B. annual loss expectancy (ALE).
C. point of synchronization.
D. priority of restoration.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1139
The **PRIMARY** purpose of a periodic threat and risk assessment report to senior management is to communicate the:

A. cost-benefit of security controls.
B. status of the security posture.
C. probability of future incidents.
D. risk acceptance criteria.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1140
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do?

A. Lack of IT documentation is not usually material to the controls tested in an IT audit.
B. The auditor should at least document the informal standards and policies. Furthermore, the IS auditor should create formal documented policies to be implemented.
C. The auditor should at least document the informal standards and policies, and test for a compliance. Furthermore, the IS auditor should recommend management that formal documented policies be developed and implemented.
D. The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should create formal documented policies to be implemented.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, the auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.

QUESTION 1141
Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data- calculation procedures. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Fourth-generation languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

QUESTION 1142
Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Network environments often add to the complexity of program-to-program communication, making application systems implementation and maintenance more difficult.

QUESTION 1143
_____ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

A. Quantitative; qualitative
B. Qualitative; quantitative
C. Residual; subjective
D. Quantitative; subjective

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Quantitative risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a qualitative risk assessment is more appropriate.

QUESTION 1144
What must an IS auditor understand before performing an application audit?

A. The potential business impact of application risks.
B. Application risks must first be identified.
C. Relative business processes.
D. Relevant application risks.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An IS auditor must first understand relative business processes before performing an application audit.

QUESTION 1145
Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

A. Redundancy check
B. Completeness check
C. Accuracy check
D. Parity check

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of data.

QUESTION 1146
A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

A. Deletion
B. Input
C. Access
D. Duplication

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A transaction journal provides the information necessary for detecting unauthorized input from a terminal.

QUESTION 1147
When are benchmarking partners identified within the benchmarking process?

A. In the design stage
B. In the testing stage
C. In the research stage
D. In the development stage

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Benchmarking partners are identified in the research stage of the benchmarking process.

QUESTION 1148
Parity bits are a control used to validate:
A. Data authentication
B. Data completeness
C. Data source
D. Data accuracy

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Parity bits are a control used to validate data completeness.

QUESTION 1149
The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

A. Implementor
B. Facilitator
C. Developer
D. Sponsor

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a facilitator.

QUESTION 1150
Which of the following is the MOST critical step in planning an audit?

A. Implementing a prescribed auditing framework such as COBIT
B. Identifying current controls
C. Identifying high-risk audit targets
D. Testing controls

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In planning an audit, the most critical step is identifying the areas of high risk.

QUESTION 1151
To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following?

A. The business objectives of the organization
B. The effect of segregation of duties on internal controls
C. The point at which controls are exercised as data flows through the system
D. Organizational control policies

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of the point at which controls are exercised as data flows through the system.

QUESTION 1152
What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

A. Document existing internal controls
B. Perform compliance testing on internal controls
C. Establish a controls-monitoring steering committee
D. Identify high-risk areas within the organization

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
When implementing continuous-monitoring systems, an IS auditor's first step is to identify high-risk areas within the organization.

QUESTION 1153
An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

A. True
B. False

Correct Answer: B

Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

QUESTION 1154
An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

QUESTION 1155
If an IS auditor finds evidence of risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

A. To advise senior management.
B. To reassign job functions to eliminate potential fraud.
C. To implement compensator controls.
D. Segregation of duties is an administrative control not considered by an IS auditor.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor's primary responsibility is to advise senior management of the risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function.

QUESTION 1156
Who is responsible for implementing cost-effective controls in an automated system?

A. Security policy administrators
B. Business unit management
C. Senior management
D. Board of directors

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Business unit management is responsible for implementing cost-effective controls in an automated system.

QUESTION 1157
When auditing third-party service providers, an IS auditor should be concerned with which of the following?

A. Ownership of the programs and files
B. A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster C. A statement of due care
D. Ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

Correct Answer: D
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation:
When auditing third-party service providers, an auditor should be concerned with ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster.

QUESTION 1158
What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels?

A. Business impact assessment
B. Risk assessment
C. IS assessment methods
D. Key performance indicators (KPIs)

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
IS assessment methods allow IS management to determine whether the activities of the organization differ from the planned or expected levels.

QUESTION 1159
What can be implemented to provide the highest level of protection from external attack?

A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
B. Configuring the firewall as a screened host behind a router
C. Configuring the firewall as the protecting bastion host
D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

QUESTION 1160
How is the risk of improper file access affected upon implementing a database system?

A. Risk varies.
B. Risk is reduced.
C. Risk is not affected.
D. Risk is increased.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Improper file access becomes a greater risk when implementing a database system.

QUESTION 1161
In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

A. The data should be deleted and overwritten with binary 0s.
B. The data should be demagnetized.
C. The data should be low-level formatted.
D. The data should be deleted.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
To properly protect against unauthorized disclosure of sensitive data, hard disks should be demagnetized before disposal or release.

QUESTION 1162
Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

QUESTION 1163
How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

A. Modems convert analog transmissions to digital, and digital transmission to analog.
B. Modems encapsulate analog transmissions within digital, and digital transmissions within analog.
C. Modems convert digital transmissions to analog, and analog transmissions to digital.
D. Modems encapsulate digital transmissions within analog, and analog transmissions within digital.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

QUESTION 1164
What supports data transmission through split cable facilities or duplicate cable facilities?

A. Diverse routing
B. Dual routing
C. Alternate routing
D. Redundant routing

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Diverse routing supports data transmission through split cable facilities, or duplicate cable facilities.

QUESTION 1165
What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

A. A first-generation packet-filtering firewall
B. A circuit-level gateway
C. An application-layer gateway, or proxy firewall, and stateful-inspection firewalls
D. An application-layer gateway, or proxy firewall, but not stateful-inspection firewalls

Correct Answer: C

Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An application-layer gateway, or proxy firewall, and stateful-inspection firewalls provide the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic.

QUESTION 1166
Which of the following can degrade network performance?

A. Superfluous use of redundant load-sharing gateways
B. Increasing traffic collisions due to host congestion by creating new collision domains
C. Inefficient and superfluous use of network devices such as switches
D. Inefficient and superfluous use of network devices such as hubs

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Inefficient and superfluous use of network devices such as hubs can degrade network performance.

QUESTION 1167
Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

A. Automated electronic journaling and parallel processing
B. Data mirroring and parallel processing
C. Data mirroring
D. Parallel processing

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data mirroring and parallel processing are both used to provide near- immediate recoverability for time-sensitive systems and transaction processing.

QUESTION 1168
What is an effective control for granting temporary access to vendors and external support personnel?

A. Creating user accounts that automatically expire by a predetermined date
B. Creating permanent guest accounts for temporary use
C. Creating user accounts that restrict logon access to certain hours of the day
D. Creating a single shared vendor administrator account on the basis of least-privileged access

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

QUESTION 1169
Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack?

A. Inbound traffic filtering
B. Using access control lists (ACLs) to restrict inbound connection attempts
C. Outbound traffic filtering
D. Recentralizing distributed systems

Correct Answer: C

Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Outbound traffic filtering can help prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack.

QUESTION 1170
What is a common vulnerability, allowing denial-of-service attacks?

A. Assigning access to users according to the principle of least privilege
B. Lack of employee awareness of organizational security policies
C. Improperly configured routers and router access lists
D. Configuring firewall access rules

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Improperly configured routers and router access lists are a common vulnerability for denial-of- service attacks.

QUESTION 1171
What are trojan horse programs?

A. A common form of internal attack
B. Malicious programs that require the aid of a carrier program such as email
C. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
D. A common form of Internet attack

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Trojan horse programs are a common form of Internet attack.

QUESTION 1172
Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

A. Traffic analysis
B. SYN flood
C. Denial of service (DoS)
D. Distributed denial of service (DoS)

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Traffic analysis is a passive attack method used by intruders to determine potential network vulnerabilities. All others are active attacks.

QUESTION 1173
What is a callback system?

A. It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fails.
B. It is a remote-access system whereby the user's application automatically redials the remote access server if the initial connection attempt fails.
C. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.
D. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of time.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A callback system is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

QUESTION 1174
What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

A. A dry-pipe sprinkler system
B. A deluge sprinkler system
C. A wet-pipe system
D. A halon sprinkler system

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A dry-pipe sprinkler system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

QUESTION 1175
What process is used to validate a subject's identity?

A. Identification
B. Nonrepudiation
C. Authorization
D. Authentication

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Authentication is used to validate a subject's identity.

QUESTION 1176
Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource?

A. Systems logs
B. Access control lists (ACL)
C. Application logs
D. Error logs

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
IS auditors should review access-control lists (ACL) to determine user permissions that have been granted for a particular resource.

QUESTION 1177
What should IS auditors always check when auditing password files?
A. That deleting password files is protected
B. That password files are encrypted
C. That password files are not accessible over the network

D. That password files are archived

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
IS auditors should always check to ensure that password files are encrypted.

QUESTION 1178
Which of the following is the most fundamental step in preventing virus attacks?

A. Adopting and communicating a comprehensive antivirus policy
B. Implementing antivirus protection software on users' desktop computers
C. Implementing antivirus content checking at all network-to-Internet gateways
D. Inoculating systems with antivirus code

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks. All other antivirus prevention efforts rely upon decisions established and communicated via policy.

QUESTION 1179
Which of the following is of greatest concern when performing an IS audit?

A. Users' ability to directly modify the database
B. Users' ability to submit queries to the database
C. Users' ability to indirectly modify the database
D. Users' ability to directly view the database

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A major IS audit concern is users' ability to directly modify the database.

QUESTION 1180
Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Instead of simply reviewing the effectiveness and utilization of assets, an IS auditor is more concerned with adequate access control, appropriate access policies, and effectiveness of safeguards and procedures.

QUESTION 1181
If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions. True or false?

A. True
B. False

Correct Answer: A

Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions.

QUESTION 1182
Organizations should use off-site storage facilities to maintain _____ (fill in the blank) of current and critical information within backup files.

A. Confidentiality
B. Integrity
C. Redundancy
D. Concurrency

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Redundancy is the best answer because it provides both integrity and availability. Organizations should use off-site storage facilities to maintain redundancy of current and critical information within backup files.

QUESTION 1183
The purpose of business continuity planning and disaster-recovery planning is to:

A. Transfer the risk and impact of a business interruption or disaster
B. Mitigate, or reduce, the risk and impact of a business interruption or disaster
C. Accept the risk and impact of a business
D. Eliminate the risk and impact of a business interruption or disaster

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The primary purpose of business continuity planning and disaster-recovery planning is to mitigate, or reduce, the risk and impact of a business interruption or disaster.
Total elimination of risk is impossible.

QUESTION 1184
How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

A. By implementing redundant systems and applications onsite
B. By geographically dispersing resources
C. By retaining onsite data backup in fireproof vaults
D. By preparing BCP and DRP documents for commonly identified disasters

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Minimizing single points of failure or vulnerabilities of a common disaster is mitigated by geographically dispersing resources.

QUESTION 1185
Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Mitigating the risk and impact of a disaster or business interruption usually takes priority over transferring risk to a third party such as an insurer.

QUESTION 1186
Off-site data storage should be kept synchronized when preparing for recovery of time- sensitive data such as that resulting from which of the following?

A. Financial reporting
B. Sales reporting
C. Inventory reporting
D. Transaction processing

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Off-site data storage should be kept synchronized when preparing for the recovery of timesensitive data such as that resulting from transaction processing.
QUESTION 1187
What is an acceptable mechanism for extremely time-sensitive transaction processing?

A. Off-site remote journaling
B. Electronic vaulting
C. Shadow file processing
D. Storage area network

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Shadow file processing can be implemented as a recovery mechanism for extremely time- sensitive transaction processing.

QUESTION 1188
Off-site data backup and storage should be geographically separated so as to _____ (fill in the blank) the risk of a widespread physical disaster such as a hurricane or earthquake.

A. Accept
B. Eliminate
C. Transfer
D. Mitigate

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Off-site data backup and storage should be geographically separated, to mitigate the risk of a widespread physical disaster such as a hurricane or an earthquake.

QUESTION 1189
Why is a clause for requiring source code escrow in an application vendor agreement important?

A. To segregate systems development and live environments
B. To protect the organization from copyright disputes
C. To ensure that sufficient code is available when needed

D. To ensure that the source code remains available even if the application vendor goes out of business

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A clause for requiring source code escrow in an application vendor agreement is important to ensure that the source code remains available even if the application vendor goes out of business.

QUESTION 1190
What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

A. Assigning copyright to the organization
B. Program back doors
C. Source code escrow
D. Internal programming expertise

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Source code escrow protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business.

QUESTION 1191
What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

A. Contrived data
B. Independently created data
C. Live data
D. Data from previous tests

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Regression testing should use data from previous tests to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors.

QUESTION 1192
An IS auditor should carefully review the functional requirements in a system-development project to ensure that the project is designed to:

A. Meet business objectives
B. Enforce data security
C. Be culturally feasible
D. Be financially feasible

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to meet business objectives.

QUESTION 1193
Which of the following processes are performed during the design phase of the systems development life cycle (SDLC) model?

A. Develop test plans.
B. Baseline procedures to prevent scope creep.

C. Define the need that requires resolution, and map to the major requirements of the solution.
D. Program and test the new system. The tests verify and validate what has been developed.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Procedures to prevent scope creep are baselined in the design phase of the systems- development life cycle (SDLC) model.

QUESTION 1194
When should application controls be considered within the system-development process?

A. After application unit testing
B. After application module testing
C. After applications systems testing
D. As early as possible, even in the development of the project's functional specifications

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Application controls should be considered as early as possible in the system- development process, even in the development of the project's functional specifications.

QUESTION 1195
What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality?

A. Rapid application development (RAD)
B. GANTT
C. PERT
D. Decision trees

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Rapid application development (RAD) is used to develop strategically important systems faster, reduce development costs, and still maintain high quality.

QUESTION 1196
Test and development environments should be separated. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Test and development environments should be separated, to control the stability of the test environment.

QUESTION 1197
What kind of testing should programmers perform following any changes to an application or system?

A. Unit, module, and full regression testing
B. Module testing

C. Unit testing
D. Regression testing

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Programmers should perform unit, module, and full regression testing following any changes to an application or system.

QUESTION 1198
When should plans for testing for user acceptance be prepared?

A. In the requirements definition phase of the systems-development project
B. In the feasibility phase of the systems-development project
C. In the design phase of the systems-development project
D. In the development phase of the systems-development project

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Plans for testing for user acceptance are usually prepared in the requirements definition phase of the systems-development project.

QUESTION 1199
Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

A. Failing to perform user acceptance testing
B. Lack of user training for the new system
C. Lack of software documentation and run manuals
D. Insufficient unit, module, and systems testing

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Above almost all other concerns, failing to perform user acceptance testing often results in the greatest negative impact on the implementation of new application software.

QUESTION 1200
Input/output controls should be implemented for which applications in an integrated systems environment?

A. The receiving application
B. The sending application
C. Both the sending and receiving applications
D. Output on the sending application and input on the receiving application

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

QUESTION 1201
Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following?

A. Unsynchronized transactions
B. Unauthorized transactions

C. Inaccurate transactions
D. Incomplete transactions

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Authentication techniques for sending and receiving data between EDI systems are crucial to prevent unauthorized transactions.

QUESTION 1202
After identifying potential security vulnerabilities, what should be the IS auditor's next step?

A. To evaluate potential countermeasures and compensatory controls
B. To implement effective countermeasures and compensatory controls
C. To perform a business impact analysis of the threats that would exploit the vulnerabilities
D. To immediately advise senior management of the findings

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
After identifying potential security vulnerabilities, the IS auditor's next step is to perform a business impact analysis of the threats that would exploit the vulnerabilities.

QUESTION 1203
What is the primary security concern for EDI environments?

A. Transaction authentication
B. Transaction completeness
C. Transaction accuracy
D. Transaction authorization

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Transaction authorization is the primary security concern for EDI environments.

QUESTION 1204
Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

A. Exposures
B. Threats
C. Hazards
D. Insufficient controls

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Threats exploit vulnerabilities to cause loss or damage to the organization and its assets.

QUESTION 1205
Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.

A. Increased; a greater
B. Increased; a fewer
C. Less; a fewer
D. Increased; the same

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Business process re-engineering often results in increased automation, which results in a greater number of people using technology.

QUESTION 1206
When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?
A. Before transaction completion
B. Immediately after an EFT is initiated
C. During run-to-run total testing
D. Before an EFT is initiated

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An application-level edit check to verify availability of funds should be completed at the electronic funds transfer (EFT) interface before an EFT is initiated.

QUESTION 1207
_____ should be implemented as early as data preparation to support data integrity at the earliest point possible.

A. Control totals
B. Authentication controls
C. Parity bits
D. Authorization controls

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Control totals should be implemented as early as data preparation to support data integrity at the earliest point possible.

QUESTION 1208
Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Database snapshots can provide an excellent audit trail for an IS auditor.

QUESTION 1209
Which of the following is a substantive test?

A. Checking a list of exception reports
B. Ensuring approval for parameter changes

C. Using a statistical sample to inventory the tape library
D. Reviewing password history reports

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A substantive test confirms the integrity of actual processing. A substantive test would determine if the tape library records are stated correctly. A compliance test determines if controls are being applied in a manner that is consistent with management policies and procedures. Checking the authorization of exception reports, reviewing authorization for changing parameters and reviewing password history reports are all compliance tests.

QUESTION 1210
An audit charter should:

A. be dynamic and change often to coincide with the changing nature of technology and the audit profession.
B. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
C. document the audit procedures designed to achieve the planned audit objectives.
D. outline the overall authority, scope and responsibilities of the audit function.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An audit charter should state management's objectives for and delegation of authority to IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

QUESTION 1211
Which of the following sampling methods is MOST useful when testing for compliance?

A. Attribute sampling
B. Variable sampling
C. Stratified mean per unit
D. Difference estimation

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

QUESTION 1212
Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

A. Multiple cycles of backup files remain available.
B. Access controls establish accountability for e-mail activity.
C. Data classification regulates what information should be communicated via e-mail.
D. Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

QUESTION 1213
An IS auditor is assigned to perform a post implementation review of an application system. Which pf the following situations may have impaired the independence of the IS auditor? The IS auditor:

A. implemented a specific control during the development of the application system.
B. designed an embedded audit module exclusively for auditing the application system.
C. participated as a member of the application system project team, but did not have operational responsibilities.
D. provided consulting advice concerning application system best practices.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Independence may be impaired if an IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system. Choices B and C are situations that do not impair an IS auditor's independence. Choice D is incorrect because an IS auditor's independence is not impaired by providing advice on known best practices.

QUESTION 1214
When developing a risk-based audit strategy, an IS auditor conduct a risk assessment to ensure that:

A. controls needed to mitigate risks are in place.
B. vulnerabilities and threats are identified.
C. audit risks are considered.
D. a gap analysis is appropriate.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage.
Understanding whether appropriate controls required to mitigate risks are in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be done to compare the actual state to an expected or desirable state.

QUESTION 1215
In planning an audit, the MOST critical step is the identification of the:

A. areas of high risk.
B. skill sets of the audit staff.
C. test steps in the audit.
D. time allotted for the audit.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

Explanation:
When designing an audit plan, it is important to identify the areas of highest risk to determine the areas to be audited. The skill sets of the audit staff should have been considered before deciding and selecting the audit. Test steps for the audit are not as critical as identifying the areas of risk, and the time allotted for an audit is determined by the areas to be audited, which are primarily selected based on the identification of risks.

QUESTION 1216
The extent to which data will be collected during an IS audit should be determined based on the:

A. availability of critical and required information.
B. auditor's familiarity with the circumstances.
C. auditee's ability to find relevant evidence.
D. purpose and scope of the audit being done.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An audit with a narrow purpose and scope would result most likely in less data collection, than an audit with a wider purpose and scope. The scope of an IS audit should not be constrained by the ease of obtaining the information or by the auditor's familiarity with the area being audited. Collecting all the required evidence is a required element of an IS audit, and the scope of the audit should not be limited by the auditee's ability to find relevant evidence.

QUESTION 1217
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

A. the probability of error must be objectively quantified.
B. the auditor wishes to avoid sampling risk.C. generalized audit software is unavailable.
D. the tolerable error rate cannot be determined.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Given an expected error rate and confidence level, statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size and quantify the probability of error (confidence coefficient). Choice B is incorrect because sampling risk is the risk of a sample not being representative of the population. This risk exists for both judgment and statistical samples. Choice C is incorrect because statistical sampling does not require the use of generalized audit software. Choice D is incorrect because the tolerable error rate must be predetermined for both judgment and statistical sampling.

QUESTION 1218
When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

A. sufficient evidence will be collected.
B. all significant deficiencies identified will be corrected within a reasonable period.
C. all material weaknesses will be identified.
D. audit costs will be kept at a minimum level.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Procedures are processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising in the course of an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate and the auditor's past experience plays a key role in making a judgment. ISACA's guidelines provide information on how to meet the standards when performing IS audit work. Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit and not of professional judgment. Professional judgment is not a primary input to the financial aspects of the audit.

QUESTION 1219
An IS auditor evaluating logical access controls should FIRST:

A. document the controls applied to the potential access paths to the system.
B. test controls over the access paths to determine if they are functional.

C. evaluate the security environment in relation to written policies and practices
D. obtain an understanding of the security risks to information processing.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation and evaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths-to determine if the controls are functioning. Lastly, the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

QUESTION 1220
In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

A. identify and assess the risk assessment process used by management.
B. identify information assets and the underlying systems.
C. disclose the threats and impacts to management.
D. identify and evaluate the existing controls.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

QUESTION 1221
When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?
A. The point at which controls are exercised as data flow through the system
B. Only preventive and detective controls are relevant
C. Corrective controls can only be regarded as compensating
D. Classification allows an IS auditor to determine which controls are missing

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect, since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

QUESTION 1222
During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

A. test data to validate data input.
B. test data to determine system sort capabilities.
C. generalized audit software to search for address field duplications.
D. generalized audit software to search for account field duplications.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Since the name is not the same {due to name variations), one method to detect duplications would be to compare other common fields, such as addresses. A subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

QUESTION 1223
Which of the following would be the BEST population to take a sample from when testing program changes? A. Test library listings

B. Source program listings
C. Program change requests
D. Production library listings

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational data. Source program listings would be timeintensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

QUESTION 1224
An integrated test facility is considered a useful audit tool because it:

A. is a cost-efficient approach to auditing application controls.
B. enables the financial and IS auditors to integrate their audit tests.
C. compares processing output with independently calculated data.
D. provides the IS auditor with a tool to analyze a large range of information

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated data. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

QUESTION 1225
Data flow diagrams are used by IS auditors to:

A. order data hierarchically.
B. highlight high-level data definitions.
C. graphically summarize data paths and storage.
D. portray step-by-step details of data generation.
Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

QUESTION 1226
Which of the following forms of evidence for the auditor would be considered the MOST reliable?

A. An oral statement from the auditee
B. The results of a test performed by an IS auditor
C. An internally generated computer accounting report
D. A confirmation letter received from an outside source

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Evidence obtained from outside sources is usually more reliable than that obtained from within the organization. Confirmation letters received from outside parties, such as those used to verify accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable, if the auditor did not have a good understanding of the technical area under review.

QUESTION 1227
An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

A. Availability of online network documentation
B. Support of terminal access to remote hosts
C. Handling file transfer between hosts and interuser communications
D. Performance management, audit and control

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Network operating system user features include online availability of network documentation. Other features would be user access to various resources of network hosts, user authorization to access particular resources, and the network and host computers used without special user actions or commands. Choices B, C and D are examples of network operating systems functions.

QUESTION 1228
An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storage.
B. interview programmers about the procedures currently being followed.
C. compare utilization records to operations schedules.
D. review data file access records to test the librarian function.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

QUESTION 1229
An IS auditor performing a review of an application's controls would evaluate the:

A. efficiency of the application in meeting the business processes.
B. impact of any exposures discovered.
C. business processes served by the application.
D. application's optimization.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

QUESTION 1230
In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

A. Testing whether inappropriate personnel can change application parameters
B. Tracing purchase orders to a computer listing
C. Comparing receiving reports to purchase order details
D. Reviewing the application documentation

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
To determine purchase order validity, testing access controls will provide the best evidence. Choices B and C are based on after-the-fact approaches, while choice D does not serve the purpose because what is in the system documentation may not be the same as what is happening.

QUESTION 1231
Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

A. Embedded audit module
B. Integrated test facility
C. Snapshots
D. Audit hooks

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The audit hook technique involves embedding code in application systems for the examination of selected transactions. This helps an IS auditor to act before an error or an irregularity gets out of hand. An embedded audit module involves embedding specially-written software in the organization's host application system so that application systems are monitored on a selective basis. An integrated test facility is used when it is not practical to use test data, and snapshots are used when an audit trail is required.

QUESTION 1232
When assessing the design of network monitoring controls, an IS auditor should FIRST review network:
A. topology diagrams.
B. bandwidth usage.
C. traffic analysis reports.
D. bottleneck locations.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The first step in assessing network monitoring controls should be the review of the adequacy of network documentation, specifically topology diagrams. If this information is not up to date, then monitoring processes and the ability to diagnose problems will not be effective.

QUESTION 1233
When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

A. analysis.
B. evaluation.
C. preservation.
D. disclosure.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Preservation and documentation of evidence for review by law enforcement and judicial authorities are of primary concern when conducting an investigation. Failure to properly preserve the evidence could jeopardize the acceptance of the evidence in legal proceedings. Analysis, evaluation and disclosure are important but not of primary concern in a forensic investigation.

QUESTION 1234
An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

A. conclude that the controls are inadequate.
B. expand the scope to include substantive testing
C. place greater reliance on previous audits.
D. suspend the audit.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests. There is no evidence that whatever controls might exist are either inadequate or adequate. Placing greater reliance on previous audits or suspending the audit are inappropriate actions as they provide no current knowledge of the adequacy of the existing controls.

QUESTION 1235
The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

A. understand the business process.
B. comply with auditing standards.
C. identify control weakness.
D. plan substantive testing.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Understanding the business process is the first step an IS auditor needs to perform. Standards do not require an IS auditor to perform a process walkthrough. Identifying control weaknesses is not the primary reason for the walkthrough and typically occurs at a later stage in the audit, while planning for substantive testing is performed at a later stage in the audit.

QUESTION 1236
In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

A. examine source program changes without information from IS personnel.
B. detect a source program change made between acquiring a copy of the source and the comparison run.
C. confirm that the control copy is the current version of the production program.
D. ensure that all changes made in the current source copy are detected.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
An IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify changes. Choice B is incorrect, because the changes made since the acquisition of the copy are not included in the copy of the software. Choice C is incorrect, as an IS auditor will have to gain this assurance separately.
Choice D is incorrect, because any changes made between the time the control copy was acquired and the source code comparison is made will not be detected.

QUESTION 1237
Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

A. Test data run
B. Code review
C. Automated code comparison
D. Review of code migration procedures

Correct Answer: C

Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An automated code comparison is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure. Test data runs permit the auditor to verify the processing of preselected transactions, but provide no evidence about unexercised portions of a program. Code review is the process of reading program source code listings to determine whether the code contains potential errors or inefficient statements. A code review can be used as a means of code comparison but it is inefficient. The review of code migration procedures would not detect program changes.

QUESTION 1238
While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

A. audit trail of the versioning of the work papers.
B. approval of the audit phases.
C. access rights to the work papers.
D. confidentiality of the work papers.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Encryption provides confidentiality for the electronic work papers. Audit trails, audit phase approvals and access to the work papers do not, of themselves, affect the confidentiality but are part of the reason for requiring encryption.

QUESTION 1239
After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:

A. expand activities to determine whether an investigation is warranted
B. report the matter to the audit committee.
C. report the possibility of fraud to top management and ask how they would like to be proceed.
D. consult with external legal counsel to determine the course of action to be taken.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An IS auditor's responsibilities for detecting fraud include evaluating fraud indicators and deciding whether any additional action is necessary or whether an investigation should be recommended. The IS auditor should notify the appropriate authorities within the organization only if it has determined that the indicators of fraud are sufficient to recommend an investigation. Normally, the IS auditor does not have authority to consult with external legal counsel.

QUESTION 1240
Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

A. Attribute sampling
B. Generalized audit software (GAS)
C. Test data
D. Integrated test facility (ITF)

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Generalized audit software (GAS) would enable the auditor to review the entire invoice file to look for those items that meet the selection criteria. Attribute sampling would aid in identifying records meeting specific conditions, but would not compare one record to another to identify duplicates. To detect duplicate invoice records, the IS auditor should check all of the items that meet the criteria and not just a sample of the items. Test data are used to verify program processing, but will not identify duplicate records. An integrated test facility (ITF) allows the IS auditor to test transactions through the production system, but would not compare records to identify duplicates.

QUESTION 1241
Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

A. System log analysis
B. Compliance testing

C. Forensic analysis
D. Analytical review

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Determining that only authorized modifications are made to production programs would require the change management process be reviewed to evaluate the existence of a trail of documentary evidence. Compliance testing would help to verify that the change management process has been applied consistently. It is unlikely that the system log analysis would provide information about the modification of programs. Forensic analysis is a specialized technique for criminal investigation. An analytical review assesses the general control environment of an organization.

QUESTION 1242
An IS auditor who was involved in designing an organization's business continuity plan(BCP) has been assigned to audit the plan. The IS auditor should:

A. decline the assignment.
B. inform management of the possible conflict of interest after completing the audit assignment.
C. inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment.
D. communicate the possibility of conflict of interest to management prior to starting the assignment.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Communicating the possibility of a conflict of interest to management prior to starting the assignment is the correct answer. A possible conflict of interest, likely to affect the auditor's independence, should be brought to the attention of management prior to starting the assignment. Declining the assignment is not the correct answer because the assignment could be accepted after obtaining management approval. Informing management of the possible conflict of interest after completion of the audit assignment is not correct because approval should be obtained prior to commencement and not after the completion of the assignment. Informing the business continuity planning (BCP) team of the possible conflict of interest prior to starting of the assignment is not the correct answer since the BCP team would not have the authority to decide on this issue.

QUESTION 1243
Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

A. include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
B. not include the finding in the final report, because the audit report should include only unresolved findings.
C. not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
D. include the finding in the closing meeting for discussion purposes only.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken. An audit report should reflect the situation, as it existed at the start of the audit. All corrective actions taken by the auditee should be reported in writing.

QUESTION 1244
During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

A. ask the auditee to sign a release form accepting full legal responsibility.
B. elaborate on the significance of the finding and the risks of not correcting it.
C. report the disagreement to the audit committee for resolution.
D. accept the auditee's position since they are the process owners.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure. The goal should be to enlighten the auditee or uncover new information of which an IS auditor may not have been aware. Anything that appears to threaten the auditee will lessen effective communications and set up an adversarial relationship. By the same token, an IS auditor should not automatically agree just because the auditee expresses an alternate point of view.

QUESTION 1245
The final decision to include a material finding in an audit report should be made by the:

A. audit committee.
B. auditee's manager.
C. IS auditor.
D. CEO of the organization

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The IS auditor should make the final decision about what to include or exclude from the audit report. The other choices would limit the independence of the auditor.

QUESTION 1246
The success of control self-assessment (CSA) highly depends on:

A. having line managers assume a portion of the responsibility for control monitoring.
B. assigning staff managers the responsibility for building, but not monitoring, controls.
C. the implementation of a stringent control policy and rule-driven controls.
D. the implementation of supervision and the monitoring of controls of assigned duties.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a control self-assessment (CSA) program depends on the degree to which line managers assume responsibility for controls- Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

QUESTION 1247
Which of the following is an attribute of the control self-assessment (CSA) approach?

A. Broad stakeholder involvement
B. Auditors are the primary control analysts
C. Limited employee participation
D. Policy driven

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The control self-assessment (CSA) approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training, at! of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

QUESTION 1248
An IT steering committee should review information systems PRIMARILY to assess:

A. whether IT processes support business requirements.
B. if proposed system functionality is adequate
C. the stability of existing software.

D. the complexity of installed technology.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IS processes support the business requirements. Assessing proposed additional functionality and evaluating software stability and the complexity of technology are too narrow in scope to ensure that IT processes are, in fact, supporting the organization's goals.

QUESTION 1249
The MOST likely effect of the lack of senior management commitment to IT strategic planning is: A. a lack of investment in technology.

B. a lack of a methodology for systems development.
C. technology not aligning with the organization's objectives.
D. an absence of control over technology contracts.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

QUESTION 1250
Which of the following is a function of an IS steering committee?

A. Monitoring vendor-controlled change control and testing
B. Ensuring a separation of duties within the information's processing environment
C. Approving and monitoring major projects, the status of IS plans and budgets
D. Liaising between the IS department and the end users

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaising between the IS department and the end users is a function of the individual parties and not a committee.

QUESTION 1251
An IS steering committee should:

A. include a mix of members from different departments and staff levels.
B. ensure that IS security policies and procedures have been executed properly.
C. have formal terms of reference and maintain minutes of its meetings.
D. be briefed about new trends and products at each meeting by a vendor.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is important to keep detailed steering committee minutes to document the decisions and activities of the IS steering committee, and the board of directors should be informed about those decisions on a timely basis. Choice A is incorrect because only senior management or high-level staff members should be on this committee because of its strategic mission. Choice B is not a responsibility of this committee, but the responsibility of the security administrator. Choice D is incorrect because a vendor should be invited to meetings only when appropriate.

QUESTION 1252
Involvement of senior management is MOST important in the development of:

A. strategic plans.
B. IS policies.
C. IS procedures.
D. standards and guidelines.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

QUESTION 1253
Effective IT governance will ensure that the IT plan is consistent with the organization's:

A. business plan.
B. audit plan.
C. security plan.
D. investment plan.
Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, while the security plan should be at a corporate level.

QUESTION 1254
Establishing the level of acceptable risk is the responsibility of:

A. quality assurance management.
B. senior business management.
C. the chief information officer.
D. the chief security officer.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Senior management should establish the acceptable risk level, since they have the ultimate or final responsibility for the effective and efficient operation of the organization. Choices A, C and D should act as advisors to senior management in determining an acceptable risk level.

QUESTION 1255
IT governance is PRIMARILY the responsibility of the:

A. chief executive officer.
B. board of directors.
C. IT steering committee.
D. audit committee.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
IT governance is primarily the responsibility of the executives and shareholders {as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

QUESTION 1256
Which of the following would be of **MOST** concern during an audit of an end user computing system containing sensitive information?

A. Audit logging is not available.
B. System data is not protected.
C. Secure authorization is not available.
D. The system is not included in inventory.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1257
Following a recent internal data breach, an IS auditor was asked to evaluate information security practices within the organization. Which of the following findings would be **MOST** important to report to senior management?

A. Employees are not required to sign a non-compete agreement.
B. Security education and awareness workshops have not been completed.
C. Users lack technical knowledge related to security and data protection.
D. Desktop passwords do not require special characters.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1258
Which of the following is the **BEST** way to protect the confidentiality of data on a corporate smartphone?
A. Disabling public wireless connections
B. Using remote data wipe capabilities
C. Using encryption
D. Changing the default PIN for Bluetooth connections

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1259
To help ensure the organization's information assets are adequately protected, which of the following considerations is **MOST** important when developing an information classification and handling policy?

A. The policy has been mapped against industry frameworks for classifying information assets.
B. The policy is owned by the head of information security, who has the authority to enforce the policy.
C. The policy specifies requirements to safeguard information assets based on their importance to the organization.
D. The policy is subject to periodic reviews to ensure its provisions are up to date.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1260
An organization's current end-user computing practices include the use of a spreadsheet for financial statements. Which of the following is the **GREATEST** concern?

A. Formulas are not protected against unintended changes.
B. The spreadsheet contains numerous macros.
C. Operational procedures have not been reviewed in the current fiscal year.
D. The spreadsheet is not maintained by IT.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1261
An IS auditor is assessing an organization's data loss prevention (DLP) solution for protecting intellectual property from insider theft. Which of the following would the auditor consider **MOST** important for effective data protection?

A. Employee training on information handling
B. Creation of DLP policies and procedures
C. Encryption of data copied to flash drives
D. Identification and classification of sensitive data

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1262
An IS auditor finds that the process for removing access for terminated employees is not documented. What is the **MOST** significant risk from this observation?

A. Procedures may not align with best practices.
B. HR records may not match system access.
C. Unauthorized access cannot be identified.
D. Access rights may not be removed in a timely manner.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1263
Which of the following is **MOST** important to include in an organization's incident response plan to help prevent similar incidents from happening in the future?

A. Documentation of incident details
B. Incident closure procedures
C. Containment and neutralization actions
D. Post-incident review

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1264
Which of the following is the **BEST** indication of an effective incident management process?

A. Percentage of incidents where root cause has been identified
B. Percentage of incidents closed without escalation
C. Number of calls to the help desk
D. Number of incidents reviewed by the IT management

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1265
Which of the following metrics would be **MOST** helpful to an IS auditor in evaluating an organization's security incident response management capability?

A. Number of business interruptions due to IT security incidents per year.
B. Number of IT security incidents reported per month
C. Number of malware infections in business applications detected per day.
D. Number of alerts generated by intrusion detection systems (IDS) per minute.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1266
Which of the following is **MOST** important for the improvement of an organization's incident response processes?

A. Post-event reviews by the incident response team
B. Regular upgrades to incident management software
C. Ongoing incident response training for users
D. Periodic walk-through of incident response procedures

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1267
An IS auditor has discovered that unauthorized customer management software was installed on a workstation. The auditor determines the software has been uploading customer data to an external party. Which of the following is the IS auditor's **BEST** course of action?

A. Review other workstations to determine the extent of the incident.
B. Determine the number of customer records that were uploaded.
C. Notify the incident response team.
D. Present the issue at the next audit progress meeting.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1268
Which of the following is the **MAIN** purpose of implementing an incident response process?
A. Provide substantial audit-trail evidence.
B. Assign roles and responsibilities.

C. Comply with policies and procedures.
D. Manage impact due to breaches.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1269
An IS auditor learns a server administration team regularly applies workarounds to address repeated failures of critical data processing services. Which of the following would **BEST** enable the organization to resolve this issue?

A. Service level management
B. Change management
C. Problem management
D. Incident management

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1270
Which of the following is **MOST** important for an IS auditor to consider when reviewing the effectiveness of an incident response program?

A. Incidents are categorized according to industry standards.
B. Lessons learned are incorporated into incident response processes.
C. Incidents are escalated to senior management in a timely manner.
D. The plan is reviewed and updated annually.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1271
Which of the following is the **GREATEST** benefit of implementing an incident management process?

A. Opportunity for frequent reassessment of incidents
B. Reduction in security threats
C. Reduction in the business impact of incidents
D. Reduction of costs by the efficient use of resources

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1272
The **PRIMARY** advantage of object-oriented technology is enhanced:

A. efficiency due to the re-use of elements of logic.
B. management of sequential program execution for data access.
C. management of a restricted variety of data types for a data object.
D. grouping of objects into methods for data access.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1273
Which of the following is the **MOST** effective control for a utility program?
A. Renaming the versions in the programmers' libraries
B. Installing the program on a separate server
C. Storing the program in a production library
D. Allowing only authorized personnel to use the program

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1274
An airline's online booking system uses an automated script that checks whether fares are within the defined threshold of what is reasonable before the fares are displayed on the website. Which type of control is in place?

A. Compensating control
B. Preventive control
C. Detective control
D. Corrective control

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1275
Which of the following is the **MOST** effective way to assess whether an outsourcer's controls are following the service level agreement (SLA)?

A. Perform an onsite review of the outsourcer.
B. Review the outsourcer's monthly service reports.
C. Perform a review of penalty clauses for non-performance.
D. Review an internal audit report from the outsourcer's auditor.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1276
Which of the following **BEST** indicates the effectiveness of an organization's risk management program?

A. Control risk is minimized.
B. Inherent risk is eliminated.
C. Residual risk is minimized.
D. Overall risk is quantified.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1277
A retirement system verifies that the field for employee status has either a value of A (for active) or R (for retired). This is an example of which type of check?

A. Validity
B. Existence
C. Limit
D. Completeness

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1278
Which of the following controls would **BEST** decrease the exposure if a password is compromised? A. Passwords are masked.

B. Passwords are encrypted.
C. Passwords have format restrictions.
D. Password changes are forced periodically.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1279
Which of the following would **BEST** enable effective IT resource management?

A. Assessing the risk associated with IT resources
B. Outsourcing IT processes and activities
C. Establishing business priorities
D. Automating business processes

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1280
Which of the following **BEST** determines if a batch update job was completed?

A. Reviewing the job log
B. Testing a sample of transactions
C. Reviewing a copy of the script
D. Obtaining process owner confirmation

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 1281
Which of the following would be **MOST** important to include in a data security policy to adequately manage the privacy of customer information?

A. Information classification criteria
B. Encryption technology
C. Backup strategy
D. Data ownership

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1282
Which of the following is the **MOST** effective control to ensure electronic records beyond their retention periods are deleted from IT systems?

A. Review the record retention register regularly to initiate data deletion.
B. Build in system logic to trigger data deletion at predefined times.
C. Perform a sample check of current data against the retention schedule.
D. Execute all data deletions at a predefined month during the year.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1283
The lack of which of the following represents the **GREATEST** risk to the quality of developed software?

A. Code reviews
B. Periodic internal audits
C. Load testing
D. An enterprise architecture

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1284
An enterprise receiving email should have procedures to control:

A. insufficient end-points.
B. unsolicited executable code.
C. outdated protocols.
D. insufficient connectivity.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1285
Nonrepudiation of the client for e-commerce transactions is accomplished through which of the following control mechanisms?

A. Password security

B. Internet protocol (IP) address verification
C. Public key infrastructure (PKI)
D. Secure Sockets Layer (SSL)

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 1286
To ensure the integrity of a recovered database, which of the following would be **MOST** useful?

A. Before-and-after transaction images
B. Database defragmentation tools
C. A copy of the data dictionary
D. Application transaction logs

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1287
Which of the following would **BEST** detect that a distributed-denial-of-service attack (DDoS) is occurring?

A. Server crashes
B. Automated monitoring of logs
C. Penetration testing
D. Customer service complaints

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1288
Which of the following is the **BEST** source of information for assessing the effectiveness of IT process monitoring?

A. Participative management techniques
B. Quality assurance (QA) reviews
C. Performance data
D. Real-time audit software

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1289
Which of the following would be the **MOST** appropriate reason for an organization to purchase fault-tolerant hardware?

A. Reducing hardware maintenance costs.
B. Improving system performance.
C. Minimizing business loss.
D. Compensating for the lack of contingency planning

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1290
Which of the following is the **BEST** method for uncovering shadow IT within an organization?

A. Analyze help desk tickets.
B. Review secondary approval thresholds.
C. Use a cloud access security broker (CASB).
D. Review business processes.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1291
Which of the following would help determine the maturity of an information security awareness program?
A. A review of the annual penetration test results
B. A network vulnerability assessment
C. A simulated social engineering test
D. A gap assessment against an established model

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1292
A user of a telephone banking system has forgotten his personal identification number (PIN). After the user has been authenticated, the **BEST** method of issuing a new PIN is to have:

A. the user enter a new PIN twice.
B. banking personnel verbally assign a new PIN.
C. a randomly generated PIN communicated by banking personnel.
D. banking personnel assign the user a new PIN via email.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1293
Privileged account access is required to start an ad hoc batch job. Which of the following would **MOST** effectively detect unauthorized job execution?

A. Requiring manual approval by an authorized user
B. Executing the job through two-factor authentication
C. Introducing job execution request procedures
D. Reconciling user activity logs against authorizations

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1294
Which of the following is the **MOST** critical step prior to performing a network penetration test?

A. Informing management of the potential risk involved with penetration testing
B. Identifying a scanning tool for use in identifying vulnerabilities
C. Communicating the location of the penetration test targets to management
D. Reviewing the results of previous penetration tests

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1295
Which of the following is the **MOST** significant concern when backup tapes are encrypted?

A. Loss of the encryption key
B. Lack of physical security over the tapes
C. Incompatibility with future software versions
D. Inaccurate data due to encryption processing

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1296
Based on the guidance of internal audit, an IT steering committee is considering the use of a balanced scorecard to evaluate its project management process. Which of the following is the **GREATEST** advantage to using this approach?
A. Project schedule and budget management will improve.
B. Performance is measured from different perspectives.
C. Information is provided in a consistent and timely manner.
D. Project will be prioritized based on value.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1297
The quality assurance (QA) function should be prevented from:

A. developing naming conventions.
B. establishing analysis techniques.
C. amending review procedures.
D. changing programs for business functions.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1298
Which of the following provides the **GREATEST** assurance that any confidential information on a disk is no longer accessible but the device is still usable by other internal users?

A. Reformatting the disk

B. Erasing the disk
C. Degaussing the disk
D. Password-protecting the disk

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1299
The demilitarized zone (DMZ) is the part of a network where servers that are placed are:

A. running internal department applications.
B. running mission-critical, non-web applications.
C. interacting with the public Internet.
D. external to the organization.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1300
An organization has installed blade server technology in its data center. To determine whether higher cooling demands are maintained, which of the following should the IS auditor review?

A. Ventilation systems
B. Uninterruptible power supply (UPS) systems
C. Air conditioning capacity
D. Duct maintenance

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1301
An employee loses a mobile device resulting in loss of sensitive corporate data. Which of the following would have **BEST** prevented data leakage?
A. Awareness training for mobile device users
B. Data encryption on the mobile device
C. The triggering of remote data wipe capabilities
D. Complex password policy for mobile devices

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1302
Which of the following components of a scheduling tool **BEST** prevents job failures due to insufficient system resources?

A. Job dependencies
B. Delayed job starts
C. Exception handling
D. Error alerts

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1303
Which of the following is the **MOST** effective control for emergency changes to application programs?

A. Processing the change through change control with review of the change the following day
B. Keeping a sealed envelope containing a password that operators can use to make emergency changes
C. Periodically checking the application program libraries to detect whether unauthorized changes have been made
D. Preparing and approving program change forms before the changes are made

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1304
Which of the following is **BEST** for providing uninterrupted services?

A. Snapshots
B. Differential backup
C. Televaulting
D. Mirroring

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1305
An organization globally distributes a free phone application that includes a module to gather and report user information. The application includes a privacy notice alerting users to the data gathering. Which of the following presents the **GREATEST** risk?

A. The data gathering notice is available in only one language.
B. There is no framework to delete personal data.
C. There may be a backlash among users when the data gathering is revealed.
D. The data is not properly encrypted on the application server.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1306
Which of the following is the **BEST** detective control for a job scheduling process involving data transmission?
A. Metrics denoting the volume of monthly job failures are reported and reviewed by senior management.
B. Job failure alerts are automatically generated and routed to support personnel.
C. Jobs are scheduled and a log of this activity is retained for subsequent review.
D. Jobs are scheduled to be completed daily and data is transmitted using a secure File Transfer Protocol (FTP).

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1307
An organization is running servers with critical business applications that are in an area subject to frequent but brief power outages. Knowledge of which of the following would allow the organization's management to monitor the ongoing adequacy of the uninterrupted power supply (UPS)?

A. Duration and interval of the power outages
B. Business impact of server downtime
C. Number of servers supported by the UPSD. Mean time to recover servers after failure

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1308
The **GREATEST** risk of database denormalization is:

A. decreased performance.
B. loss of data confidentiality.
C. loss of database integrity.
D. incorrect metadata.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1309
Which of the following would **MOST** effectively aid executive management in achieving IT and business alignment?

A. Risk assessment
B. Value delivery assessment
C. Balanced scorecard
D. Performance measurement

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1310
Loading of illegal software packages onto a network by an employee is **MOST** effectively detected by:

A. diskless workstations.
B. regular scanning of hard drivesC. maintaining current antivirus software.
D. logging of activity on network drives.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1311

Effective IT governance requires organizational structures and processes to ensure that: A. the organization's strategies and objectives extend the IT strategy.

B. the business strategy is derived from an IT strategy.
C. IT governance is separate and distinct from the overall governance.
D. the IT strategy extends the organization's strategies and objectives.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

QUESTION 1312
The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

A. IT budget.
B. existing IT environment.
C. business plan.
D. investment plan.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall IT strategy. IT strategy should be aligned with the business strategy and, hence, reviewing the business plan should be the major consideration. Choices A, B and D are important but secondary to the importance of reviewing the business plan,

QUESTION 1313
When implementing an IT governance framework in an organization the MOST important objective is:

A. IT alignment with the business.
B. accountability.
C. value realization with IT.
D. enhancing the return on IT investments.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business {choice A). To achieve alignment, all other choices need to be tied to business practices and strategies.

QUESTION 1314
The ultimate purpose of IT governance is to:

A. encourage optimal use of IT.
B. reduce IT costs.
C. decentralize IT resources across the organization.
D. centralize control of IT.

Correct Answer: A

Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
IT governance is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise. Reducing IT costs may not be the best IT governance outcome for an enterprise. Decentralizing IT resources across the organization is not always desired, although it may be desired in a decentralized environment. Centralizing control of IT is not always desired. An example of where it might be desired is an enterprise desiring a single point of customer contact.

QUESTION 1315
What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

A. Repeatable but Intuitive
B. Defined
C. Managed and Measurable
D. Optimized

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Defined (level 3) is the lowest level at which an IT balanced scorecard is defined.

QUESTION 1316
Responsibility for the governance of IT should rest with the:

A. IT strategy committee.
B. chief information officer (CIO).
C. audit committee.
D. board of directors.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. The audit committee, the chief information officer (CIO) and the IT strategy committee all play a significant role in the successful implementation of IT governance within an organization, but the ultimate accountability resides with the board of directors.

QUESTION 1317
An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

A. User acceptance testing (UAT) occur for all reports before release into production
B. Organizational data governance practices be put in place
C. Standard software tools be used for report development
D. Management sign-off on requirements for new reports

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
This choice directly addresses the problem. An organization wide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

QUESTION 1318
An IS auditor should be concerned when a telecommunication analyst:

A. monitors systems performance and tracks problems resulting from program changes.
B. reviews network load requirements in terms of current and future transaction volumes.
C. assesses the impact of the network load on terminal response times and network data transfer rates.
D. recommends network balancing procedures and improvements.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes {choice B), assessing the impact of network load or terminal response times and network data transfer rates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes {choice A) would put the analyst in a selfmonitoring role.

QUESTION 1319
Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

A. Senior management is aware of critical information assets and demonstrates an adequate concern for their protection.
B. Job descriptions contain clear statements of accountability for information security.
C. In accordance with the degree of risk and business impact, there is adequate funding for security efforts.
D. No actual incidents have occurred that have caused a loss or a public embarrassment.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Inclusion in job descriptions of security responsibilities is a form of security training and helps ensure that staff and management are aware of their roles with respect to information security. The other three choices are not criterion for evaluating security awareness training. Awareness is a criterion for evaluating the importance that senior management attaches to information assets and their protection. Funding is a criterion that aids in evaluating whether security vulnerabilities are being addressed, while the number of incidents that have occurred is a criterion for evaluating the adequacy of the risk management program.

QUESTION 1320
Which of the following is a risk of cross-training?

A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

QUESTION 1321
In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

A. there is an integration of IS and business staffs within projects.
B. there is a clear definition of the IS mission and vision.
C. a strategic information technology planning methodology is in place.
D. the plan correlates business objectives to IS goals and objectives.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

QUESTION 1322
Which of the following goals would you expect to find in an organization's strategic plan?

A. Test a new accounting package.
B. Perform an evaluation of information technology needs.
C. Implement a new project planning system within the next 12 months.
D. Become the supplier of choice for the product offered.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time- and project-oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

QUESTION 1323
An IS auditor reviewing an organization's IT strategic plan should FIRST review:

A. the existing IT environment.
B. the business plan.
C. the present IT budget.
D. current technology trends.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

QUESTION 1324
When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS: A. has all the personnel and equipment it needs.

B. plans are consistent with management strategy.
C. uses its equipment and personnel efficiently and effectively.
D. has sufficient excess capacity to respond to changing directions.

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

QUESTION 1325
In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

A. Optimized
B. Managed
C. Defined
D. Repeatable

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

QUESTION 1326
When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

A. incorporates state of the art technology.
B. addresses the required operational controls.
C. articulates the IT mission and vision.
D. specifies project management practices.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

QUESTION 1327
When reviewing an organization's strategic IT plan an IS auditor should expect to find:

A. an assessment of the fit of the organization's application portfolio with business objectives.
B. actions to reduce hardware procurement cost.
C. a listing of approved suppliers of IT contract resources.
D. a description of the technical architecture for the organization's network perimeter security.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is to set out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail ofa specific technical architecture.

QUESTION 1328
An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive information.
B. information security is not critical to all functions.
C. IS audit should provide security training to the employees.
D. the audit finding will cause management to provide continuous training to staff.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

QUESTION 1329
The development of an IS security policy is ultimately the responsibility of the:

A. IS department.
B. security committee.
C. security administrator.
D. board of directors.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

QUESTION 1330
Which of the following is the initial step in creating a firewall policy?

A. A cost-benefit analysis of methods for securing the applications
B. Identification of network applications to be externally accessed
C. Identification of vulnerabilities associated with network applications to be externally accessed
D. Creation of an applications traffic matrix showing protection methods

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

QUESTION 1331
The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

A. Utilization of an intrusion detection system to report incidents
B. Mandating the use of passwords to access all software
C. Installing an efficient user log system to track the actions of each user D. Training provided on a regular basis to all current and new employees

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

QUESTION 1332
In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

A. implementation.
B. compliance.
C. documentation.
D. sufficiency.

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

Explanation:
An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

QUESTION 1333
To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

A. the IT infrastructure.
B. organizational policies, standards and procedures.
C. legal and regulatory requirements.
D. the adherence to organizational policies, standards and procedures.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

QUESTION 1334
A top-down approach to the development of operational policies will help ensure:

A. that they are consistent across the organization.
B. that they are implemented as a part of risk assessment.
C. compliance with all policies.
D. that they are reviewed periodically.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Deriving lower level policies from corporate policies {a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

QUESTION 1335
Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

A. Time zone differences could impede communications between IT teams.
B. Telecommunications cost could be much higher in the first year.
C. Privacy laws could prevent cross-border flow of information.
D. Software development may require more detailed specifications.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

QUESTION 1336
A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

A. Issues of privacy
B. Wavelength can be absorbed by the human body
C. RFID tags may not be removable
D. RFID eliminates line-of-sight reading

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The purchaser of an item will not necessarily be aware of the presence of the tag. If a tagged item is paid for by credit card, it would be possible to tie the unique ID of that item to the identity of the purchaser. Privacy violations are a significant concern because RFID can carry unique identifier numbers. If desired it would

A.

B.

be possible for a firm to track individuals who purchase an item containing an RFID. Choices B and C are concerns of less importance. Choice D is not a concern.

QUESTION 1337
When developing a security architecture, which of the following steps should be executed FIRST?

Developing security procedures
Defining a security policy
C. Specifying an access control methodology
D. Defining roles and responsibilities

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Defining a security policy for information and related technology is the first step toward building a security architecture. A security policy communicates a coherent security standard to users, management and technical staff. Security policies will often set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

QUESTION 1338
An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

A. technical platforms between the two companies are interoperable.
B. parent bank is authorized to serve as a service provider.
C. security features are in place to segregate subsidiary trades.
D. subsidiary can join as a co-owner of this payment system.

Correct Answer: B
Section: Protection of Information Assets
Explanation

B.

C.

Explanation/Reference:
Explanation:
Even between parent and subsidiary companies, contractual agreement(s) should be in place to conduct shared services. This is particularly important in highly regulated organizations such as banking. Unless granted to serve as a service provider, it may not be legal for the bank to extend business to the subsidiary companies. Technical aspects should always be considered; however, this can be initiated after confirming that the parent bank can serve as a service provider. Security aspects are another important factor; however, this should be considered after confirming that the parent bank can serve as a service provider. The ownership of the payment system is not as important as the legal authorization to operate the system.

QUESTION 1339
Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

A. Define a balanced scorecard (BSC) for measuring performance Consider user satisfaction in the key performance indicators (KPIs) Select projects according to business benefits and risks
D. Modify the yearly process of defining the project portfolio

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Prioritization of projects on the basis of their expected benefit(s) to business, and the related risks, is the best measure for achieving alignment of the project portfolio to an organization's strategic priorities. Modifying the yearly process of the projects portfolio definition might improve the situation, but only if the portfolio definition process is currently not tied to the definition of corporate strategies; however, this is unlikely since the difficulties are in maintaining the alignment, and not in setting it up initially. Measures such as balanced scorecard (BSC) and key performance indicators (KPIs) are helpful, but they do not guarantee that the projects are aligned with business strategy.

QUESTION 1340
A benefit of open system architecture is that it:

A. facilitates interoperability.
B. facilitates the integration of proprietary components.
C.

D.

C. will be a basis for volume discounts from equipment vendors.
D. allows for the achievement of more economies of scale for equipment.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

QUESTION 1341
Which of the following BEST supports the prioritization of new IT projects?

A. Internal control self-assessment (CSA)
B. Information systems auditInvestment portfolio analysis

D.

E.

Business risk assessment

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is most desirable to conduct an investment portfolio analysis, which will present not only a clear focus on investment strategy, but will provide the rationale for terminating nonperforming IT projects. Internal control self-assessment (CSA) may highlight noncompliance to the current policy, but may not necessarily be the best source for driving the prioritization of IT projects. Like internal CSA, IS audits may provide only part of the picture for the prioritization of IT projects. Business risk analysis is part of the investment portfolio analysis but, by itself, is not the best method for prioritizing new IT projects.

QUESTION 1342
Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

A. Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan.
B. Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract.
C. No, because the backup to be provided should be specified adequately in the contract.
D. No, because the service bureau's business continuity plan is proprietary information.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary responsibility of an IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

QUESTION 1343
When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

A. There could be a question regarding the legal jurisdiction.
B. Having a provider abroad will cause excessive costs in future audits.
C. The auditing process will be difficult because of the distance.
D. There could be different auditing norms.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

QUESTION 1344
An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

A. That an audit clause is present in all contracts
B. That the SLA of each contract is substantiated by appropriate KPIs
C. That the contractual warranties of the providers support the business needs of the organization
D. That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be met. All other choices are important, but not as potentially dangerous as the interplay of the diverse and critical areas of the contractual responsibilities of the outsourcers.

QUESTION 1345
With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

A. Outsourced activities are core and provide a differentiated advantage to the organization.
B. Periodic renegotiation is specified in the outsourcing contract.
C. The outsourcing contract fails to cover every action required by the arrangement.
D. Similar activities are outsourced to more than one vendor.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An organization's core activities generally should not be outsourced, because they are what the organization does best; an IS auditor observing that should be concerned. An IS auditor should not be concerned about the other conditions because specification of periodic renegotiation in the outsourcing contract is a best practice. Outsourcing contracts cannot be expected to cover every action and detail expected of the parties involved, while multisourcing is an acceptable way to reduce risk.

QUESTION 1346
While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the:

A. requirement for protecting confidentiality of information could be compromised.
B. contract may be terminated because prior permission from the outsourcer was not obtained.
C. other service provider to whom work has been outsourced is not subject to audit.
D. outsourcer will approach the other service provider directly for further work.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Many countries have enacted regulations to protect the confidentiality of information maintained in their countries and/or exchanged with other countries. Where a service provider outsources part of its services to another service provider, there is a potential risk that the confidentiality of the information will be compromised. Choices B and C could be concerns but are no related to ensuring the confidentiality of information. There is no reason why an IS auditor should be concerned with choice D.

QUESTION 1347
An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

A. documentation of staff background checks.
B. independent audit reports or full audit access.
C. reporting the year-to-year incremental cost reductions.
D. reporting staff turnover, development or training.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When the functions of an IS department are outsourced, an IS auditor should ensure that a provision is made for independent audit reports that cover all essential areas, or that the outsourcer has full audit access. Although it is necessary to document the fact that background checks are performed, this is not as important as provisions for audits. Financial measures such as year-to-year incremental cost reductions are desirable to have in a service level agreement (SLA); however, cost reductions are not as important as the availability of independent audit reports or full audit access. An SLA might include human relationship measures such as resource planning, staff turnover, development or training, but this is not as important as the requirements for independent reports or full audit access by the outsourcing organization.

QUESTION 1348
Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

A. meets or exceeds industry security standards.
B. agrees to be subject to external security reviews.
C. has a good market reputation for service and experience.
D. complies with security policies of the organization.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization policies is important, but there is no way to verify or prove that that is the case without an independent review. Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

QUESTION 1349
The risks associated with electronic evidence gathering would MOST likely be reduced by an e- mail:

A. destruction policy.
B. security policy.
C. archive policy.
D. audit policy.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

QUESTION 1350
Which of the following should be the **PRIMARY** basis for how digital evidence is handled during a forensics investigation?

A. Industry best practices
B. Regulatory requirements
C. Organizational risk culture
D. Established business practices

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1351
Which of the following firewall technologies involves examining the header of every packet of data traveling between the Internet and the corporate network without examining the previous packets?

A. Proxy servers
B. Bastion host
C. Stateful filtering
D. Stateless filtering

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
QUESTION 1352
A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is **MOST** effective in detecting such an intrusion?

A. Installing biometrics-based authentication
B. Configuring the router as a firewall
C. Periodically reviewing log files
D. Using smart cards with one-time passwords

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1353
Which of the following are used in a firewall to protect the entity's internal resources?

A. Internet Protocol (IP) address restrictions
B. Remote access servers
C. Secure Sockets Layers (SSLs)
D. Fail-over services

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1354
Which of the following is the **BEST** way to address potential data privacy concerns associated with inadvertent disclosure of machine identifier information contained within security logs?

A. Only collect logs from servers classified as business critical.
B. Limit the use of logs to only those purposes for which they were collected.
C. Limit log collection to only periods of increased security activity.
D. Restrict the transfer of log files from host machine to online storage.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1355
On a public-key cryptosystem when there is no previous knowledge between parties, which of the following will **BEST** help to prevent one person from using a fictitious key to impersonate someone else?

A. Encrypt the message containing the sender's public key, using a private-key cryptosystem.
B. Send a certificate that can be verified by a certification authority with the public key.
C. Encrypt the message containing the sender's public key; using the recipient's pubic key.

D. Send the public key to the recipient prior to establishing the connection.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1356
In an online application, which of the following would provide the **MOST** information about the transaction audit trail?

A. File layouts
B. System/process flowchart
C. Source code documentation
D. Data architecture

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
QUESTION 1357
The drives of a tile server are backed up at a hot site. Which of the following is the **BEST** way to duplicate the files stored on the server for forensic analysis?

A. Capture a bit-by-bit image of the file server's drives.
B. Run forensic analysis software on the backup drive.
C. Create a logical copy of the file server’s drives.
D. Replicate the server's volatile data to another drive.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1358
Which of the following **BEST** helps to ensure data integrity across system interfaces?

A. Environment segregation
B. System backups
C. Reconciliations
D. Access controls

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1359
When implementing a software product (middleware) to pass data between local area network (LAN) servers and the mainframe, the **MOST** critical control consideration is:

A. cross-platform authentication.
B. time synchronization of databases.
C. network traffic levels between platforms.
D. time-stamping of transactions to facilitate recovery.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1360
Which of the following is the **GREATEST** advantage of using a framework to guide an organization's governance of IT?

A. It enables consistency when making strategic IT investments across the organization.

B. It enables better management of the annual IT budget provided by the board of directors.
C. It enables improvements to the security of high-risk systems in the organization.
D. It enables the achievement of service levels between IT and true business departments.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1361
Which of the following is the **BEST** point in time to conduct a post-implementation review (PIR)?

A. After a full processing cycle
B. Immediately after deployment
C. To coincide with annual PIR cycle
D. Six weeks after deployment

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 1362
Which of the following activities provides an IS auditor with the **MOST** insight regarding potential single person dependencies that might exist withing the organization?

A. Reviewing user activity logs
B. Mapping IT processes to roles
C. Reviewing vacation patterns
D. Interviewing senior IT management

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1363
Which of the following is the **PRIMARY** reason for an IS auditor to map out the narrative of a business process?

A. To verify the business process is as described in the engagement letter
B. To identify the resources required to perform the audit
C. To ensure alignment with organizational objectives
D. To gain insight into potential risks

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1364
Which of the following ensures components of an IT system are identified and baselined, and that changes to them are implemented in a controlled manner?

A. Restricted production access
B. Configuration management process
C. Change management process
D. Software versioning control

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1365

At which stage of the software development life cycle should an organization identity privacy considerations?

A. Design
B. Testing
C. Development
D. Requirements

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1366
Which of the following test approaches would utilize data analytics to test a dual approval payment control?

A. Review payments completed in the past month that do not have a unique approver.
B. Attempt to complete a payment without a secondary approval.
C. Review users within the payment application who are assigned an approver role.
D. Evaluate configuration settings for the secondary approval requirements.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1367
Which of the following would be of **MOST** concern when determining if information assets are adequately safeguard during transport and disposal?

A. Lack of password protection
B. Lack of recent awareness training
C. Lack of appropriate data classification

D. Lack of appropriate labeling

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1368
Which of the following is the **BEST** way for an IS auditor to assess the effectiveness of backup procedures?

A. Review the backup schedule.
B. Evaluate the latest data restore.
C. Inspect backup logs.
D. Interview the data owner.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 1369
Which of the following mechanisms for process improvement involves examination of industry best practice?

A. Continuous improvement
B. Knowledge management
C. Business process reengineering (BPR)
D. Benchmarking

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1370
An IS auditor determines that a business impact analysis (BIA) was not conducted during the development of a business continuity plan (BCP). What is the **MOST** significant risk that could result from this situation?

A. Responsibilities are not property defined.
B. Recovery time objectives (RTOs) are not correctly determined.
C. Key performance indicators (KPIs) are not aligned.
D. Critical business applications are not covered.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1371
To mitigate the risk of exposing data through application programming interface (API) queries, which of the following design considerations is **MOST** important?

A. Data minimalization
B. Data quality
C. Data retention
D. Data integrity

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1372
Which of the following is the **BEST** way to transmit documents classified as confidential over the Internet?
A. Hashing the document contents and destroying the hash value
B. Sending documents as multiple packets over different network routes

C. Converting documents to proprietary format before transmission
D. Using a virtual private network (VPN)

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1373
An IS auditor is auditing the infrastructure of an organization that hosts critical applications withing a virtual environment. Which of the following is **MOST** important for the auditor to focus on?

A. The ability to copy and move virtual machines in real time
B. The controls in place to prevent compromise of the host
C. Issues arising from system management of a virtual infrastructure
D. Qualifications of employees managing the applications

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1374
An audit report notes that terminated employees have been retaining their access rights after their departure. Which of the following strategies would **BEST** ensure that obsolete access rights are identified in a timely manner?

A. Delete user IDs at a predetermined date after their creation.
B. Automatically delete user IDs after they are unused for a predetermined time.
C. Implement an automated interface with the organization's human resources system.
D. Require local supervisors to initiate connection.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1375
A small organization does not have enough employees to implement adequate segregation of duties in accounts payable. Which of the following is the **BEST** compensating control to mitigate the risk associated with this situation?

A. Regular reconciliation of key transactions approved by a supervisor
B. Supervisory review of logs to detect changes in vendors
C. Review of transactions exceeding a specific threshold
D. Rotation of duties among existing personnel

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1376
When reviewing a database supported by a third-party service provider, an IS auditor found minor control deficiencies. The auditor should **FIRST** discuss recommendations with the:

A. service provider support team manager
B. organization's service level manager
C. organization's chief information officer (CIO)
D. service provider contract liaison

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1377
Following an IT audit, management has decided to accept the risk highlighted in the audit report. Which of the following would provide the **MOST** assurance to the IS auditor that management is adequately balancing the needs of the business with the need to manage risk?

A. Established criteria exist for accepting and approving risk.
B. Identified risk is reported into the organization's risk committee.
C. Potential impact and likelihood is adequately documented.
D. A communication plan exists for informing parties impacted by the risk.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1378
During a review of operations, it is noted that during a batch update, an error was detected and the database initiated a roll-back. An IT operator stopped the rollback and re-initiated the update. What should the operator have done **PRIOR** to re-initiating the update?

A. Determined the cause of the error
B. Obtained approval before re-initiating the update
C. Allowed the roll-back to complete

D. Scheduled the roll-back for a later time

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
QUESTION 1379
Which of the following provides the **BEST** evidence that network filters are functioning?

A. Reviewing network configuration rules
B. Reviewing network filtering policy
C. Performing network port scans
D. Analyzing network performance

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1380
An IS auditor is performing a routine procedure to test for the possible existence of fraudulent transactions. Given there is no reason to suspect the existence of fraudulent transactions, which of the following data analytics techniques should be employed?

A. Association analysis
B. Classification analysis
C. Anomaly detection analysis
D. Regression analysis

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1381
Following an acquisition, it was decided that legacy applications subject to compliance requirements will continue to be used until they can be phased out. The IS auditor needs to determine where there are control redundancies and where gaps may exist. Which of the following activities would be **MOST** helpful in making this determination?

A. Control self-assessments
B. Risk assessment
C. Control testing
D. Control mapping

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1382
Which of the following threats is **MOST** effectively controlled by a firewall?

A. Network congestion
B. Denial of service (DoS) attack
C. Network sniffing
D. Password cracking

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1383
After discussing findings with an auditee, an IS auditor is required to obtain approval of the report from the CEO before issuing it to the audit committee. This requirement **PRIMARILY** affects the IS auditor's:

A. judgment
B. effectiveness
C. independence
D. integrity

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
QUESTION 1384
During a post-incident review of a security breach, what type of analysis should an IS auditor expect to be performed by the organization's information security team?

A. Gap analysis
B. Business impact analysis (BIA)
C. Qualitative risk analysis
D. Root cause analysis

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1385
Which of the following is **MOST** important for an IS auditor to consider when auditing a vulnerability scanning software solution?

A. The scanning software was purchased from an approved vendor.

B. The scanning software was approved for release into production.
C. The scanning software covers critical systems.
D. The scanning software is cost-effective.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1386
Which of the following is the **BEST** indication that an organization has achieved legal and regulatory compliance?

A. The board of directors and senior management accept responsibility for compliance.
B. An independent consultant has been appointed to ensure legal and regulatory compliance.
C. Periodic external and internal audits have not identified instances of noncompliance.
D. The risk management process incorporates noncompliance as a risk.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 1387
Which of the following is the **PRIMARY** objective of using a capability maturity model as a tool to communicate audit results to senior management?

A. To evaluate management's action plan
B. To confirm audit findings
C. To illustrate improvement opportunities
D. To prioritize remediation efforts

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference: