CISA.810q

Number: CISA
Passing Score: 800
Time Limit: 120 min

CISA

Certified Information Systems Auditor

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

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 2

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 3
Multiple invoices are usually received for individual purchase orders, since purchase orders require staggered delivery dates. Which of the following is the **BEST** audit technique to test for duplicate payments?

A. Run the data on the software programs used to process supplier payments.
B. Use generalized audit software on the invoice transaction file.
C. Run the data on the software programs used to process purchase orders.
D. Use generalized audit software on the purchase order transaction file.

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

Explanation/Reference:

QUESTION 4
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 5
In a data center audit, an IS auditor finds that the humidity level is very low. The IS auditor would be **MOST** concerned because of an expected increase in:

A. employee discomfort
B. risk of fire
C. static electricity problems
D. backup tape failures

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

Explanation/Reference:

QUESTION 6
Before concluding that internal controls can be relied upon, the IS auditor should:

A. discuss the internal control weakness 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 7
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 8

Section: The process of Auditing Information System
Explanation

Explanation/Reference:
Which of the following should an IS auditor review **FIRST** when planning a customer data privacy audit?

A. Legal and compliance requirements
B. Customer agreements
C. Organizational policies and procedures
D. Data classification

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

Explanation/Reference:

QUESTION 9
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 10
Which of the following should be established **FIRST** when initiating a control self-assessment program in a small organization?

A. Control baselines
B. Client questionnaires
C. External consultants
D. Facilitated workshops

B

QUESTION 11
What is an IS auditor's **BEST** course of action if informed by a business unit's representatives that they are too busy to cooperate with a scheduled audit?

A. Reschedule the audit for a time more convenient to the business unit.
B. Notify the chief audit executive who can negotiate with the head of the business unit.
C. Begin the audit regardless and insist on cooperation from the business unit.
D. Notify the audit committee immediately and request they direct the audit begin on schedule.

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

Explanation/Reference:

QUESTION 12
An IS auditor has completed an audit of an organization's accounts payable system. Which of the following should be rated as the **HIGHEST** risk in the audit report and requires immediate remediation?

A. Lack of segregation of duty controls for reconciliation of payment transactions
B. Lack of segregation of duty controls for removal of vendor records
C. Lack of segregation of duty controls for updating the vendor master file
D. Lack of segregation of duty controls for reversing payment transactions

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

Explanation/Reference:

QUESTION 13
An IS auditor is planning on utilizing attribute sampling to determine the error rate for health care claims processed. Which of the following factors will cause the sample size to decrease?

Correct Answer:

Section: The process of Auditing Information System
Explanation

Explanation/Reference:
A. Population size increase
B. Expected error rate increase
C. Acceptable risk level decrease
D. Tolerate error rate increase

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

Explanation/Reference:

QUESTION 14
Which of the following is the **PRIMARY** benefit of using an integrated audit approach?

A. Higher acceptance of the findings from the audited business areas
B. The avoidance of duplicated work and redundant recommendations
C. Enhanced allocation of resources and reduced audit costs
D. A holistic perspective of overall risk and a better understanding of controls

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

Explanation/Reference:

QUESTION 15
Which of the following is an analytical review procedure for a payroll system?

A. Performing penetration attempts on the payroll system
B. Evaluating the performance of the payroll system, using benchmarking software
C. Performing reasonableness tests by multiplying the number of employees by the average wage rate
D. Testing hours reported on time sheets

C

QUESTION 16

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 17
Two servers are deployed in a cluster to run a mission-critical application. To determine whether the system has been designed for optimal efficiency, the IS auditor should verify that:

A. the security features in the operating system are all enabled
B. the number of disks in the cluster meets minimum requirements
C. the two servers are of exactly the same configuration
D. load balancing between the servers has been implemented

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

Explanation/Reference:

QUESTION 18
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:

Section: The process of Auditing Information System
Explanation

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

Explanation/Reference:

QUESTION 19
An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor's **BEST** recommendation for the organization?

A. Continue using the existing application since it meets the current requirements
B. Prepare a maintenance plan that will support the application using the existing code
C. Bring the escrow version up to date
D. Undertake an analysis to determine the business risk

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

Explanation/Reference:

QUESTION 20
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

A

QUESTION 21
An IS auditor finds a number of system accounts that do not have documented approvals. Which of the following should be performed **FIRST** by the auditor?

A. Have the accounts removed immediately
B. Obtain sign-off on the accounts from the application owner
C. Document a finding and report an ineffective account provisioning control
D. Determine the purpose and risk of the accounts

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

Explanation/Reference:

QUESTION 22
An IS auditor is a member of an application development team that is selecting software. Which of the following would impair the auditor's independence?

A. Verifying the weighting of each selection criteria
B. Approving the vendor selection methodology
C. Reviewing the request for proposal (RFP)
D. Witnessing the vendor selection process

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

Explanation/Reference:

QUESTION 23
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?

Correct Answer:

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 24
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 25
Which of the following would be best suited to oversee the development of an information security policy?

A. System Administrators
B. End User
C. Security Officers
D. Security administrators

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

Explanation/Reference:

The security officer would be the best person to oversee the development of such policies.

Security officers and their teams have typically been charged with the responsibility of creating the security policies. The policies must be written and communicated appropriately to ensure that they can be understood by the end users. Policies that are poorly written, or written at too high of an education level (common industry practice is to focus the content for general users at the sixth- to eighth-grade reading level), will not be understood.

Implementing security policies and the items that support them shows due care by the company and its management staff. Informing employees of what is expected of them and the consequences of noncompliance can come down to a liability issue.

While security officers may be responsible for the development of the security policies, the effort should be collaborative to ensure that the business issues are addressed.

The security officers will get better corporate support by including other areas in policy development. This helps build buy-in by these areas as they take on a greater ownership of the final product. Consider including areas such as HR, legal, compliance, various IT areas and specific business area representatives who represent critical business units.

When policies are developed solely within the IT department and then distributed without business input, they are likely to miss important business considerations. Once policy documents have been created, the basis for ensuring compliance is established. Depending on the organization, additional documentation may be necessary to support policy. This support may come in the form of additional controls described in standards, baselines, or procedures to help personnel with compliance. An important step after documentation is to make the most current version of the documents readily accessible to those who are expected to follow them. Many organizations place the documents on their intranets or in shared file folders to facilitate their accessibility. Such placement of these documents plus checklists, forms, and sample documents can make awareness more effective.

For your exam you should know the information below:

End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.

Executive Management/Senior Management -Executive management maintains the overall responsibility for protection of the information assets. The business operations are dependent upon information being available, accurate, and protected from individuals without a need to know.

Security Officer - The security officer directs, coordinates, plans, and organizes information security activities throughout the organization. The security officer works with many different individuals, such as executive management, management of the business units, technical staff, business partners, auditors, and third parties such as vendors. The security officer and his or her team are responsible for the design, implementation, management, and review of the organization's security policies, standards, procedures, baselines, and guidelines.

Information Systems Security Professional-Drafting of security policies, standards and supporting guidelines, procedures, and baselines is coordinated through these individuals. Guidance is provided for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed in this role.

Data/Information/Business/System Owners - A business executive or manager is typically responsible for an information asset. These are the individuals that assign the appropriate classification to information assets. They ensure that the business information is protected with appropriate controls. Periodically, the information asset owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners or their delegates are responsible for understanding the risks that exist with regards to the information that they control.

Data/Information Custodian/Steward - A data custodian is an individual or function that takes care of the information on behalf of the owner. These individuals ensure that the information is available to the end users and is backed up to enable recovery in the event of data loss or corruption. Information may be stored in files, databases, or systems whose technical infrastructure must be managed, by systems administrators. This group administers access rights to the information assets.

Information Systems Auditor-IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.

Business Continuity Planner -Business continuity planners develop contingency plans to prepare for any occurrence that could have the ability to impact the company's objectives negatively. Threats may include earthquakes, tornadoes, hurricanes, blackouts, changes in the economic/political climate, terrorist activities, fire, or other major actions potentially causing significant harm. The business continuity planner ensures that business processes can continue through the disaster and coordinates those activities with the business areas and information technology personnel responsible for disaster recovery.

Information Systems/ Technology Professionals-These personnel are responsible for designing security controls into information systems, testing the controls, and implementing the systems in production environments through agreed upon operating policies and procedures. The information systems professionals work with the business owners and the security professionals to ensure that the designed solution provides security controls commensurate with the acceptable criticality, sensitivity, and availability requirements of the application.

Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Network/Systems Administrator - A systems administrator (sysadmin

/netadmin)

configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The

administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.
Physical Security - The individuals assigned to the physical security role establish relationships with external law enforcement, such as the local police agencies, state police, or the Federal Bureau of Investigation (FBI) to assist in investigations. Physical security personnel manage the installation, maintenance, and ongoing operation of the closed circuit television (CCTV) surveillance systems, burglar alarm systems, and card reader access control systems. Guards are placed where necessary as a deterrent to unauthorized access and to provide safety for the company employees. Physical security personnel interface with systems security, human resources, facilities, and legal and business areas to ensure that the practices are integrated.

Security Analyst - The security analyst role works at a higher, more strategic level than the previously described roles and helps develop policies, standards, and guidelines, as well as set various baselines. Whereas the previous roles are “in the weeds” and focus on pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level.

Administrative Assistants/Secretaries - This role can be very important to information security; in many companies of smaller size, this may be the individual who greets visitors, signs packages in and out, recognizes individuals who desire to enter the offices, and serves as the phone screener for executives. These individuals may be subject to social engineering attacks, whereby the potential intruder attempts to solicit confidential information that may be used for a subsequent attack. Social engineers prey on the goodwill of the helpful individual to gain entry. A properly trained assistant will minimize the risk of divulging useful company information or of providing unauthorized entry.

Help Desk Administrator - As the name implies, the help desk is there to field questions from users that report system problems. Problems may include poor response time, potential virus infections, unauthorized access, inability to access system resources, or questions on the use of a program. The help desk is also often where the first indications of security issues and incidents will be seen. A help desk individual would contact the computer security incident response team (CIRT) when a situation meets the criteria developed by the team. The help desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control.

Supervisor - The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. For example, suppose Kathy is the supervisor of ten employees. Her responsibilities would include ensuring that these employees understand their responsibilities with respect to security; making sure the employees’ account information is up-to-date; and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee’s role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

Change Control Analyst Since the only thing that is constant is change, someone must make sure changes happen securely. The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Or, a company can choose to just roll out the change and see what happens.

The following answers are incorrect:

Systems Administrator - A systems administrator (sysadmin/ netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.

Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 109
Harris, Shun (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 108). McGraw-Hill. Kindle Edition.

QUESTION 26
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:
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.

Following reference(s) were/was used to create this question:

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 27
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

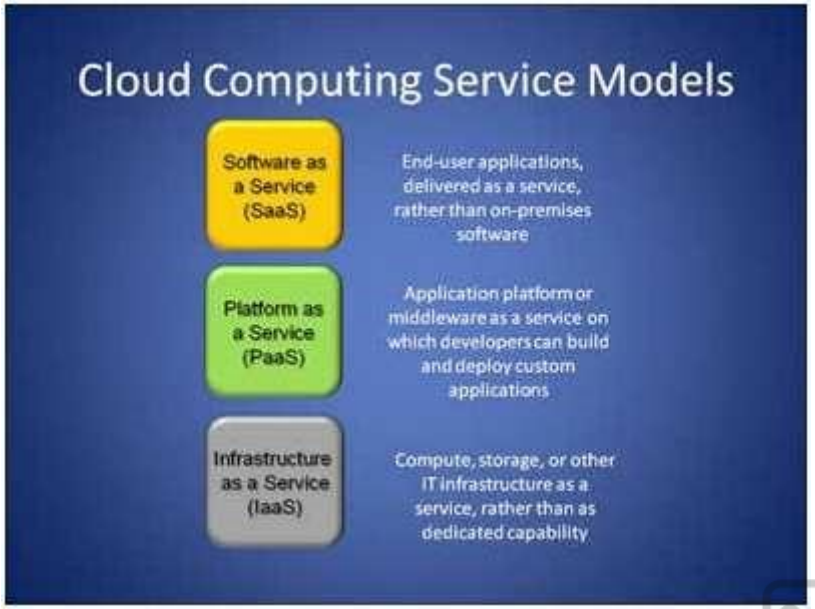
Correct Answer: A
Section: Governance and Management of IT
Explanation

Explanation/Reference:
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.

The following reference(s) were/was used to create this question:

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 28
Which of the following cloud computing service model provides a way to rent operating systems, storage and network capacity over the Internet?

A. Software as a service
B. Data as a service
C. Platform as a service
D. Infrastructure as a service

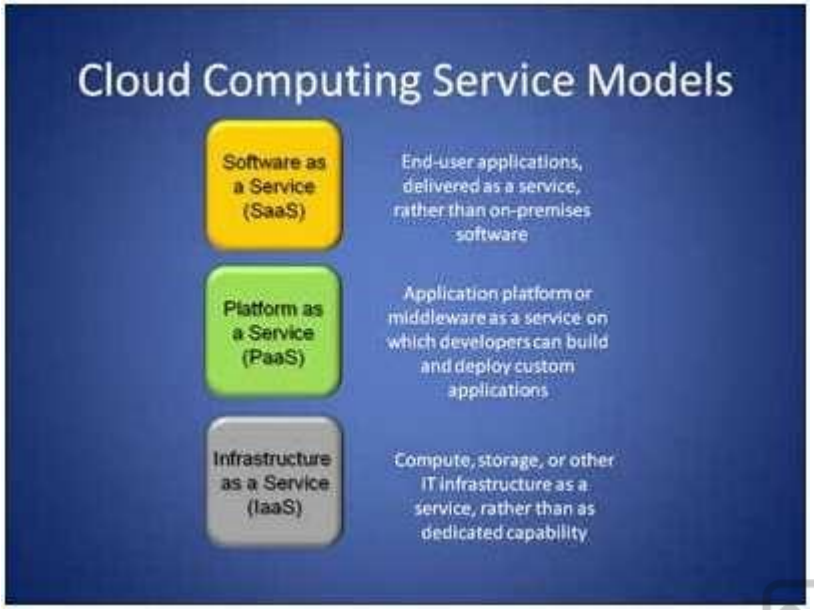
Correct Answer: C
Section: Governance and Management of IT
Explanation

Explanation/Reference:
Platform as a Service (Peas) is a way to rent 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.

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 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.

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.

The following reference(s) were/was used to create this question:

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 29
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?

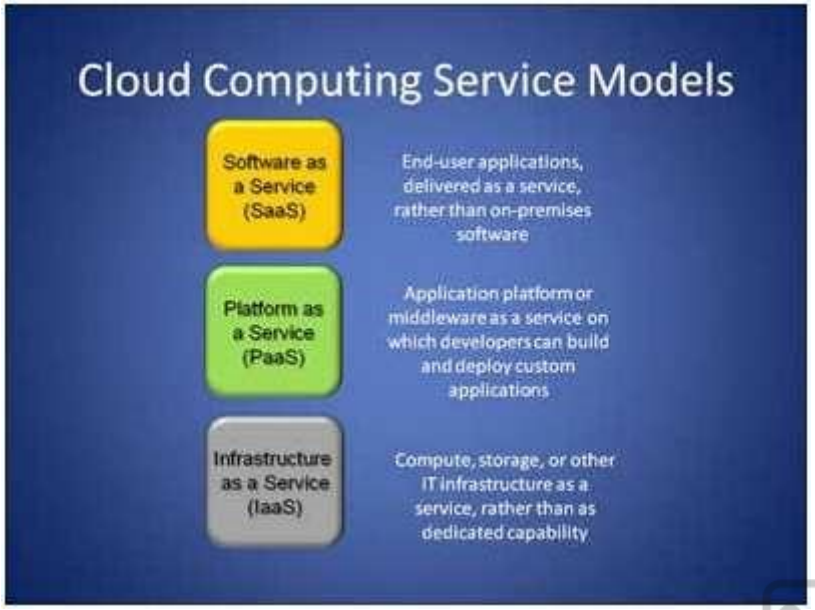
A. Software as a service
B. Data as a service
C. Platform as a service
D. Infrastructure as a service

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

Explanation/Reference:
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.

The following reference(s) were/was used to create this question:

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 30
Which of the following cloud deployment model operates solely for an organization?

A. Private Cloud
B. Community Cloud
C. Public Cloud
D. Hybrid Cloud

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

Explanation/Reference:
In 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.

For your exam you should know below information about Cloud Computing deployment models:

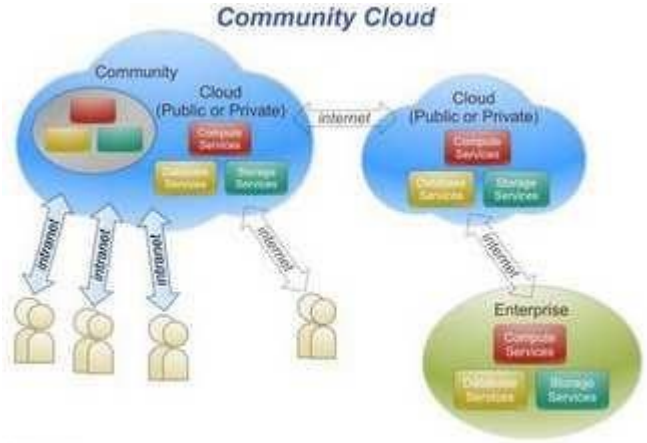
Private cloud

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:

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.

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.

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)
The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102
Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

QUESTION 31
Which of the following cloud deployment model can be shared by several organizations?

A. Private Cloud\
B. Community Cloud
C. Public Cloud
D. Hybrid Cloud

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

Explanation/Reference:
In 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.

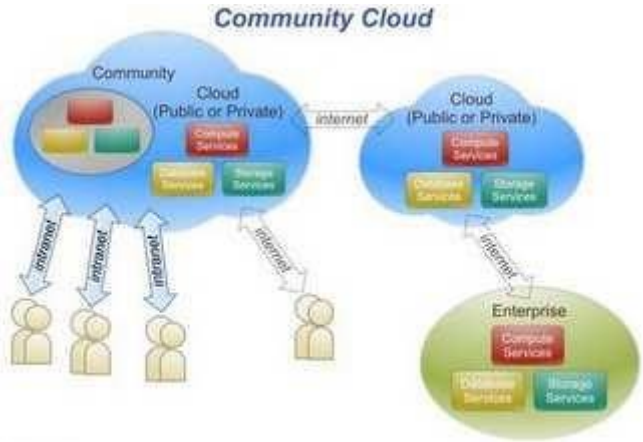
For your exam you should know below information about Cloud Computing deployment models:

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

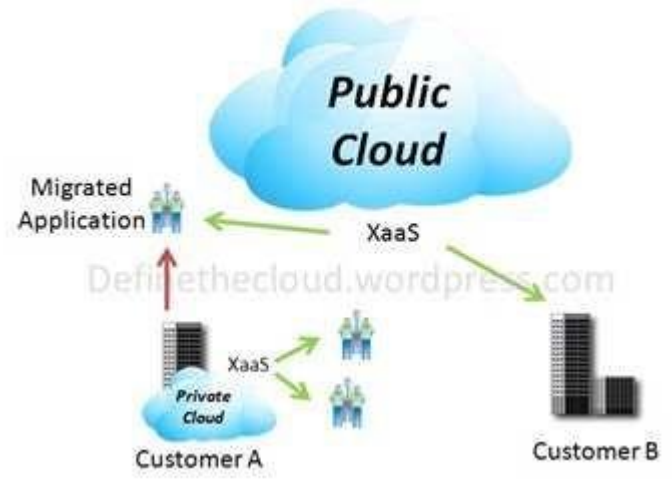
The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the 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.

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.

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)
The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102
Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

QUESTION 32
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:
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.

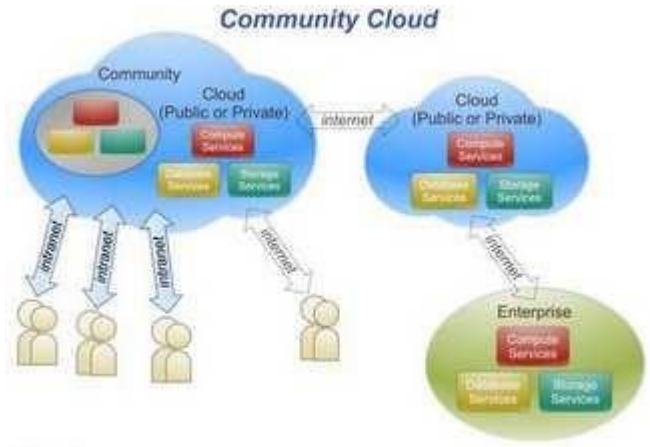
For your exam you should know below information about Cloud Computing deployment models:

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)

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102
Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

QUESTION 33
Which of the following cloud deployment model is formed by the composition of two or more cloud deployment mode?

A. Private Cloud
B. Community Cloud
C. Public Cloud
D. Hybrid Cloud

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

Explanation/Reference:
In 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)

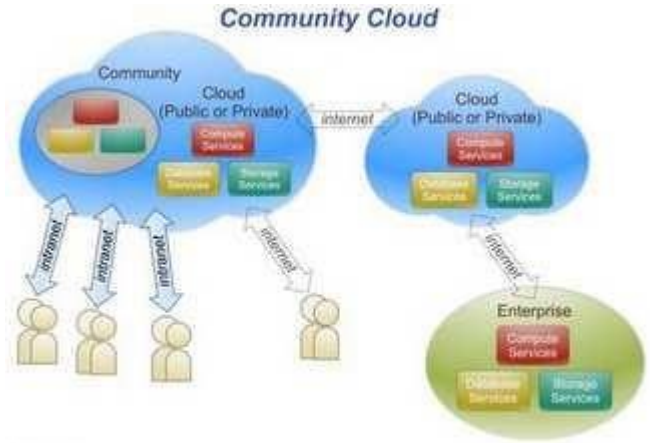
For your exam you should know below information about Cloud Computing deployment models:

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.

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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102
Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

QUESTION 34
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:
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

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 107

QUESTION 35
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:
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

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 107

QUESTION 36
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:
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

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 107

QUESTION 37
Which of the following step of PDCA request a corrective actions on significant differences between the actual versus the planned result?

A. Plan
B. Do
C. Check
D. Act

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

Explanation/Reference:
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.

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.

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

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 107

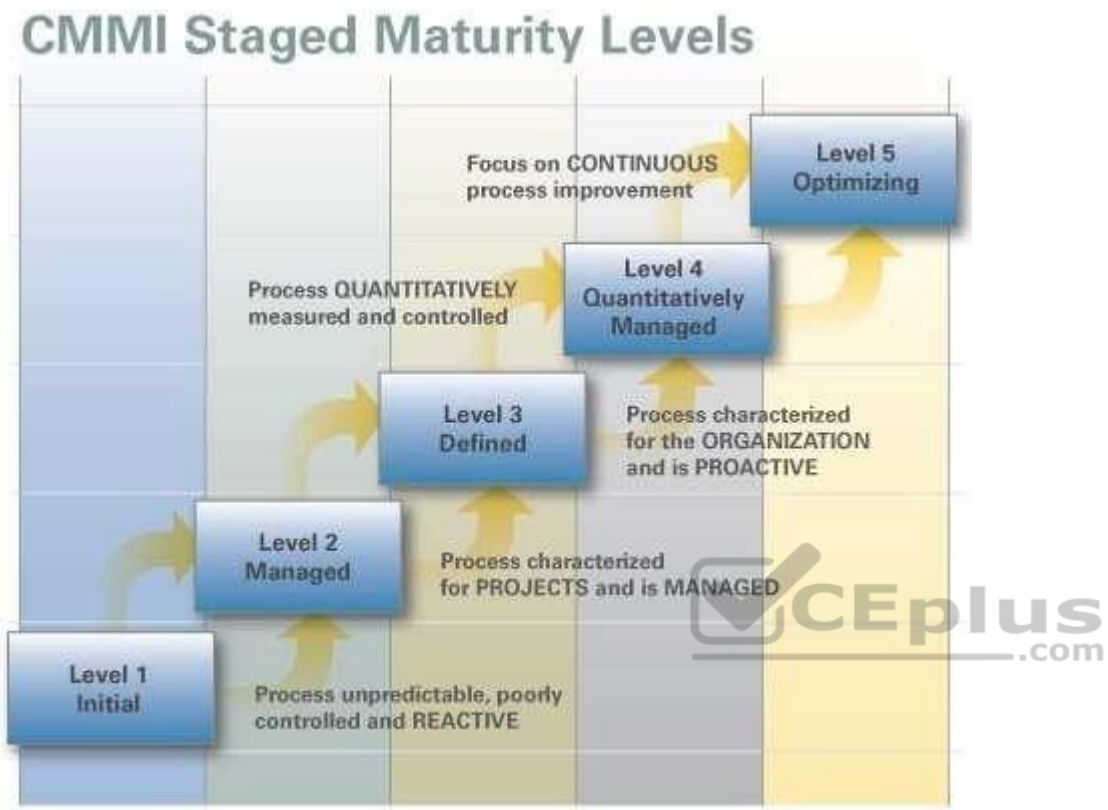
QUESTION 38
Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?

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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188
CISSP Official study guide page number 693

QUESTION 39
Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a pattern of behaviors, effects, assumptions, attitude and ways of doing things?

A. Governing
B. Culture
C. Enabling and support
D. Emergence

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

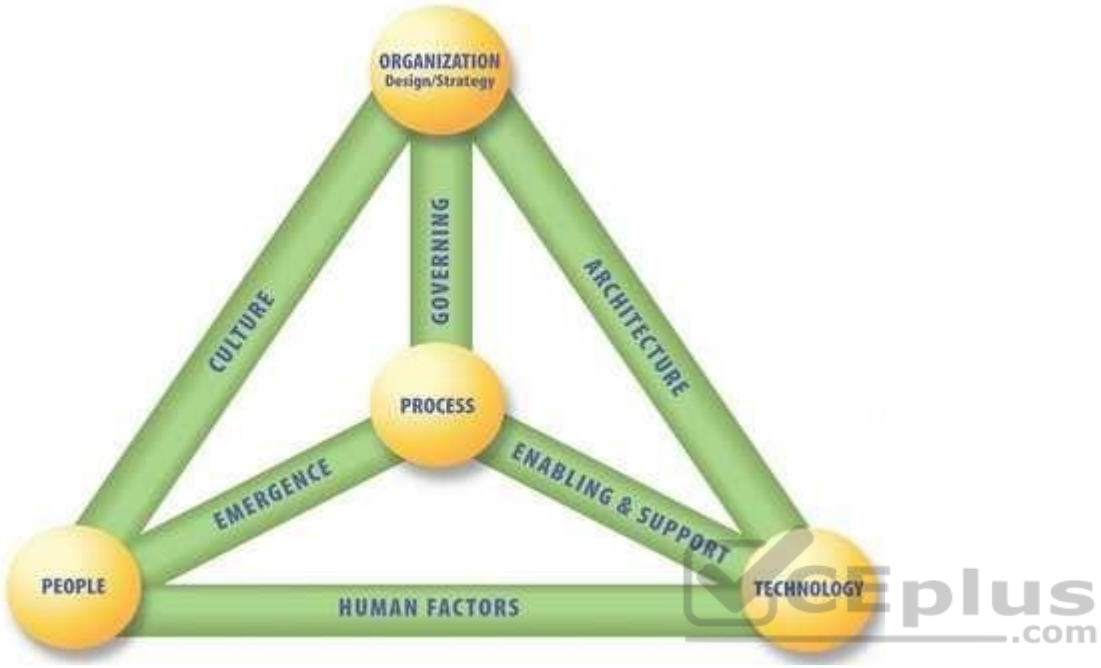
Explanation/Reference:
Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

For your exam you should know the information below.

Business Model for Information Security
The Business Model for Information Security (BMIS) originated at the Institute for Critical Information Infrastructure Protection at the Marshall School of Business at the University of Southern California in the USA. ISACA has undertaken the development of the Systemic Security Management Model. The BMIS takes a business-oriented approach to managing information security, building on the foundational concepts developed by the Institute. The model utilizes systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The BMIS provides the context for frameworks such as Cubit.

The essence of systems theory is that a system needs to be viewed holistically—not merely as a sum of its parts—to be accurately understood. A holistic approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system. “Systems thinking” is a widely recognized term that refers to the examination of how systems interact, how complex systems work and why “the whole is more than the sum of its parts.” Systems theory is most accurately described as a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unseen and unexpected ways. Studying the behaviors and results of the interactions can assist the manager to better understand the organizational system and the way it functions. While management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections.
All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

1. Organization Design and Strategy—An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.
An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important in determining the design.

2. People—The human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:
Recruitment strategies (access, background checks, interviews, roles and responsibilities)
Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)
Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. Process—Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections.
Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.
To be advantageous to the enterprise, processes must:
Meet business requirements and align with policy
Consider emergence and be adaptable to changing requirements
Be well documented and communicated to appropriate human resources
Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology—Composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.
Technology is often seen by the enterprise's management team as a way to resolve security threats and risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed as an information security solution.
Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology; some have not learned to use it; and others feel it slows them down. Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections
The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

1. Governing—Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.
2. Culture—Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted

and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3. Enabling and support—The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.
4. Emergence—Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.
5. Human factors—The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection. Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.
6. Architecture—A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

The following answers are incorrect:

Governing - Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Emergence - Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is

a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 37 and 38
http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

QUESTION 40
Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management?

A. Governing
B. Culture
C. Enabling and support
D. Emergence

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

Explanation/Reference: Explanation:

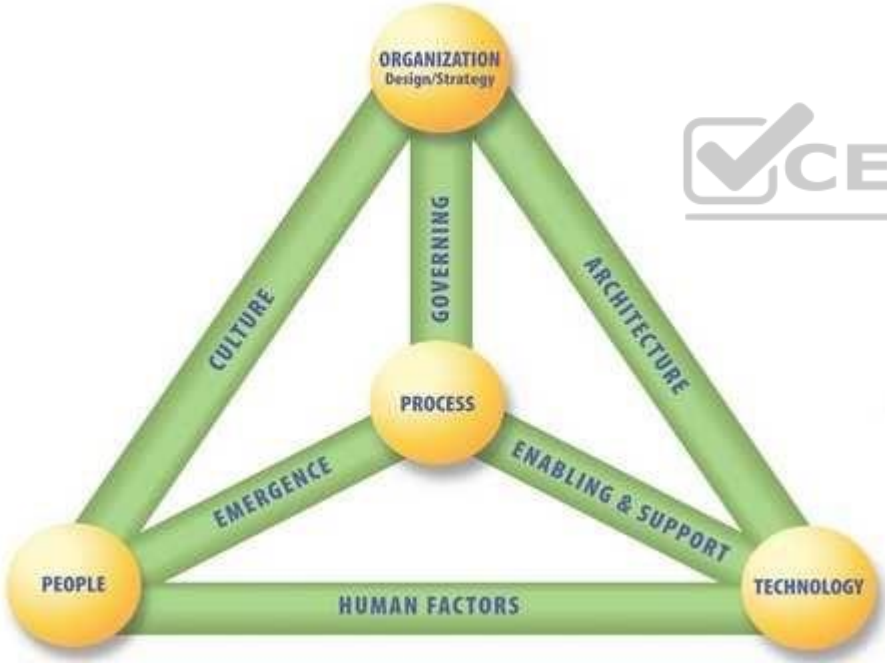
Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

For your exam you should know the information below.

Business Model for Information Security
The Business Model for Information Security (BMIS) originated at the Institute for Critical Information Infrastructure Protection at the Marshall School of Business at the University of Southern California in the USA. ISACA has undertaken the development of the Systemic Security Management Model. The BMIS takes a business-oriented approach to managing information security, building on the foundational concepts developed by the Institute. The model utilizes systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The BMIS provides the context for frameworks such as Cubit.

The essence of systems theory is that a system needs to be viewed holistically—not merely as a sum of its parts—to be accurately understood. A holistic approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system. “Systems thinking” is a widely recognized term that refers to the examination of how systems interact, how complex systems work and why “the whole is more than the sum of its parts.” Systems theory is most accurately described as a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unseen and unexpected ways. Studying the behaviors and results of the interactions can assist the manager to better understand the organizational system and the way it functions. While management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections.

All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

1. Organization Design and Strategy—An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.
An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important in determining the design.

2. People—The human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:
Recruitment strategies (access, background checks, interviews, roles and responsibilities)
Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)
Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. Process—Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections.
Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.
To be advantageous to the enterprise, processes must:
Meet business requirements and align with policy
Consider emergence and be adaptable to changing requirements
Be well documented and communicated to appropriate human resources
Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology—Composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.
Technology is often seen by the enterprise's management team as a way to resolve security threats and risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed as an information security solution.
Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology; some have not learned to use it; and others feel it slows them down. Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

1. Governing—Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.
2. Culture—Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3. Enabling and support—The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. Emergence—Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

5. Human factors—The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection. Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.

6. Architecture—A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

The following answers are incorrect:
Governing - Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Culture - Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

The following reference(s) were/was used to create this question: CISA review manual 2014 page number 37 and 38
http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

QUESTION 41
A maturity model can be used to aid the implementation of IT governance by identifying:

A. critical success factors
B. performance drivers
C. improvement opportunities
D. accountabilities

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

Explanation/Reference:

QUESTION 42
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 43
Which of the following is the **MOST** important requirement for the successful implementation of security governance?

A. Aligning to an international security framework
B. Mapping to organizational strategies
C. Implementing a security balanced scorecard
D. Performing an enterprise-wide risk assessment

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

Explanation/Reference:

QUESTION 44
Which of the following is the **PRIMARY** advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

A. An emerging technologies strategy would be in place
B. A cost-benefit analysis process would be easier to perform
C. An effective security risk management process is established
D. End-user acceptance of emerging technologies has been established

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

Explanation/Reference:

QUESTION 45
From a risk management perspective, which of the following is **MOST** important to be tracked in continuous monitoring?

A. Number of prevented attacks
B. Changes in the threat environment
C. Changes in user privileges
D. Number of failed logins

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

Explanation/Reference:

QUESTION 46
Which of the following should be the **PRIMARY** objective of an information security governance framework?

A. Increase the organization's return on security investment.
B. Provide a baseline for optimizing the security profile of the organization.
C. Ensure that users comply with the organization's information security policies.
D. Demonstrate compliance with industry best practices to external stakeholders.

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

Explanation/Reference:

QUESTION 47

An organization has developed mature risk management practices that are followed across all departments. What is the **MOST** effective way for the audit team to leverage this risk management maturity?

A. Facilitating audit risk identification and evaluation workshops
B. Implementing risk responses on management's behalf
C. Providing assurances to management regarding risk
D. Integrating the risk register for audit planning purposes

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

Explanation/Reference:

QUESTION 48
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 49
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 50
A vulnerability in which of the following virtual systems would be of **GREATEST** concern to the IS auditor?
A. The virtual machine management server
B. The virtual file server
C. The virtual application server
D. The virtual antivirus server

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

Explanation/Reference:

QUESTION 51
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 52
Which of the following is the **MOST** important role of the information security manager when the organization is in the process of adopting emerging technologies?

A. Understanding the impact on existing resources
B. Assessing how peer organizations using the same technologies have been impacted
C. Developing training for end users to familiarize them with the new technology
D. Reviewing vendor documentation and service levels agreements

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

QUESTION 53
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 54
Which of the following is the **MOST** important element when developing an information security strategy?

A. Identifying applicable laws and regulations
B. Identifying information assets
C. Determining the risk management methodology
D. Aligning security activities with organizational goals

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

Explanation/Reference:

QUESTION 55
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 56
When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be **MAINLY** driven by:

A. cost-benefit analysis
B. regulatory requirements
C. best practices
D. control framework

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

Explanation/Reference:

QUESTION 57
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 58
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus **PRIMARILY** on defining:

A. security requirements for the process being outsourced
B. security metrics
C. service level agreements (SLAs)
D. risk-reporting methodologies

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

Explanation/Reference:

QUESTION 59
The **MOST** useful technique for maintaining management support for the information security program is:

A. identifying the risks and consequences of failure to comply with standards
B. benchmarking the security programs of comparable organizations
C. implementing a comprehensive security awareness and training program
D. informing management about the security of business operations

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

Explanation/Reference:

QUESTION 60
An organization developed a comprehensive three-year IT strategic plan. Halfway into the plan, a major legislative change impacting the organization is enacted. Which of the following should be management's **NEXT** course of action?

A. Develop specific procedural documentation related to the changed legislation.
B. Assess the legislation to determine whether are required to the strategic IT plan.
C. Perform a risk management of the legislative changes.
D. Develop a new IT strategic plan that encompasses the new legislation.

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

Explanation/Reference:

QUESTION 61
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 62
Which of the following is the **MOST** important advantage of participating in beta testing of software products?

A. It improves vendor support and training.
B. It enables an organization to gain familiarity with new products and their functionality.
C. It increases an organization's ability to retain staff who prefer to work with new technology.
D. It enhances security and confidentiality.

Correct Answer: B

Section: Governance and Management of IT Explanation

Explanation/Reference:

QUESTION 63

The maturity level of an organization's problem management support function is optimized when the function:

A. proactively provides solutions
B. has formally documented the escalation process
C. analyzes critical incidents to identify root cause
D. resolves requests in a timely manner

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

Explanation/Reference:

QUESTION 64

To preserve chain-of-custody following an internal server compromise, which of the following should be the **FIRST** step?

A. Take a system image including memory dump
B. Safely shut down the server
C. Replicate the attack using the remaining evidence
D. Trace the attacking route

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

Explanation/Reference:

QUESTION 65

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 66
An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes. Which of the following recommendations would **BEST** help to reduce the risk of data leakage?

A. Requiring policy acknowledgment and nondisclosure agreements signed by employees
B. Providing education and guidelines to employees on use of social networking sites
C. Establishing strong access controls on confidential data
D. Monitoring employees' social networking usage

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

Explanation/Reference:

QUESTION 67
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 68
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 69
An organization which uses external cloud services extensively is concerned with risk monitoring and timely response. The **BEST** way to address this concern is to ensure:

A. the availability of continuous technical support
B. internal security standards are in place
C. a right-to-audit clause is included in contracts
D. appropriate service level agreements (SLAs) are in place

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

Explanation/Reference:

QUESTION 70
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 71
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 72
When an information security manager presents an information security program status report to senior management, the **MAIN** focus should be:

A. key performance indicators (KPIs)
B. critical risks indicators
C. net present value (NPV)
D. key controls evaluation

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

Explanation/Reference:
QUESTION 73
An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager's **FIRST** step to support this strategy?

A. Develop a business case for a data loss prevention solution
B. Develop a guideline on the acceptable use of social media
C. Incorporate social media into the security awareness program
D. Employ the use of a web content filtering solution

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

Explanation/Reference:

QUESTION 74
The information in the knowledge base can be expressed in several ways. Which of the following way uses questionnaires to lead the user through a series of choices until a conclusion is reached?

A. Decision tree
B. Rules
C. Semantic nets
D. Knowledge interface

Correct Answer: A
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
Decision tree uses 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.

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:

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.
Knowledge interface - Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 187

QUESTION 75
An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model depict data entities and how they relate?

A. Context Diagrams

B. Activity Diagrams
C. Swim-lane diagrams
D. Entity relationship diagrams

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
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.

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:

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.

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.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 188

QUESTION 76
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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 77
Which of the following layer of an enterprise data flow architecture is concerned with basic data communication?

A. Data preparation layer
B. Desktop Access Layer
C. Internet/Intranet layer
D. Data access layer

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 78
Which of the following layer of an enterprise data flow architecture is concerned with transporting information between the various layers?

A. Data preparation layer
B. Desktop Access Layer
C. Application messaging layer
D. Data access layer

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
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.
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 79

Which of the following layer of an enterprise data flow architecture does the scheduling of the tasks necessary to build and maintain the Data Warehouse (DW) and also populates Data Marts?

A. Data preparation layer
B. Desktop Access Layer
C. Warehouse management layer
D. Data access layer

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:

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.
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 80
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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 81

Which of the following layer of an enterprise data flow architecture is concerned with the assembly and preparation of data for loading into data marts?

A. Data preparation 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:

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. 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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 82
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:

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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 83
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:
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.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 188

QUESTION 84
Which of the following layer from an enterprise data flow architecture captures all data of interest to an organization and organize it to assist in reporting and analysis?

A. Desktop access layer
B. Data preparation layer
C. Core data warehouse
D. Data access layer

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
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. 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.
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 85
Which of the following layer in an enterprise data flow architecture derives enterprise information from operational data, external data and nonoperational data?

A. Data preparation layer
B. Data source layer
C. Data mart layer

D. Data access layer

Correct Answer: B
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
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.

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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 86
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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 87
Which of the following property of the core date warehouse layer of an enterprise data flow architecture uses common attributes to access a cross section of an information in the warehouse?

A. Drill up
B. Drill down
C. Drill across
D. Historical Analysis

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
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.

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:

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.

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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 88
Which of the following level in CMMI model focuses on process innovation and continuous optimization?

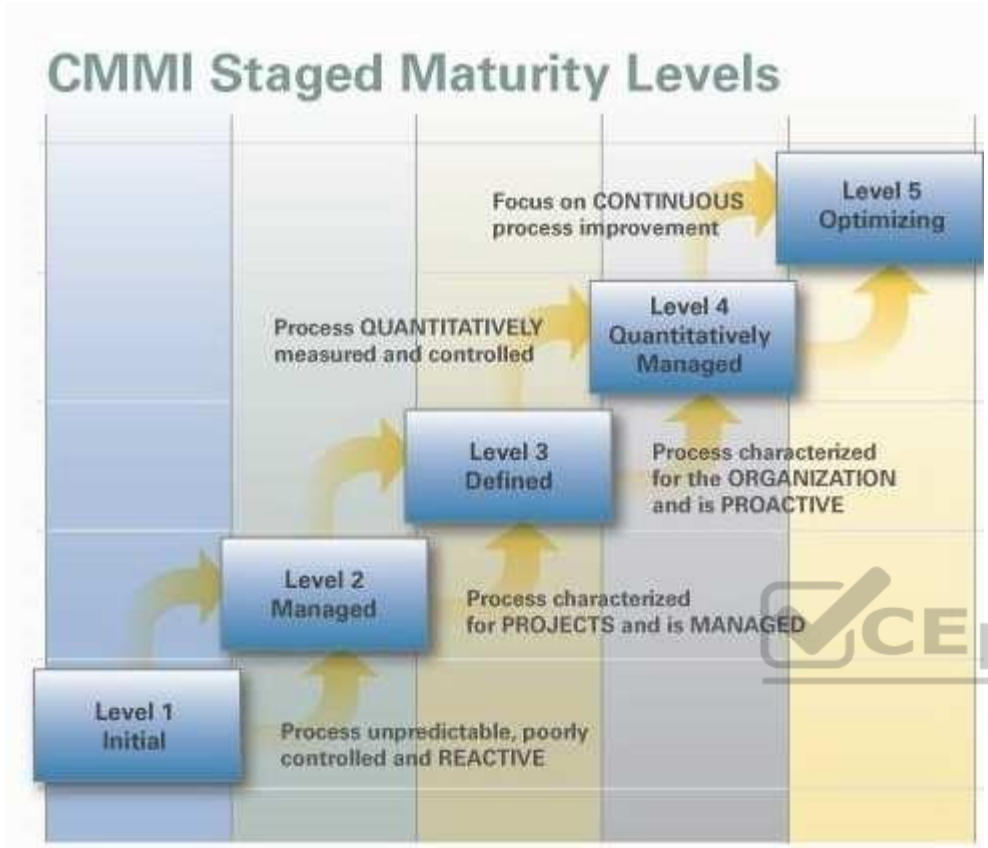
A. Level 4
B. Level 5
C. Level 3
D. Level 2

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Level 5 is the optimizing process and focus on process innovation and continuous integration.
For CISA Exam you should know below information about Capability Maturity Model Integration (CMMI) mode:

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.

CMMI Levels



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".[citation needed]

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 were incorrect answers:

Level 4 – Focus on process management and process control
Level 3 – Process definition and process deployment.
Level 2 – Performance management and work product management.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 89
Which of the following level in CMMI model focuses on process definition and process deployment?

A. Level 4
B. Level 5
C. Level 3
D. Level 2

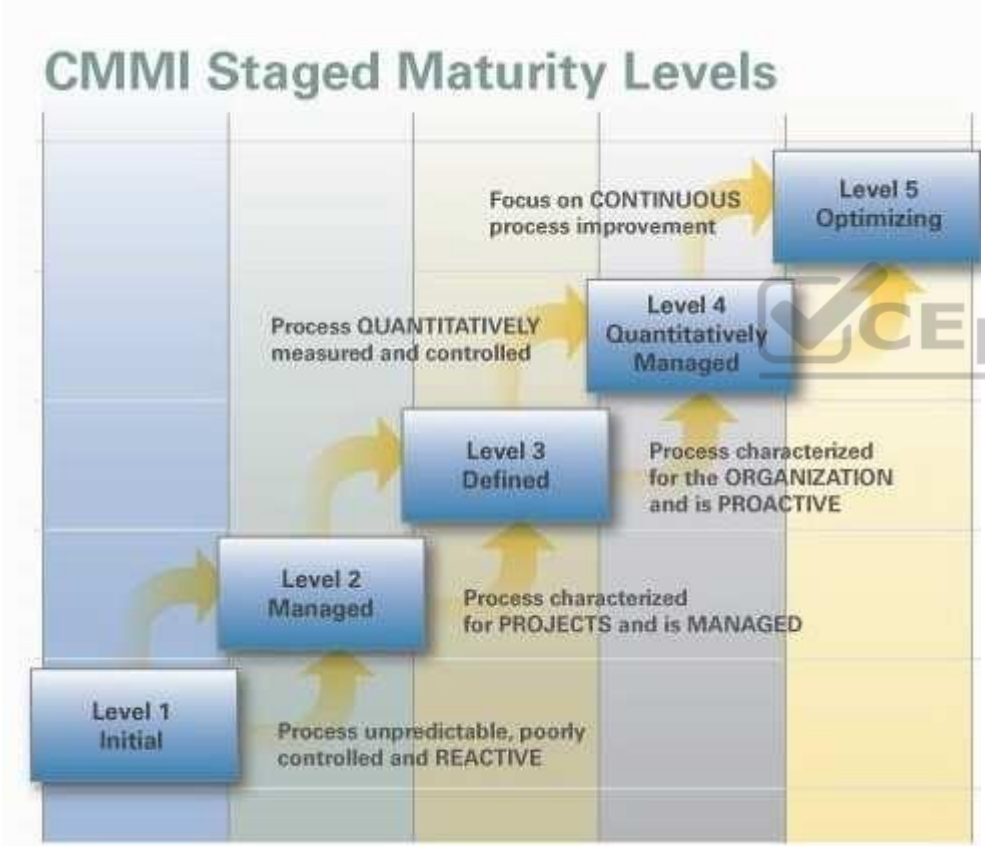
Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation
Explanation/Reference:

Level 3 is the defined step and focus on process definition and process deployment.

For CISA Exam you should know below information about Capability Maturity Model Integration (CMMI) mode:

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.

CMMI Levels



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".[citation needed]

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 were incorrect answers:

Level 4 – Focus on process management and process control
Level 5 – Process innovation and continuous optimization.
Level 2 – Performance management and work product management.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 90

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

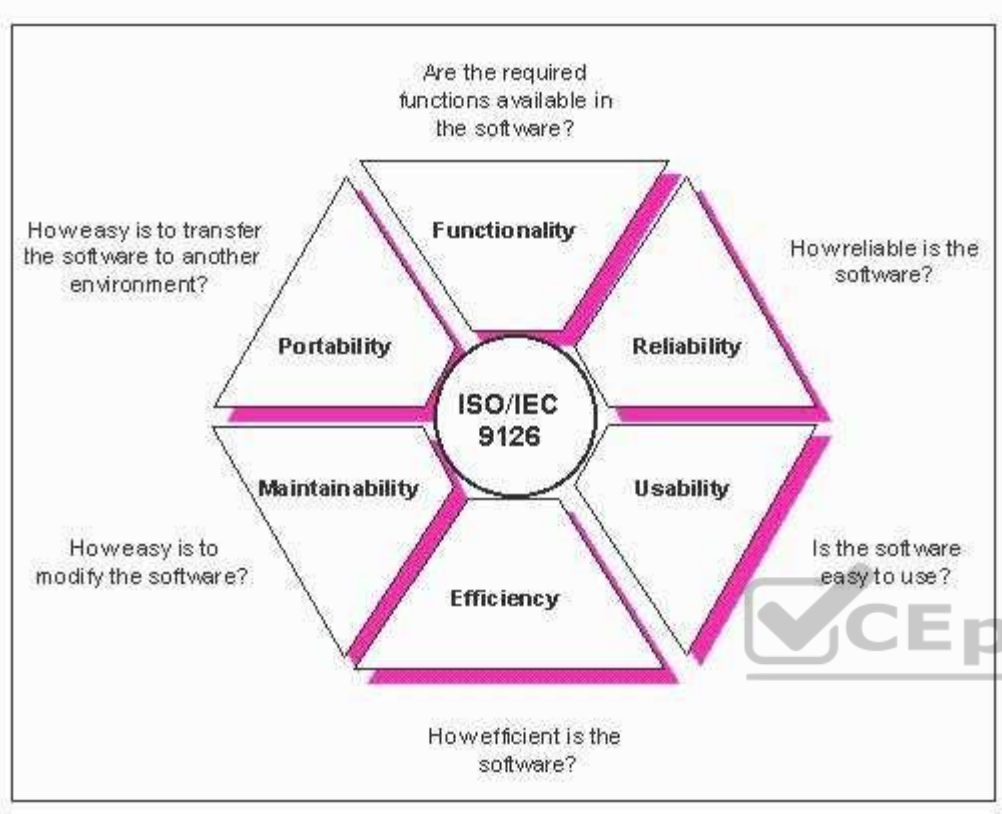
Explanation/Reference:
Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties.

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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 91
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:
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.
The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 218

QUESTION 92
Which of the following ACID property in DBMS requires that each transaction is "all or nothing"?

A. Atomicity
B. Consistency
C. Isolation
D. Durability

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
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.

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:

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.

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 218

QUESTION 93
Which of the following ACID property in DBMS means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors?

A. Atomicity
B. Consistency
C. Isolation
D. Durability

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

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:

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.

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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 218

QUESTION 94
Which of the following ACID property in DBMS 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?

A. Atomicity
B. Consistency

C. Isolation
D. Durability

Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
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.

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:

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.

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 218

QUESTION 95
Which of the following software development methods is based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams?

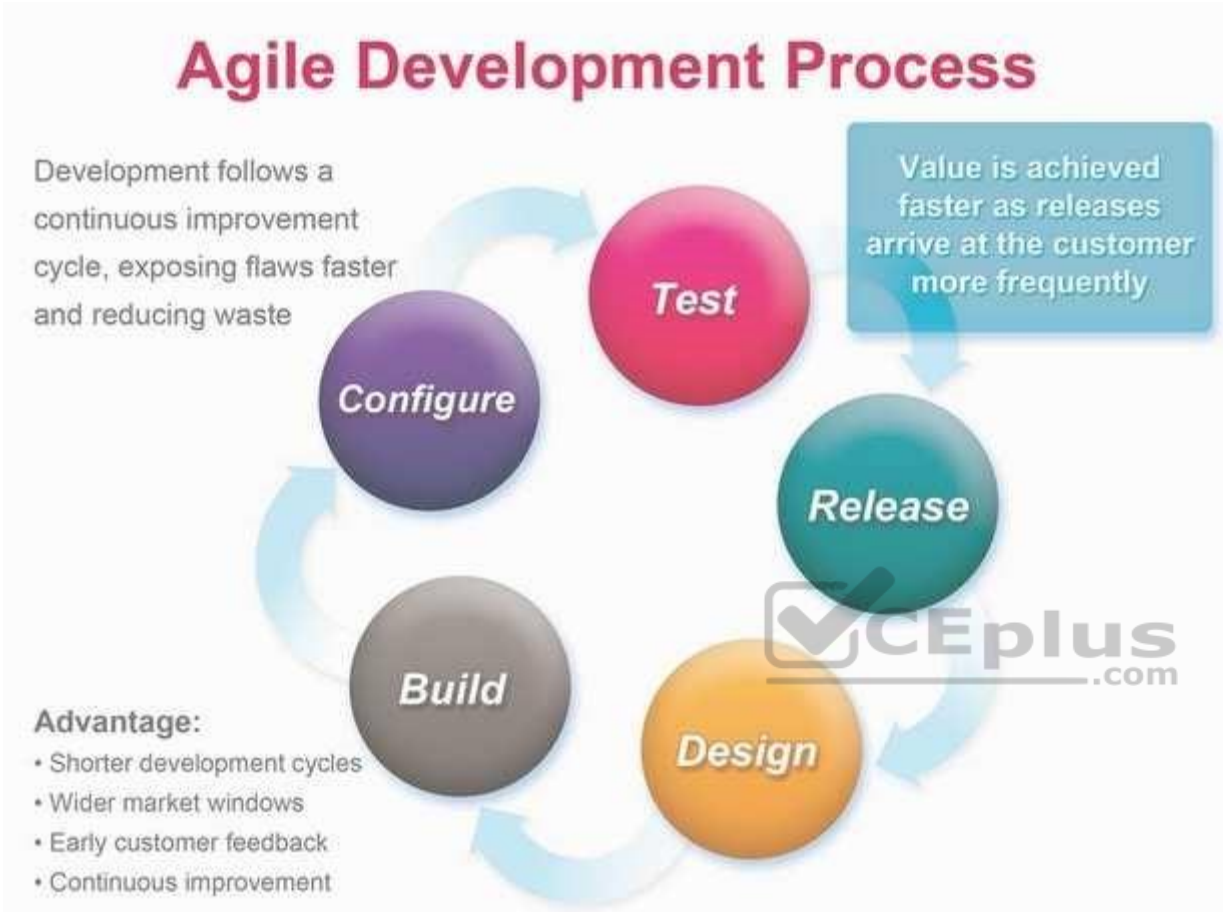
A. Agile Development
B. Software prototyping
C. Rapid application development
D. Component based development

Correct Answer: A
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
For your exam you should know below information about agile development:

Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen tight iterations throughout the development cycle.

Agile Development



The Agile Manifesto introduced the term in 2001. Since then, the Agile Movement, with all its values, principles, methods, practices, tools, champions and practitioners, philosophies and cultures, has significantly changed the landscape of the modern software engineering and commercial software development in the Internet era.

Agile principles

The Agile Manifesto is based on twelve principles:

Customer satisfaction by rapid delivery of useful software
Welcome changing requirements, even late in development
Working software is delivered frequently (weeks rather than months)
Close, daily cooperation between business people and developers
Projects are built around motivated individuals, who should be trusted
Face-to-face conversation is the best form of communication (co-location)
Working software is the principal measure of progress
Sustainable development, able to maintain a constant pace
Continuous attention to technical excellence and good design
Simplicity—the art of maximizing the amount of work not done—is essential
Self-organizing teams
Regular adaptation to changing circumstances

What is Scrum?
Scrum is the most popular way of introducing Agility due to its simplicity and flexibility. Because of this popularity, many organizations claim to be “doing Scrum” but aren’t doing anything close to Scrum’s actual definition. Scrum emphasizes empirical feedback, team self-management, and striving to build properly tested product increments within short iterations. Doing Scrum as it’s actually defined usually comes into conflict with existing habits at established non-Agile organizations.

The following were incorrect answers:

Software prototyping- Software prototyping, refers to the activity of creating prototypes of software applications, i.e., incomplete versions of the software program being developed. It is an activity that can occur in software development and is comparable to prototyping as known from other fields, such as mechanical engineering or manufacturing.

Rapid application development (RAD) is a software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive per-planning generally allows software to be written much faster, and makes it easier to change requirements.

Component Based Development - It is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems. This practice aims to bring about an equally wide-ranging degree of benefits in both the short-term and the long-term for the software itself and for organizations that sponsor such software.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 194

QUESTION 96
Which of the following software development methodology is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems?

A. Agile Developments
B. Software prototyping
C. Rapid application development
D. Component based development

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Component-based software engineering (CBSE) (also known as component-based development (CBD)) is a branch of software engineering that emphasizes the separation of concerns in respect of the wide-ranging functionality available throughout a given software system. It is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems. This practice aims to bring about an equally wide-ranging degree of benefits in both the short-term and the long-term for the software itself and for organizations that sponsor such software.

Software engineers[who?] regard components as part of the starting platform for service-orientation. Components play this role, for example, in web services, and more recently, in service-oriented architectures (SOA), whereby a component is converted by the web service into a service and subsequently inherits further characteristics beyond that of an ordinary component.

Components can produce or consume events and can be used for event-driven architectures (EDA).

Definition and characteristics of components

An individual software component is a software package, a web service, a web resource, or a module that encapsulates a set of related functions (or data).

All system processes are placed into separate components so that all of the data and functions inside each component are semantically related (just as with the contents of classes). Because of this principle, it is often said that components are modular and cohesive.

With regard to system-wide co-ordination, components communicate with each other via interfaces. When a component offers services to the rest of the system, it adopts a provided interface that specifies the services that other components can utilize, and how they can do so. This interface can be seen as a signature of the component - the client does not need to know about the inner workings of the component (implementation) in order to make use of it. This principle results in components referred to as encapsulated. The UML illustrations within this article represent provided interfaces by a lollipop-symbol attached to the outer edge of the component.

However, when a component needs to use another component in order to function, it adopts a used interface that specifies the services that it needs. In the UML illustrations in this article, used interfaces are represented by an open socket symbol attached to the outer edge of the component. A simple example of several software components - pictured within a hypothetical holiday-reservation system represented in UML 2.0.

Another important attribute of components is that they are substitutable, so that a component can replace another (at design time or run-time), if the successor component meets the requirements of the initial component (expressed via the interfaces). Consequently, components can be replaced with either an updated version or an alternative without breaking the system in which the component operates.

As a general rule of thumb for engineers substituting components, component B can immediately replace component A, if component B provides at least what component A provided and uses no more than what component A used.

Software components often take the form of objects (not classes) or collections of objects (from object-oriented programming), in some binary or textual form, adhering to some interface description language (IDL) so that the component may exist autonomously from other components in a computer.

When a component is to be accessed or shared across execution contexts or network links, techniques such as serialization or marshalling are often employed to deliver the component to its destination.

Reusability is an important characteristic of a high-quality software component. Programmers should design and implement software components in such a way that many different programs can reuse them. Furthermore, component-based usability testing should be considered when software components directly interact with users.

It takes significant effort and awareness to write a software component that is effectively reusable. The component needs to be:

fully documented thoroughly
tested
robust - with comprehensive input-validity checking able to pass
back appropriate error messages or return codes designed with an
awareness that it will be put to unforeseen uses The following were
incorrect answers:

Agile Development - Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

Software prototyping- Software prototyping, refers to the activity of creating prototypes of software applications, i.e., incomplete versions of the software program being developed. It is an activity that can occur in software development and is comparable to prototyping as known from other fields, such as mechanical engineering or manufacturing.

Rapid application development (RAD) is a software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive per-planning generally allows software to be written much faster, and makes it easier to change requirements.

The following reference(s) were/was used to create this question:

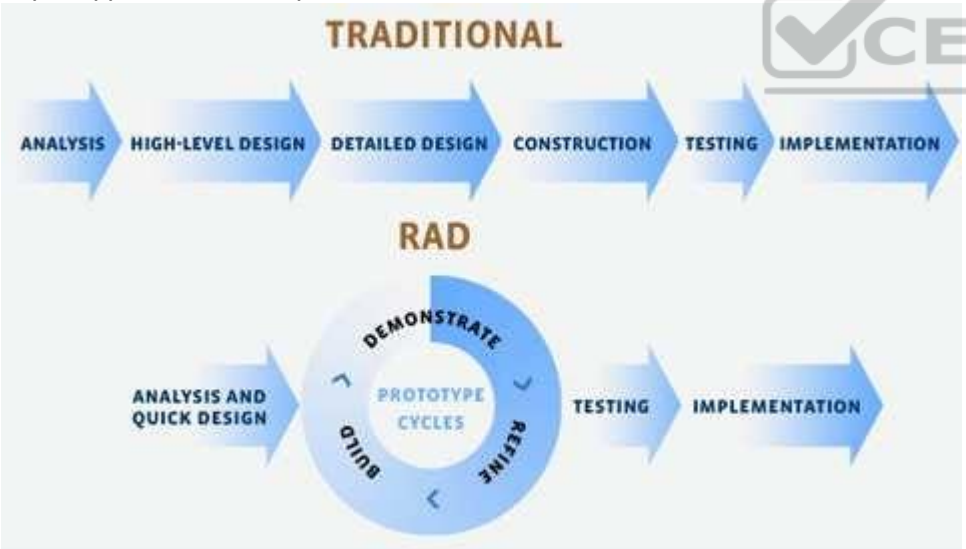
CISA review manual 2014 Page number 194

QUESTION 97
Which of the following software development methodology uses minimal planning and in favor of rapid prototyping?

A. Agile Developments
B. Software prototyping
C. Rapid application development
D. Component based development

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
Rapid application development (RAD) is a software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive per-planning generally allows software to be written much faster, and makes it easier to change requirements.
Rapid Application Development



Four phases of RAD

Requirements Planning phase – combines elements of the system planning and systems analysis phases of the Systems Development Life Cycle (SDLC). Users, managers, and IT staff members discuss and agree on business needs, project scope, constraints, and system requirements. It ends when the team agrees on the key issues and obtains management authorization to continue.

User design phase – during this phase, users interact with systems analysts and develop models and prototypes that represent all system processes, inputs, and outputs. The RAD groups or subgroups typically use a combination of Joint Application Development (JAD) techniques and CASE tools to translate user needs into working models. User Design is a continuous interactive process that allows users to understand, modify, and eventually approve a working model of the system that meets their needs.

Construction phase – focuses on program and application development task similar to the SDLC. In RAD, however, users continue to participate and can still suggest changes or improvements as actual screens or reports are developed. Its tasks are programming and application development, coding, unit-integration and system testing.

Cutover phase – resembles the final tasks in the SDLC implementation phase, including data conversion, testing, changeover to the new system, and user training. Compared with traditional methods, the entire process is compressed. As a result, the new system is built, delivered, and placed in operation much sooner.

The following were incorrect answers:

Agile Development - Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

Software prototyping- Software prototyping, refers to the activity of creating prototypes of software applications, i.e., incomplete versions of the software program being developed. It is an activity that can occur in software development and is comparable to prototyping as known from other fields, such as mechanical engineering or manufacturing.

Component Based Development - It is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems. This practice aims to bring about an equally wide-ranging degree of benefits in both the short-term and the long-term for the software itself and for organizations that sponsor such software.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 195

QUESTION 98

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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 154

QUESTION 99
Which of the following is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources?

A. Functional Point analysis
B. Gantt Chart
C. Critical path methodology
D. Time box management

Correct Answer: D
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Time box management is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources. There is a need to balance software quality and meet the delivery requirements within the time box or timeframe. The project manager has some degree of flexibility and uses discretion is scoping the requirement. Timebox management can be used to accomplish prototyping or RAPID application development type in which key feature are to be delivered in a short period of time.

The following were incorrect answers:

Critical path Method -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.

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 following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 154

QUESTION 100
Who is mainly responsible for protecting information assets they have been entrusted with on a daily basis by defining who can access the data, it's sensitivity level, type of access, and adhering to corporate information security policies?

A. Data Owner
B. Security Officer
C. Senior Management
D. End User

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
The Data Owner is the person who has been entrusted with a data set that belong to the company. As such they are responsible to classify the data according to it's value and sensitivity. The Data Owner decides who will get access to the data, what type of access would be granted. The Data Owner will tell the Data Custodian or System Administrator what access to configure within the systems.

A business executive or manager is typically responsible for an information asset. These are the individuals that assign the appropriate classification to information assets. They ensure that the business information is protected with appropriate controls. Periodically, the information asset owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners or their delegates are responsible for understanding the risks that exist with regards to the information that they control.

The following answers are incorrect:

Executive Management/Senior Management - Executive management maintains the overall responsibility for protection of the information assets. The business operations are dependent upon information being available, accurate, and protected from individuals without a need to know.

Security Officer - The security officer directs, coordinates, plans, and organizes information security activities throughout the organization. The security officer works with many different individuals, such as executive management, management of the business units, technical staff, business partners, auditors, and third parties such as vendors. The security officer and his or her team are responsible for the design, implementation, management, and review of the organization's security policies, standards, procedures, baselines, and guidelines.

End User - The end user does not decide on classification of the data

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 108
Official ISC2 guide to CISSP CBK 3rd Edition Page number 342

QUESTION 101
Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of it's internals?

A. Black-box testing
B. Parallel Test
C. Regression Testing
D. Pilot Testing

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings (see white-box testing). This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

For your exam you should know the information below:

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 answers are incorrect:

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

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.

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

The following reference(s) were/was used to create this question: CISA
review manual 2014 Page number 167
Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

QUESTION 102
Which of the following testing method examines internal structure or working of an application?

A. White-box testing
B. Parallel Test
C. Regression Testing
D. Pilot Testing

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT).

White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system–level test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. For your exam you should know the information below:

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 answers are incorrect:

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

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.

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

The following reference(s) were/was used to create this question: CISA
review manual 2014 Page number 167
Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

QUESTION 103
Identify the correct sequence of Business Process Reengineering (BPR) benchmarking process from the given choices below?

A. PLAN, RESEARCH, OBSERVE, ANALYZE, ADOPT and IMPROVE
B. OBSERVE, PLAN, RESEACH, ANALYZE, ADOPT and IMPROVE
C. PLAN, OBSERVE, RESEARCH, ANALYZE, ADOPT and IMPROVE
D. PLAN, RESEARCH, ANALYZE, OBSERVE, ADOPT and IMPROVE

Correct Answer: A
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
The correct sequence of BRP benchmarking is PLAN, RESEARCH, OBSERVE, ANALYZE, ADOPT and IMPROVE.

For your exam you should know the information below:

Overview of Business Process Reengineering
One of the principles in business that remains constant is the need to improve your processes and procedures. Most trade magazines today contain discussions of the detailed planning necessary for implementing change in an organization. The concept of change must be accepted as a fundamental principle. Terms such as business evolution and continuous improvement ricochet around the room in business meetings. It's a fact that organizations which fail to change are destined to perish.

As a CISA, you must be prepared to investigate whether process changes within the organization are accounted for with proper documentation. All internal control frameworks require that management be held responsible for safeguarding all the assets belonging to their organization. Management is also responsible for increasing revenue.

BPR Application Steps
ISACA cites six basic steps in their general approach to BPR. These six steps are simply an extension of Stewart's Plan-Do-Check-Act model for managing projects:
Envision -Visualize a need (envision). Develop an estimate of the ROI created by the proposed change. Elaborate on the benefit with a preliminary project plan to gain sponsorship from the organization. The plan should define the areas to be reviewed and clarify the desired result at the end of the project (aka end state objective). The deliverables of the envision phase include the following:
Project champion working with the steering committee to gain top management approval
Brief description of project scope, goals, and objectives description of the specific deliverables from this project with a preliminary charter to evidence management's approval, the project may proceed into the initiation phase.

Initiate -This phase involves setting BPR goals with the sponsor. Focus on planning the collection of detailed evidence necessary to build the subsequent BPR plan for redesigning the process. Deliverables in the initiation phase include the following: Identifying internal and external requirements (project specifications)
Business case explaining why this project makes sense (justification) and the estimated return on investment compared to the total cost (net ROI)
Formal project plan with budget, schedule, staffing plan, procurement plan, deliverables, and project risk analysis
Level of authority the BPR project manager will hold and the composition of any support committee or task force that will be required
From the profit and loss (P&L) statement, identify the item line number that money will be debited from to pay for this project and identify the specific P&L line number that the financial return will later appear under (to provide strict monitoring of the ROI performance)
Formal project charter signed by the sponsors It's important to realize that some BPR projects will proceed to their planned conclusion and others may be halted because of insufficient evidence. After a plan is formally approved, the BPR project may proceed to the diagnostic phase.

Diagnose Document existing processes. Now it's time to see what is working and identify the source of each requirement. Each process step is reviewed to calculate the value it creates. The goal of the diagnostic phase is to gain a better understanding of existing processes. The data collected in the diagnostic phase forms the basis of all planning decisions: Detailed documentation of the existing process
Performance measurement of individual steps in the process
Evidence of specific process steps that add customer value

Identification of process steps that don't add value
Definition of attributes that create value and quality
Put in the extra effort to do a good job of collecting and analyzing the evidence. All future assumptions will be based on evidence from the diagnostic phase.

Redesign- Using the evidence from the diagnostic phase, it's time to develop the new process.
This will take several planning iterations to ensure that the strategic objectives are met. The formal redesign plans will be reviewed by sponsors and stakeholders. A final plan will be presented to the steering committee for approval. Here's an example of deliverables from the redesign phase. Comparison of the envisioned objective to actual specifications
Analysis of alternatives (AoA)
Prototyping and testing of the redesigned process
Formal documentation of the final design
The project will need formal approval to proceed into the reconstruction phase. Otherwise, the redesign is halted pending further scrutiny while comparing the proposed design with available evidence. Insufficient evidence warrants halting the project.

Reconstruct With formal approval received, it's time to begin the implementation phase.
The current processes are deconstructed and reassembled according to the plan. Reconstruction may be in the form of a parallel process, modular changes, or complete transition. Each method presents a unique risk and reward opportunity. Deliverables from this phase include the following: Conversion plan with dependencies in time sequence
Change control management
Execution of conversion plan with progress monitoring
Training of users and support personnel
Pilot implementation to ensure a smooth migration Formal approval by the sponsor.
The reconstructed process must be formally approved by management to witness their consent for fitness of use. IT governance dictates that executive management shall be held responsible for any failures and receive recognition for exceptional results. System performance will be evaluated again after entering production use.

Evaluate (post evaluation) The reconstructed process is monitored to ensure that it works and is producing the strategic value as forecast in the original justification.
Comparison of original forecast to actual performance Identification of lessons learned
Total quality management plan to maintain the new process
A method of continuous improvement is implemented to track the original goals against actual process performance. Annual reevaluation is needed to adapt new requirements or new opportunities.

Benchmarking as a BPR Tool
Benchmarking is the process of comparing performance data (aka metrics). It can be used to evaluate business processes that are under consideration for reengineering. Performance data may be obtained by using a self-assessment or by auditing for compliance against a standard (reference standard). Evidence captured during the diagnostic phase is considered the key to identifying areas for performance improvement and documenting obstacles. ISACA offers the following general guidelines for performing benchmarks:

Plan Identify the critical processes and create measurement techniques to grade the processes.
Research Use information about the process and collect regular data (samples) to build a baseline for comparison. Consider input from your customers and use analogous data from other industries.
Observe Gather internal data and external data from a benchmark partner to aid the comparison results. Benchmark data can also be compared against published standards.
Analyze Look for root cause-effect relationships and other dependencies in the process. Use predefined tools and procedures to collate the data collected from all available sources.
Adapt Translate the findings into hypotheses of how these findings will help or hurt strategic business goals. Design a pilot test to prove or disprove the hypotheses. Improve Implement a prototype of the new processes. Study the impact and note any unexpected results. Revise the process by using controlled change management. Measure the process results again. Use reestablished procedures such as total quality management for continuous improvement.

The following answers are incorrect:

The other options specified does not represent the correct sequence of BRP benchmarking steps.
The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 219 to 211
CISA certified information system auditor study guide Second Edition Page Number 154 to 158

QUESTION 104
Identify the correct sequence of Business Process Reengineering (BPR) application steps from the given choices below?

A. Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate
B. Initiate, Envision, Diagnose, Redesign, Reconstruct and Evaluate
C. Envision, Diagnose, Initiate, Redesign, Reconstruct and Evaluate
D. Evaluate, Envision, Initiate, Diagnose, Redesign, Reconstruct

Correct Answer: A
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:
The correct sequence of BRP application step is Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate.

For your exam you should know the information below:

Overview of Business Process Reengineering
One of the principles in business that remains constant is the need to improve your processes and procedures. Most trade magazines today contain discussions of the detailed planning necessary for implementing change in an organization. The concept of change must be accepted as a fundamental principle. Terms such as

business evolution and continuous improvement ricochet around the room in business meetings. It's a fact that organizations which fail to change are destined to perish.

As a CISA, you must be prepared to investigate whether process changes within the organization are accounted for with proper documentation. All internal control frameworks require that management be held responsible for safeguarding all the assets belonging to their organization. Management is also responsible for increasing revenue.

BPR Application Steps
ISACA cites six basic steps in their general approach to BPR. These six steps are simply an extension of Stewart's Plan-Do-Check-Act model for managing projects:
Envision -Visualize a need (envision). Develop an estimate of the ROI created by the proposed change. Elaborate on the benefit with a preliminary project plan to gain sponsorship from the organization. The plan should define the areas to be reviewed and clarify the desired result at the end of the project (aka end state objective). The deliverables of the envision phase include the following:
Project champion working with the steering committee to gain top management approval
Brief description of project scope, goals, and objectives description of the specific deliverables from this project with a preliminary charter to evidence management's approval, the project may proceed into the initiation phase.

Initiate -This phase involves setting BPR goals with the sponsor. Focus on planning the collection of detailed evidence necessary to build the subsequent BPR plan for redesigning the process. Deliverables in the initiation phase include the following:

Identifying internal and external requirements (project specifications)
Business case explaining why this project makes sense (justification) and the estimated return on investment compared to the total cost (net ROI)
Formal project plan with budget, schedule, staffing plan, procurement plan, deliverables, and project risk analysis
Level of authority the BPR project manager will hold and the composition of any support committee or task force that will be required
From the profit and loss (P&L) statement, identify the item line number that money will be debited from to pay for this project and identify the specific P&L line number that the financial return will later appear under (to provide strict monitoring of the ROI performance) Formal project charter signed by the sponsors

It's important to realize that some BPR projects will proceed to their planned conclusion and others may be halted because of insufficient evidence. After a plan is formally approved, the
BPR project may proceed to the diagnostic phase.

Diagnose Document existing processes. Now it's time to see what is working and identify the source of each requirement. Each process step is reviewed to calculate the value it creates. The goal of the diagnostic phase is to gain a better understanding of existing processes. The data collected in the diagnostic phase forms the basis of all planning decisions:

Detailed documentation of the existing process
Performance measurement of individual steps in the process
Evidence of specific process steps that add customer value
Identification of process steps that don't add value

Definition of attributes that create value and quality

Put in the extra effort to do a good job of collecting and analyzing the evidence. All future assumptions will be based on evidence from the diagnostic phase.

Redesign- Using the evidence from the diagnostic phase, it's time to develop the new process.
This will take several planning iterations to ensure that the strategic objectives are met. The formal redesign plans will be reviewed by sponsors and stakeholders.
A final plan will be presented to the steering committee for approval. Here's an example of deliverables from the redesign phase.

Comparison of the envisioned objective to actual specifications
Analysis of alternatives (AoA)
Prototyping and testing of the redesigned process
Formal documentation of the final design

The project will need formal approval to proceed into the reconstruction phase. Otherwise, the redesign is halted pending further scrutiny while comparing the proposed design with available evidence. Insufficient evidence warrants halting the project.

Reconstruct With formal approval received, it's time to begin the implementation phase.
The current processes are deconstructed and reassembled according to the plan. Reconstruction may be in the form of a parallel process, modular changes, or complete transition. Each method presents a unique risk and reward opportunity. Deliverables from this phase include the following:

Conversion plan with dependencies in time sequence
Change control management
Execution of conversion plan with progress monitoring
Training of users and support personnel
Pilot implementation to ensure a smooth migration Formal approval by the sponsor.

The reconstructed process must be formally approved by management to witness their consent for fitness of use. IT governance dictates that executive management shall be held responsible for any failures and receive recognition for exceptional results. System performance will be evaluated again after entering production use.

Evaluate (post evaluation) The reconstructed process is monitored to ensure that it works and is producing the strategic value as forecast in the original justification.
Comparison of original forecast to actual performance Identification of lessons learned
Total quality management plan to maintain the new process
A method of continuous improvement is implemented to track the original goals against actual process performance. Annual reevaluation is needed to adapt new requirements or new opportunities.

Benchmarking as a BPR Tool

Benchmarking is the process of comparing performance data (aka metrics). It can be used to evaluate business processes that are under consideration for reengineering. Performance data may be obtained by using a self-assessment or by auditing for compliance against a standard (reference standard). Evidence captured during the diagnostic phase is considered the key to identifying areas for performance improvement and documenting obstacles. ISACA offers the following general guidelines for performing benchmarks:

Plan Identify the critical processes and create measurement techniques to grade the processes.
Research Use information about the process and collect regular data (samples) to build a baseline for comparison. Consider input from your customers and use analogous data from other industries.
Observe Gather internal data and external data from a benchmark partner to aid the comparison results. Benchmark data can also be compared against published standards.
Analyze Look for root cause-effect relationships and other dependencies in the process. Use predefined tools and procedures to collate the data collected from all available sources.
Adapt Translate the findings into hypotheses of how these findings will help or hurt strategic business goals. Design a pilot test to prove or disprove the hypotheses. Improve Implement a prototype of the new processes. Study the impact and note any unexpected results. Revise the process by using controlled change management. Measure the process results again. Use reestablished procedures such as total quality management for continuous improvement.

The following answers are incorrect:

The other options specified does not represent the correct sequence of BRP application steps.
The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 219 to 211
CISA certified information system auditor study guide Second Edition Page Number 154 to 158

QUESTION 105
Following request for proposal (RFP) responses, a project seeking to acquire a new application system has identified a short list of vendors. At this point, the IS auditor should:

A. encourage contact with current users of the vendor's products
B. perform a detailed cost-benefit exercise on the proposed application
C. require that contract terms include a right-to-audit clause
D. recommend performing system integration tests

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 106
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 107
During the due diligence phase of an acquisition, the **MOST** important course of action for an information security manager would be to:

A. review the state of security awareness
B. perform a gap analysis
C. perform a risk assessment
D. review information security policies

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 108
When an organization and its IT-hosting service provider are establishing a contract with each other, it is **MOST** important that the contract includes:

A. each party's security responsibilities
B. details of expected security metrics
C. penalties for noncompliance with security policy
D. recovery time objectives (RTOs)

Correct Answer: A

Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 109
An organization is in the process of acquiring a competitor. The information security manager has been asked to report on the security posture of the target acquisition. Which of the following should be the security manager's **FIRST** course of action?

A. Implement a security dashboard
B. Quantity the potential risk
C. Perform a gap analysis
D. Perform a vulnerability assessment

Correct Answer: A
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 110
A review of an organization's IT portfolio revealed several applications that are not in use. The **BEST** way to prevent this situation from recurring would be to implement:

A. a formal request for proposal (RFP) process
B. an information asset acquisition policy
C. asset life cycle management
D. business development procedures

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 111
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 112
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 113
Which of the following **BEST** describes a common risk in implementing a new application software package?

A. Parameter settings are incorrect
B. Transaction volume is excessive
C. Sensitivity of transactions is high
D. The application lacks audit trails

Correct Answer: D
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 114

An organization is replacing a mission-critical system. Which of the following is the **BEST** implementation strategy to mitigate and reduce the risk of system failure?

A. Stage
B. Phase
C. Parallel
D. Big-bang

Correct Answer: C
Section: Information System Acquisition, Development and Implementation Explanation

Explanation/Reference:

QUESTION 115
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 116
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 117

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 118

An organization has implemented an automated match between purchase orders, good 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 119

Which of the following device in Frame Relay WAN technique is generally customer owned device that provides a connectivity between company's own network and the frame relays network?

A. DTE
B. DCE
C. DME
D. DLE

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
Data Terminal Equipment (DTE) - Usually a customer owned device that provides connectivity between company's own network and the frame relay's network.

For your exam you should know below information about WAN Technologies:

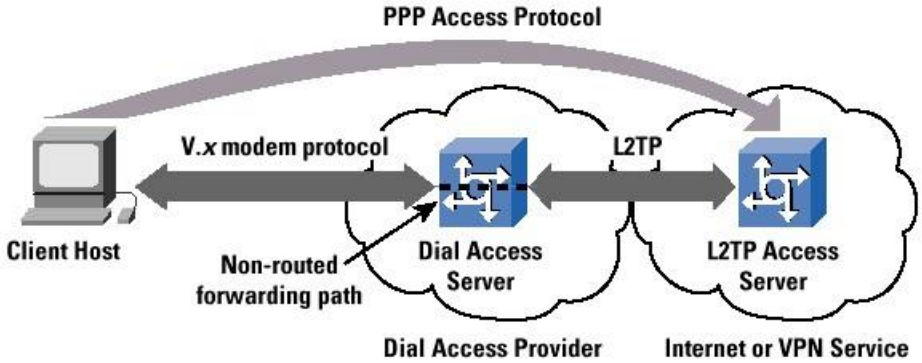
Point-to-point protocol
PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's 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 other protocol as well). 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.

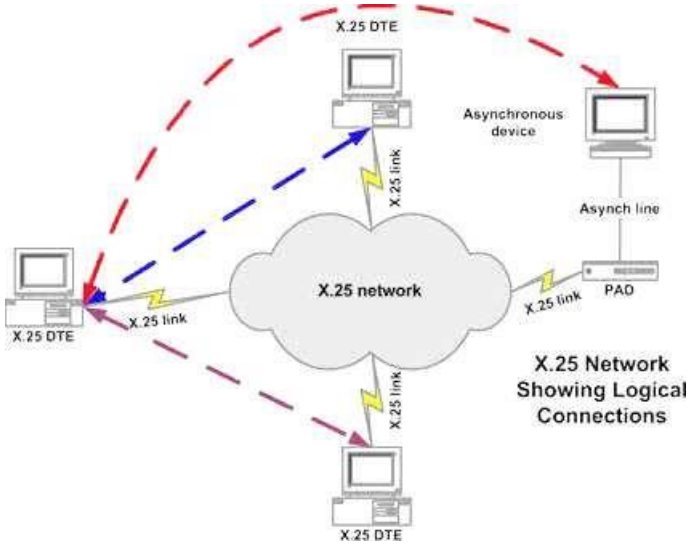
Point-to-point protocol



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



Frame Relay

Works as 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

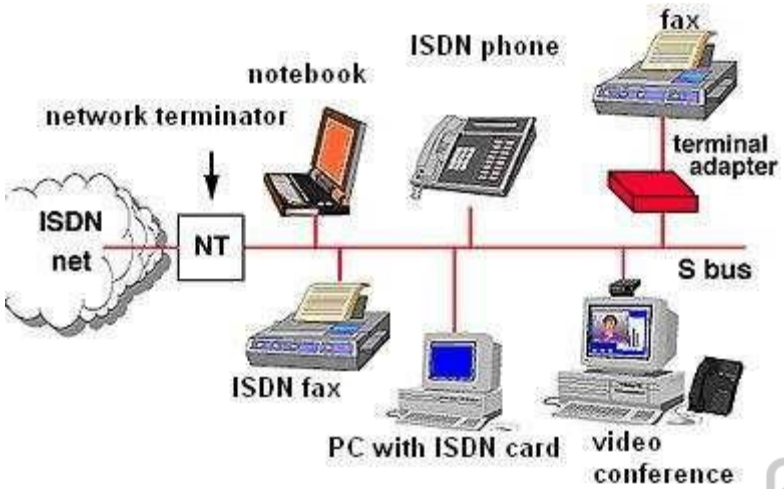
Two main types of equipment's are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides 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.

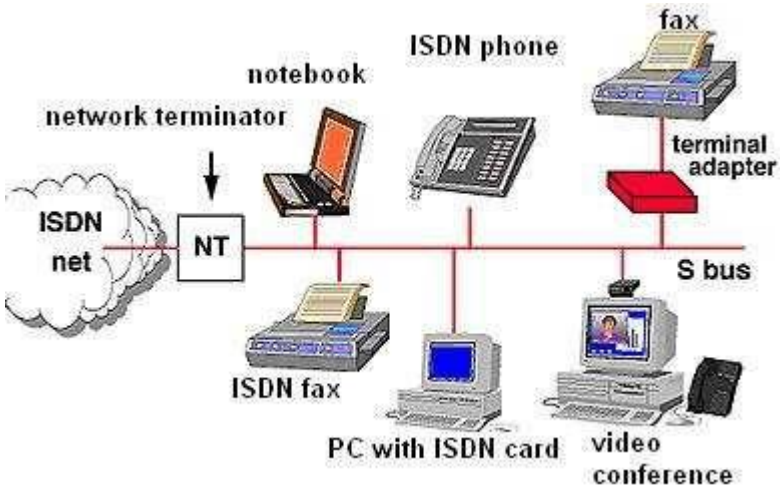
Frame Relay



Integrated Service Digital Network (ISDN)

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.
Runs on top of the Plain Old Telephone System (POTS). The same copper telephone wire is used. Provide digital
point-to-point circuit switching medium.

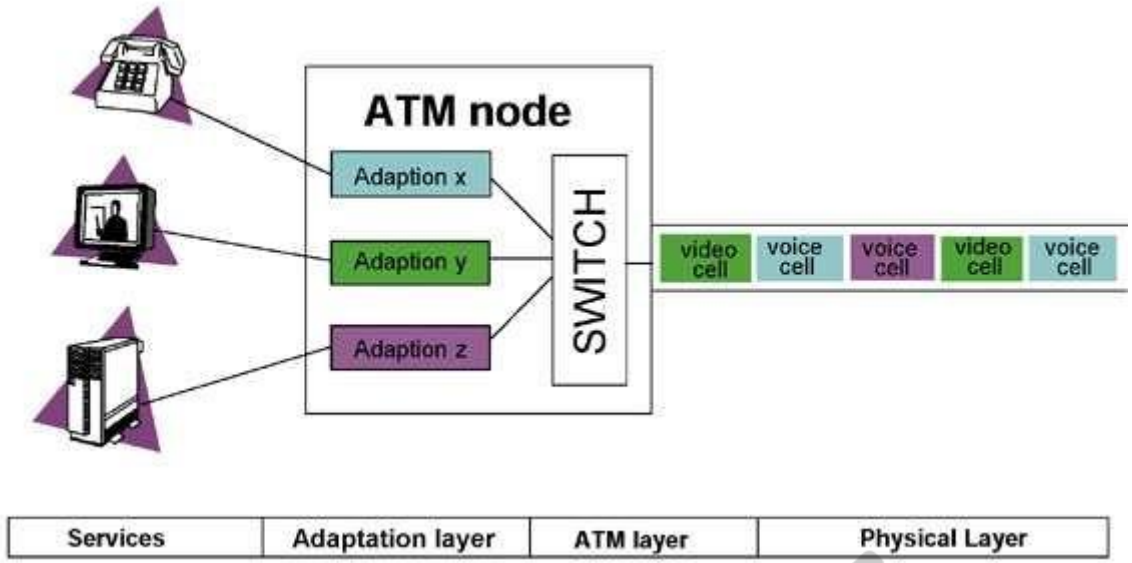
ISDN



Asynchronous Transfer Mode (ATM)

Uses Cell switching method
High speed network technology used for LAN, MAN and WAN
Like 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)

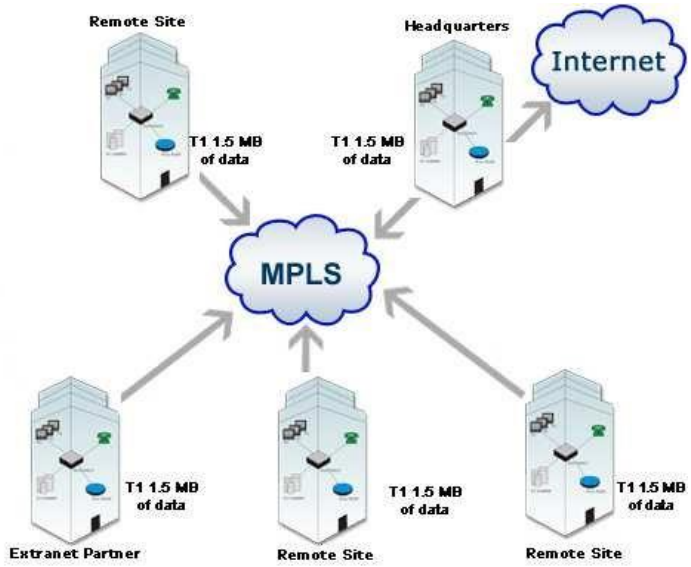
Multiprotocol Label Switching (MPLS) is a standard-approved technology for speeding up network traffic flow and making things easier to manage.MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to 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.

In reference to the Open Systems Interconnection, or OSI model, MPLS allows most packets to be forwarded at 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:

DCE - Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.
DME – Not a valid frame relay technique DLE – Not a valid frame relay technique

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 266

QUESTION 120
Which of the following device in Frame Relay WAN technique is a service provider device that does the actual data transmission and switching in the frame relay cloud?

A. DTE
B. DCE
C. DME
D. DLE

Correct Answer: B
Section: Information System Operations, Maintenance and Support

Explanation

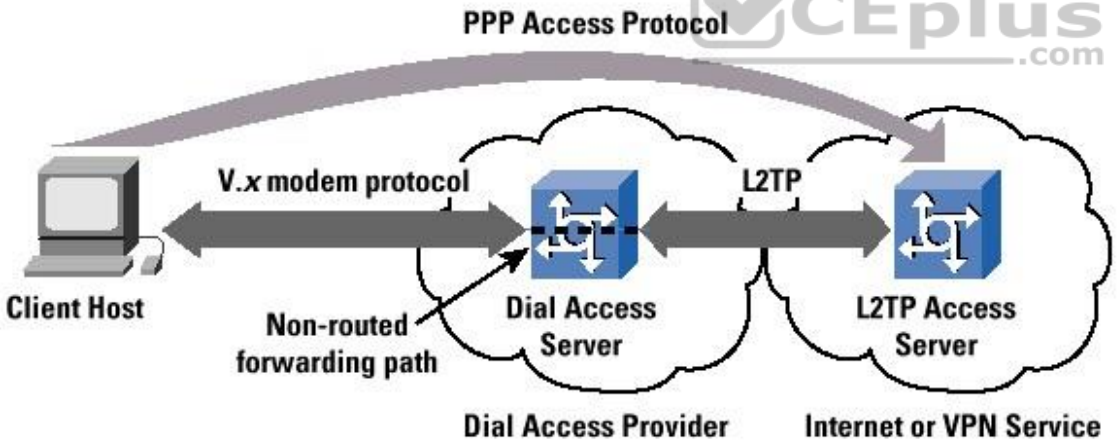
Explanation/Reference:
Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

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.



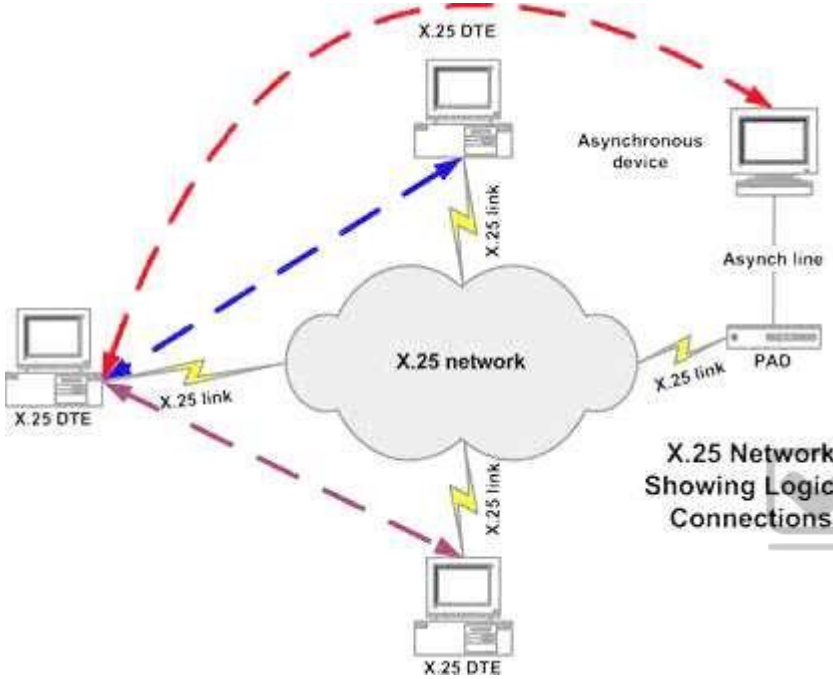
Point-to-point protocol

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



X.25 Network Showing Logical Connections

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 equipments 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.

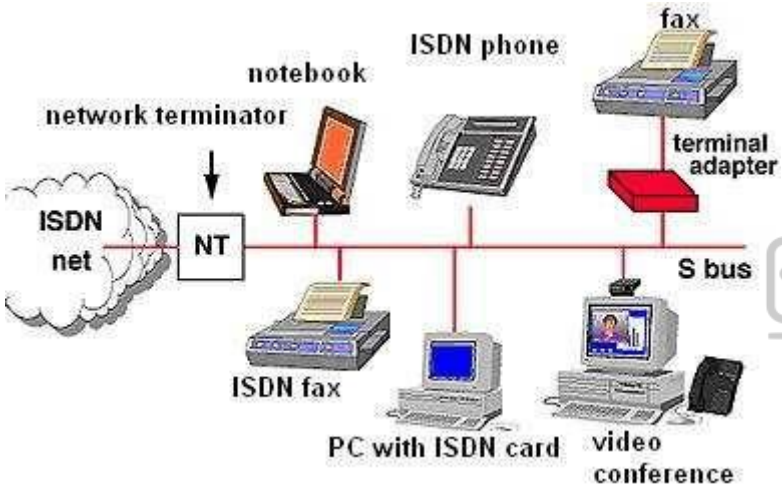
2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

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

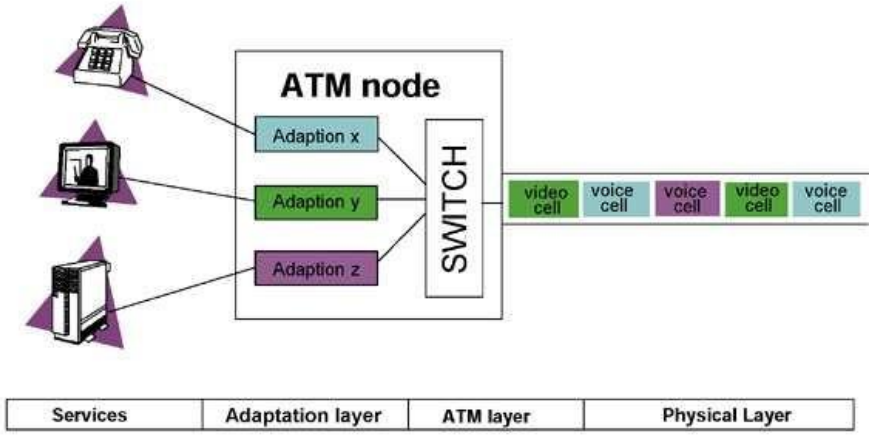
ISDN



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

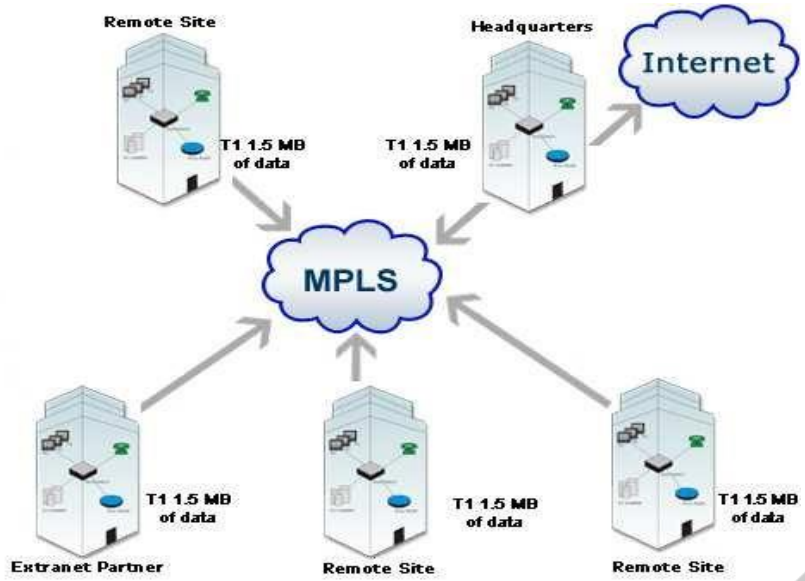
Asynchronous Transfer Mode



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:

DTE - Data Terminal Equipment (DTE) is usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

DME – Not a valid frame relay technique
DLE – Not a valid frame relay technique

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 266

QUESTION 121
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:
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

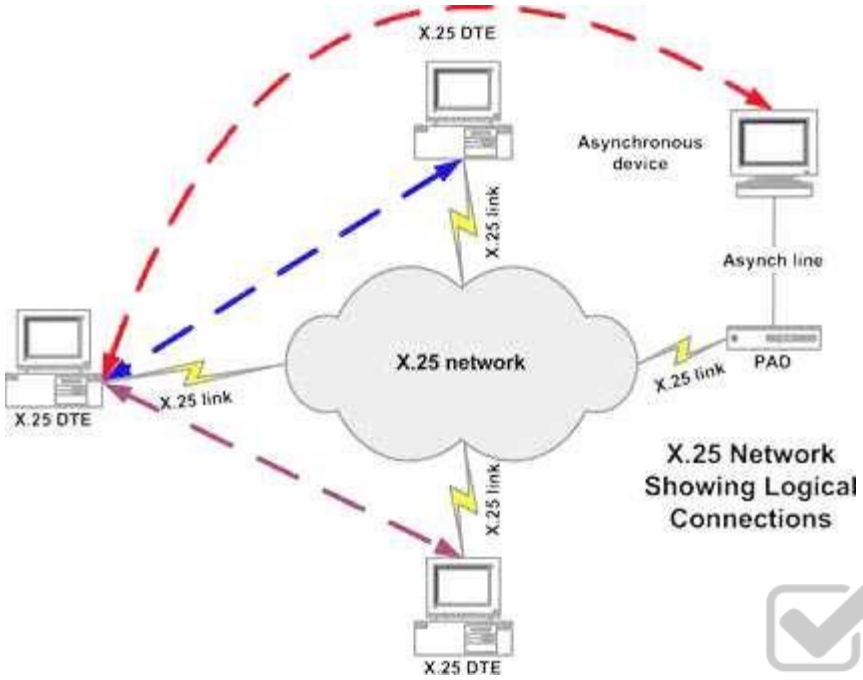
For your exam you should know below information about WAN Technologies:

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

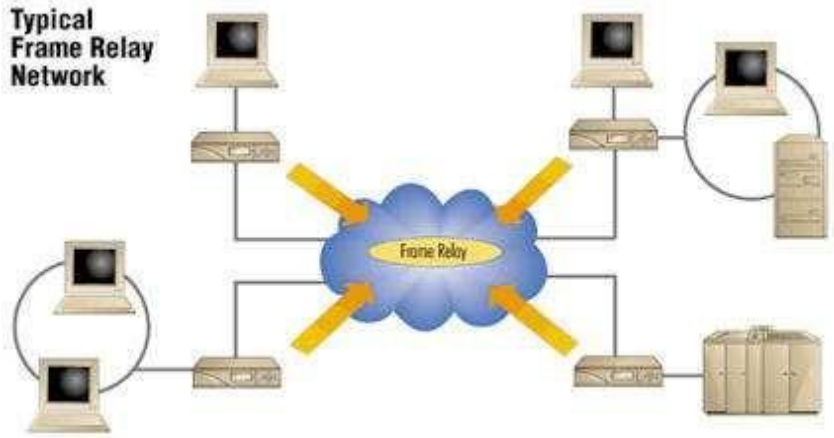
Works on a packet switching
Operates at data link layer of an OSI model
Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

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.

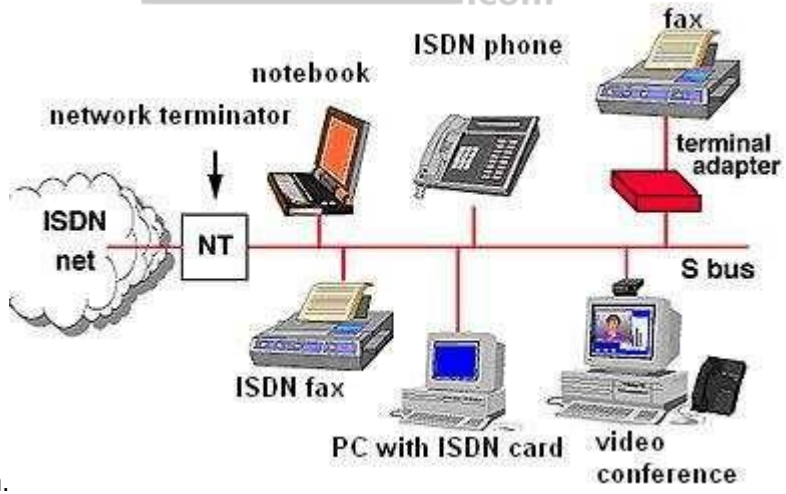
The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.



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.

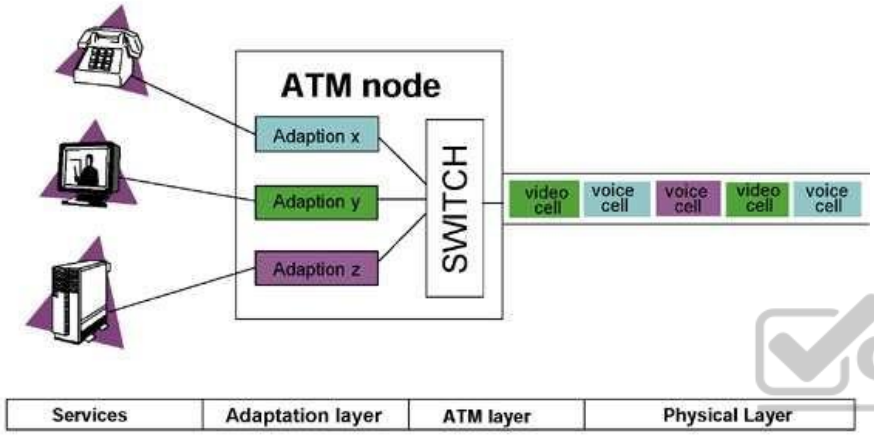


Provide digital point-to-point circuit switching medium.

ISDN

Asynchronous Transfer Mode (ATM)

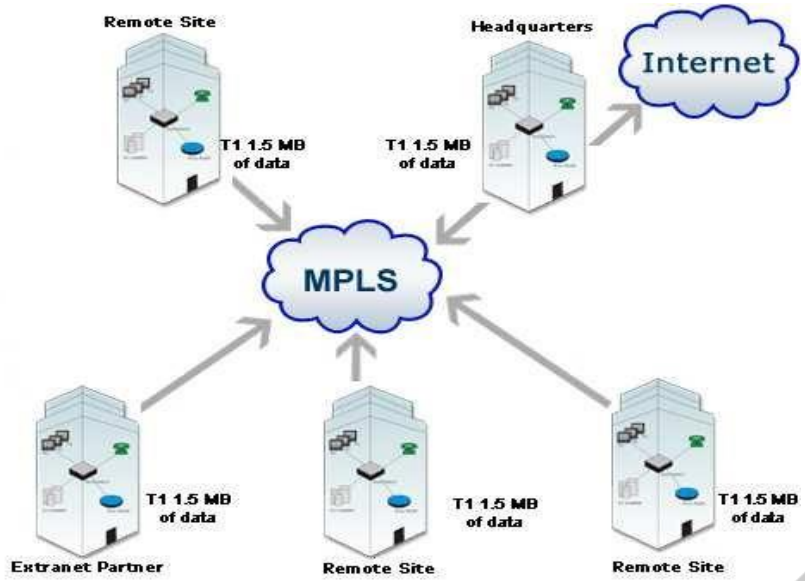
Uses Cell switching method
High speed network technology used for LAN, MAN and WAN
Like a frame relay it is connection oriented technology which creates and uses fixed channel
Data are segmented into fixed size cell of 53 bytes
Some companies have replaces FDDI back-end with ATM



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.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 266

QUESTION 122
Which of the following technique is used for speeding up network traffic flow and making it easier to manage?

A. Point-to-point protocol
B. X.25
C. MPLS
D. ISDN

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

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.

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.

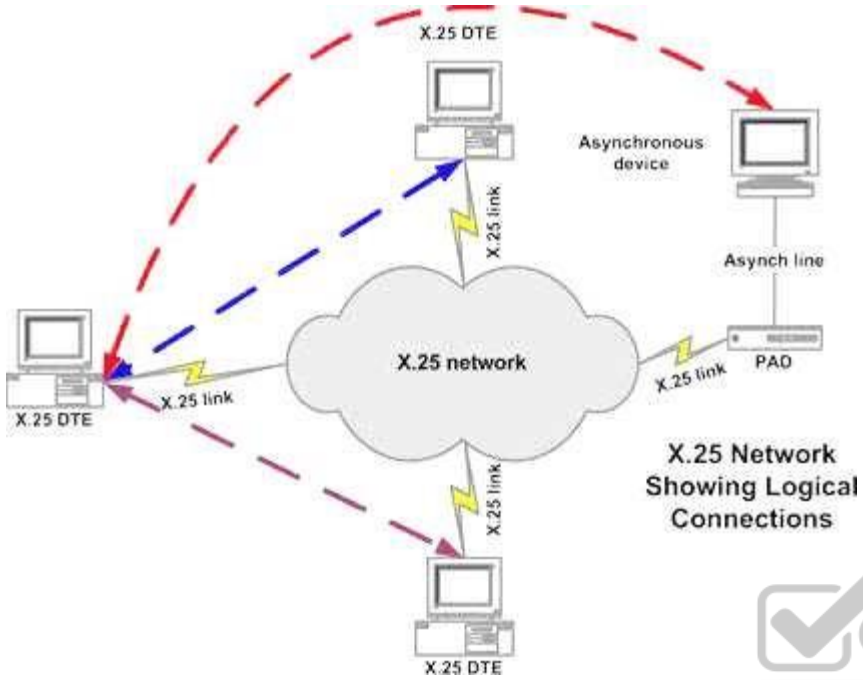
PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

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

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

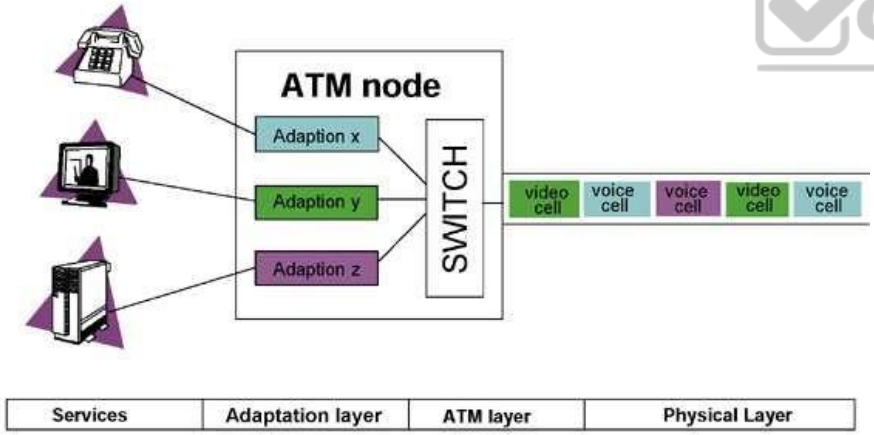
Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.
Same copper telephone wire is used.
Provide digital point-to-point circuit switching medium.

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

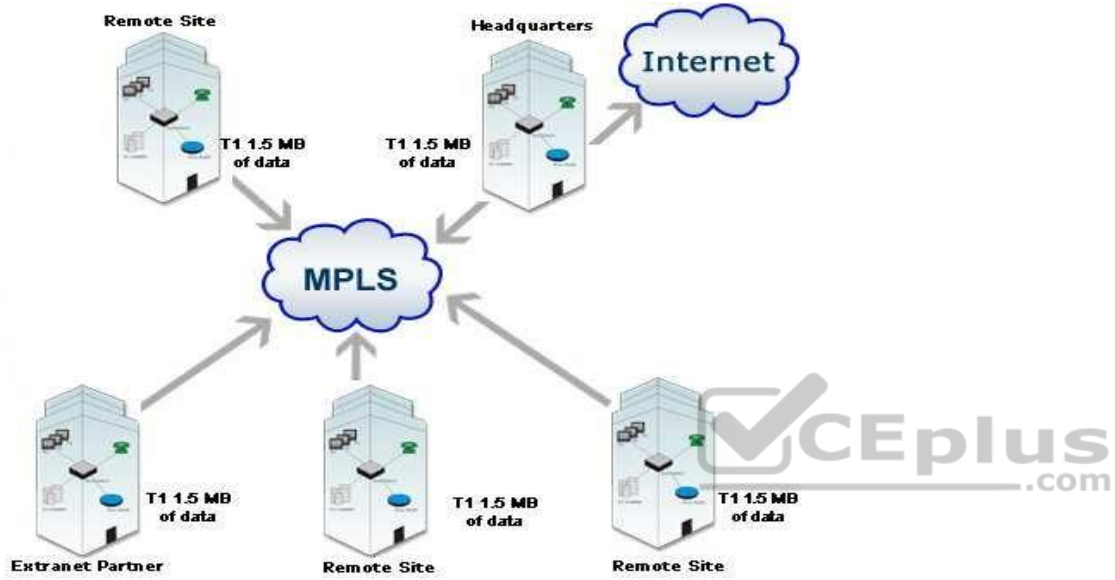
Asynchronous Transfer Mode



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:

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.

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.

ISDN -Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 266

QUESTION 123
An IS auditor should know information about different network transmission media. Which of the following transmission media is used for short distance transmission?

A. Copper cable
B. Fiber Optics
C. Satellite Radio Link
D. Satellite Radio Link

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

For your exam you should know below information about transmission media:

Copper Cable
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.
Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.
Copper Cable

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

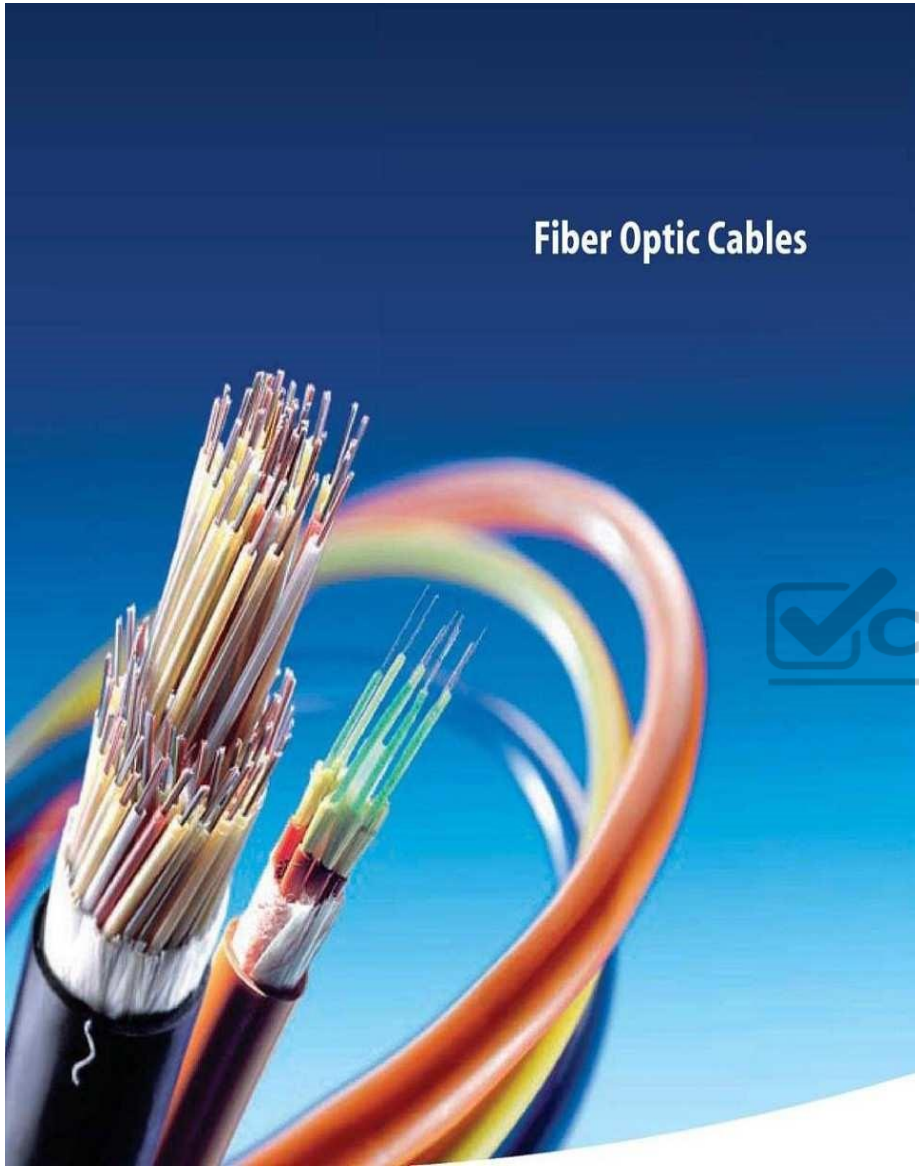
Coaxial Cable

Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics



Radio System

Radio systems are used for short distance, cheap and easy to intercept.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Microwave radio system

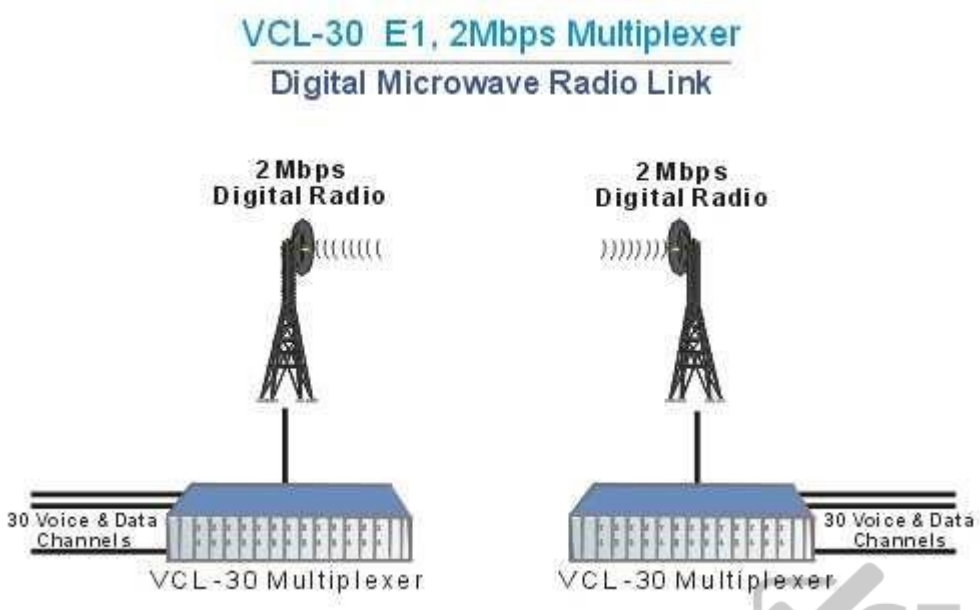
Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

The following answers are incorrect:

Fiber optics - Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 265

QUESTION 124

Which of the following transmission media is MOST difficult to tap?

A. Copper cable
B. Fiber Optics
C. Satellite Radio Link
D. Radio System

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

For your exam you should know below information about transmission media:

Copper Cable
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.
Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors. Copper Cable

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

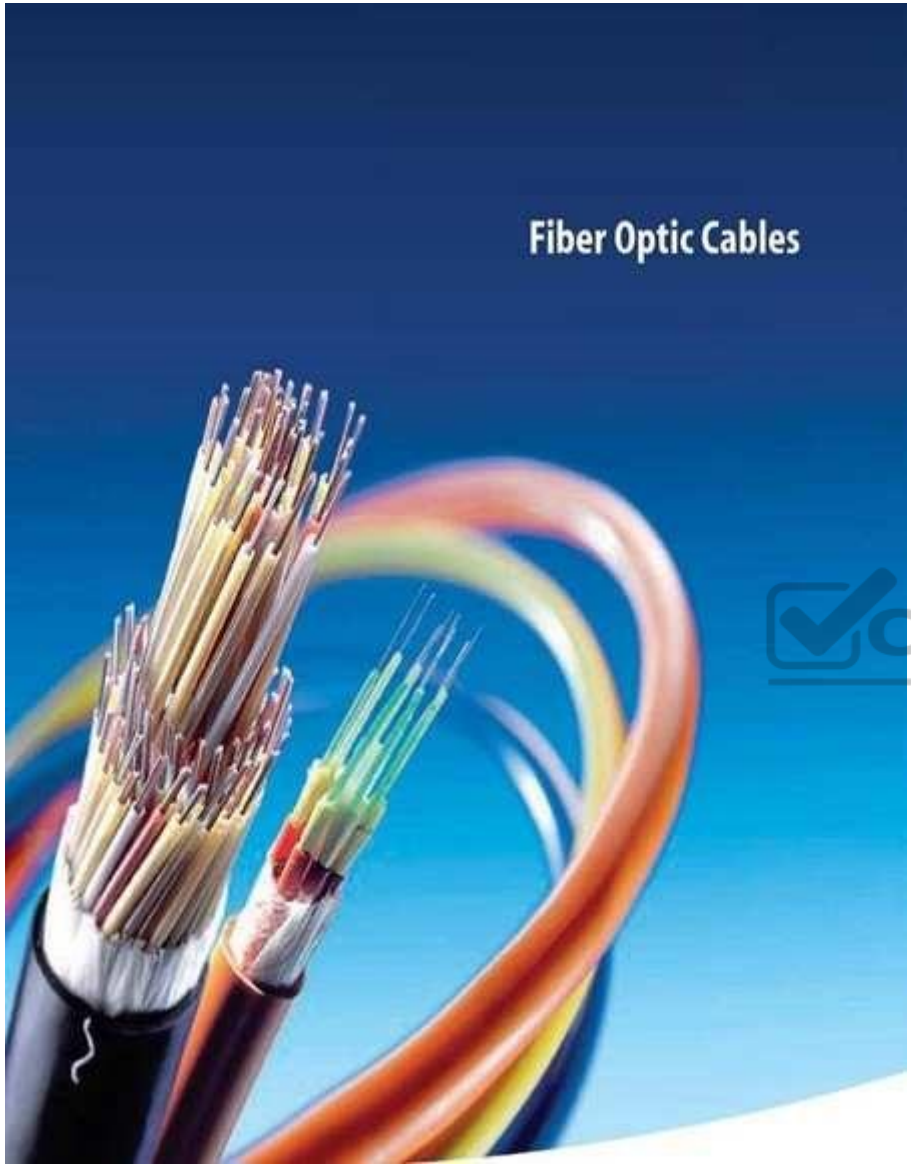
Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Coaxial Cable

Fiber optics
An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics



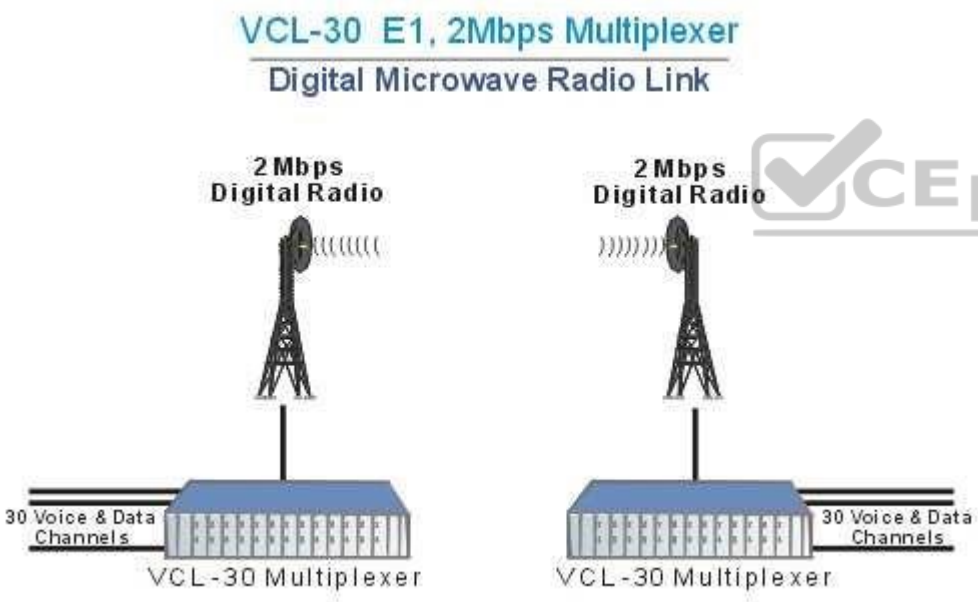
Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to intercept.

Microwave Radio System



Satellite Radio Link
Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Radio System
Radio systems are used for short distance, cheap and easy to intercept.
Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 265

QUESTION 125
Which of the following transmission media uses a transponder to send information?

A. Copper cable
B. Fiber Optics
C. Satellite Radio Link
D. Coaxial cable

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Satellite radio link uses transponder to send information and are easy to intercept.

For your exam you should know below information about transmission media:

Copper Cable
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors. Copper Cable

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

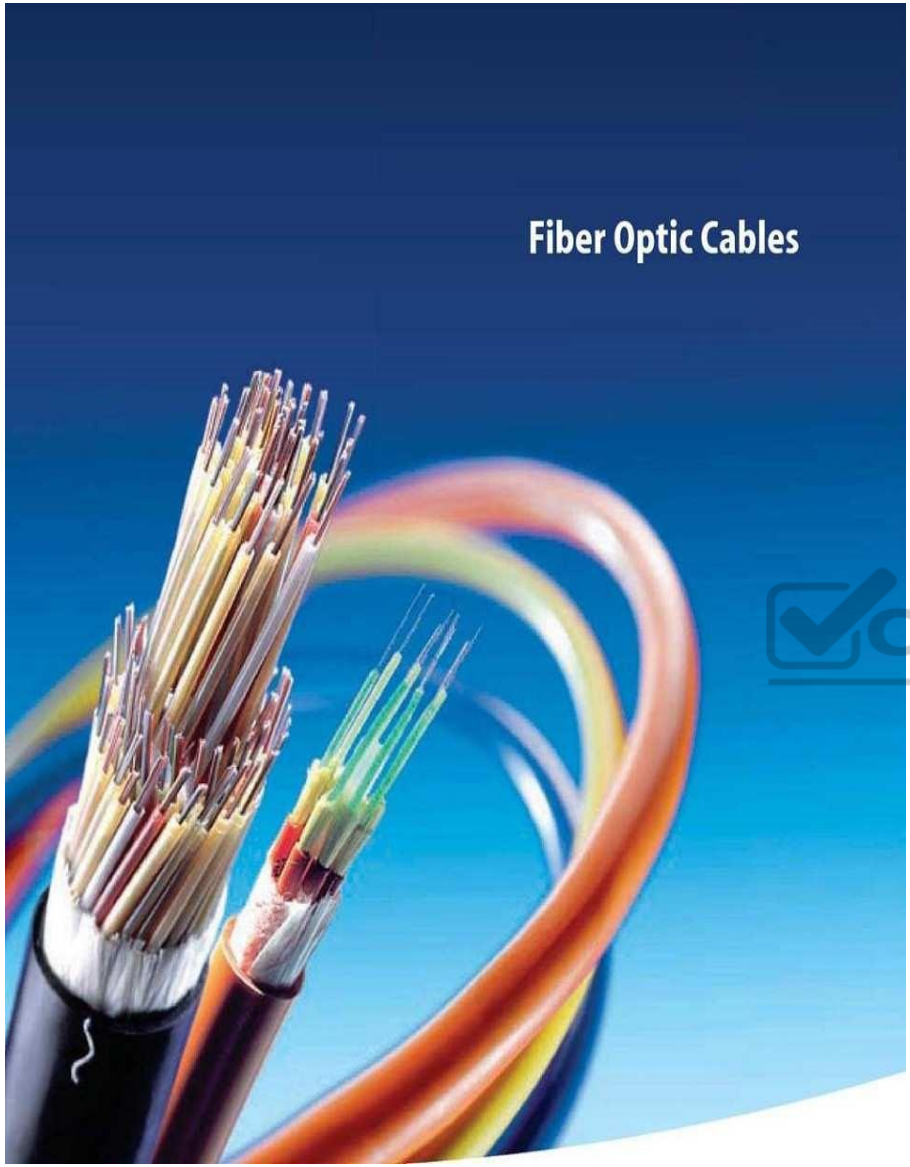
Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Coaxial Cable

Fiber optics
An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics



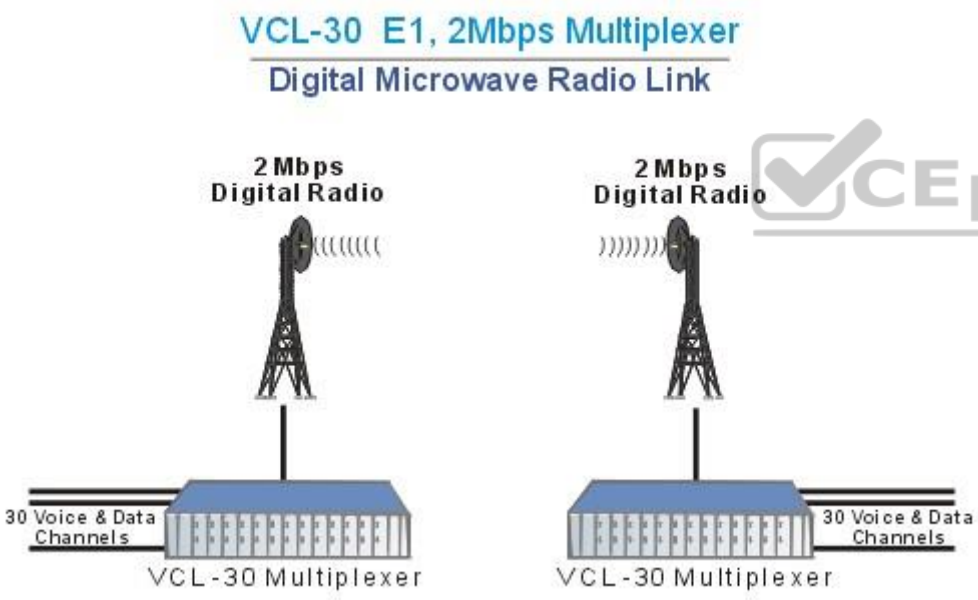
Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to intercept.

Microwave Radio System



Satellite Radio Link
Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Radio System
Radio systems are used for short distance, cheap and easy to intercept.
Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 265

QUESTION 126
Which of the following transmission media is LEAST vulnerable to cross talk?

A. Copper cable
B. Fiber Optics
C. Satellite Radio Link
D. Coaxial cable

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

For your exam you should know below information about transmission media:

Copper Cable
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors. Copper Cable

Coaxial cable
Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

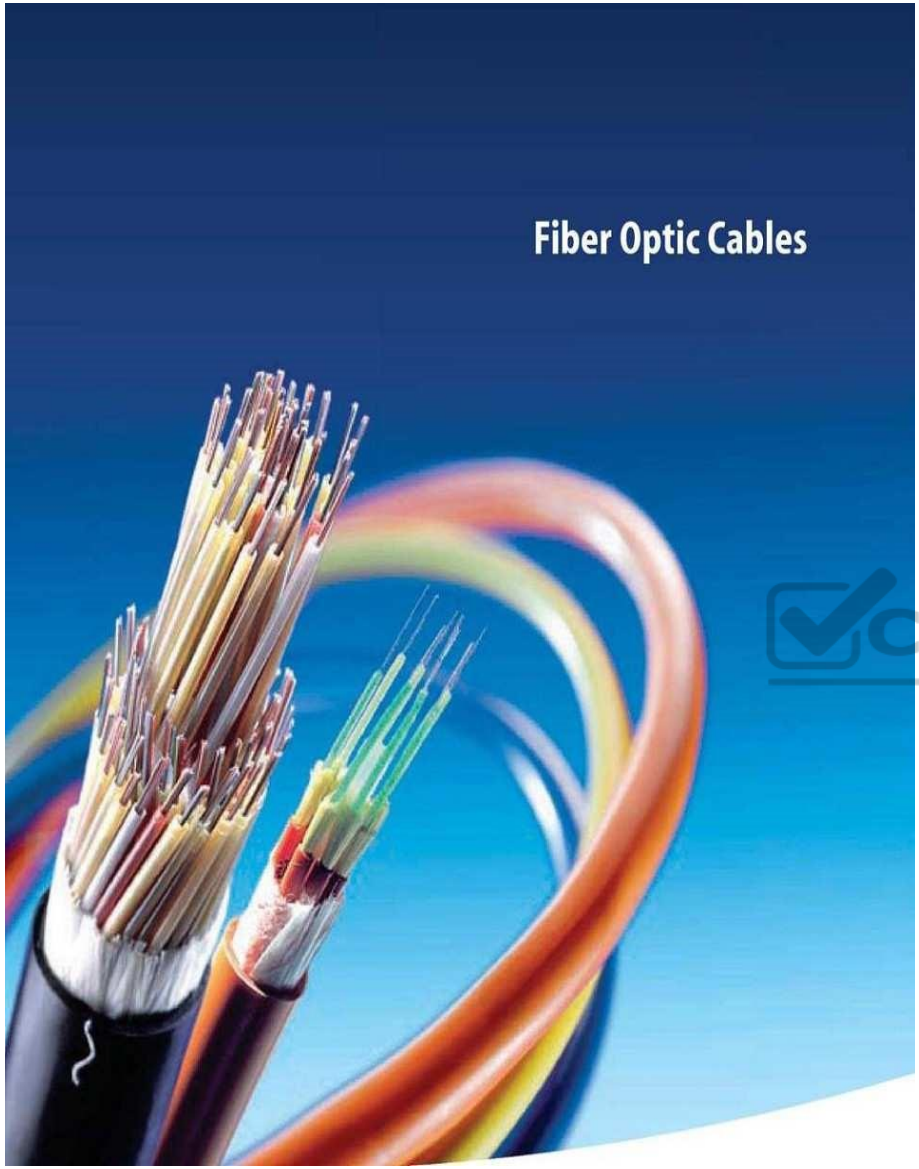
Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Coaxial Cable

Fiber optics
An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics



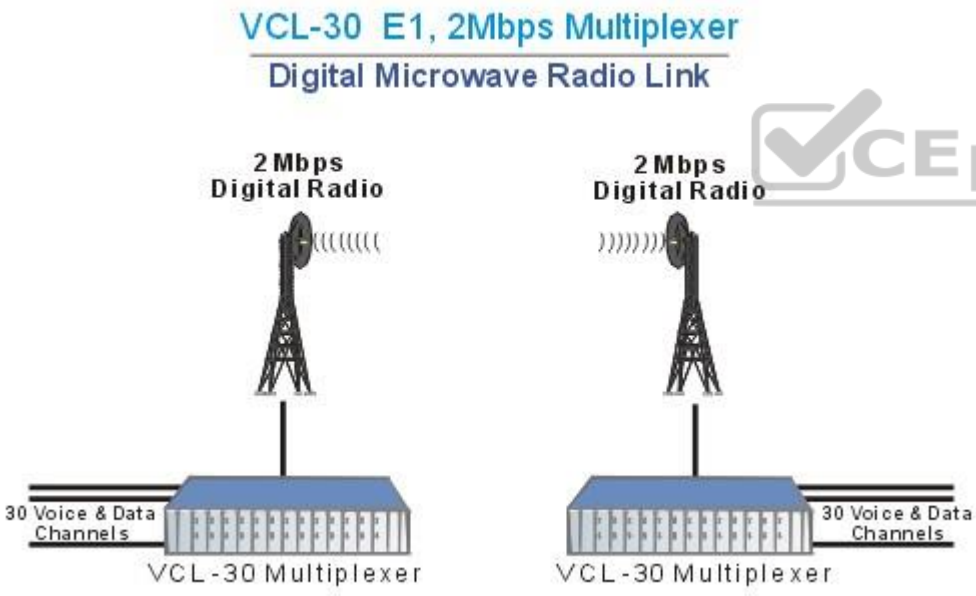
Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to intercept.

Microwave Radio System



Satellite Radio Link
Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.
Radio System
Radio systems are used for short distance, cheap and easy to tap.
Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

Coaxial cable - Coaxial cable are expensive and does not support many LAN's. It supports data and video

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 265

QUESTION 127
In which of the following transmission media it is MOST difficult to modify the information traveling across the network?

A. Copper cable
B. Fiber Optics
C. Satellite Radio Link
D. Coaxial cable

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

For your exam you should know below information about transmission media:

Copper Cable
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.
Copper Cable

Coaxial cable
Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line. Coaxial cable is expensive and does not support many LAN's. It supports data and video.

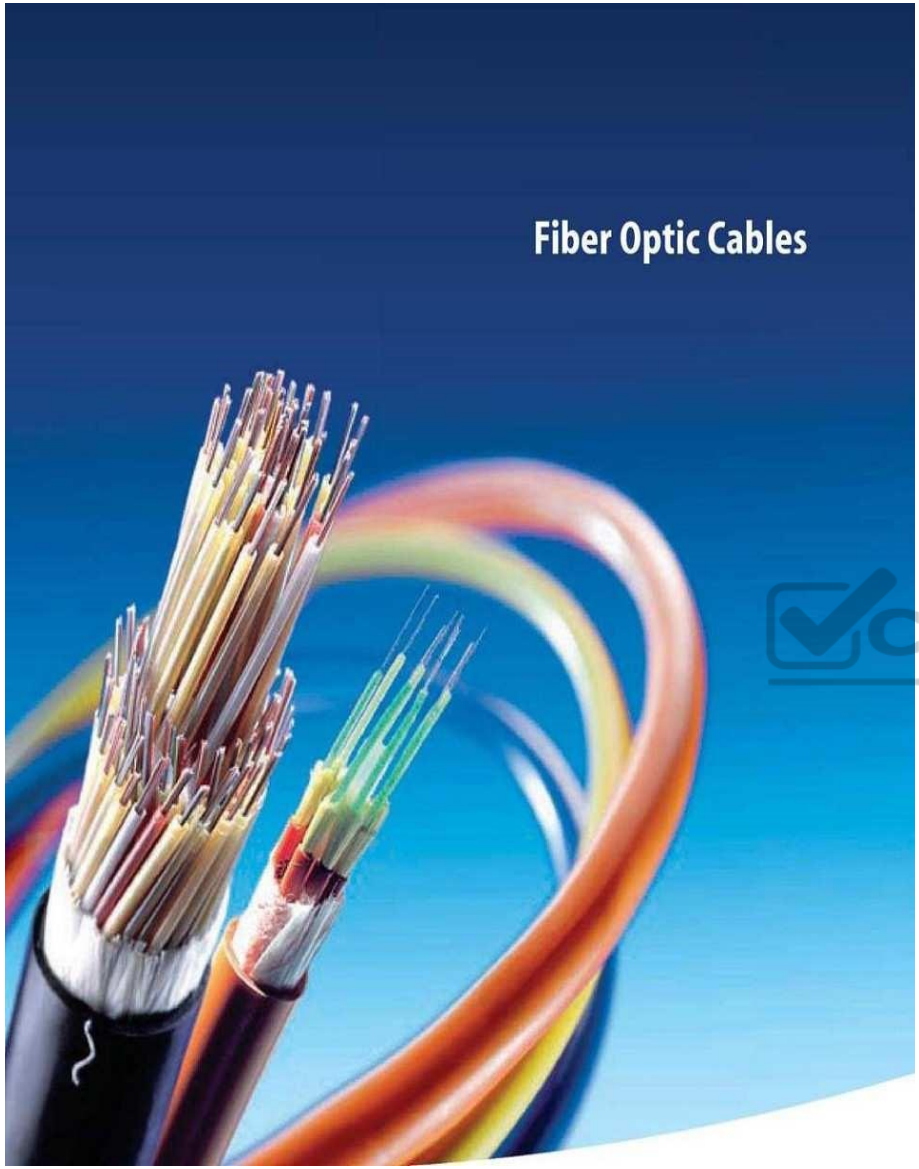
Coaxial Cable

Fiber optics
An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.
Radio System
Radio systems are used for short distance, cheap and easy to tap.
Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Fiber Optics



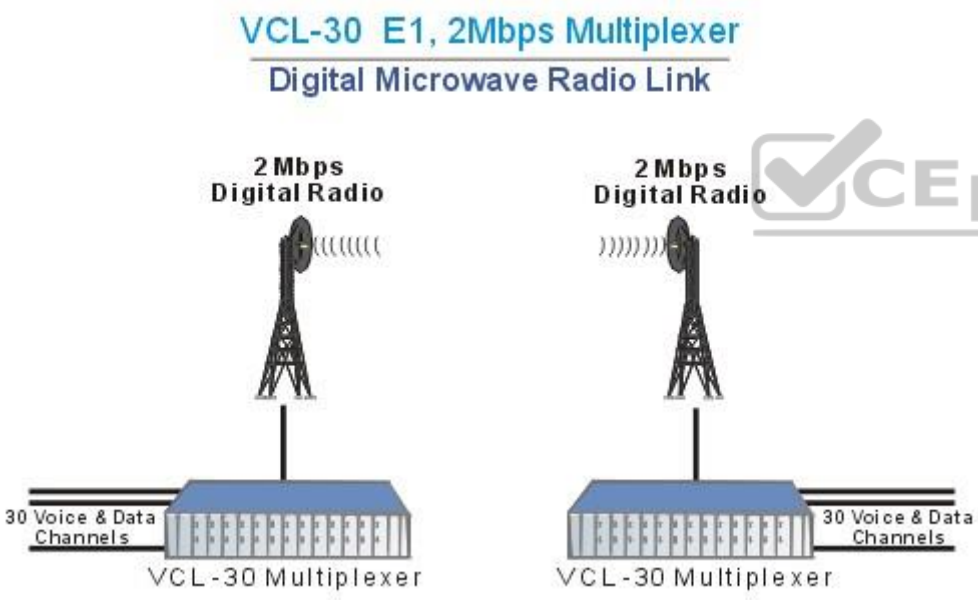
Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System



Satellite Radio Link
Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to tap.
The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

Coaxial cable - Coaxial cable are expensive and does not support many LAN's. It supports data and video

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265

QUESTION 128
Which of the following is the INCORRECT Layer to Protocol mapping used in the DOD TCP/IP model?

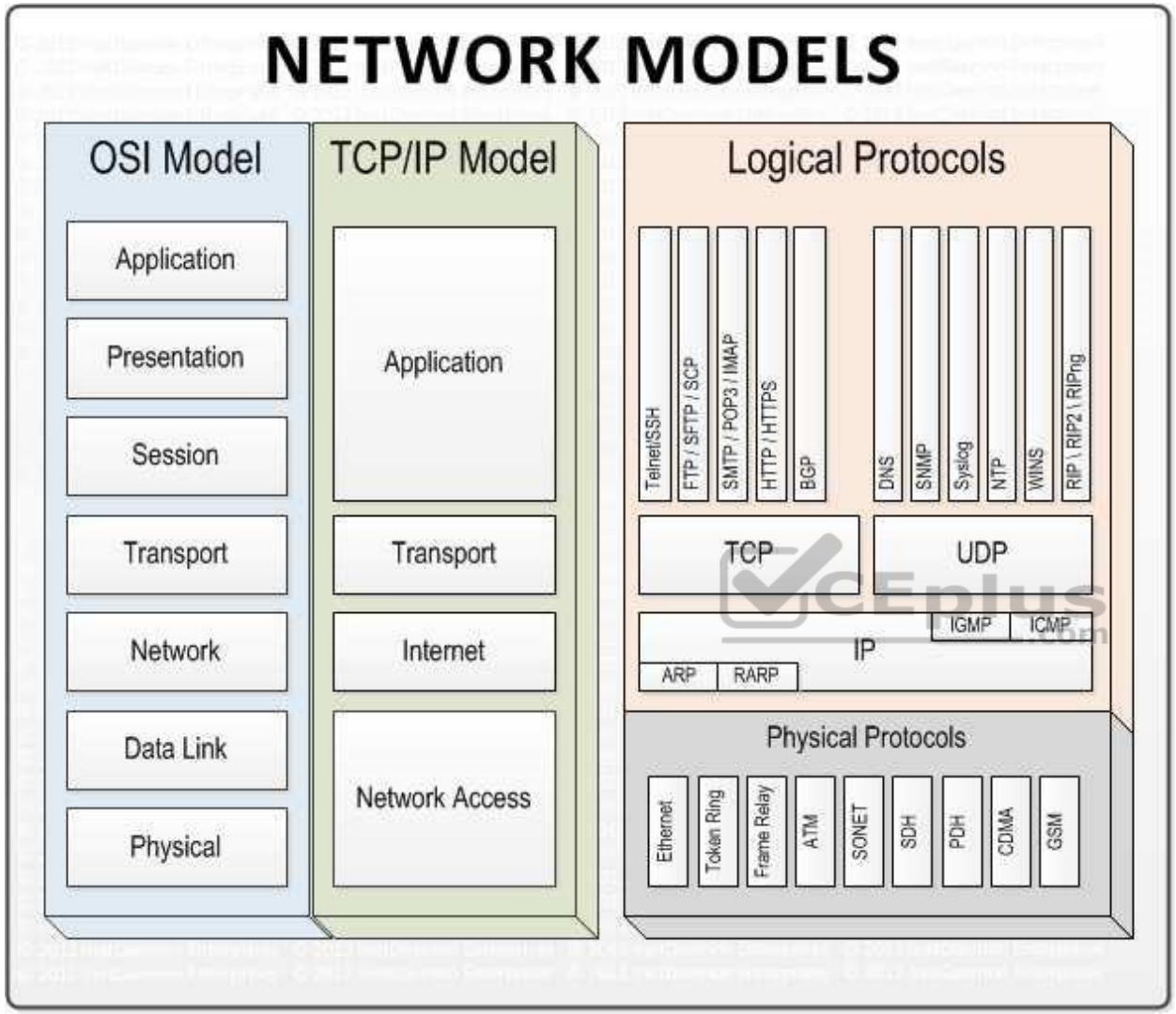
A. Application layer – Telnet
B. Transport layer – ICMP
C. Internet layer – IP
D. Network Access layer – Ethernet

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
The keyword INCORRECT is used within the question. You need to find out the incorrect Layer to Protocol mapping.

The ICMP protocol works at Internet layer of the DoD TCP/IP model, not at the Transport Layer.

For your exam you should know below information about the TCP/IP models:
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.

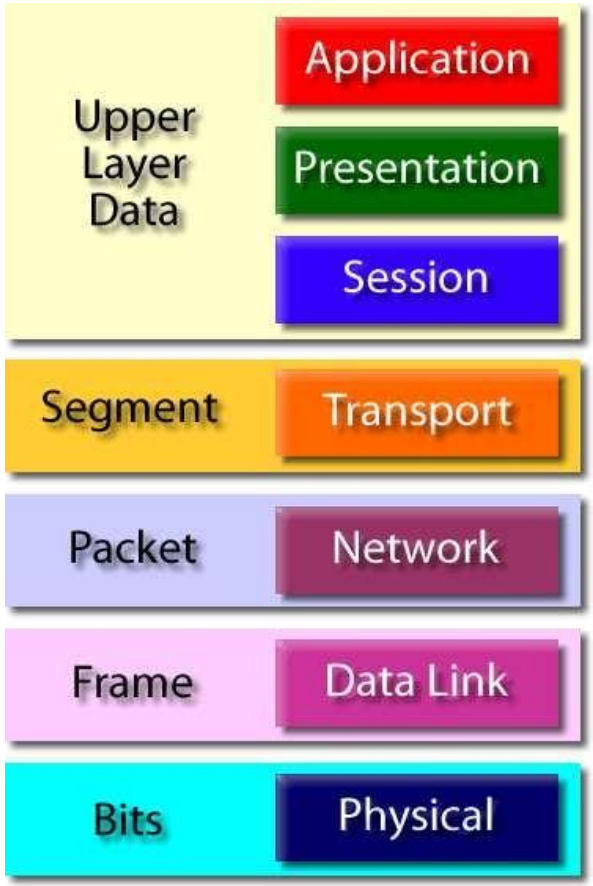
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other options correctly describe the Layer to Protocol mapping of the DoD TCP/IP model protocols.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 272

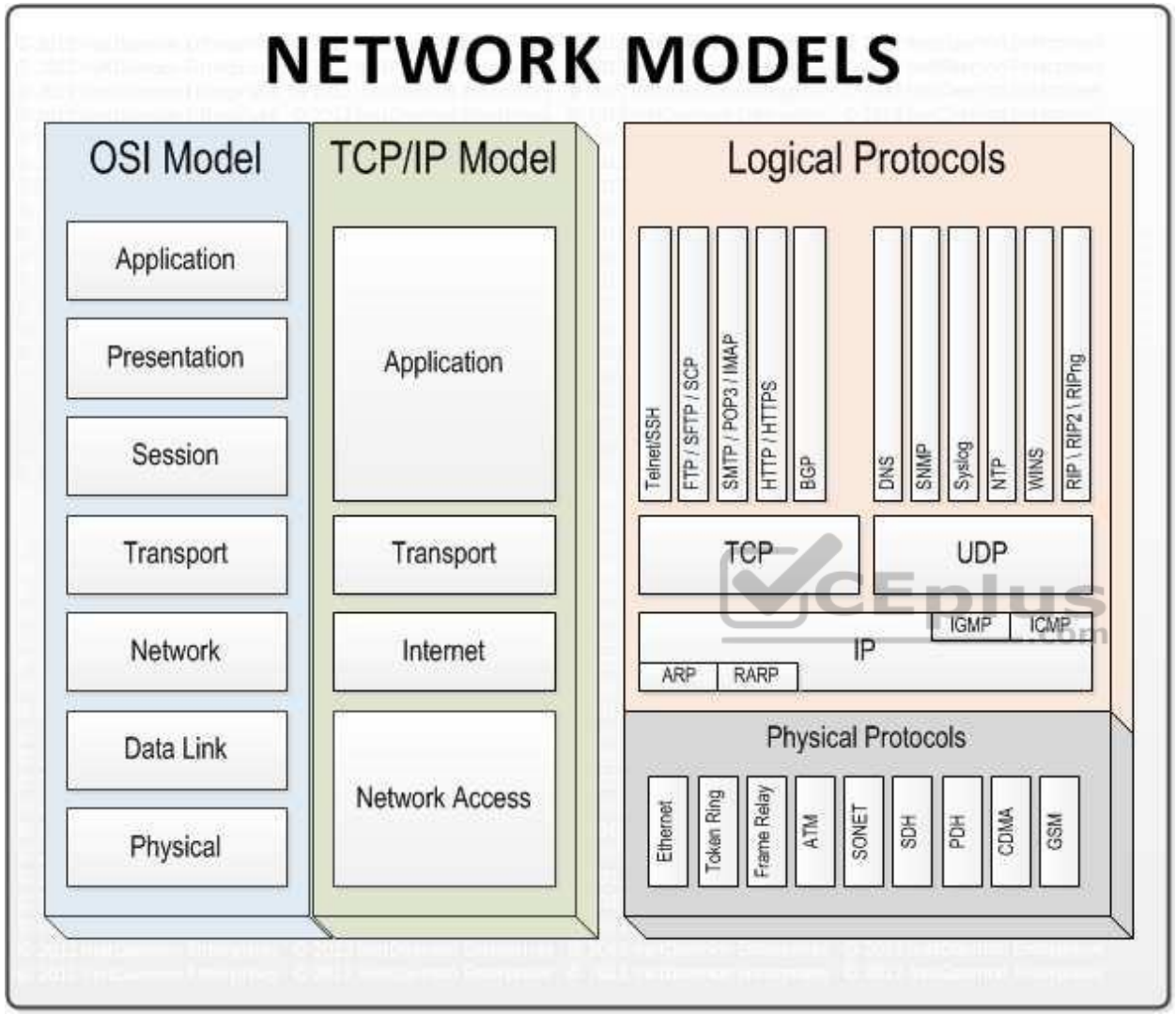
QUESTION 129
Which of the following protocol does NOT work at the Application layer of the TCP/IP Models?
A. HTTP
B. FTP
C. NTP
D. TCP

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
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.

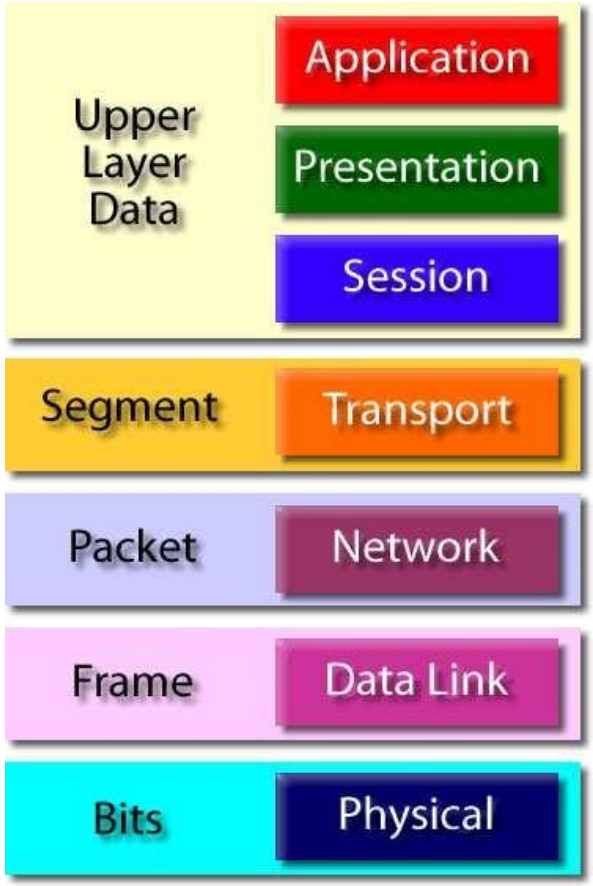
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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):

Protocol Data Unit - PDU



The following answers are incorrect:

HTTP, FTP and NTP protocols works at application layer in TCP/IP model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

QUESTION 130
Which of the following statement INCORRECTLY describes device and where they sit within the TCP/IP model?

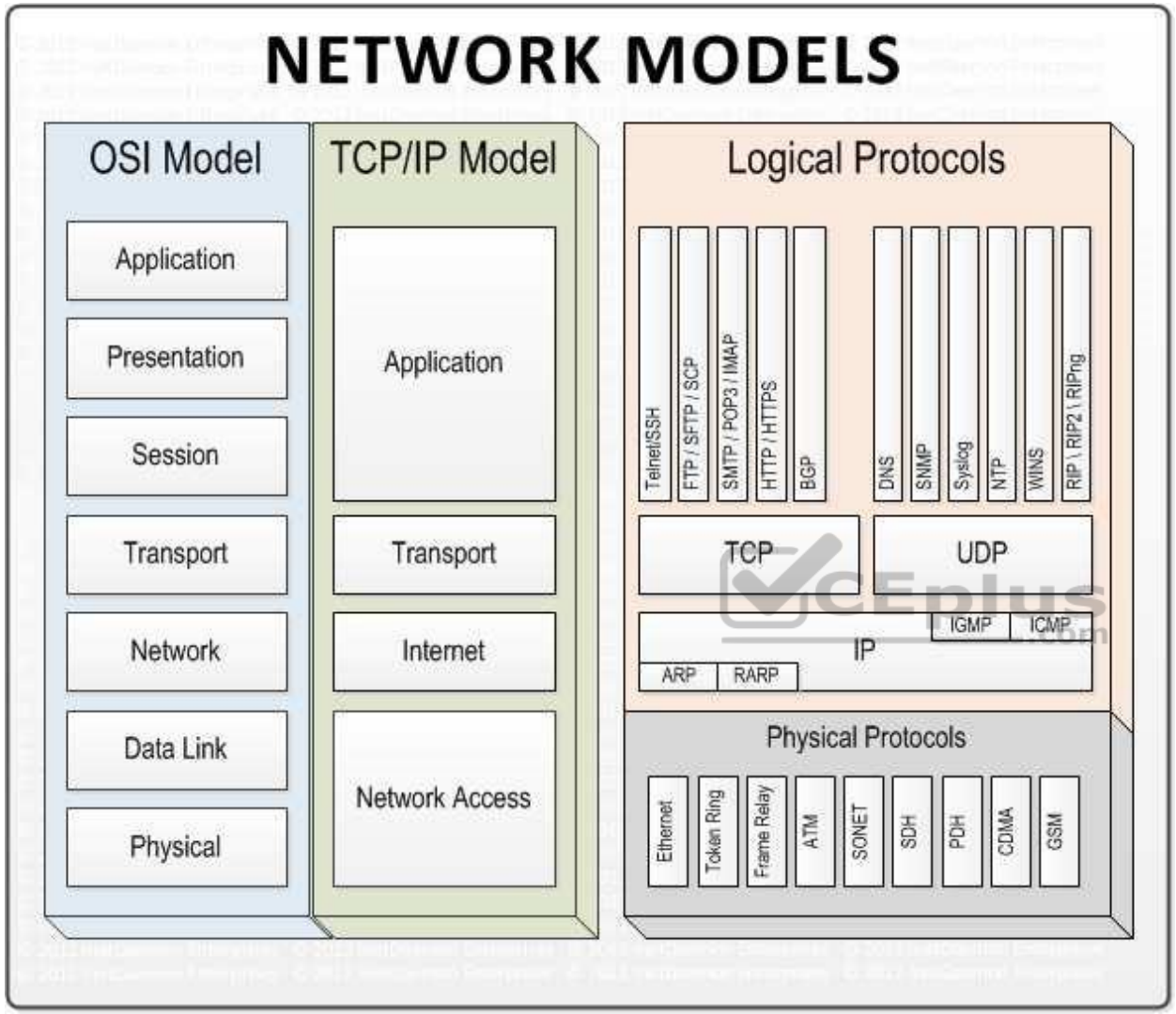
A. Layer 4 switch work at Network interface layer in TCP/IP model
B. Router works at Network interface layer in TCP/IP model
C. Layer 3 switch work at Network interface layer in TCP/IP model
D. Hub works at LAN or WAN interface layer of a TCP/IP model

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
The keyword within the question is INCORRECTLY. You need to find out incorrect statement.

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).

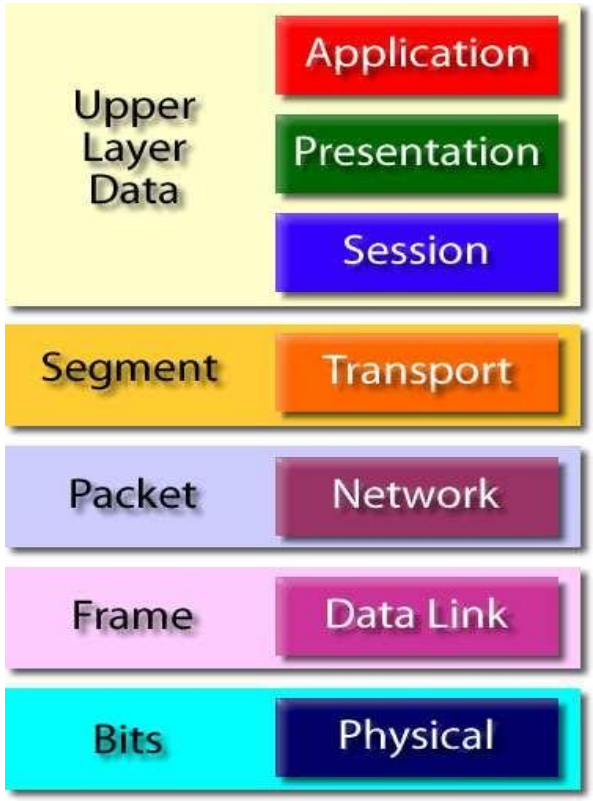
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network 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) :



Protocol Data Unit - PDU
The following answers are incorrect:

The other options correctly describe about network device functioning based on TCP/IP model

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 272

QUESTION 131
Which of the following protocol does NOT work at Network interface layer in TCP/IP model?
A. ICMP

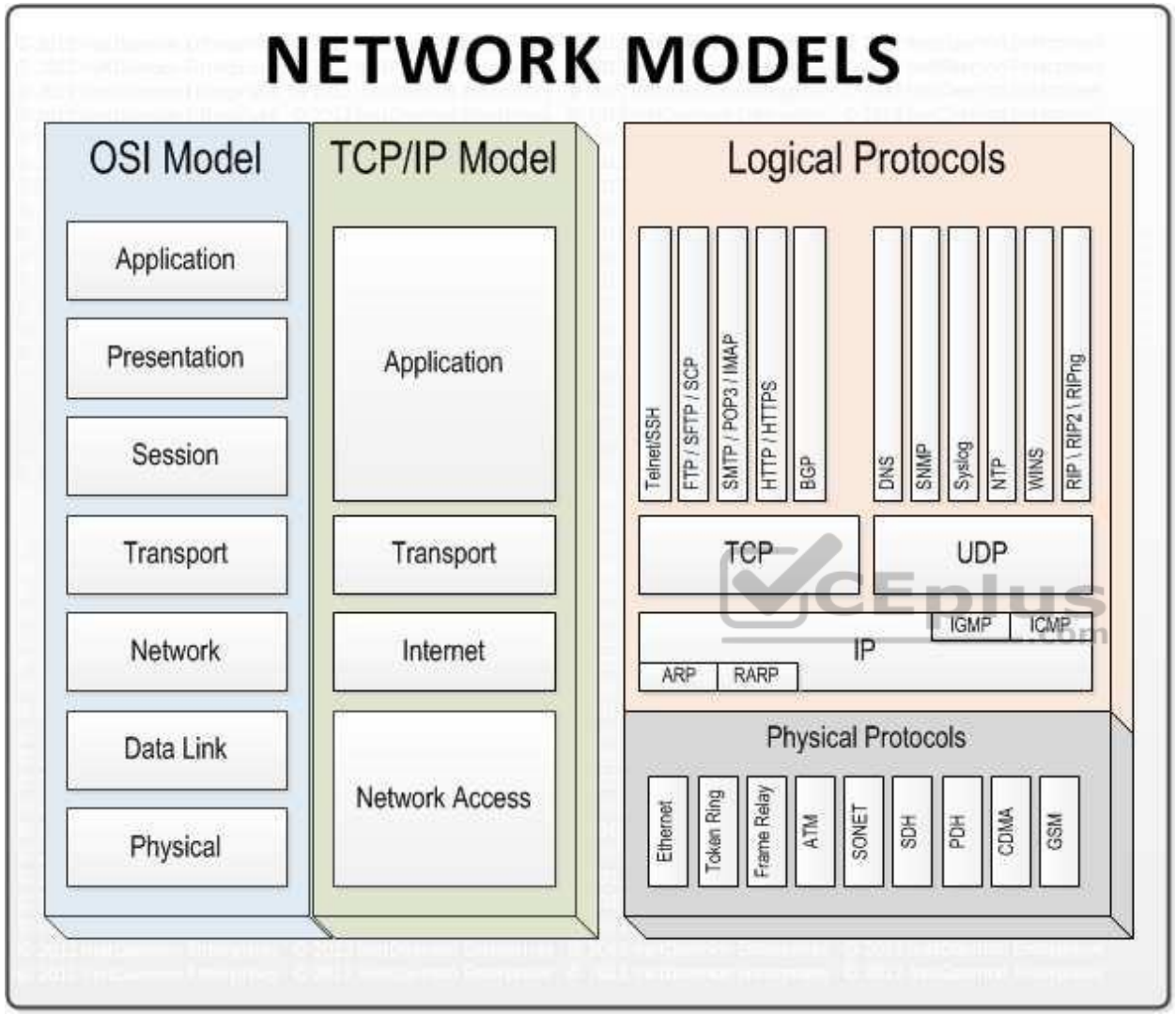
B. DNS
C. ARP
D. Internet protocol

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
The NOT is the keyword used in the question. You need to find out a protocol which does not work at network interface layer in TCP/IP model. DNS protocol works at application layer of a 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).

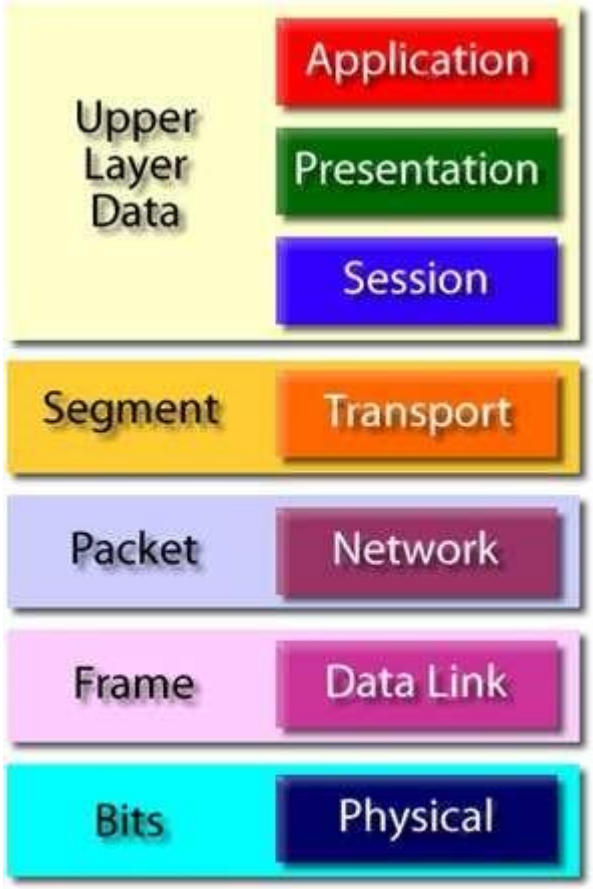
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network 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) :



Protocol Data Unit - PDU
The following answers are incorrect:

ICMP, ARP and Internet protocol works at Network interface layer of a TCP/IP model.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 272

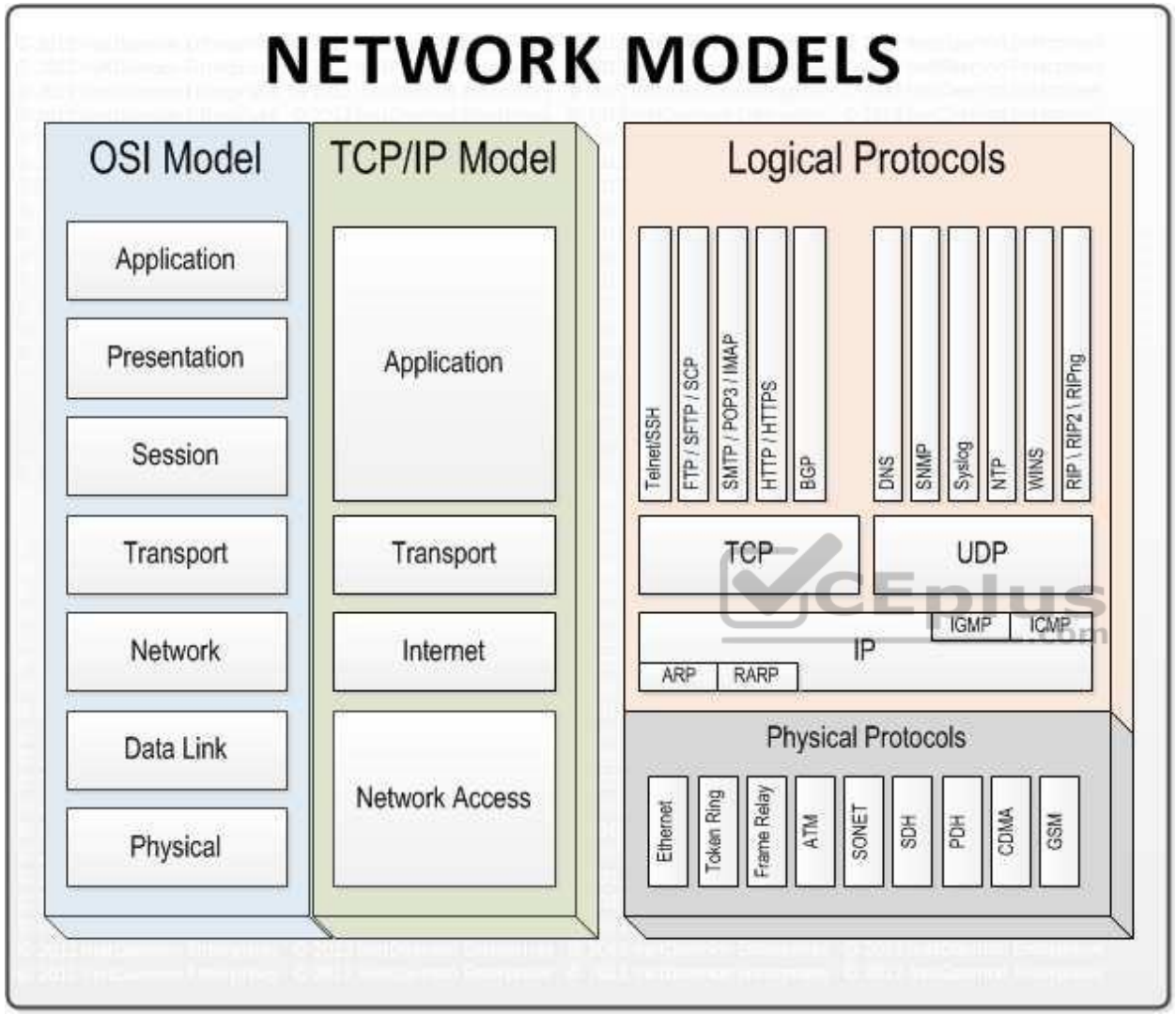
QUESTION 132
Which of the following is the protocol data unit (PDU) of application layer in TCP/IP model?

A. Data
B. Segment
C. Packet
D. Frame

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
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).

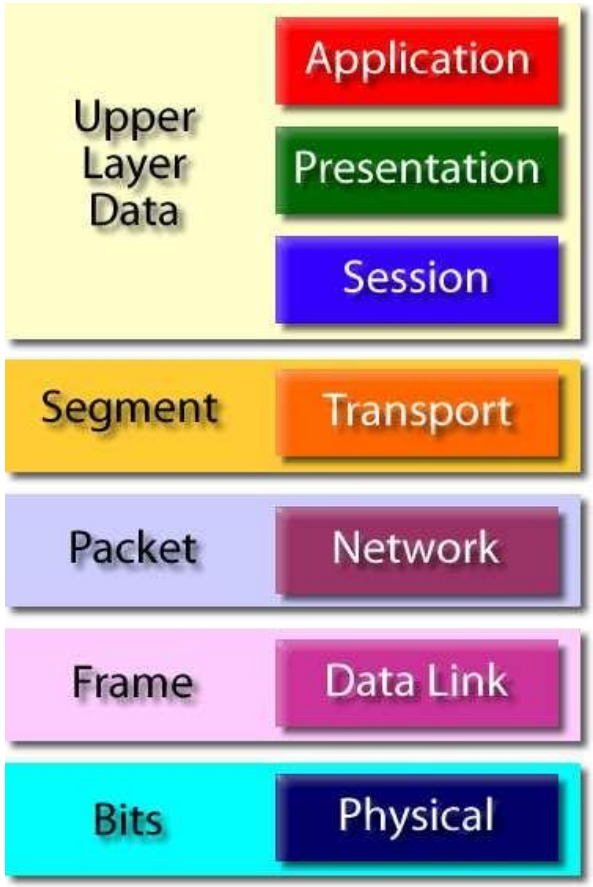
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network 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) :
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

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 272

QUESTION 133

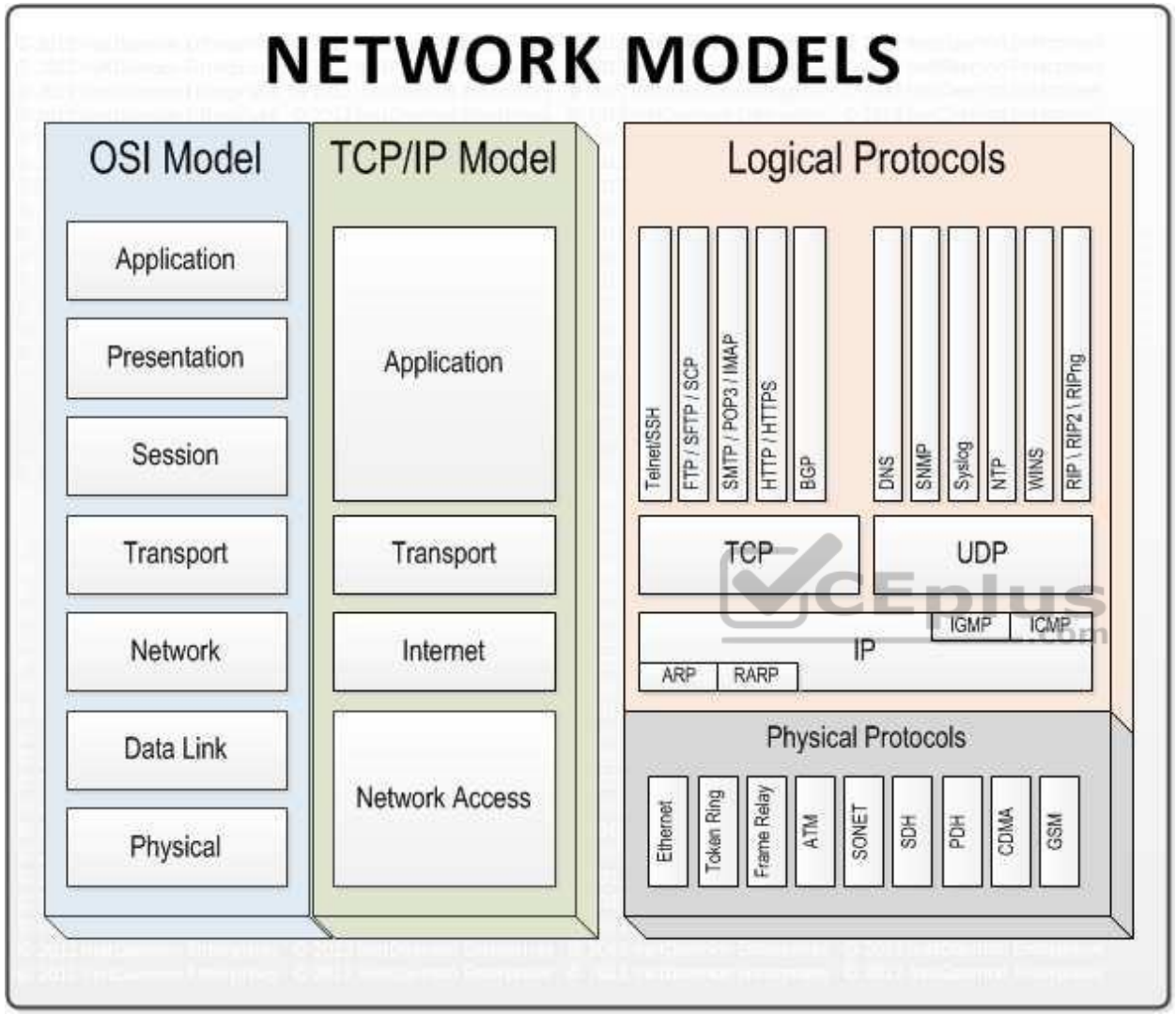
Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

A. Data
B. Segment
C. Packet
D. Frame

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
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.

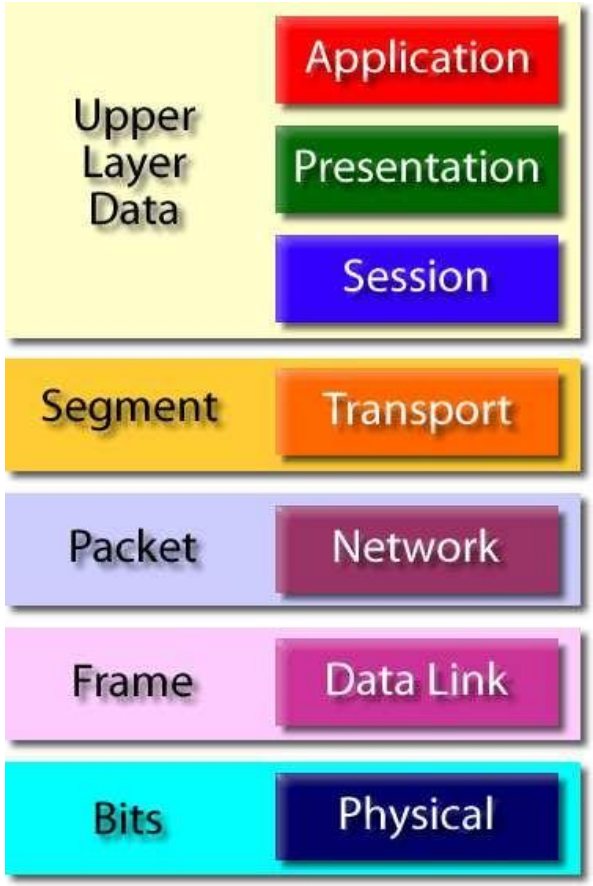
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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) :

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

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 272

QUESTION 134
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:
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.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 30 (The process of auditing information system)

QUESTION 135

An IS auditor finds that a company is using a payroll provider hosted in a foreign country. Of the following, the **MOST** important audit consideration is whether the provider's operations:

A. meet industry best practice and standards
B. comply with applicable laws and regulations
C. are shared with other companies using the provider
D. are aligned with the company's culture

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 136
A business unit cannot achieve desired segregation of duties between operations and programming due to size constraints. Which of the following is **MOST** important for the IS auditor to identify?

A. Unauthorized user controls
B. Compensating controls
C. Controls over operational effectiveness
D. Additional control weaknesses

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 137
An organization has shifted from a bottom-up approach to a top-down approach in the development of IT policies. This should result in:

A. a synthesis of existing operational policies
B. greater consistency across the organization
C. greater adherence to best practices
D. a more comprehensive risk assessment plan

Correct Answer: D
Section: Information System Operations, Maintenance and Support

Explanation

Explanation/Reference:

QUESTION 138
Which of the following weaknesses would have the **GREATEST** impact on the effective operation of a perimeter firewall?

A. Ad-hoc monitoring of firewall activity
B. Potential back doors to the firewall software
C. Misconfiguration on the firewall rules
D. Use of stateful firewalls with default configuration

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 139
An IS auditor is reviewing database log settings and notices that only INSERT and DELETE operations are being monitored in the database. What is the **MOST** significant risk?

A. Metadata may not be logged
B. Newly added records may not be logged
C. Purged records may not be logged
D. Changes to existing records may not be logged

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 140
Adding security requirements late in the software development life cycle would **MOST** likely result in:
A. cost savings
B. clearer understanding of requirements

C. operational efficiency
D. compensating controls

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 141
A reduction in which of the following would indicate improved performance in the administration of information security?

A. 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 142
What is the **PRIMARY** objective of performing a vulnerability assessment following a business system update?

A. Update the threat landscape
B. Review the effectiveness of controlsC. Determine operational losses
D. Improve the change control process

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:

QUESTION 143
Which of the following is the **BEST** evidence of the maturity of an organization's information security program?

A. The number of reported incidents has increased.
B. The information security department actively monitors security operations.
C. The number of reported incidents has decreased.
D. IT security staff implements strict technical security controls.

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 144
Which of the following types of controls would be **MOST** important to implement when digitizing human resource (HR) records?

A. Change management controls
B. Software development controls
C. Project management controls
D. Access management controls

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 145
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 146
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.
D. Organizational standards are documented in operational procedures.

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 147
What should be a security manager's **PRIMARY** objective in the event of a security incident?

A. Identify the source of the breach and how it was perpetrated.
B. Contain the threat and restore operations in a timely manner.
C. Ensure that normal operations are not disrupted.
D. Identify lapses in operational control effectiveness.

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
QUESTION 148
Which of the following is the **BEST** indication that an information security program is effective?

A. The number of reported and confirmed security incidents has increased after awareness training.
B. The security awareness program was developed following industry best practices.
C. The security team has performed a risk assessment to understand the organization's risk appetite.
D. The security team is knowledgeable and uses the best available tools.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 149
Which of the following would be of **GREATEST** concern to an IS auditor receiving an organization's security incident handling procedures?

A. Annual tabletop exercises are performed instead of functional incident response exercises.
B. Roles for computer emergency response team (CERT) members have not been formally documented.
C. Guidelines for prioritizing incidents have not been identified.
D. Workstation antivirus software alerts are not regularly reviewed.

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 150
An organization has suffered a number of incidents in which USB flash drives with sensitive data have been lost. Which of the following be **MOST** effective in preventing loss of sensitive data?

A. Modifying the disciplinary policy to be more stringent
B. Implementing a check-in/check-out process for USB flash drives
C. Issuing encrypted USB flash drives to staff
D. Increasing the frequency of security awareness training

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 151
Which of the following backup schemes is the **BEST** option when storage media is limited?

A. Virtual backup
B. Real-time backup
C. Differential backup
D. Full backup

Correct Answer: C

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 152
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 153
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

Explanation/Reference:

QUESTION 154
Which of the following is the **BEST** way to increase the effectiveness of security incident detection?

A. Educating end users on identifying suspicious activity
B. Establishing service level agreements (SLAs) with appropriate forensic service providers

C. Determining containment activities based on the type of incident
D. Documenting root cause analysis procedures

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 155
Which of the following is a passive attack on a network?

A. 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 156
Which of the following is the **MAIN** purpose of an information security management system?

A. To enhance the impact of reports used to monitor information security incidents
B. To reduce the frequency and impact of information security incidents
C. To identify and eliminate the root causes of information security incidents
D. To keep information security policies and procedures up-to-date

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 157

Which of the following would be an **INAPPROPRIATE** activity for a network administrator?

A. Analyzing network security incidents
B. Prioritizing traffic between subnets
C. Modifying a router configuration
D. Modifying router log files

Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:

QUESTION 158
There is a concern that a salesperson may download an organization's full customer list from the Software as a Service (SaaS) when leaving to work for a competitor. Which of the following would **BEST** help to identify this type of incident?

A. Monitor applications logs
B. Disable remote access to the application
C. Implement a web application firewall
D. Implement an intrusion detection system (IDS)

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 159
Which of the following is the **MOST** important incident management consideration for an organization subscribing to a cloud service?

A. Decision on the classification of cloud-hosted data
B. Expertise of personnel providing incident response
C. Implementation of a SIEM in the organization
D. An agreement on the definition of a security incident

Correct Answer: D

Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 160
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 161
An information security manager is preparing an incident response plan. Which of the following is the **MOST** important consideration when responding to an incident involving sensitive customer data?

A. The assignment of a forensics teams
B. The ability to recover from the incident in a timely manner
C. Following defined post-incident review procedures
D. The ability to obtain incident information in a timely manner

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 162
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

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:
QUESTION 163
The effectiveness of an incident response team will be **GREATEST** when:

A. the incident response process is updated based on lessons learned
B. incidents are identified using a security information and event monitoring (SIEM) system
C. the incident response team members are trained security personnel
D. the incident response team meets on a regular basis to review log files

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 164
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 165

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)
D. learn of potential areas of improvement

Correct Answer: D
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 166
When developing an incident response plan, the information manager should:

A. allow IT to decide which systems can be removed from the infrastructure
B. include response scenarios that have been approved previously by business management
C. require IT to invoke the business continuity plan
D. determine recovery time objectives (RTOs)

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 167
Which of the following should be done **FIRST** when handling multiple confirmed incidents raised at the same time?

A. 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 168
Which of the following is the **BEST** indication of a successful information security culture?

A. Penetration testing is done regularly and findings remediated.
B. End users know how to identify and report incidents. C. Individuals are given access based on job functions.
D. The budget allocated for information security is sufficient.

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 169
Which of the following **BEST** contributes to the successful management of security incidents?

A. Tested controls
B. Established procedures
C. Established policies
D. Current technologies

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 170
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 171
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 172
An external security audit risk has reported multiple instances of control noncompliance. Which of the following would be **MOST** important for the information security manager to communicate to senior management?

A. The impact of noncompliance on the organization's risk profile
B. An accountability report to initiate remediation activities
C. A plan for mitigating the risk due to noncompliance
D. Control owner responses based on a root cause analysis

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 173
Which of the following is the **MOST** important outcome of effective risk treatment?
A. Timely reporting of incidents
B. Elimination of risk
C. Implementation of corrective actions
D. Reduced cost of maintaining controls

Correct Answer: C
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 174
To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:

A. rely on senior management to enforce security
B. promote the relevance and contribution of security
C. reiterate the necessity of security
D. focus on compliance

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 175
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 176
Which of the following is the **MOST** important reason for logging firewall activity?

A. Intrusion detection
B. Auditing purposes
C. Firewall tuning
D. Incident investigation

Correct Answer: B
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 177
The **PRIMARY** purpose of a security information and event management (SIEM) system is to:

A. identify potential incidents
B. provide status of incidents
C. resolve incidents
D. track ongoing incidents

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 178
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 179
Information security awareness programs are **MOST** effective when they are:

A. customized for each target audience
B. conducted at employee orientation
C. reinforced by computer-based training
D. sponsored by senior management

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 180
An information security manager has discovered a potential security breach in a server that supports a critical business process. Which of the following should be the information security manager's **FIRST** course of action?

A. Validate that there has been an incident
B. Notify the business process owner
C. Shut down the server in an organized manner
D. Inform senior management of the incident

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:

QUESTION 181
Which of the following is the **MOST** important outcome of testing incident response plans?

A. Internal procedures are improved.
B. An action plan is available for senior management.
C. Staff is educated about current threats.
D. Areas requiring investment are identified.

Correct Answer: A
Section: Information System Operations, Maintenance and Support Explanation

Explanation/Reference:

QUESTION 182
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 183
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 184
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 185
An IS auditor is reviewing the remote access methods of a company used to access system remotely. Which of the following is LEAST preferred remote access method from a security and control point of view?

A. RADIUS
B. TACACS
C. DIAL-UP
D. DIAMETER

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Dial-up connectivity not based on centralize control and least preferred from security and control standpoint.

Remote access user can connect remotely to their organization's networks with the same level of functionality as if they would access from within their office.

In connecting to an organization's network, a common method is to use dial-up lines. Access is granted through the organization's network access server (NAS) working in concert with an organization network firewall and router. The NAS handle user authentication, access control and accounting while maintaining connectivity. The most common protocol for doing this is the Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Controller System (TACACS).

Remote access Controls include:

Policy and standard
Proper authorization

Identification and authentication mechanism
Encryption tool and technique such as use of VPN System
and network management

The following reference(s) were/was used to create this question:
CISA Review Manual 2014 Page number 334

QUESTION 186
There are many types of audit logs analysis tools available in the market. Which of the following audit logs analysis tools will look for anomalies in user or system behavior?

A. Attack Signature detection tool
B. Variance detection tool
C. Audit Reduction tool
D. Heuristic detection tool

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Trend/Variance Detection tool are used to look for anomalies in user or system behavior. For example, if a user typically logs in at 9:00 am, but one day suddenly access the system at 4:30 am, this may indicate a security problem that may need to be investigated. Other types of audit trail analysis tools should also be known for your CISA exam

The following were incorrect answers:
Audit Reduction tool - They are preprocessor designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tool can remove many audit records known to have little security significance.

Attack-signature detection tool - They look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed logon attempts.
Heuristic detection tool - Heuristic analysis is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. MultiCriteria analysis (MCA) is one of the means of weighing. This method differs with statistical analysis, which bases itself on the available data/statistics.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 336 and

http://en.wikipedia.org/wiki/Heuristic_analysis

QUESTION 187
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:
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

The following reference(s) were/was used to create this question:

Reference used - CISA review manual 2014. Page number 338

QUESTION 188
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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 34

QUESTION 189
Which of the following statement correctly describes difference between packet filtering firewall and stateful inspection firewall?

A. Packet filtering firewall do not maintain client session whereas Stateful firewall maintains client session.
B. Packet filtering firewall and Stateful firewall both maintain session of client.
C. Packet filtering firewall is a second generation firewall whereas Stateful is a first generation of firewall.
D. Packet filtering firewall and Stateful firewall do not maintain any session of client.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Packet Filtering Firewall

Also Known as First Generation Firewall
Do not maintain client session
The advantage of this type of firewall are simplicity and generally stable performance since the filtering rules are performed at the network layer.
Its simplicity is also disadvantage, because it is vulnerable to attack from improperly configured filters and attack tunneled over permitted services.
Some of the more common attack on packet filtering are IP Spoofing, Source Routing specification, Miniature fragment attack.

Stateful Inspection Firewall
A stateful inspection firewall keep track of the destination IP address of each packet that leaves the organization's internal network.
The session tracking is done by mapping the source IP address of incoming packet with the list of destination IP addresses that is maintained and updated
This approach prevent any attack initiated and originated by outsider.
The disadvantage includes stateful inspection firewall can be relatively complex to administer as compare to other firewall.

The following were incorrect answers:

All other choices presented were incorrect answers because they all had the proper definition.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 345 and 346

QUESTION 190
There are many firewall implementations provided by firewall manufacturers. Which of the following implementation utilize two packet filtering routers and a bastion host? This approach creates the most secure firewall system since it supports network and application level security while defining a separate DMZ.

A. Dual Homed firewall
B. Screened subnet firewall
C. Screened host firewall
D. Anomaly based firewall

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
In network security, a screened subnet firewall is a variation of the dual-homed gateway and screened host firewall. It can be used to separate components of the firewall onto separate systems, thereby achieving greater throughput and flexibility, although at some cost to simplicity. As each component system of the screened subnet firewall needs to implement only a specific task, each system is less complex to configure. A screened subnet firewall is often used to establish a demilitarized zone (DMZ).

Below are few examples of Firewall implementations: Screened

host Firewall

Utilizing a packet filtering router and a bastion host, this approach implements a basic network layer security and application server security.
An intruder in this configuration has to penetrate two separate systems before the security of the private network can be compromised
This firewall system is configured with the bastion host connected to the private network with a packet filtering router between internet and the bastion host Dual-

homed Firewall

A firewall system that has two or more network interface, each of which is connected to a different network
In a firewall configuration, a dual homed firewall system usually acts to block or filter some or all of the traffic trying to pass between the network A dual-homed firewall system is more restrictive form of screened-host firewall system

Demilitarize Zone (DMZ) or screened-subnet firewall

Utilizing two packet filtering routers and a bastion host
This approach creates the most secure firewall system since it supports network and application level security while defining a separate DMZ network Typically, DMZs are configured to limit access from the internet and organization's private network.

The following were incorrect answers:

The other types of firewall mentioned in the option do not utilize two packet filtering routers and a bastion host.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 346

QUESTION 191
Which of the following type of IDS has self-learning functionality and over a period of time will learned what is the expected behavior of a system?

A. Signature Based IDS
B. Host Based IDS
C. Neural Network based IDS
D. Statistical based IDS

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Neural Network based IDS monitors the general patterns of activity and traffic on the network, and create a database of normal activities within the system. This is similar to statistical model but with added self-learning functionality.

Also, you should know below categories and types of IDS for CISA exam:

An IDS works in conjunction with routers and firewall by monitoring network usage anomalies.

Broad category of IDS includes:

Network based IDS
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

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.

Types of IDS includes

Signature Based IDS – These IDS system protect against detected intrusion patterns. The intrusive pattern they can identify are stored in the form of signature.
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

The following were incorrect answers:

The other types of IDS mentioned in the options do not monitor general patterns of activities and contains self-learning functionalities.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 346 and 347

QUESTION 192
Which of the following type of an IDS resides on important systems like database, critical servers and monitors various internal resources of an operating system?

A. Signature based IDS
B. Host based IDS
C. Network based IDS
D. Statistical based IDS

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Host Based IDS resides on important systems like database, critical servers and monitors various internal resources of an operating system.
Also, you should know below mentioned categories and types of IDS for CISA exam

An IDS works in conjunction with routers and firewall by monitoring network usage anomalies. Broad categories of IDS include:

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 types of IDS mentioned in the options do not resides on important systems like database and critical servers

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 346 and 347

QUESTION 193
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:

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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 346 and 347

QUESTION 194
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:
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.

The following reference(s) were/was used to create this question:

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 195
Which of the following type of honey pot essentially gives a hacker a real environment to attack?

A. High-interaction
B. Low-interaction
C. Med-interaction
D. None of the choices

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: http://www.ce-infosys.com/english/free_compusec/free_compusec.aspx High-interaction

type of honey pot essentially gives an attacker a real environment to attack.

Also, you should know below information about honey pot for CISA exam:

A Honey pot is a software application that pretends to be an unfortunate server on the internet and is not set up actively protect against break-ins.
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:

Med-interaction – Not a real type of honey pot

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348
http://en.wikipedia.org/wiki/Honeypot_%28computing%29

QUESTION 196
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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348

QUESTION 197
Which of the following statement correctly describes the difference between symmetric key encryption and asymmetric key encryption?

A. In symmetric key encryption the same key is used for encryption and decryption where as asymmetric key uses private key for encryption and decryption
B. In symmetric key encryption the public key is used for encryption and the symmetric key for decryption. Where as in asymmetric key encryption the public key is used for encryption and private key is used for decryption
C. In symmetric key encryption the same key is used for encryption and decryption where as in asymmetric key encryption the public key is used for encryption and private key is used for decryption.
D. Both uses private key for encryption and the decryption process can be done using public key

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
There are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption.)

Symmetric 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. Few examples of symmetric key algorithms are DES, AES, Blowfish, etc

Asymmetric Encryption
The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is the usage of asymmetric encryption, in which there are two related keys, usually called a key pair. The public key is made freely available to anyone who might want to send you a message. The second key, called the private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted using the public key can only be decrypted by the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public).A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message. Few examples of asymmetric key algorithms are RSA, Elliptic key Cryptography (ECC), El Gamal, Differ-Hellman, etc

The following were incorrect answers:

The other options don't describe correctly the difference between symmetric key and asymmetric key encryption.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348 and 349
http://support.microsoft.com/kb/246071

QUESTION 198
Which policy helps an auditor to gain a better understanding of biometrics system in an organization?

A. BIMS Policy
B. BOMS Policy
C. BMS Policy
D. BOS Policy

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The auditor should use a Biometric Information Management System (BIMS) Policy to gain better understanding of the biometric system in use.

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.

Management should develop and approve a Biometric Information Management and Security (BIMS) policy. The auditor should use the BIMS policy to gain better understanding of the biometric system in use. With respect to testing, the auditor should make sure this policy has been developed and biometric information system is being secured appropriately.

The identification and authentication procedures for individual enrollment and template creation should be specified in BIMS policy.

The following were incorrect answers:

All other choices presented were incorrect answers because they are not valid policies.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 331 and 332

QUESTION 199
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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 331
http://en.wikipedia.org/wiki/Biometrics

QUESTION 200
The goal of an information system is to achieve integrity, authenticity and non-repudiation of information's sent across the network. Which of the following statement correctly describe the steps to address all three?

A. Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message.
B. Encrypt the message digest using receiver's public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key.
C. Encrypt the message digest using sender's public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key.
D. Encrypt message digest using sender's private key and then send the encrypted digest to the receiver along with original message. Receiver can decrypt the same using sender's public key.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The digital signature is used to achieve integrity, authenticity and non-repudiation. In a digital signature, the sender's private key is used to encrypt the message digest of the message. Encrypting the message digest is the act of Signing the message. The receiver will use the matching public key of the sender to decrypt the Digital Signature using the sender's public key.

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures cannot be forged by someone else who does not possess the private key, it can also be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real and has not been modified since the day it was issued.

How Digital Signature Works
Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

You copy-and-paste the contract (it's a short one!) into an e-mail note.
Using special software, you obtain a message hash (mathematical summary) of the contract.
You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

To make sure it's intact and from you, your lawyer makes a hash of the received message.
Your lawyer then uses your public key to decrypt the message hash or summary.
If the hashes match, the received message is valid.

Below are some common reasons for applying a digital signature to communications:

Authentication
Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. The importance of high assurance in the sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a serious mistake.

Integrity
In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it.(Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after the signature has been applied would invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that authentication, non-repudiation, and other properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". This is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen.

Tip for the exam
Digital Signature does not provide confidentiality. It provides only authenticity and integrity. The sender's private key is used to encrypt the message digest to calculate the digital signature

Encryption provides only confidentiality. The receiver's public key or symmetric key is used for encryption

The following were incorrect answers:

Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message - Symmetric key encryption does not provide non-repudiation as symmetric key is shared between users

Encrypt the message digest using receiver's public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key - Receiver's public key is known to everyone. This will not address non-repudiation

Encrypt the message digest using sender's public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key -The sender public key is known to everyone. If sender's key is used for encryption, then sender's private key is required to decrypt data. The receiver will not be able to decrypt the digest as receiver will not have sender's private key.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 331
http://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg
http://en.wikipedia.org/wiki/Digital_signature http://searchsecurity.techtarget.com/definition/digital-signature

QUESTION 201
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:
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.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348

QUESTION 202
Which of the following process consist of identification and selection of data from the imaged data set in computer forensics?

A. Investigation
B. Interrogation

C. Reporting
D. Extraction

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Extraction is the process 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.

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:

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.
Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

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.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 367 and 368

QUESTION 203
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:
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.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 369

QUESTION 204
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:
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.

The Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 369

QUESTION 205
Which of the following is an environmental issue caused by electric storms or noisy electric equipment and may also cause computer system to hang or crash?

A. Sag
B. Blackout
C. Brownout
D. EMI

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
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.

Because Unshielded Twisted Pair cables does not have shielding like shielded twisted-pair cables, UTP is susceptible to interference from external electrical sources, which could reduce the integrity of the signal. Also, to intercept transmitted data, an intruder can install a tap on the cable or monitor the radiation from the wire. Thus, UTP may not be a good choice when transmitting very sensitive data or when installed in an environment with much electromagnetic interference (EMI) or radio frequency interference (RFI). Despite its drawbacks, UTP is the most common cable type. UTP is inexpensive, can be easily bent during installation, and, in most cases, the risk from the above drawbacks is not enough to justify more expensive cables.

For your 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.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number372
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6507-6512). Acerbic Publications. Kindle Edition.

QUESTION 206
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:
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.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number372

QUESTION 207
Which of the following statement is NOT true about smoke detector?

A. The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised in the computer room floor
B. The smoke detector should produce an audible alarm when activated and be linked to a monitored station
C. The location of the smoke detector should be marked on the tiling for easy identification and access
D. Smoke detector should replace fire suppression system

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The word NOT is the keyword used in the question. You need to find out a statement which is not applicable to smoke detector. Smoke detector should supplement, not replace, fire suppression system.

For CISA exam you should know below information about smoke detector.

The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised computer room floor. The smoke detector should produce an audible alarm when activated be linked to a monitored station The location of the smoke detector should be marked on the tiling for easy identification and access. Smoke detector should supplement, not replace, fire suppression system The following were incorrect answers:

The other presented options are valid statement about smoke detector.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number373

QUESTION 208

Which of the following statement correctly describes the difference between total flooding and local application extinguishing agent?

A. The local application design contain physical barrier enclosing the fire space where as physical barrier is not present in total flooding extinguisher
B. The total flooding design contain physical barrier enclosing the fire space where as physical barrier is not present in local application design extinguisher
C. The physical barrier enclosing fire space is not present in total flooding and local application extinguisher agent
D. The physical barrier enclosing fire space is present in total flooding and local application extinguisher agent

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
For CISA exam you should know below information about Fire Suppression Systems

Fire Suppression System
This system is designed to automatically activate immediately after detection of heat, typically generated by fire. Like smoke detectors, the system will produce an audible alarm when activated and be linked to a central guard station that is regularly monitored. The system should also be inspected and tested annually. Testing interval should comply with industry and insurance standard and guideline.

Broadly speaking there are two methods for applying an extinguisher agent: total flooding and local application.

Total Flooding - System working under total flooding application apply an extinguishing agent to a three dimensional enclosed space in order to achieve a concentration of the agent (volume percentage of agent in air) adequate to extinguish the fire. These type of system may be operated automatically by detection and related controls or manually by the operation of a system actuator.

Local Application - System working under a local application principle apply an extinguishing agent directly onto a fire (usually a two dimensional area) or into a three dimensional region immediately surrounding the substance or object on a fire. The main difference between local application and total flooding design is the absence of physical barrier enclosing the fire space in the local application design.

The medium of fire suppression varies but usually one of the following:

Water based systems are typically referred to as sprinkler system. These systems are effective but are also unpopular because they damage equipment and property. The system can be dry-pipe or charged (water is always in system piping). A charged system is more reliable but has the disadvantage of exposing the facility to expensive water damage if the pipe leak or break.

Dry-pipe sprinkling system do not have water in the pipe until an electronic fire alarm activates the water to send water into system. This is opposed to fully charged water pipe system. Dry-pipe system has the advantage that any failure in the pipe will not result in water leaking into sensitive equipment from above. Since water and electricity do not mix these systems must be combined with an automatic switch to shut down the electric supply to the area protected.

Holon system releases pressurize halos gases that removes oxygen from air, thus starving the fire. Holon was popular because it is an inert gas and does not damage and does not damage equipment like water does. Because halos adversely affect the ozone layer, it was banned in Montreal (Canada) protocol 1987,

which stopped Holon production as of 1 January 1994. As a banned gas, all Holon installation are now required by international agreement to be removed. The Holon substitute is FM-200, which is the most effective alternative.

FM-220TM: Also called heptafluoropropane, HFC-227 or HFC-227ea(ISO Name)is a colorless odorless gaseous fire suppression agent. It is commonly used as a gaseous fire suppression agent.

Aragonite is the brand name for a mixture of 50% argon and 50% nitrogen. It is an inert gas used in gaseous fire suppression systems for extinguishing fires where damage to equipment is to be avoided. Although argon is a nontoxic, it does not satisfy the body's need for oxygen and is simple asphyxiate.

CO2 system releases pressurized carbon dioxide gas into the area protected to replace the oxygen required for combustion. Unlike halos and its later replacement, however, CO2 is unable to sustain human life. Therefore, in most of countries it is illegal to for such a system to be set to automatic release if any human may be in the area. Because of this, these systems are usually discharged manually, introducing an additional delay in combating fire.

The following were incorrect answers:

The other presented options do not describe valid difference between total flooding and local application extinguishing agent.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 373 and 374

QUESTION 209
Which of the following type of lock uses a numeric keypad or dial to gain entry?

A. Bolting door locks
B. Cipher lock
C. Electronic door lock
D. Biometric door lock

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The combination door lock or cipher lock uses a numeric key pad, push button, or dial to gain entry, it is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.

A cipher lock, is controlled by a mechanical key pad, typically 5 to 10 digits that when pushed in the right combination the lock will releases and allows entry. The drawback is someone looking over a shoulder can see the combination. However, an electric version of the cipher lock is in production in which a display screen

will automatically move the numbers around, so if someone is trying to watch the movement on the screen they will not be able to identify the number indicated unless they are standing directly behind the victim.

Remember locking devices are only as good as the wall or door that they are mounted in and if the frame of the door or the door itself can be easily destroyed then the lock will not be effective. A lock will eventually be defeated and its primary purpose is to delay the attacker.

For your exam you should know below types of lock

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique physical attribute such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when sensitive facilities must be protected such as in the military.

Electronic door lock – This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

The following were incorrect answers:

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique body features such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.

Electronic door lock – This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 376
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25144-25150). Acerbic Publications. Kindle Edition.

QUESTION 210
Which of the following type of lock uses a magnetic or embedded chip based plastic card key or token entered into a sensor/reader to gain access?

A. Bolting door locks
B. Combination door lock
C. Electronic door lock
D. Biometric door lock

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Electronic door lock uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

For CISA exam you should know below types of lock

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique body features such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.

Electronic door lock – This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

The Combination door lock or cipher lock uses a numeric key pad or dial to gain entry, and is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.

The following were incorrect answers:

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique body features such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.

The Combination door lock or cipher lock uses a numeric key pad or dial to gain entry, and is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 376

QUESTION 211
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:
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.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 310

QUESTION 212
Which of the following attack redirects outgoing message from the client back onto the client, preventing outside access as well as flooding the client with the sent packets?

A. Banana attack
B. Brute force attack
C. Buffer overflow
D. Pulsing Zombie

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
A "banana attack" is another particular type of DoS. It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets.

The Banana attack uses a router to change the destination address of a frame. In the Banana attack:

A compromised router copies the source address on an inbound frame into the destination address.
The outbound frame bounces back to the sender.
This sender is flooded with frames and consumes so many resources that valid service requests can no longer be processed.

The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 321

QUESTION 213
Which of the following attack is against computer network and involves fragmented or invalid ICMP packets sent to the target?

A. Nuke attack
B. Brute force attack
C. Buffer overflow
D. Pulsing Zombie

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
A Nuke attack is an old denial-of-service attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.

A specific example of a nuke attack that gained some prominence is the Win Nuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A string of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a Blue Screen of Death (BSOD).

The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 322

QUESTION 214
Which of the following attack involves sending forged ICMP Echo Request packets to the broadcast address on multiple gateways in order to illicit responses from the computers behind the gateway where they all respond back with ICMP Echo Reply packets to the source IP address of the ICMP Echo Request packets?

A. Reflected attack
B. Brute force attack
C. Buffer overflow
D. Pulsing Zombie

Correct Answer: A
Section: Protection of Information Assets
Explanation

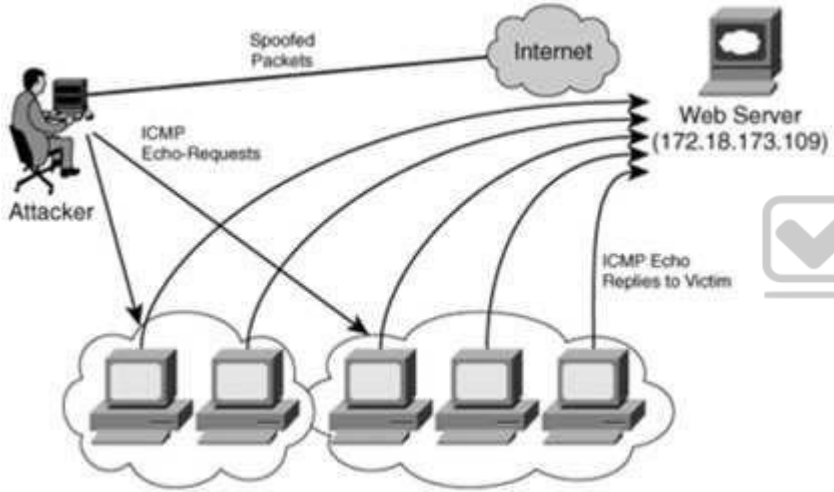
Explanation/Reference:
Reflected attack involves sending forged requests to a large number of computers that will reply to the requests. The source IP address is spoofed to that of the targeted victim, causing replies to flood.

A distributed denial of service attack may involve sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. (This reflected attack form is sometimes called a "DRDOS".

ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mix-configured networks, thereby enticing hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack.

In the surf attack, the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to a victim's network broadcast address. This means that each system on the victim's subnet receives an ICMP ECHO REQUEST packet. Each system then replies to that request with an ICMP ECHO REPLY packet to the spoof address provided in the packets—which is the victim's address. All of these response packets go to the victim system and overwhelm it because it is being bombarded with packets it does not necessarily know how to process. The victim system may freeze, crash, or reboot. The Smurf attack is illustrated in Figure below:

surf-attack



The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers,

corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 322

QUESTION 215
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:
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.

Following reference(s) were/was used to create this question:

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 216

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:

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.

Following reference(s) were/was used to create this question:
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 217
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:
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.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 322

QUESTION 218
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:
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.

Following reference(s) were/was used to create this question:

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 219
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:
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.

Following reference(s) were/was used to create this question:
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 220
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:
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.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 330 and 331

Official ISC2 guide to CISSP CBK 3rd Edition Page number 924

QUESTION 221
Which of the following attack could be avoided by creating more security awareness in the organization and provide adequate security knowledge to all employees?

A. surf attack
B. Traffic analysis
C. Phishing
D. Interrupt attack

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Phishing techniques include social engineering, link manipulation, spear phishing, whaling, dishing, 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 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.

Following reference(s) were/was used to create this question:

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 222
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:

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.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 314
Official ISC2 guide to CISSP CBK 3rd Edition Page number 350

QUESTION 223
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:

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.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 338

QUESTION 224
During an IS audit, one of your auditor has observed that some of the critical servers in your organization can be accessed ONLY by using shared/common user name and password. What should be the auditor's PRIMARY concern be with this approach?

A. Password sharing
B. Accountability
C. Shared account management
D. Difficulty in auditing shared account

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The keyword PRIMARY is used in the question. Accountability should be the primary concern if critical servers can be accessed only by using shared user id and password. It would be very difficult to track the changes done by employee on critical server.

For your exam you should know the information below:

Accountability
Ultimately one of the drivers behind strong identification, authentication, auditing and session management is accountability. Accountability is fundamentally about being able to determine who or what is responsible for an action and can be held responsible. A closely related information assurance topic is non-repudiation. Repudiation is the ability to deny an action, event, impact or result. Non-repudiation is the process of ensuring a user may not deny an action. Accountability relies heavily on non-repudiation to ensure users, processes and actions may be held responsible for impacts.

The following contribute to ensuring accountability of actions:
Strong identification
Strong authentication
User training and awareness
Comprehensive, timely and thorough monitoring
Accurate and consistent audit logs
Independent audits
Policies enforcing accountability
Organizational behavior supporting accountability

The following answers are incorrect:

The other options are also valid concern. But the primary concern should be accountability.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 328 and 329
Official ISC2 guide to CISSP CBK 3rd Edition Page number 114

QUESTION 225
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:
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.

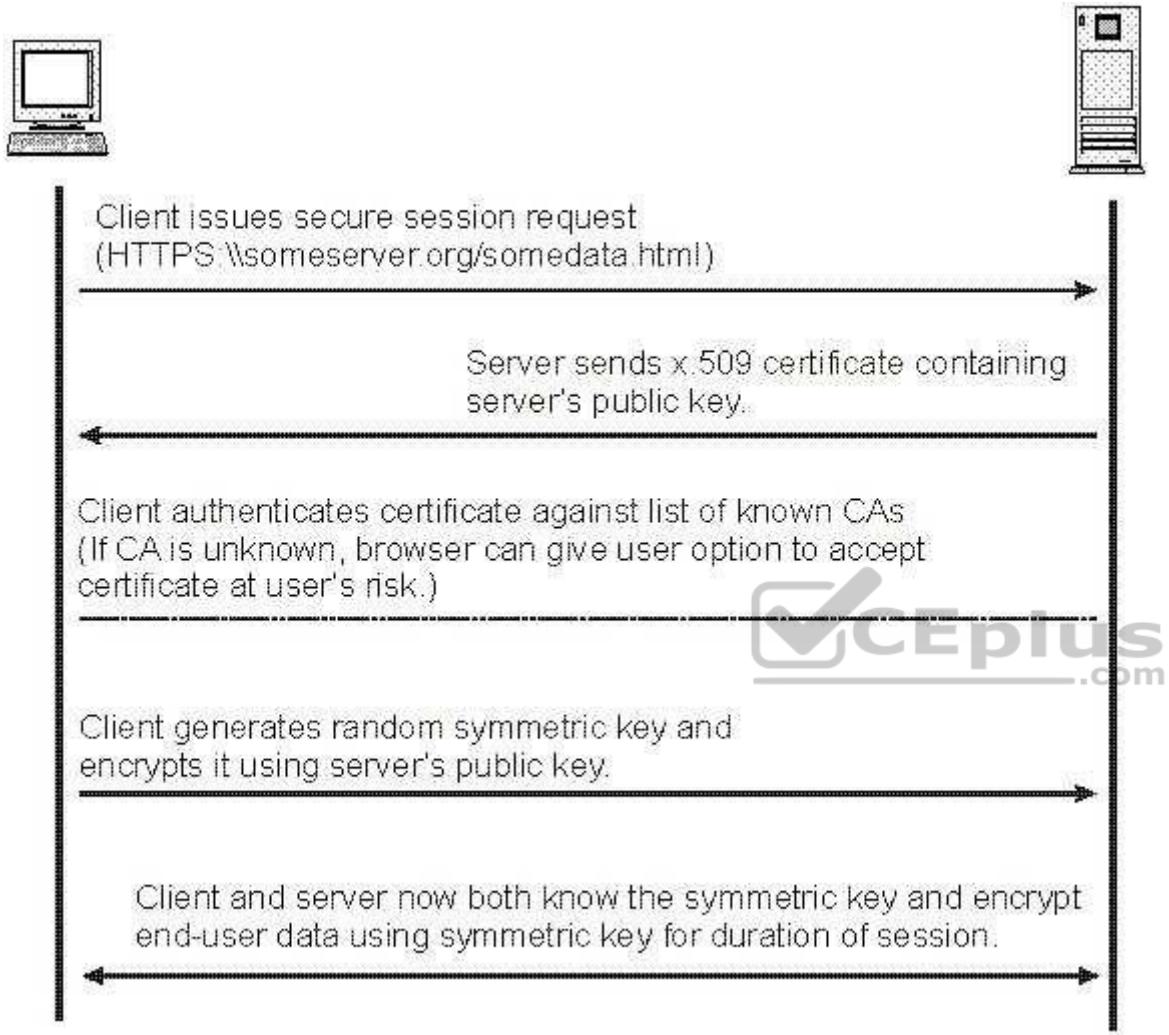
Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client 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).

Following reference(s) were/was used to create this question:
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 226
Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

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: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
PERMANENTLY is the keyword used in the question. You need to find out data removal method which remove data permanently from magnetic media.

Degaussing is the most effective method out of all provided choices to erase sensitive data on magnetic media provided magnetic media is not requiring to be reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

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 the 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 is 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:

Overwrite every sector of magnetic media with pattern of 1's and 0's-Less effective than degaussing provided magnetic media is not requiring to be reuse.
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.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 338
Official ISC2 guide to CISSP CBK 3rd Edition Page number 720.

QUESTION 227
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 228
Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

A. Field checks
B. Control totals
C. Reasonableness checks
D. A before-and-after maintenance report

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

QUESTION 229

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Blackbox test
B. Desk checking
C. Structured walk-through
D. Design and code

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A blackbox test is a dynamic analysis tool for testing software modules. During the testing of software modules, a blackbox test works first in a cohesive manner as one single unit/entity, consisting of numerous modules and second, with the user data that flows across software modules. In some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and someone closely examines it by applying their mind, without actually activating the software. Therefore, these cannot be referred to as dynamic analysis tools.

QUESTION 230
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 231
Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

A. Router
B. Bridge
C. Repeater
D. Gateway

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A bridge connects two separate networks to form a logical network (e.g., joining an Ethernet and token network) and has the storage capacity to store frames and act as a storage and forward device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet.

QUESTION 232
Which of the following is a benefit of using callback devices?

A. Provide an audit trail
B. Can be used in a switchboard environment
C. Permit unlimited user mobility
D. Allow call forwarding

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

QUESTION 233
A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

A. dials back to the user machine based on the user id and password using a telephone number from its database.
B. dials back to the user machine based on the user id and password using a telephone number provided by the user during this connection.
C. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its database.

D. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender's database.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A call-back system in a net centric environment would mean that a user with an id and password calls a remote server through a dial-up line first, and then the server disconnects and dials back to the user machine based on the user id and password using a telephone number from its database. Although the server can depend upon its own database, it cannot know the authenticity of the dialer when the user dials again. The server cannot depend upon the sender's database to dial back as the same could be manipulated.

QUESTION 234
Structured programming is BEST described as a technique that:

A. provides knowledge of program functions to other programmers via peer reviews.
B. reduces the maintenance time of programs by the use of small-scale program modules.
C. makes the readable coding reflect as closely as possible the dynamic execution of the program.
D. controls the coding and testing of the high-level functions of the program in the development process.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well-known restriction of the style, since go-to statements were common at the time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

QUESTION 235
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 236
An offsite information processing facility having 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.

QUESTION 237
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 238
In an EDI process, the device which transmits and receives electronic documents is the:

A. communications handler.
B. EDI translator.
C. application interface.
D. EDI interface.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs).

QUESTION 239
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 240
Which of the following network configuration options contains a direct link between any two host machines?

A. Bus
B. Ring
C. Star
D. Completely connected (mesh)

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A completely connected mesh configuration creates a direct link between any two host machines.

QUESTION 241
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 242
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 243
A data administrator is responsible for:

A. maintaining database system software.
B. defining data elements, data names and their relationship.
C. developing physical database structures.
D. developing data dictionary system software.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

QUESTION 244
A database administrator is responsible for:

A. defining data ownership.
B. establishing operational standards for the data dictionary.
C. creating the logical and physical database.
D. establishing ground rules for ensuring data integrity and security.

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

QUESTION 245
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 246
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 247
If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

A. IT cannot be implemented if senior management is not committed to strategic planning.
B. More likely.
C. Less likely.
D. Strategic planning does not affect the success of a company's implementation of IT.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A company's implementation of IT will be less likely to succeed if senior management is not committed to strategic planning.

QUESTION 248
Which of the following could lead to an unintentional loss of confidentiality?

A. Lack of employee awareness of a company's information security policy
B. Failure to comply with a company's information security policy
C. A momentary lapse of reason
D. Lack of security policy enforcement procedures

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Lack of employee awareness of a company's information security policy could lead to an unintentional loss of confidentiality.

QUESTION 249
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 250
An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

A. Evidence collected through personal observation
B. Evidence collected through systems logs provided by the organization's security administration C. Evidence collected through surveys collected from internal staff
D. Evidence collected through transaction reports provided by the organization's IT administration

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor usually places more reliance on evidence directly collected, such as through personal observation.

QUESTION 251
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 252
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 253
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 254
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 255
Why does the IS auditor often review the system logs?

A. To get evidence of password spoofing
B. To get evidence of data copy activities
C. To determine the existence of unauthorized access to data by a user or program
D. To get evidence of password sharing

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When trying to determine the existence of unauthorized access to data by a user or program, the IS auditor will often review the system logs.

QUESTION 256
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 257
How is risk affected if users have direct access to a database at the system level?

A. Risk of unauthorized access increases, but risk of untraceable changes to the database decreases.
B. Risk of unauthorized and untraceable changes to the database increases.
C. Risk of unauthorized access decreases, but risk of untraceable changes to the database increases.
D. Risk of unauthorized and untraceable changes to the database decreases.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If users have direct access to a database at the system level, risk of unauthorized and untraceable changes to the database increases.

QUESTION 258
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 259
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 260
What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program?

A. Network-monitoring software
B. A system downtime log
C. Administration activity reports
D. Help-desk utilization trend reports

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

A system downtime log can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program.

QUESTION 261
What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information?

A. Referential integrity controls
B. Normalization controls
C. Concurrency controls
D. Run-to-run totals

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Concurrency controls are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information.

QUESTION 262
What increases encryption overhead and cost the most?

A. A long symmetric encryption key
B. A long asymmetric encryption key
C. A long Advance Encryption Standard (AES) key
D. A long Data Encryption Standard (DES) key

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A long asymmetric encryption key (public key encryption) increases encryption overhead and cost. All other answers are single shared symmetric keys.

QUESTION 263
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 264
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 265
What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

A. With public-key encryption, or symmetric encryption
B. With public-key encryption, or asymmetric encryption
C. With shared-key encryption, or symmetric encryption
D. With shared-key encryption, or asymmetric encryption

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
With public key encryption or asymmetric encryption, data is encrypted by the sender using the recipient's public key; the data is then decrypted using the recipient's private key.

QUESTION 266
How does the SSL network protocol provide confidentiality?

A. Through symmetric encryption such as RSA
B. Through asymmetric encryption such as Data Encryption Standard, or DES
C. Through asymmetric encryption such as Advanced Encryption Standard, or AES
D. Through symmetric encryption such as Data Encryption Standard, or DES

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption. Standard, or DES.

QUESTION 267
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 268

Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

A. Concurrency controls
B. Reasonableness checks
C. Time stamps
D. Referential integrity controls

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference: Explanation:
Time stamps are an effective control for detecting duplicate transactions such as payments made or received.

QUESTION 269
Which of the following is a good control for protecting confidential data residing on a PC?

A. Personal firewall
B. File encapsulation
C. File encryption
D. Host-based intrusion detection

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
File encryption is a good control for protecting confidential data residing on a PC.

QUESTION 270
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 271
What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

A. A combination of public-key cryptography and digital certificates and two-factor authentication
B. A combination of public-key cryptography and two-factor authentication
C. A combination of public-key cryptography and digital certificates
D. A combination of digital certificates and two-factor authentication

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

QUESTION 272
Which of the following do digital signatures provide?

A. Authentication and integrity of data
B. Authentication and confidentiality of data
C. Confidentiality and integrity of data
D. Authentication and availability of data

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary purpose of digital signatures is to provide authentication and integrity of data.

QUESTION 273
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 274
Which of the following would provide the highest degree of server access control?

A. A mantrap-monitored entryway to the server room
B. Host-based intrusion detection combined with CCTV
C. Network-based intrusion detection
D. A fingerprint scanner facilitating biometric access control

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A fingerprint scanner facilitating biometric access control can provide a very high degree of server access control.

QUESTION 275
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 276
Which of the following is often used as a detection and deterrent control against Internet attacks?

A. Honeypots
B. CCTV
C. VPN
D. VLAN

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Honeypots are often used as a detection and deterrent control against Internet attacks.

QUESTION 277
Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

A. A monitored double-doorway entry system
B. A monitored turnstile entry system
C. A monitored doorway entry system

D. A one-way door that does not allow exit after entry

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
A monitored double-doorway entry system, also referred to as a mantrap or deadman door, is used a deterrent control for the vulnerability of piggybacking.

QUESTION 278
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 279
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 280
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 281
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 282
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 283
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 284
Which of the following is used to evaluate biometric access controls?

A. FAR
B. EER
C. ERR
D. FRR

Correct Answer: B
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
When evaluating biometric access controls, a low equal error rate (EER) is preferred. EER is also called the crossover error rate (CER).

QUESTION 285
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 286
Establishing data ownership is an important first step for which of the following processes?

A. Assigning user access privileges
B. Developing organizational security policies
C. Creating roles and responsibilities
D. Classifying data

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To properly implement data classification, establishing data ownership is an important first step.

QUESTION 287
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 288
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 289
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 290
Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

A. Parallel
B. Preparedness
C. Walk-thorough
D. Paper

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Of the three major types of BCP tests (paper, walk-through, and preparedness), a walk-through test requires only that representatives from each operational area meet to review the plan.

QUESTION 291
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 292
Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

A. Cold site
B. Alternate site
C. Hot site
D. Warm site

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

QUESTION 293
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 294

Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

A. Cold site
B. Hot site
C. Alternate site
D. Warm site

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data.

QUESTION 295
Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following?

A. IT strategic plan
B. Business continuity plan
C. Business impact analysis
D. Incident response plan

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

QUESTION 296
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _____. (fill-in-the-blank)

A. Security administrator
B. Systems auditor
C. Board of directors

D. Financial auditor

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the board of directors.

QUESTION 297
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 298
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 299
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 300
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 301
What is a primary high-level goal for an auditor who is reviewing a system development project?

A. To ensure that programming and processing environments are segregated
B. To ensure that proper approval for the project has been obtained
C. To ensure that business objectives are achieved
D. To ensure that projects are monitored and administrated effectively

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A primary high-level goal for an auditor who is reviewing a systems- development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

QUESTION 302
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 303
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 304
Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs.
True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Function point analysis (FPA) provides an estimate of the size of an information system based on the number and complexity of a system's inputs, outputs, and files.

QUESTION 305
The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs
B. recreating program logic using generalized audit software to calculate monthly totals.
C. preparing simulated transactions for processing and comparing the results to predetermined results.
D. automatic flowcharting and analysis of the source code of the calculation programs.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

QUESTION 306
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 307
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 308
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 309
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 310
While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

A. Observe the response mechanism.
B. Clear the virus from the network.
C. Inform appropriate personnel immediately.
D. Ensure deletion of the virus.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The first thing an IS auditor should do after detecting the virus is to alert the organization to its presence, then wait for their response. Choice A should be taken after choice
C. This will enable an IS auditor to examine the actual workability and effectiveness of the response system. An IS auditor should not make changes to the system being audited, and ensuring the deletion of the virus is a management responsibility.

QUESTION 311
A substantive test to verify that tape library inventory records are accurate is:

A. determining whether bar code readers are installed.
B. determining whether the movement of tapes is authorized.
C. conducting a physical count of the tape inventory.
D. checking if receipts and issues of tapes are accurately recorded.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A substantive test includes gathering evidence to evaluate the integrity of individual transactions, data or other information. Conducting a physical count of the tape inventory is a substantive test. Choices A, B and D are compliance tests.

QUESTION 312
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 313
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 314
An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

A. professional independence B.
organizational independence.
C. technical competence.
D. professional competence.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When an IS auditor recommends a specific vendor, they compromise professional independence. Organizational independence has no relevance to the content of an audit report and should be considered at the time of accepting the engagement. Technical and professional competence is not relevant to the requirement of independence.

QUESTION 315
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 316
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 317
The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

A. confirm that the auditors did not overlook any important issues.
B. gain agreement on the findings.
C. receive feedback on the adequacy of the audit procedures.
D. test the structure of the final presentation.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary purpose for meeting with auditees prior to formally closing a review is to gain agreement on the findings. The other choices, though related to the formal closure of an audit, are of secondary importance.

QUESTION 318
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 319
Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

A. include the statement of management in the audit report.
B. identify whether such software is, indeed, being used by the organization.
C. reconfirm with management the usage of the software.
D. discuss the issue with senior management since reporting this could have a negative impact on the organization.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in the report. With respect to this matter, representations obtained from management cannot be independently verified. If the organization is using software that is not licensed, the auditor, to maintain objectivity and independence, must include this in the report.

QUESTION 320
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 321
The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

A. comply with regulatory requirements.
B. provide a basis for drawing reasonable conclusions.
C. ensure complete audit coverage.
D. perform the audit according to the defined scope.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them.
Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

QUESTION 322
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 323
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 324
Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new enterprise resource planning (ERP) implementation?

A. Reviewing a report of security rights in the system
B. Reviewing the complexities of authorization objects
C. Building a program to identify conflicts in authorization
D. Examining recent access rights violation cases

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since the objective is to identify violations in segregation of duties, it is necessary to define the logic that will identify conflicts in authorization. A program could be developed to identify these conflicts. A report of security rights in the enterprise resource planning (ERP) system would be voluminous and time consuming to review; therefore, this technique is not as effective as building a program. As complexities increase, it becomes more difficult to verify the effectiveness of the systems and complexity is not, in itself, a link to segregation of duties. It is good practice to review recent access rights violation cases; however, it may require a significant amount of time to truly identify which violations actually resulted from an inappropriate segregation of duties.

QUESTION 325
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 326
During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

A. Recommend redesigning the change management process.
B. Gain more assurance on the findings through root cause analysis.
C. Recommend that program migration be stopped until the change process is documented.
D. Document the finding and present it to management.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A change management process is critical to IT production systems. Before recommending that the organization take any other action (e.g., stopping migrations, redesigning the change management process), the IS auditor should gain assurance that the incidents reported are related to deficiencies in the change management process and not caused by some process other than change management.

QUESTION 327
During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

A. Dumping the memory content to a file
B. Generating disk images of the compromised system
C. Rebooting the system
D. Removing the system from the network

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

QUESTION 328
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 329
An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

A. Personally delete all copies of the unauthorized software.
B. Inform the auditee of the unauthorized software, and follow up to confirm deletion.
C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management.
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. An IS auditor must convince the user and user management of the risk and the need to eliminate the risk. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing or deleting the unauthorized software.

QUESTION 330
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 331
During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not being checked properly. While preparing the audit report, the IS auditor should:

A. record the observations separately with the impact of each of them marked against each respective finding.
B. advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
C. record the observations and the risk arising from the collective weaknesses.
D. apprise the departmental heads concerned with each observation and properly document it in the report.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure. Choices A and D reflect a failure on the part of an IS auditor to recognize the combined effect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

QUESTION 332
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 333
When preparing an audit report, the IS auditor should ensure that the results are supported by:

A. statements from IS management.
B. workpapers of other auditors.
C. an organizational control self-assessment.
D. sufficient and appropriate audit evidence.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
ISACA's standard on 'reporting' requires the IS auditor have sufficient and appropriate audit evidence to support the reported results. Statements from IS management provide a basis for obtaining concurrence on matters that cannot be verified with empirical evidence. The report should be based on evidence collected during the course of the review even though the auditor may have access to the work papers of other auditors. The results of an organizational control self-assessment (CSA) could supplement the audit findings. Choices A, B and C might be referenced during an audit but, of themselves, would not be considered a sufficient basis for issuing a report.

QUESTION 334
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 335
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 336
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 337
Which of the following is the key benefit of control self-assessment (CSA)?

A. Management ownership of the internal controls supporting business objectives is reinforced.
B. Audit expenses are reduced when the assessment results are an input to external audit work.
C. Improved fraud detection since internal business staff are engaged in testing controls
D. Internal auditors can shift to a consultative approach by using the results of the assessment.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The objective of control self-assessment is to have business management become more aware of the importance of internal control and their responsibility in terms of corporate governance.
Reducing audit expenses is not a key benefit of control self-assessment (CSA). improved fraud detection is important, but not as important as ownership, and is not a principal objective of CSA. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

QUESTION 338
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 339
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 340
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 341
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 342
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 343
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 344
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 345
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 346
As an outcome of information security governance, strategic alignment provides:

A. security requirements driven by enterprise requirements.
B. baseline security following best practices.
C. institutionalized and commoditized solutions.
D. an understanding of risk exposure.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

QUESTION 347
Which of the following IT governance best practices improves strategic alignment?

A. Supplier and partner risks are managed.
B. A knowledge base on customers, products, markets and processes is in place.
C. A structure is provided that facilitates the creation and sharing of business information.
D. Top management mediate between the imperatives of business and technology.

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being managed is a risk management best practice. A knowledge base on customers, products, markets and processes being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management.

QUESTION 348
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 349
Which of the following is the MOST important element for the successful implementation of IT governance?
A. Implementing an IT scorecard
B. Identifying organizational strategies
C. Performing a risk assessment
D. Creating a formal security policy

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance. Without identification of organizational strategies, the remaining choices-even if implemented-would be ineffective.

QUESTION 350
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 351
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 352
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 353
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 354

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 355
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 356
From a control perspective, the key element in job descriptions is that they:

A. provide instructions on how to do the job and define authority.
B. are current, documented and readily available to the employee.
C. communicate management's specific job performance expectations.
D. establish responsibility and accountability for the employee's actions.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

QUESTION 357
Which of the following would BEST provide assurance of the integrity of new staff?

A. background screening
B. References
C. Bonding
D. Qualifications listed on a resume

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

QUESTION 358
When an employee is terminated from service, the MOST important action is to:

A. hand over all of the employee's files to another designated employee.

B. complete a backup of the employee's work.
C. notify other employees of the termination.
D. disable the employee's logical access.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

QUESTION 359
Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a good quality of life, which will lead to greater productivity.
B. reduce the opportunity for an employee to commit an improper or illegal act.
C. provide proper cross-training for another employee.
D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time, it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

QUESTION 360
A local area network (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 may also be responsible for security administration over the LAN.

QUESTION 361
A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

A. length of service, since this will help ensure technical competence.
B. age, as training in audit techniques may be impractical.
C. IS knowledge, since this will bring enhanced credibility to the audit function.
D. ability, as an IS auditor, to be independent of existing IS relationships.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. The fact that the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any candidate should be evaluated against those requirements. The length of service will not ensure technical competency. Evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

QUESTION 362
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 363
When segregation of duties concerns exists between IT support staff and end users, what would be suitable compensating control?

A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs
C. Performing background checks prior to hiring IT staff
D. Locking user sessions after a specified period of inactivity

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently} of access privileges that have officially been granted.

QUESTION 364
An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. dependency on a single person.
B. inadequate succession planning.
C. one person knowing all parts of a system.
D. a disruption of operations.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Cross-training is a process of training more than one individual to perform a specific job or procedure. This practice helps decrease the dependence on a single person and assists in succession planning. This provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations. However, in using this approach, it is prudent to have first assessed the risk of any person knowing all parts of a system and the related potential exposures. Cross-training reduces the risks addressed in choices A, B and D.

QUESTION 365
Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

A. Overlapping controls
B. Boundary controls
C. Access controls
D. Compensating controls

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated.
Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-be user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

QUESTION 366
Which of the following reduces the potential impact of social engineering attacks?

A. Compliance with regulatory requirements
B. Promoting ethical understanding
C. Security awareness programs
D. Effective performance incentives

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

QUESTION 367
Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

A. Deleting database activity logs
B. Implementing database optimization tools
C. Monitoring database usage
D. Defining backup and recovery procedures

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

QUESTION 368
To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

A. enterprise data model.
B. IT balanced scorecard (BSC).
C. IT organizational structure.
D. historical financial statements.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The IT balanced scorecard (BSC) is a tool that provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. An enterprise data model is a document defining the data structure of an organization and how data interrelate. It is useful, but it does not provide information on investments. The IT organizational structure provides an overview of the functional and reporting relationships in an IT entity. Historical financial statements do not provide information about planning and lack sufficient detail to enable one to fully understand management's activities regarding IT assets. Past costs do not necessarily reflect value, and assets such as data are not represented on the books of accounts.

QUESTION 369
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 370
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 371
Which of the following is normally a responsibility of the chief security officer (CSO)?

A. Periodically reviewing and evaluating the security policy
B. Executing user application and software testing and evaluation
C. Granting and revoking user access to IT resources
D. Approving access to data and applications

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

QUESTION 372
To support an organization's goals, an IS department should have:

A. a low-cost philosophy.
B. long- and short-range plans.
C. leading-edge technology.
D. plans to acquire new hardware and software.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

QUESTION 373
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 374
Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

A. Allocating resources
B. Keeping current with technology advances
C. Conducting control self-assessment
D. Evaluating hardware needs

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

QUESTION 375
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 376
Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line management.
B. does not vary from the IS department's preliminary budget.
C. complies with procurement procedures.
D. supports the business objectives of the organization.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Strategic planning sets corporate or department objectives into motion. Both long-term and short- term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Choice A is incorrect since line management prepared the plans.

QUESTION 377
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 378
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 379
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 380

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

A. control self-assessments.
B. a business impact analysis.
C. an IT balanced scorecard.
D. business process reengineering.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IT balanced scorecard (BSC) provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. Control self- assessment (CSA), business impact analysis (BIA) and business process reengineering (BPR) are insufficient to align IT with organizational objectives.

QUESTION 381
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 382
When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

A. establishment of a review board.

B. creation of a security unit.
C. effective support of an executive sponsor.
D. selection of a security process owner.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level of management is the most critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

QUESTION 383
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 384
The advantage of a bottom-up approach to the development of organizational policies is that the policies:

A. are developed for the organization as a whole

B. are more likely to be derived as a result of a risk assessment.
C. will not conflict with overall corporate policy.
D. ensure consistency across the organization.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies. Choices A, C and D are advantages of a top-down approach for developing organizational policies. This approach ensures that the policies will not be in conflict with overall corporate policy and ensure consistency across the organization.

QUESTION 385
Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?
A. User management coordination does not exist.
B. Specific user accountability cannot be established.
C. Unauthorized users may have access to originate, modify or delete data.
D. Audit recommendations may not be implemented.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

QUESTION 386
The PRIMARY objective of an audit of IT security policies is to ensure that:

A. they are distributed and available to all staff.
B. security and control policies support business and IT objectives.
C. there is a published organizational chart with functional descriptions.

D. duties are appropriately segregated.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

QUESTION 387
The rate of change in technology increases the importance of:

A. outsourcing the IS function.
B. implementing and enforcing good processes.
C. hiring personnel willing to make a career within the organization.
D. meeting user requirements.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated; usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

QUESTION 388
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 389
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 390
Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

A. Response
B. Correction
C. Detection
D. Monitoring

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

QUESTION 391
Which of the following should be included in an organization's IS security policy?

A. A list of key IT resources to be secured
B. The basis for access authorization
C. Identity of sensitive security features
D. Relevant software security features

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The security policy provides the broad framework of security, as laid down and approved by senior management. It includes a definition of those authorized to grant access and the basis for granting the access. Choices A, B and C are more detailed than that which should be included in a policy.

QUESTION 392
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 393
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 394
Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties
B. Management support and approval for the implementation and maintenance of a security policy
C. Enforcement of security rules by providing punitive actions for any violation of security rules
D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

QUESTION 395
A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

A. recovery.
B. retention.
C. rebuilding.
D. reuse.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e- mail communication is held in the same regard as the official form of classic 'paper* makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

QUESTION 396
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 397
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 398
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 399
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 400
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 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 401
When developing a security architecture, which of the following steps should be executed FIRST?

A. Developing security procedures
B. 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 402
An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

A. report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy.
B. verify that user access rights have been granted on a need-to-have basis.
C. recommend changes to the IS policy to ensure deactivation of user IDs upon termination.
D. recommend that activity logs of terminated users be reviewed on a regular basis.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Although a policy provides a reference for performing IS audit assignments, an IS auditor needs to review the adequacy and the appropriateness of the policy. If, in the opinion of the auditor, the time frame defined for deactivation is inappropriate, the auditor needs to communicate this to management and recommend changes to the policy. Though the deactivation happens as stated in the policy, it cannot be concluded that the control is effective. Best practice would require that the ID of a terminated user be deactivated immediately. Verifying that user access rights have been granted on a need-to-have basis is necessary when permissions are granted.
Recommending that activity logs of terminated users be reviewed on a regular basis is a good practice, but not as effective as deactivation upon termination.

QUESTION 403
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

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 404
IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

A. desired result or purpose of implementing specific control procedures.
B. best IT security control practices relevant to a specific entity.
C. techniques for securing information.
D. security policy.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

QUESTION 405
Which of the following provides the best evidence of the adequacy of a security awareness program?

A. The number of stakeholders including employees trained at various levels
B. Coverage of training at all locations across the enterprise
C. The implementation of security devices from different vendors
D. Periodic reviews and comparison with best practices

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The adequacy of security awareness content can best be assessed by determining whether it is periodically reviewed and compared to industry best practices. Choices A, B and C provide metrics for measuring various aspects of a security awareness program, but do not help assess the content.

QUESTION 406
The PRIMARY objective of implementing corporate governance by an organization's management is to:

A. provide strategic direction.
B. control business operations.
C. align IT with business.
D. implement best practices.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Corporate governance is a set of management practices to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed and organizational resources are properly utilized. Hence, the primary objective of corporate governance is to provide strategic direction. Based on the strategic direction, business operations are directed and controlled.

QUESTION 407
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
B. Consider user satisfaction in the key performance indicators (KPIs)
C. 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 408
An example of a direct benefit to be derived from a proposed IT-related business investment is:

A. enhanced reputation.
B. enhanced staff morale.
C. the use of new technology.
D. increased market penetration.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A comprehensive business case for any proposed IT-related business investment should have clearly defined business benefits to enable the expected return to be calculated. These benefits usually fall into two categories: direct and indirect, or soft. Direct benefits usually comprise the quantifiable financial benefits that the new system is expected to generate. The potential benefits of enhanced reputation and enhanced staff morale are difficult to quantify, but should be quantified to the extent possible. IT investments should not be made just for the sake of new technology but should be based on a quantifiable business need.

QUESTION 409
To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

A. project management tools.
B. an object-oriented architecture.
C. tactical planning.
D. enterprise architecture (EA).

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Enterprise architecture (EA) involves documenting the organization's IT assets and processes in a structured manner to facilitate understanding, management and planning for IT investments. It involves both a current state and a representation of an optimized future state. In attempting to complete an EA, organizations can address the problem either from a technology perspective or a business process perspective. Project management does not consider IT investment aspects; it is a tool to aid in delivering projects. Object-oriented architecture is a software development methodology and does not assist in planning for IT investment, while tactical planning is relevant only after high-level IT investment decisions have been made.

QUESTION 410
A benefit of open system architecture is that it:

A. facilitates interoperability.
B. facilitates the integration of proprietary components.
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 411
In the context of effective information security governance, the primary objective of value delivery is to:

A. optimize security investments in support of business objectives.
B. implement a standard set of security practices.
C. institute a standards-based solution.
D. implement a continuous improvement culture.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commoditization of standards-based solutions, and implementation of a continuous improvement culture considering security as a process, not an event.

QUESTION 412
Which of the following BEST supports the prioritization of new IT projects?

A. Internal control self-assessment (CSA)
B. Information systems audit
C. Investment portfolio analysis
D. 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 413
After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

A. Project management and progress reporting is combined in a project management office which is driven by external consultants.
B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach.
C. The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy systems.
D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
The efforts should be consolidated to ensure alignment with the overall strategy of the post-merger organization. If resource allocation is not centralized, the separate projects are at risk of overestimating the availability of key knowledge resources for the in-house developed legacy applications. In post-merger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralize dependencies of project deliverables or resources. The experience of external consultants can be valuable since project management practices do not require in-depth knowledge of the legacy systems. This can free up resources for functional tasks. Itis a good idea to first get familiar with the old systems, to understand what needs to be done in a migration and to evaluate the implications of technical decisions. In most cases, mergers result in application changes and thus in training needs as organizations and processes change to leverage the intended synergy effects of the merger.

QUESTION 414
Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider
B. Participating in systems design with the provider
C. Renegotiating the provider's fees
D. Monitoring the outsourcing provider's performance

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a byproduct of monitoring the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

QUESTION 415
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 416
An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

A. hardware configuration.
B. access control software.
C. ownership of intellectual property.
D. application development methodology.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be of no real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

QUESTION 417
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 418
An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

A. References from other customers
B. Service level agreement (SLA) template
C. Maintenance agreement
D. Conversion plan

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor should look for an independent verification that the ISP can perform the tasks being contracted for. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows-issues which would be of concern to an IS auditor. Checking references is a means of obtaining an independent verification that the vendor can perform the services it says it can. A maintenance agreement relates more to equipment than to services, and a conversion plan, while important, is less important than verification that the ISP can provide the services they propose.

QUESTION 419
To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

A. O/S and hardware refresh frequencies
B. Gain-sharing performance bonuses
C. Penalties for noncompliance
D. Charges tied to variable cost metrics

Correct Answer: B

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

QUESTION 420
When an organization is outsourcing their information security function, which of the following should be kept in the organization?

A. Accountability for the corporate security policy
B. Defining the corporate security policy
C. Implementing the corporate security policy
D. Defining security procedures and guidelines

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

QUESTION 421
Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

A. System owners
B. System users
C. System designers
D. System builders

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system.
Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

QUESTION 422
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 423
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 424
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 425
An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?

A. Use a process-based maturity model such as the capability maturity model (CMM)
B. Regular monitoring of task-level progress against schedule
C. Extensive use of software development tools to maximize team productivity
D. Postiteration reviews that identify lessons learned for future use in the project

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A key tenet of the Agile approach to software project management is team learning and the use of team learning to refine project management and software development processes as the project progresses. One of the best ways to achieve this is that, at the end of each iteration, the team considers and documents

what worked well and what could have worked better, and identifies improvements to be implemented in subsequent iterations. CMM and Agile really sit at opposite poles. CMM places heavy emphasis on predefined formal processes and formal project management and software development deliverables. Agile projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics.
Additionally, less importance is placed on formal paper- based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile projects produce releasable software in short iterations, typically ranging from 4 to 8 weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant. Agile projects do make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of greater importance.

QUESTION 426
An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

A. Consider feasibility of a separate user acceptance environment
B. Schedule user testing to occur at a given time each day
C. implement a source code version control tool
D. Only retest high priority defects

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A separate environment or environments is normally necessary for testing to be efficient and effective, and to ensure the integrity of production code, it is important that the development and testing code base be separate. When defects are identified they can be fixed in the development environment, without interrupting testing, before being migrated in a controlled manner to the test environment. A separate test environment can also be used as the final staging area from which code is migrated to production. This enforces a separation between development and production code. The logistics of setting up and refreshing customized test data is easier if a separate environment is maintained. If developers and testers are sharing the same environment, they have to work effectively at separate times of the day. It is unlikely that this would provide optimum productivity. Use of a source code control tool is a good practice, but it does not properly mitigate the lack of an appropriate testing environment. Even low priority fixes run the risk of introducing unintended results when combined with the rest of the system code. To prevent this, regular regression testing covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

QUESTION 427
Which of the following types of testing would determine whether a new or modifies system can operate in its target environment without adversely impacting other existing systems?

A. Parallel testing

B. Pilot testing
C. Interface/integration testing
D. Sociability testing

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a clientserver or web development. Parallel testing is the process of feeding data into two systems-the modified system and an alternate system- and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. Pilot testing takes place first at one location and is then extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure.

QUESTION 428
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 429
Which of the following is an implementation risk within the process of decision support systems?

A. Management control
B. Semistructured dimensions
C. inability to specify purpose and usage patterns
D. Changes in decision processes

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DDS.

QUESTION 430
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 431
Which of the following system and data conversion strategies provides the GREATEST redundancy?

A. Direct cutover
B. Pilot study
C. Phased approach

D. Parallel run

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Parallel runs are the safest-though the most expensive-approach, because both the old and new systems are run, thus incurring what might appear to be double costs. Direct cutover is actually quite risky, since it does not provide for a 'shake down period' nor does it provide an easy fallback option. Both a pilot study and a phased approach are performed incrementally, making rollback procedures difficult to execute.

QUESTION 432
Which of the following would impair the independence of a quality assurance team?

A. Ensuring compliance with development methods
B. Checking the testing assumptions
C. Correcting coding errors during the testing process
D. Checking the code to ensure proper documentation

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Correction of code should not be a responsibility of the quality assurance team as it would not ensure segregation of duties and would impair the team's independence. The other choices are valid quality assurance functions.

QUESTION 433
From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

A. a big bang deployment after proof of concept.
B. prototyping and a one-phase deployment.
C. a deployment plan based on sequenced phases.
D. to simulate the new infrastructure before deployment.

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
When developing a large and complex IT infrastructure, the best practice is to use a phased approach to fitting the entire system together. This will provide greater assurance of quality results. The other choices are riskier approaches.

QUESTION 434
An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:

A. correlation of semantic characteristics of the data migrated between the two systems.
B. correlation of arithmetic characteristics of the data migrated between the two systems.
C. correlation of functional characteristics of the processes between the two systems.
D. relative efficiency of the processes between the two systems.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Due to the fact that the two systems could have a different data representation, including the database schema, the IS auditor's main concern should be to verify that the interpretation of the data is the same in the new as it was in the old system. Arithmetic characteristics represent aspects of data structure and internal definition in the database, and therefore are less important than the semantic characteristics. A review of the correlation of the functional characteristics or a review of the relative efficiencies of the processes between the two systems is not relevant to a data migration review.

QUESTION 435
The reason a certification and accreditation process is performed on critical systems is to ensure that:

A. security compliance has been technically evaluated.
B. data have been encrypted and are ready to be stored.
C. the systems have been tested to run on different platforms. D. the systems have followed the phases of a waterfall model.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:

Explanation:
Certified and accredited systems are systems that have had their security compliance technically evaluated for running on a specific production server. Choice B is incorrect because not all data of certified systems are encrypted. Choice C is incorrect because certified systems are evaluated to run in a specific environment. A waterfall model is a software development methodology and not a reason for performing a certification and accrediting process.

QUESTION 436
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 437
During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

A. implement data backup and recovery procedures.
B. Define standards and closely monitor for compliance.
C. Ensure that only authorized personnel can update the database.
D. Establish controls to handle concurrent access problems.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:

Explanation:
Implementing data backup and recovery procedure is a corrective control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, while monitoring for compliance is a detective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is also a preventive control.

QUESTION 438
An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

A. Log all table update transactions.
B. implement before-and-after image reporting.
C. Use tracing and tagging.
D. implement integrity constraints in the database.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

QUESTION 439
Responsibility and reporting lines cannot always be established when auditing automated systems since:

A. diversified control makes ownership irrelevant.
B. staff traditionally changes jobs with greater frequency.
C. ownership is difficult to establish where resources are shared.
D. duties change frequently in the rapid development of technology.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Because of the diversified nature of both data and application systems, the actual owner of data and applications may be hard to establish.

QUESTION 440
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 441
Which of the following would help to ensure the portability of an application connected to a database?

A. Verification of database import and export procedures
B. Usage of a structured query language (SQL)
C. Analysis of stored procedures/triggers
D. Synchronization of the entity-relation model with the database physical schema

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of SQL facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design entity- relation model will be helpful, but none of these contribute to the portability of an application connecting to a database.

QUESTION 442

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 443
A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be an IS auditor's main concern about the new process?

A. Whether key controls are in place to protect assets and information resources
B. If the system addresses corporate customer requirements
C. Whether the system can meet the performance goals (time and resources)
D. Whether owners have been identified who will be responsible for the process

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the business process reengineering (BPR) process should achieve, but they are not the auditor's primary concern.

QUESTION 444

A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced? A. Verifying production to customer orders

B. Logging all customer orders in the ERP system C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processing centrally. Production supervisory approval is a time consuming, manual process that does not guarantee proper control.

QUESTION 445
When two or more systems are integrated, input/output controls must be reviewed by an IS auditor in the:

A. systems receiving the output of other systems.
B. systems sending output to other systems.
C. systems sending and receiving data.
D. interfaces between the two systems.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Both of the systems must be reviewed for input/output controls, since the output for one system is the input for the other.

QUESTION 446
An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

A. EDI trading partner agreements.

B. physical controls for terminals.
C. authentication techniques for sending and receiving messages.
D. program change control procedures.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

QUESTION 447
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 448
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.

QUESTION 449
Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:

A. pre-BPR process flowcharts.
B. post-BPR process flowcharts.
C. BPR project plans.
D. continuous improvement and monitoring plans.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Choice A is incorrect because an IS auditor must review the process as it is today, not as it was in the past. Choices C and D are incorrect because they are steps within a BPR project.

QUESTION 450
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.
B. 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 451
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

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 452
The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentiality.
B. increased redundancy.
C. unauthorized accesses.
D. application malfunctions.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy. Redundancy which is usually considered positive when it is a question of resource availability is negative in a database environment, since it demands additional and otherwise unnecessary data handling efforts.
Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

QUESTION 453
Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

A. protect the organization from viruses and nonbusiness materials.
B. maximize employee performance.
C. safeguard the organization's image.
D. assist the organization in preventing legal issues

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e- mail. Choice B could be true in some circumstances (i.e., it would need to be implemented along with an awareness program, so that employee performance can be significantly improved). However, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

QUESTION 454
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 455
An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:

A. source documentation retention.
B. data file security.
C. version usage control.
D. one-for-one checking.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
For processing to be correct, it is essential that the proper version of a file is used. Transactions should be applied to the most current database, while restart procedures should use earlier versions. Source documentation should be retained for an adequate time period to enable documentation retrieval, reconstruction or verification of data, but it does not aid in ensuring that the correct version of a file will be used. Data file security controls prevent access by unauthorized users who could then alter the data files; however, it does not ensure that the correct file will be used. It is necessary to ensure that all documents have been received for processing, one-for-one; however, this does not ensure the use of the correct file.

QUESTION 456
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 457
When reviewing a hardware maintenance program, an IS auditor should assess whether:
A. the schedule of all unplanned maintenance is maintained.
B. it is in line with historical trends.
C. it has been approved by the IS steering committee.
D. the program is validated against vendor specifications.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Though maintenance requirements vary based on complexity and performance workloads, a hardware maintenance schedule should be validated against the vendor-provided specifications. For business reasons, an organization may choose a more aggressive maintenance program than the vendor's program. The maintenance program should include maintenance performance history, be it planned, unplanned, executed or exceptional. Unplanned maintenance cannot be scheduled. Hardware maintenance programs do not necessarily need to be in line with historical trends. Maintenance schedules normally are not approved by the steering committee.

QUESTION 458
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 459
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 460
Which of the following is the BEST type of program for an organization to implement to aggregate, correlate and store different log and event files, and then produce weekly and monthly reports for IS auditors?

A. A security information event management (SIEM) product
B. An open-source correlation engine
C. A log management tool
D. An extract, transform, load (ETL) system

Correct Answer: C
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation:
A log management tool is a product designed to aggregate events from many log files (with distinct formats and from different sources), store them and typically correlate them offline to produce many reports (e.g., exception reports showing different statistics including anomalies and suspicious activities), and to answer time-based queries (e.g., how many users have entered the system between 2 a.m. and 4 a.m. over the past three weeks?). A SIEM product has some similar features. It correlates events from log files, but does it online and normally is not oriented to storing many weeks of historical information and producing audit reports. A correlation engine is part of a SIEM product. It is oriented to making an online correlation of events. An extract, transform, load (ETL) is part of a business intelligence system, dedicated to extracting operational or production data, transforming that data and loading them to a central repository (data warehouse or data mart); an ETL does not correlate data or produce reports, and normally it does not have extractors to read log file formats.

QUESTION 461
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 462
Which of the following would BEST maintain the integrity of a firewall log?

A. Granting access to log information only to administrators
B. Capturing log events in the operating system layer
C. Writing dual logs onto separate storage media
D. Sending log information to a dedicated third-party log server

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Establishing a dedicated third-party log server and logging events in it is the best procedure for maintaining the integrity of a firewall log. When access control to the log server is adequately maintained, the risk of unauthorized log modification will be mitigated, therefore improving the integrity of log information. To enforce segregation of duties, administrators should not have access to log files. This primarily contributes to the assurance of confidentiality rather than integrity. There are many ways to capture log information: through the application layer, network layer, operating systems layer, etc.; however, there is no log integrity advantage in capturing events in the operating systems layer. If it is a highly mission-critical information system, it may be nice to run the system with a dual log mode. Having logs in two different storage devices will primarily contribute to the assurance of the availability of log information, rather than to maintaining its integrity.

QUESTION 463
Which of the following will prevent dangling tuples in a database?
A. Cyclic integrity
B. Domain integrity
C. Relational integrity
D. Referential integrity

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/ foreign key, there should be a corresponding tuple in another table, i.e., for existence of all foreign keys in the original tables, if this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized source documentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

QUESTION 464
The objective of concurrency control in a database system is to:

A. restrict updating of the database to authorized users.
B. prevent integrity problems when two processes attempt to update the same data at the same time.
C. prevent inadvertent or unauthorized disclosure of data in the database.
D. ensure the accuracy, completeness and consistency of data.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users, and controls such as passwords prevent the inadvertent or unauthorized disclosure of data from the database. Quality controls, such as edits, ensure the accuracy, completeness and consistency of data maintained in the database.

QUESTION 465
Which of the following controls would provide the GREATEST assurance of database integrity?

A. Audit log procedures

B. Table link/reference checks
C. Query/table access time checks
D. Rollback and roll forward database features

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Performing table link/reference checks serves to detect table linking errors (such as completeness and accuracy of the contents of the database), and thus provides the greatest assurance of database integrity. Audit log procedures enable recording of all events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the database's contents. Querying/monitoring table access time checks helps designers improve database performance, but not integrity. Rollback and roll forward database features ensure recovery from an abnormal disruption. They assure the integrity of the transaction that was being processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

QUESTION 466
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 467

B.

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.
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 468
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?

A. Foreign key
B. Primary key
C. Secondary key
D. Public key

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
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

B.

B.
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 469
When performing a database review, an IS auditor notices that some tables in the database are not normalized. The IS auditor should next:

A. recommend that the database be normalized.

review the conceptual data model.
C. review the stored procedures.
D. review the justification.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If the database is not normalized, the IS auditor should review the justification since, in some situations, denormalization is recommended for performance reasons. The IS auditor should not recommend normalizing the database until further investigation takes place. Reviewing the conceptual data model or the stored procedures will not provide information about normalization.

QUESTION 470
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:

B.

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.

QUESTION 471

An IS auditor finds that client requests were processed multiple times when received from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

A. increase the frequency for data replication between the different department systems to ensure timely updates.

Centralize all request processing in one department to avoid parallel processing of the same request.

B.

C.
Change the application architecture so that common data is held in just one shared database for all departments.
D. implement reconciliation controls to detect duplicates before orders are processed in the systems.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Keeping the data in one place is the best way to ensure that data are stored without redundancy and that all users have the same data on their systems. Although increasing the frequency may help to minimize the problem, the risk of duplication cannot be eliminated completely because parallel data entry is still possible. Business requirements will most likely dictate where data processing activities are performed. Changing the business structure to solve an IT problem is not practical or politically feasible. Detective controls do not solve the problem of duplicate processing, and would require that an additional process be implemented to handle the discovered duplicates.

QUESTION 472
Which of the following database controls would ensure that the integrity of transactions is maintained in an online transaction processing system's database?

A. Authentication controls
B. Data normalization controls
C. Read/write access log controls
D. Commitment and rollback controls

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Commitment and rollback controls are directly relevant to integrity. These controls ensure that database operations that form a logical transaction unit will complete in its entirety or not at all; i.e., if, for some reason, a transaction cannot be fully completed, then incomplete inserts/updates/deletes are rolled back so that the database returns to its pretransaction state. All other choices would not address transaction integrity.

QUESTION 473
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?

B.

C.

A. Permanent table-space allocation Commitment and rollback controls

User spool and database limit controls

D. Read/write access log controls

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
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 474
Which of the following is widely accepted as one of the critical components in networking management?

A. Configuration management
B. Topological mappings
C. Application of monitoring tools
D. Proxy server troubleshooting

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function internally and externally, it also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network and its connectivity. Application monitoring is not essential and proxy server troubleshooting is used for troubleshooting purposes.

B.

C.

QUESTION 475

Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

A. Parity check

Echo check

Block sum check

D. Cyclic redundancy check

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. if both of them are equal. Then the block is assumed error free, in this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. Inhigher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.

QUESTION 476

Which of the following types of firewalls provide the GREATEST degree and granularity of control?

A. Screaming router
B. Packet filter
C. Application gateway
D. Circuit gateway

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

C.

The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This means that it not only checks the packet IP addresses (layer 3) and the ports it is directed to (in this case port 80, or layer 4), it also checks every HTTP command (layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and BJ work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4, and not from higher levels. A circuit gateway (choice D) is based on a proxy or program that acts as an intermediary between external and internal accesses. This means that during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external server to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

QUESTION 477

B.

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:
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 478
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.

Correct Answer: A
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 479
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 480
In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries
B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited as suggested in choice B, this practice is not always possible in small organizations. An IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. An IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process.
Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

QUESTION 481
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 482
Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

A. Release-to-release source and object comparison reports
B. Library control software restricting changes to source code
C. Restricted access to source code and object code
D. Date and time-stamp reviews of source and object code

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Date and time-stamp reviews of source and object code would ensure that source code, which has been compiled, matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is the one being used.

QUESTION 483
Change management procedures are established by IS management to:

A. control the movement of applications from the test environment to the production environment.

B. control the interruption of business operations from lack of attention to unresolved problems.
C. ensure the uninterrupted operation of the business in the event of a disaster.
D. verify that system changes are properly documented.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Change management procedures are established by IS management to control the movement of applications from the test environment to the production environment. Problem escalation procedures control the interruption of business operations from lack of attention to unresolved problems, and quality assurance procedures verify that system changes are authorized and tested.

QUESTION 484
In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

A. application programmer copy the source program and compiled object module to the production libraries
B. application programmer copy the source program to the production libraries and then have the production control group compile the program.
C. production control group compile the object module to the production libraries using the source program in the test environment.
D. production control group copy the source program to the production libraries and then compile the program.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program.

QUESTION 485
An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

A. Allow changes to be made only with the DBA user account.
B. Make changes to the database after granting access to a normal user account.
C. Use the DBA user account to make changes, log the changes and review the change log the following day.

D. Use the normal user account to make changes, log the changes and review the change log the following day.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of a database administrator (DBA) user account is normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

QUESTION 486
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 487
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 488
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 489
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 490
An IS auditor should recommend the use of library control software to provide reasonable assurance that:

A. program changes have been authorized.
B. only thoroughly tested programs are released.
C. modified programs are automatically moved to production.
D. source and executable code integrity is maintained.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Library control software should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized. Library control software is concerned with authorized program changes and would not automatically move modified programs into production and cannot determine whether programs have been thoroughly tested. Library control software provides reasonable assurance that the source code and executable code are matched at the time a source code is moved to production. However, subsequent events such as a hardware failure can result in a lack of consistency between source and executable code.

QUESTION 491
An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

A. apply the patch according to the patch's release notes.
B. ensure that a good change management process is in place.
C. thoroughly test the patch before sending it to production.
D. approve the patch after doing a risk assessment.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor must review the change management process, including patch management procedures, and verify that the process has adequate controls and make suggestions accordingly. The other choices are part of a good change management process but are not an IS auditor's responsibility.

QUESTION 492
When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

A. allow changes, which will be completed using after-the-fact follow-up.
B. allow undocumented changes directly to the production library.
C. do not allow any emergency changes.
D. allow programmers permanent access to production programs.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
There may be situations where emergency fixes are required to resolve system problems. This involves the use of special logon IDs that grant programmers temporary access to production programs during emergency situations. Emergency changes should be completed using after-the- fact follow-up procedures, which ensure that normal procedures are retroactively applied; otherwise, production may be impacted. Changes made in this fashion should be held in an emergency library from where they can be moved to the production library, following the normal change management process. Programmers should not directly alter the production library nor should they be allowed permanent access to production programs.

QUESTION 493
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 494
The application systems of an organization using open-source software have no single recognized developer producing patches. Which of the following would be the MOST secure way of updating open-source software?

A. Rewrite the patches and apply them
B. Code review and application of available patches
C. Develop in-house patches
D. identify and test suitable patches before applying them

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Suitable patches from the existing developers should be selected and tested before applying them. Rewriting the patches and applying them is not a correct answer because it would require skilled resources and time to rewrite the patches. Code review could be possible but tests need to be performed before applying the patches. Since the system was developed outside the organization, the IT department may not have the necessary skills and resources to develop patches.

QUESTION 495
Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

A. Change management
B. Backup and recovery
C. incident management
D. Configuration management

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The configuration management process may include automated tools that will provide an automated recording of software release baselines. Should the new release fail, the baseline will provide a point to which to return. The other choices do not provide the processes necessary for establishing software release baselines and are not related to software release baselines.

QUESTION 496
An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration by IT of:

A. the training needs for users after applying the patch.
B. any beneficial impact of the patch on the operational systems.
C. delaying deployment until testing the impact of the patch.
D. the necessity of advising end users of new patches.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Deploying patches without testing exposes an organization to the risk of system disruption or failure. Normally, there is no need for training or advising users when a new operating system patch has been installed. Any beneficial impact is less important than the risk of unavailability that could be avoided with proper testing.

QUESTION 497
In a small organization, developers may release emergency changes directly to production. Which of the following will BEST control the risk in this situation?

A. Approve and document the change the next business day
B. Limit developer access to production to a specific timeframe
C. Obtain secondary approval before releasing to production
D. Disable the compiler option in the production machine

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It may be appropriate to allow programmers to make emergency changes as long as they are documented and approved after the fact. Restricting release time frame may help somewhat; however, it would not apply to emergency changes and cannot prevent unauthorized release of the programs. Choices C and D are not relevant in an emergency situation.

QUESTION 498
Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project.
Which of the following is the MOST appropriate suggestion for an auditor to make?

A. Achieve standards alignment through an increase of resources devoted to the project
B. Align the data definition standards after completion of the project
C. Delay the project until compliance with standards can be achieved
D. Enforce standard compliance by adopting punitive measures against violators

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Provided that data architecture, technical, and operational requirements are sufficiently documented, the alignment to standards could be treated as a specific work package assigned to new project resources. The usage of nonstandard data definitions would lower the efficiency of the new development, and increase the risk of errors in critical business decisions. To change data definition standards after project conclusion (choice B) is risky and is not a viable solution. On the other hand, punishing the violators (choice D) or delaying the project (choice C) would be an inappropriate suggestion because of the likely damage to the entire project profitability.

QUESTION 499
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 500
The FIRST step in managing the risk of a cyber-attack is to:

A. assess the vulnerability impact.
B. evaluate the likelihood of threats.
C. identify critical information assets.
D. estimate potential damage.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The first step in the managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

QUESTION 501
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 502
The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

A. improve internal control procedures.
B. harden the network to industry best practices.
C. highlight the importance of incident response management to management.
D. improve employee awareness of the incident response process.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A postincident review examines both the cause and response to an incident. The lessons learned from the review can be used to improve internal controls. Understanding the purpose and structure of postincident reviews and follow-up procedures enables the information security manager to continuously improve the security program. Improving the incident response plan based on the incident review is an internal (corrective) control. The network may already be hardened to industry best practices. Additionally, the network may not be the source of the incident. The primary objective is to improve internal control procedures, not to highlight the importance of incident response management (IRM), and an incident response (IR) review does not improve employee awareness.

QUESTION 503
The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users might:

A. use this information to launch attacks.
B. forward the security alert.
C. implement individual solutions.
D. fail to understand the threat.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: An organization's computer security incident response team (CSIRT) should disseminate recent threats, security guidelines and security updates to the users to assist them in understanding the security risk of errors and omissions. However, this introduces the risk that the users may use this information to launch attacks, directly or indirectly. An IS auditor should ensure that the CSIRT is actively involved with users to assist them in mitigation of risks arising from security failures and to prevent additional security incidents resulting from the same threat. Forwarding the security alert is not harmful to the organization, implementing individual solutions is unlikely and users failing to understand the threat would not be a serious concern.

QUESTION 504
The MAIN criterion for determining the severity level of a service disruption incident is:

A. cost of recovery.
B. negative public opinion.
C. geographic location.
D. downtime.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The longer the period of time a client cannot be serviced, the greater the severity of the incident. The cost of recovery could be minimal yet the service downtime could have a major impact.
Negative public opinion is a symptom of an incident. Geographic location does not determine the severity of the incident.

QUESTION 505
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 506
An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if: A.

the setup is geographically dispersed.

B. the network servers are clustered in a site.
C. a hot site is ready for activation.
D. diverse routing is implemented for the network.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A clustered setup in one location makes the entire network vulnerable to natural disasters or other disruptive events. Dispersed geographical locations and diverse routing provide backup if a site has been destroyed. A hot site would also be a good alternative for a single point-of-failure site.

QUESTION 507
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 508
A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

A. Most employees use laptops.
B. A packet filtering firewall is used.
C. The IP address space is smaller than the number of PCs.
D. Access to a network port is not restricted.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Given physical access to a port, anyone can connect to the internal network. The other choices do not present the exposure that access to a port does. DHCP provides convenience (an advantage) to the laptop users. Sharing IP addresses and the existence of a firewall can be security measures.

QUESTION 509
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 510
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 511
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 512
When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

A. they are set to meet security and performance requirements.
B. changes are recorded in an audit trail and periodically reviewed.
C. changes are authorized and supported by appropriate documents.
D. access to parameters in the system is restricted.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary concern is to find the balance between security and performance. Recording changes in an audit trail and periodically reviewing them is a detective control; however, if parameters are not set according to business rules, monitoring of changes may not be an effective control. Reviewing changes to ensure they are supported by appropriate documents is also a detective control, if parameters are set incorrectly, the related documentation and the fact that these are authorized does not reduce the impact. Restriction of access to parameters ensures that only authorized staff can access the parameters; however, if the parameters are set incorrectly, restricting access will still have an adverse impact.

QUESTION 513
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 514
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 (EMI) 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 515
Which of the following line media would provide the BEST security for a telecommunication network?

A. broadband network digital transmission
B. Baseband network
C. Dial-up

D. Dedicated lines

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Dedicated lines are set apart for a particular user or organization. Since there is no sharing of lines or intermediate entry points, the risk of interception or disruption of telecommunications messages is lower.

QUESTION 516
Which of the following types of firewalls would BEST protect a network from an internet attack?

A. Screened subnet firewall
B. Application filtering gateway
C. Packet filtering router
D. Circuit-level gateway

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A screened subnet firewall would provide the best protection. The screening router can be a commercial router or a node with routing capabilities and the ability to allow or avoid traffic between nets or nodes based on addresses, ports, protocols, interfaces, etc. Application-level gateways are mediators between two entities that want to communicate, also known as proxy gateways. The application level (proxy) works at the application level, not just at a package level. The screening controls at the package level, addresses and ports, but does not see the contents of the package. A packet filtering router examines the header of every packet or data traveling between the internet and the corporate network.

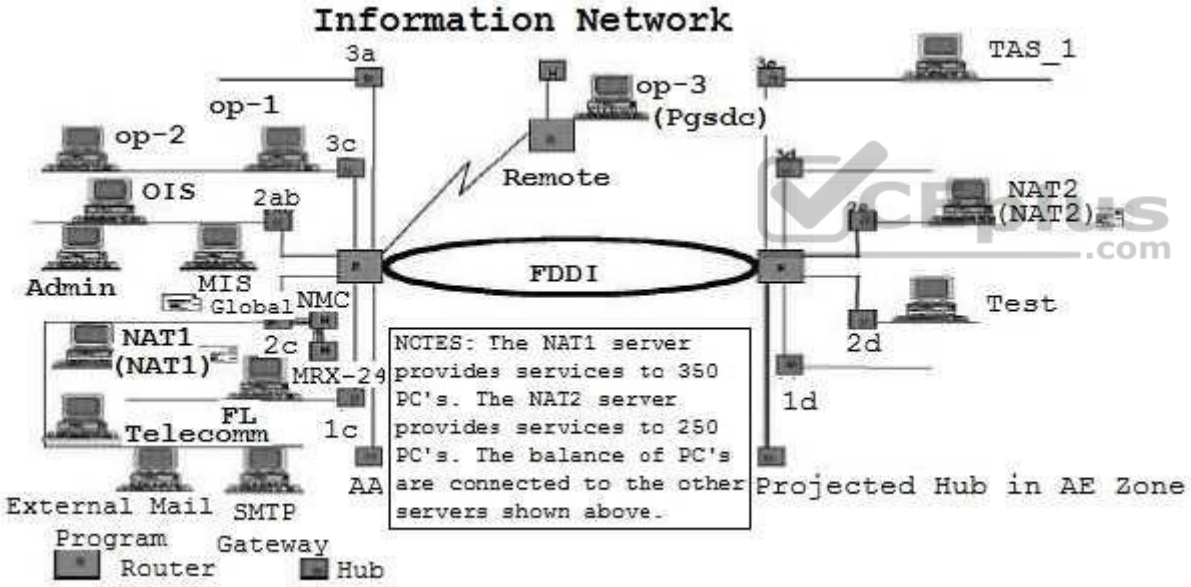
QUESTION 517
Neural networks are effective in detecting fraud because they can:

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 518
Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?

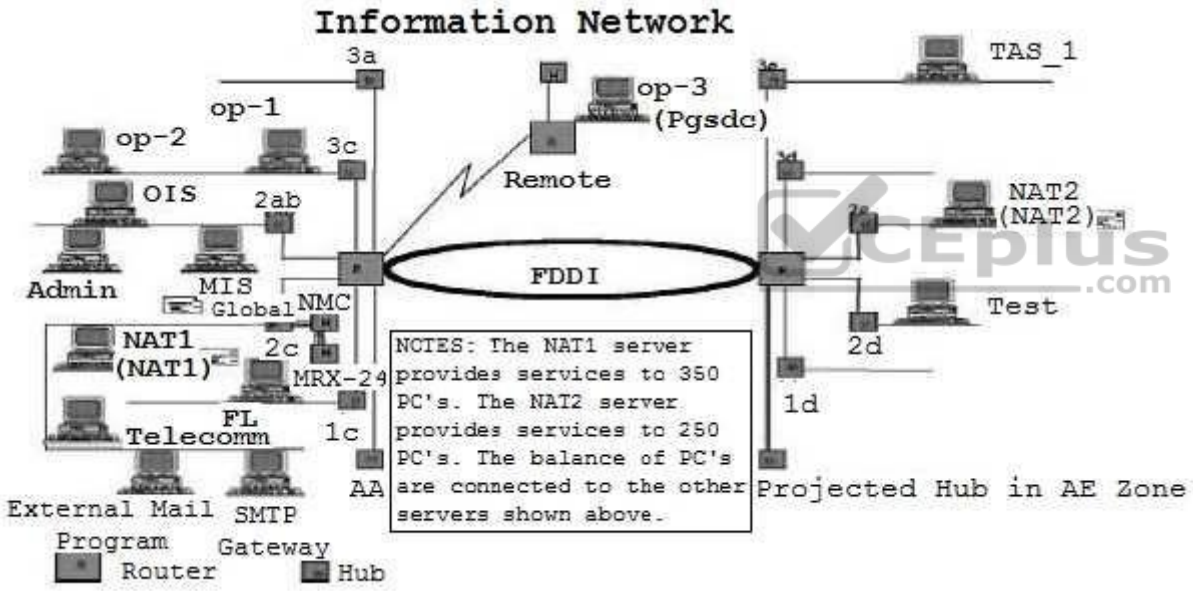


A. No firewalls are needed
B. Op-3 location only
C. MIS (Global) and NAT2
D. SMTP Gateway and op-3

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The objective of a firewall is to protect a trusted network from an untrusted network; therefore, locations needing firewall implementations would be at the existence of the external connections. All other answers are incomplete or represent internal connections.

QUESTION 519
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?



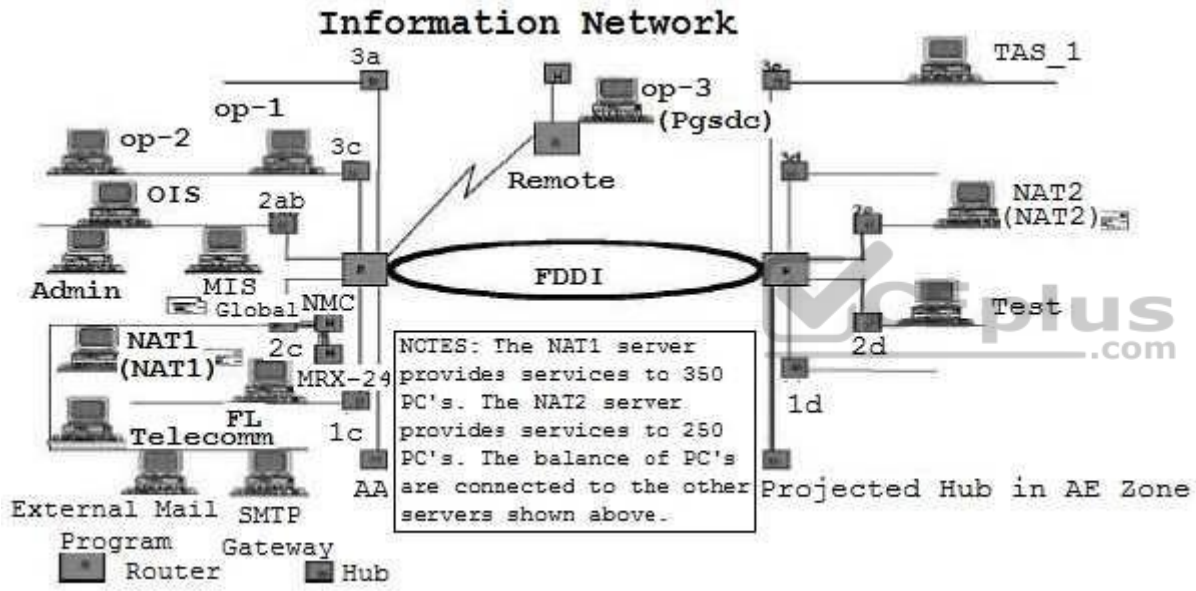
A. Intelligent hub
B. Physical security over the hubs
C. Physical security and an intelligent hub
D. No controls are necessary since this is not a weakness

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 520
In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?



A. Virus attack
B. Performance degradation
C. Poor management controls
D. Vulnerability to external hackers

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Hubs are internal devices that usually have no direct external connectivity, and thus are not prone to hackers. There are no known viruses that are specific to hub attacks. While this situation may be an indicator of poor management controls, choice B is more likely when the practice of stacking hubs and creating more terminal connections is used.

QUESTION 521
An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

A.
A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
B. Firewall policies are updated on the basis of changing requirements.
C. inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
D. The firewall is placed on top of the commercial operating system with all installation options.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

QUESTION 522
In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

A. address of the domain server.
B. resolution service for the name/address.
C. IP addresses for the internet.
D. domain name system.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
DNS is utilized primarily on the Internet for resolution of the name/address of the web site. It is an Internet service that translates domain names into IP addresses. As names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time a domain name is used, a DNS service must translate the name into the corresponding IP address. The DNS system has its own network, if one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

A.

QUESTION 523

In what way is a common gateway interface (CGI) MOST often used on a webserver?

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 524

Receiving an EDI transaction and passing it through the communication's interface stage usually requires:

A. translating and unbundling transactions.

B. routing verification procedures.

C. passing data to the appropriate application system.

D. creating a point of receipt audit log.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

A.
The communication’s interface stage requires routing verification procedures. Edi or ANSI X12 is a standard that must be interpreted by an application for transactions to be processed and then to be invoiced, paid and sent, whether they are for merchandise or services. There is no point sending and receiving EDI transactions if they cannot be processed by an internal system.
Unpacking transactions and recording audit logs are important elements that help follow business rules and establish controls, but are not part of the communication's interface stage.

QUESTION 525
Which of the following would be considered an essential feature of a network management system?

A graphical interface to map the network topology
B. Capacity to interact with the Internet to solve the problems
C. Connectivity to a help desk for advice on difficult issues
D. An export facility for piping data to spreadsheets

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To trace the topology of the network, a graphical interface would be essential. It is not necessary that each network be on the internet and connected to a help desk, while the ability to export to a spreadsheet is not an essential element.

QUESTION 526
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:

A.
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 527
When reviewing the implementation of a LAN, an IS auditor should FIRST review the:

A. node list.
B. acceptance test report.
C. network diagram.
D. user's list.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To properly review a LAN implementation, an IS auditor should first verify the network diagram and confirm the approval. Verification of nodes from the node list and the network diagram would be next, followed by a review of the acceptance test report and then the user's list.

QUESTION 528
Which of the following would be the MOST secure firewall system?

A. Screened-host firewall
B. Screened-subnet firewall
C. Dual-homed firewall
D. Stateful-inspection firewall

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A screened-subnet firewall, also used as a demilitarized zone (DMZ), utilizes two packet filtering routers and a bastion host. This provides the most secure firewall system, since it supports both network- and application-level security while defining a separate DMZ network. A screened-host firewall utilizes a packet filtering router and a bastion host. This approach implements basic network layer security (packet filtering) and application server security (proxy services). A dual- homed firewall system is a more restrictive form of a screened-host firewall system, configuring one interface for information servers and another for private network host computers. A stateful-inspection firewall working at the transport layer keeps track of the destination IP address of each packet that leaves the organization's internal network and allows a reply from the recorded IP addresses.

QUESTION 529
Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?

A. Circuit gateway
B. Application gateway
C. Packet filter
D. Screening router

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An application gateway firewall is effective in preventing applications, such as FTPs, from entering the organization network. A circuit gateway firewall is able to prevent paths or circuits, not applications, from entering the organization's network. A packet filter firewall or screening router will allow or prevent access based on IP packets/address.

QUESTION 530
Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?

A. A program that deposits a virus on a client machine
B. Applets recording keystrokes and, therefore, passwords
C. Downloaded code that reads files on a client's hard drive
D. Applets opening connections from the client machine

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An applet is a program downloaded from a web server to the client, usually through a web browser that provides functionality for database access, interactive web pages and communications with other users. Applets opening connections from the client machine to other machines on the network and damaging those machines, as a denial-of-service attack, pose the greatest threat to an organization and could disrupt business continuity. A program that deposits a virus on a client machine is referred to as a malicious attack (i.e., specifically meant to cause harm to a client machine), but may not necessarily result in a disruption of service. Applets that record keystrokes, and therefore, passwords, and downloaded code that reads files on a client's hard drive relate more to organizational privacy issues, and although significant, are less likely to cause a significant disruption of service.

QUESTION 531
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 532
Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

A. a firewall exists.
B. a secure web connection is used.
C. the source of the executable file is certain.
D. the host web site is part of the organization.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Acceptance of these mechanisms should be based on established trust. The control is provided by only knowing the source and then allowing the acceptance of the applets. Hostile applets can be received from anywhere. It is virtually impossible at this time to filter at this level. A secure web connection or firewall is considered an external defense. A firewall will find it more difficult to filter a specific file from a trusted source. A secure web connection provides confidentiality. Neither a secure web connection nor a firewall can identify an executable file as friendly. Hosting the web site as part of the organization is impractical. Enabling the acceptance of Java applets and/or Active X controls is an all-or- nothing proposition. The client will accept the program if the parameters are established to do so.

QUESTION 533
In large corporate networks having supply partners across the globe, network traffic may continue to rise. The infrastructure components in such environments should be scalable. Which of the following firewall architectures limits future scalability?

A. Appliances

B. Operating system-based
C. Host-based
D. Demilitarized

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The software for appliances is embedded into chips. Firmware-based firewall products cannot be moved to higher capacity servers. Firewall software that sits on an operating system can always be scalable due to its ability to enhance the power of servers. Host- based firewalls operate on top of the server operating system and are scalable. A demilitarized zone is a model of firewall implementation and is not a firewall architecture.

QUESTION 534
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 535
Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

A. Review the parameter settings.
B. Interview the firewall administrator.
C. Review the actual procedures.
D. Review the device's log file for recent attacks.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide audit evidence documentation. The other choices do not provide audit evidence as strong as choice A.

QUESTION 536
To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

A. business software.
B. infrastructure platform tools.
C. application services.
D. system development tools.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Projects should identify the complexities of the IT Infrastructure that can be simplified or isolated by the development of application services. Application services isolate system developers from the complexities of the IT infrastructure and offer common functionalities that are shared by many applications. Application services take the form of interfaces, middleware, etc. Business software focuses on business processes, whereas application services bridge the gap between applications and the IT Infrastructure components. Infrastructure platform tools are related to core hardware and software components required for development of the IT infrastructure. Systems development tools represent development components of the IT infrastructure development.

QUESTION 537
During the requirements definition phase for a database application, performance is listed as a top priority. To access the DBMS files, which of the following technologies should be recommended for optimal I/O performance?

A. Storage area network (SAN)
B. Network Attached Storage (NAS)
C. Network file system (NFS v2)
D. Common Internet File System (CIFS)

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In contrast to the other options, in a SAN comprised of computers, FC switches or routers and storage devices, there is no computer system hosting and exporting its mounted file system for remote access, aside from special file systems. Access to information stored on the storage devices in a SAN is comparable to direct attached storage, which means that each block of data on a disk can be addressed directly, since the volumes of the storage device are handled as though they are local, thus providing optimal performance. The other options describe technologies in which a computer (or appliance) shares its information with other systems. To access the information, the complete file has to be read.

QUESTION 538
Reverse proxy technology for web servers should be deployed if:

A. http servers' addresses must be hidden.
B. accelerated access to all published pages is required.
C. caching is needed for fault tolerance.
D. bandwidth to the user is limited.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Reverse proxies are primarily designed to hide physical and logical internal structures from outside access. Complete URLs or URIs can be partially or completely redirected without disclosing which internal or DMZ server is providing the requested data. This technology might be used if a trade-off between security, performance and costs has to be achieved. Proxy servers cache some data but normally cannot cache all pages to be published because this depends on the kind of information the web servers provide. The ability to accelerate access depends on the speed of the back-end servers, i.e., those that are cached. Thus, without making further assumptions, a gain in speed cannot be assured, but visualization and hiding of internal structures can. If speed is an issue, a scale- out approach (avoiding adding additional delays by passing firewalls, involving more servers, etc.) would be a better solution. Due to the limited caching option, reverse proxies are not suitable for enhancing fault tolerance. User requests that are handled by reverse proxy servers are using exactly the same bandwidth as direct requests to the hosts providing the data.

QUESTION 539
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 540
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 541
An IS auditor examining the configuration of an operating system to verify the controls should review the:

A. transaction logs.
B. authorization tables.
C. parameter settings.
D. routing tables.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Parameters allow a standard piece of software to be customized for diverse environments and are important in determining how a system runs. The parameter settings should be appropriate to an organization's workload and control environment, improper implementation and/or monitoring of operating systems can result in undetected errors and corruption of the data being processed, as well as lead to unauthorized access and inaccurate logging of system usage. Transaction logs are used to analyze transactions in master and/or transaction files. Authorization tables are used to verify implementation of logical access controls and will not be of much help when reviewing control features of an operating system. Routing tables do not contain information about the operating system and, therefore, provide no information to aid in the evaluation of controls.

QUESTION 542
When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:

A. an integrated services digital network (ISDN) data link.
B. traffic engineering.
C. wired equivalent privacy (WEP) encryption of data.
D. analog phone terminals.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To ensure that quality of service requirements are achieved, the Voice-over IP (VoIP) service over the wide area network (WAN) should be protected from packet losses, latency or jitter. To reach this objective, the network performance can be managed using statistical techniques such as traffic engineering. The standard bandwidth of an integrated services digital network (ISDN) data link would not provide the quality of services required for corporate VoIP services. WEP is an encryption scheme related to wireless networking. The VoIP phones are usually connected to a corporate local area network (LAN) and are not analog.

QUESTION 543

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

A. Session keys are dynamic
B. Private symmetric keys are used
C. Keys are static and shared
D. Source addresses are not encrypted or authenticated

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
WPA uses dynamic session keys, achieving stronger encryption than wireless encryption privacy (WEP), which operates with static keys (same key is used for everyone in the wireless network). All other choices are weaknesses of WEP.

QUESTION 544
During the audit of a database server, which of the following would be considered the GREATEST exposure?

A. The password does not expire on the administrator account
B. Default global security settings for the database remain unchanged
C. Old data have not been purged
D. Database activity is not fully logged

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Default security settings for the database could allow issues like blank user passwords or passwords that were the same as the username. Logging all database activity is not practical. Failure to purge old data may present a performance issue but is not an immediate security concern. Choice A is an exposure but not as serious as B.

QUESTION 545
Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

A. A user from within could send a file to an unauthorized person.

B. FTP services could allow a user to download files from unauthorized sources.
C. A hacker may be able to use the FTP service to bypass the firewall.
D. FTP could significantly reduce the performance of a DMZ server.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
Since file transfer protocol (FTP) is considered an insecure protocol, it should not be installed on a server in a demilitarized zone (DMZ). FTP could allow an unauthorized user to gain access to the network. Sending files to an unauthorized person and the risk of downloading unauthorized files are not as significant as having a firewall breach. The presence of the utility does not reduce the performance of a DMZ server; therefore, performance degradation is not a threat.

QUESTION 546
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 547
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 548
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 549
Accountability for the maintenance of appropriate security measures over information assets resides with the:

A. security administrator.
B. systems administrator.
C. data and systems owners.
D. systems operations group.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

QUESTION 550
The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

A. make unauthorized changes to the database directly, without an audit trail.
B. make use of a system query language (SQL) to access information.
C. remotely access the database.
D. update data without authentication.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Having access to the database could provide access to database utilities, which can update the database without an audit trail and without using the application. Using SQL only provides read access to information, in a networked environment, accessing the database remotely does not make a difference. What is critical is what is possible or completed through this access. To access a database, it is necessary that a user is authenticated using a user ID.

QUESTION 551
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 552
Which of the following is the MOST effective control when granting temporary access to vendors?

A. Vendor access corresponds to the service level agreement (SLA).
B. User accounts are created with expiration dates and are based on services provided.
C. Administrator access is provided for a limited period.
D. User IDs are deleted when the work is completed.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most effective control is to ensure that the granting of temporary access is based on services to be provided and that there is an expiration date (hopefully automated) associated with each ID. The SLA may have a provision for providing access, but this is not a control; it would merely define the need for access. Vendors require access for a limited period during the time of service. However, it is important to ensure that the access during this period is monitored. Deleting these user, I Dafter the work is completed is necessary, but if not automated, the deletion could be overlooked.

QUESTION 553
During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

A. an unauthorized user may use the ID to gain access.
B. user access management is time consuming.
C. passwords are easily guessed.
D. user accountability may not be established.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of a single user ID by more than one individual precludes knowing who in fact used that ID to access a system; therefore, it is literally impossible to hold anyone accountable. All user IDs, not just shared IDs, can be used by unauthorized individuals. Access management would not be any different with shared IDs, and shared user IDs do not necessarily have easily guessed passwords.

QUESTION 554
Which of the following satisfies a two-factor user authentication?

A. Iris scanning plus fingerprint scanning
B. Terminal ID plus global positioning system (GPS)
C. A smart card requiring the user's PIN
D. User ID along with password

Correct Answer: C
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). Proving who the user is usually requires a biometrics method, such as fingerprint, iris scan or voice verification, to prove biology. This is not a two-factor user authentication, because it proves only who the user is. A global positioning system (GPS) receiver reports on where the user is. The use of an ID and password (what the user knows) is a single- factor user authentication.

QUESTION 555
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 556
Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?

A. Security awareness
B. Reading the security policy
C. Security committee
D. Logical access controls

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To retain a competitive advantage and meet basic business requirements, organizations must ensure that the integrity of the information stored on their computer systems preserve the confidentiality of sensitive data and ensure the continued availability of their information systems. To meet these goals, logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy (choice B), which should be known by the organization's employees, would help to protect information, but would not prevent the unauthorized
access of information. A security committee (choice C) is key to the protection of information assets, but would address security issues within a broader perspective.

QUESTION 557
When reviewing an organization's logical access security, which of the following should be of MOST concern to an IS auditor?

A. Passwords are not shared.
B. Password files are not encrypted.
C. Redundant logon IDs are deleted.
D. The allocation of logon IDs is controlled.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When evaluating the technical aspects of logical security, unencrypted files represent the greatest risk. The sharing of passwords, checking for the redundancy of logon IDs and proper logon ID procedures are essential, but they are less important than ensuring that the password files are encrypted.

QUESTION 558
Passwords should be:

A. assigned by the security administrator for first time logon.
B. changed every 30 days at the discretion of the user.
C. reused often to ensure the user does not forget the password.
D. displayed on the screen so that the user can ensure that it has been entered properly.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days); however, changing should not be voluntary, it should be required by the system. Systems should not permit previous passwords to be used again. Old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

QUESTION 559
When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?
A. Read access to data
B. Delete access to transaction data files
C. Logged read/execute access to programs
D. Update access to job control language/script files

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
Deletion of transaction data files should be a function of the application support team, not operations staff. Read access to production data is a normal requirement of a computer operator, as is logged access to programs and access to JCL to control job execution.

QUESTION 560
To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

A. online terminals are placed in restricted areas.
B. online terminals are equipped with key locks.
C. ID cards are required to gain access to online terminals.
D. online access is terminated after a specified number of unsuccessful attempts.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most appropriate control to prevent unauthorized entry is to terminate connection after a specified number of attempts. This will deter access through the guessing of IDs and passwords. The other choices are physical controls, which are not effective in deterring unauthorized accesses via telephone lines.

QUESTION 561
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 562
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 563
Inadequate programming and coding practices introduce the risk of:

A. phishing.
B. buffer overflow exploitation.
C. SYN flood.
D. brute force attacks.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Buffer overflow exploitation may occur when programs do not check the length of the data that are input into a program. An attacker can send data that exceed the length of a buffer and override part of the program with malicious code. The countermeasure is proper programming and good coding practices. Phishing, SYN flood and brute force attacks happen independently of programming and coding practices.

QUESTION 564

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 565
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 566
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 567
Which of the following is the BEST method for preventing the leakage of confidential information in a laptop computer?

A. Encrypt the hard disk with the owner's public key.
B. Enable the boot password (hardware-based password).
C. Use a biometric authentication device.
D. Use two-factor authentication to logon to the notebook.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Only encryption of the data with a secure key will prevent the loss of confidential information. In such a case, confidential information can be accessed only with knowledge of the owner's private key, which should never be shared. Choices B, C and D deal with authentication and not with confidentiality of information. An individual can remove the hard drive from the secured laptop and install it on an unsecured computer, gaining access to the data.

QUESTION 568
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 569
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 570
Minimum password length and password complexity verification are examples of:

A. detection controls.
B. control objectives.
C. audit objectives.
D. control procedures.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Control procedures are practices established by management to achieve specific control objectives. Password controls are preventive controls, not detective controls. Control objectives are declarations of expected results from implementing controls and audit objectives are the specific goals of an audit.

QUESTION 571
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 572
When using a universal storage bus (USB) flash drive to transport confidential corporate data to an offsite location, an effective control would be to:

A. carry the flash drive in a portable safe.
B. assure management that you will not lose the flash drive.

C. request that management deliver the flash drive by courier.
D. encrypt the folder containing the data with a strong key.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Encryption, with a strong key, is the most secure method for protecting the information on the flash drive. Carrying the flash drive in a portable safe does not guarantee the safety of the information in the event that the safe is stolen or lost. No matter what measures you take, the chance of losing the flash drive still exists. It is possible that a courier might lose the flash drive or that it might be stolen.

QUESTION 573
A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?

A. Introduce a secondary authentication method such as card swipe
B. Apply role-based permissions within the application system
C. Have users input the ID and password for each database transaction
D. Set an expiration period for the database password embedded in the program

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When a single ID and password are embedded in a program, the best compensating control would be a sound access control over the application layer and procedures to ensure access to data is granted based on a user's role. The issue is user permissions, not authentication, therefore adding a stronger authentication does not improve the situation. Having a user input the ID and password for access would provide a better control because a database log would identify the initiator of the activity. However, this may not be efficient because each transaction would require a separate authentication process. It is a good practice to set an
expiration date for a password. However, this might not be practical for an ID automatically logged in from the program. Often, this type of password is set not to expire.

QUESTION 574
Which of the following is the BEST practice to ensure that access authorizations are still valid?

A. information owner provides authorization for users to gain access
B. identity management is integrated with human resource processes
C. information owners periodically review the access controls
D. An authorization matrix is used to establish validity of access

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Personnel and departmental changes can result in authorization creep and can impact the effectiveness of access controls. Many times when personnel leave an organization, or employees are promoted, transferred or demoted, their system access is not fully removed, which increases the risk of unauthorized access. The best practices for ensuring access authorization is still valid is to integrate identity management with human resources processes. When an employee transfers to a different function, access rights are adjusted at the same time.

QUESTION 575
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 576

An organization is using an enterprise resource management (ERP) application. Which of the following would be an effective access control?

A. User-level permissions
B. Role-based
C. Fine-grained
D. Discretionary

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Role-based access controls the system access by defining roles for a group of users. Users are assigned to the various roles and the access is granted based on the user's role. User-level permissions for an ERP system would create a larger administrative overhead. Fine-grained access control is very difficult to implement and maintain in the context of a large enterprise.
Discretionary access control may be configured or modified by the users or data owners, and therefore may create inconsistencies in the access control management.

QUESTION 577
What should be the GREATEST concern to an IS auditor when employees use portable media (MP3 players, flash drives)?

A. The copying of sensitive data on them
B. The copying of songs and videos on them
C. The cost of these devices multiplied by all the employees could be high
D. They facilitate the spread of malicious code through the corporate network

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The MAIN concern with MP3 players and flash drives is data leakage, especially sensitive information. This could occur if the devices were lost or stolen. The risk when copying songs and videos is copyright infringement, but this is normally a less important risk than information leakage. Choice C is hardly an issue because employees normally buy the portable media with their own funds. Choice D is a possible risk, but not as important as information leakage and can be reduced by other controls.

QUESTION 578
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 579
An IS auditor has completed a network audit. Which of the following is the MOST significant logical security finding?

A. Network workstations are not disabled automatically after a period of inactivity.
B. Wiring closets are left unlocked
C. Network operating manuals and documentation are not properly secured.
D. Network components are not equipped with an uninterruptible power supply.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choice A is the only logical security finding. Network logical security controls should be in place to restrict, identify, and report authorized and unauthorized users of the network. Disabling inactive workstations restricts users of the network. Choice D is an environmental issue and choices B and C are physical security issues. Choices B, C and D should be reported to the appropriate entity.

QUESTION 580
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 581
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 582
The responsibility for authorizing access to a business application system belongs to the:

A. data owner.
B. security administrator.
C. IT security manager.
D. requestor's immediate supervisor.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When a business application is developed, the best practice is to assign an information or data owner to the application. The Information owner should be responsible for authorizing access to the application itself or to back-end databases for queries. Choices B and C are not correct because the security administrator and manager normally do not have responsibility for authorizing access to business applications. The requestor's immediate supervisor may share the responsibility for approving user access to a business application system; however, the final responsibility should go to the information owner.

QUESTION 583
An organization has created a policy that defines the types of web sites that users are forbidden to access. What is the MOST effective technology to enforce this policy?

A. Stateful inspection firewall
B. Web content filter
C. Web cache server
D. Proxy server

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
A web content filter accepts or denies web communications according to the configured rules. To help the administrator properly configure the tool, organizations and vendors have made available URL blacklists and classifications for millions of web sites. A stateful inspection firewall is of little help in filtering web traffic since it does not review the content of the web site nor does it take into consideration the sites classification. A web cache server is designed to improve the speed of retrieving the most common or recently visited web pages. A proxy server is incorrect because a proxy server is a server which services the request of its clients by forwarding requests to other servers. Many people incorrectly use proxy server as a synonym of web proxy server even though not all web proxy servers have content filtering capabilities.

QUESTION 584
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 585
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 586
The MOST important difference between hashing and encryption is that hashing:

A. is irreversible.
B. output is the same length as the original message.
C. is concerned with integrity and security.
D. is the same at the sending and receiving end.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Hashing works one way; by applying a hashing algorithm to a message, a message hash/digest is created. If the same hashing algorithm is applied to the message digest, it will not result in the original message. As such, hashing is irreversible, while encryption is reversible. This is the basic difference between hashing and encryption. Hashing creates an output that is smaller than the original message, and encryption creates an output of the same length as the original message. Hashing is used to verify the integrity of the message and does not address security. The same hashing algorithm is used at the sending and receiving ends to generate and verify the message hash/digest. Encryption will not necessarily use the same algorithm at the sending and receiving and to encrypt and decrypt.

QUESTION 587
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 588
The MOST important success factor in planning a penetration test is:

A. the documentation of the planned testing procedure.
B. scheduling and deciding on the timed length of the test.
C. the involvement of the management of the client organization.
D. the qualifications and experience of staff involved in the test.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most important part of planning any penetration test is the involvement of the management of the client organization. Penetration testing without management approval could reasonably be considered espionage and is illegal in many jurisdictions.

QUESTION 589
Which of the following virus prevention techniques can be implemented through hardware?

A. Remote booting
B. Heuristic scanners
C. Behavior blockers
D. Immunizers

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Remote booting (e.g., diskless workstations) is a method of preventing viruses, and can be implemented through hardware. Choice C is a detection, not a prevention, although it is hardware-based. Choices B and D are not hard ware-based.

QUESTION 590
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 591
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 592
A certificate authority (CA) can delegate the processes of:

A. revocation and suspension of a subscriber's certificate.
B. generation and distribution of the CA public key.
C. establishing a link between the requesting entity and its public key.
D. issuing and distributing subscriber certificates.,

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Establishing a link between the requesting entity and its public key is a function of a registration authority. This may or may not be performed by a CA; therefore, this function can be delegated. Revocation and suspension and issuance and distribution of the subscriber certificate are functions of the subscriber certificate life cycle management, which the CA must perform.
Generation and distribution of the CA public key is a part of the CA key life cycle management process and, as such, cannot be delegated.

QUESTION 593
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 594
Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

A. Computation speed

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 595
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 596
To ensure message integrity, confidentiality and non-repudiation between two parties, the MOST effective method would be to create a message digest by applying a cryptographic hashing algorithm against:

A. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key by using the receiver's public key.

B.

B. any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key using the receiver's public key.
C. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering both the encrypted message and digest using the receiver's public key.
D. the entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Applying a cryptographic hashing algorithm against the entire message addresses the message integrity issue. Enciphering the message digest using the sender's private key addresses non repudiation. Encrypting the message with a symmetric key, thereafter allowing the key to be enciphered using the receiver's public key, most efficiently addresses the confidentiality of the message as well as the receiver's non repudiation. The other choices would address only a portion of the requirements.

QUESTION 597
Which of the following antivirus software implementation strategies would be the MOST effective in an interconnected corporate network?

A. Server antivirus software
B. Virus walls
C. Workstation antivirus software
D. Virus signature updating

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An important means of controlling the spread of viruses is to detect the virus at the point of entry, before it has an opportunity to cause damage. In an interconnected corporate network, virus scanning software, used as an integral part of firewall technologies, is referred to as a virus wall. Virus walls scan incoming traffic with the intent of detecting and removing viruses before they enter the protected network. The presence of virus walls does not preclude the necessity for installing virus detection software on servers and workstations within the network, but network- level protection is most effective the earlier the virus is detected. Virus signature updating is a must in all circumstances, networked or not.

QUESTION 598
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.
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 599
What is the BEST action to prevent loss of data integrity or confidentiality in the case of an e- commerce application running on a LAN, processing electronic fund transfers (EFT) and orders?

A. Using virtual private network (VPN) tunnels for data transfer
B. Enabling data encryption within the application
C. Auditing the access control to the network
D. Logging all changes to access lists

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

B.

Explanation:
The best way to ensure confidentiality and integrity of data is to encrypt it using virtual private network (VPN) tunnels. This is the most common and convenient way to encrypt the data traveling over the network. Data encryption within the application is less efficient than VPN. The other options are good practices, but they do not directly prevent the loss of data Integrity and confidentiality during communication through a network.

QUESTION 600
When conducting a penetration test of an IT system, an organization should be MOST concerned with:

A. the confidentiality of the report.
B. finding all possible weaknesses on the system.
C. restoring all systems to the original state.
D. logging all changes made to the production system.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
All suggested items should be considered by the system owner before agreeing to penetration tests, but the most important task is to be able to restore all systems to their original state.
Information that is created and/or stored on the tested systems should be removed from these systems. If for some reason, at the end of the penetration test, this is not possible, all files (with their location) should be identified in the technical report so that the client's technical staff will be able to remove these after the report has been received.

QUESTION 601
Which of the following penetration tests would MOST effectively evaluate incident handling and response capabilities of an organization?

A. Targeted testing
B. External testing
C. internal testing
D. Double-blind testing

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In a double-blind test, the administrator and security staff are not aware of the test, which will result in an assessment of the incident handling and response capability in an organization. In targeted, external, and internal testing, the system administrator and security staff are aware of the tests since they are informed before the start of the tests.

QUESTION 602

A.

B.

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

Personal firewall

Antivirus programs

C. Intrusion detection system (IDS)
D. Virtual local area network (VLAN) configuration

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An intrusion detection system (IDS) would be the next line of defense after the firewall. It would detect anomalies in the network/server activity and try to detect the perpetrator. Antivirus programs, personal firewalls and VIAN configurations would be later in the line of defense.

QUESTION 603
In wireless communication, which of the following controls allows the device receiving the communications to verify that the received communications have not been altered in transit?

A. Device authentication and data origin authentication
B. Wireless intrusion detection (IDS) and prevention systems (IPS)
C. The use of cryptographic hashes
D. Packet headers and trailers

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit. This prevents masquerading and message modification attacks. Device authentication and data origin authentication is not the correct answer since authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading. Wireless iDS/IPSs is not the correct answer since wireless IDS/IPS shave the ability to detect misconfigured devices and rogue devices, and detect and possibly stop certain types of attacks. Packet headers and trailers alone do not ensure that the content has not been altered.
A.

B.

QUESTION 604
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?

Implement Wired Equivalent Privacy (WEP)
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 605
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:

A.

B.

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 606
The GREATEST risk posed by an improperly implemented intrusion prevention system (IPS) is:

that there will be too many alerts for system administrators to verify.

A.

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 607
The MOST effective control for reducing the risk related to phishing is:

A. centralized monitoring of systems.
B. including signatures for phishing in antivirus software.
C. publishing the policy on antiphishing on the intranet.
D. security training for all users.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Phishing is a type of e-mail attack that attempts to convince a user that the originator is genuine, with the intention of obtaining information. Phishing is an example of a social engineering attack. Any social engineering type of attack can best Decontrolled through security and awareness training.

QUESTION 608
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 609
When using a digital signature, the message digest is computed:

A. only by the sender.
B. only by the receiver.
C. by both the sender and the receiver.
D. by the certificate authority (CA).

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A digital signature is an electronic identification of a person or entity. It is created by using asymmetric encryption. To verify integrity of data, the sender uses a cryptographic hashing algorithm against the entire message to create a message digest to be sent along with the message. Upon receipt of the message, the receiver will recompute the hash using the same algorithm and compare results with what was sent to ensure the integrity of the message.

QUESTION 610
Which of the following would effectively verify the originator of a transaction?

A. Using a secret password between the originator and the receiver
B. Encrypting the transaction with the receiver's public key
C. Using a portable document format (PDF) to encapsulate transaction content
D. Digitally signing the transaction with the source's private key

Correct Answer: D

Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A digital signature is an electronic identification of a person, created by using a public key algorithm, to verify to a recipient the identity of the source of a transaction and the integrity of its content. Since they are a 'shared secret' between the user and the system itself, passwords are considered a weaker means of authentication. Encrypting the transaction with the recipient's public key will provide confidentiality for the information, while using a portable document format(PDF) will probe the integrity of the content but not necessarily authorship.

QUESTION 611
A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network would use:

A. eavesdropping
B. spoofing.
C. traffic analysis.D. masquerading.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In traffic analysis, which is a passive attack, an intruder determines the nature of the traffic flow between defined hosts and through an analysis of session length, frequency and message length, and the intruder is able to guess the type of communication taking place. This typically is used when messages are encrypted and eavesdropping would not yield any meaningful results, in eavesdropping, which also is a passive attack, the intruder gathers the information flowing through the network with the intent of acquiring and releasing message contents for personal analysis or for third parties. Spoofing and masquerading are active attacks, in spoofing, a user receives an e-mail that appears to have originated from one source when it actually was sent from another source. In masquerading, the intruder presents an identity other than the original identity.

QUESTION 612
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 613
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 614
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 615
When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

A. hardware is protected against power surges.
B. integrity is maintained if the main power is interrupted.
C. immediate power will be available if the main power is lost.
D. hardware is protected against long-term power fluctuations.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A voltage regulator protects against short-term power fluctuations. It normally does not protect against long-term surges, nor does it maintain the integrity if power is interrupted or lost.

QUESTION 616
Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

A. Halon gas
B. Wet-pipe sprinklersC. Dry-pipe sprinklers
D. Carbon dioxide gas

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Water sprinklers, with an automatic power shutoff system, are accepted as efficient because they can be set to automatic release without threat to life, and water is environmentally friendly.
Sprinklers must be dry-pipe to prevent the risk of leakage. Halon is efficient and effective as it does not threaten human life and, therefore, can be set to automatic release, but it is environmentally damaging and very expensive. Water is an acceptable medium but the pipes should be empty to avoid leakage, so a full system is not a viable option. Carbon dioxide is accepted as an environmentally acceptable gas, but it is less efficient because it cannot be set to automatic release in a staffed site since it threatens life.

QUESTION 617
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 618
An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers-one filled with CO2, the other filled with halon. Which of the following should be given the HIGHEST priority in the auditor's report?

A. The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
B. Both fire suppression systems present a risk of suffocation when used in a closed room.
C. The CO2 extinguisher should be removed, because CO2 is ineffective for suppressing fires involving solid combustibles (paper).

D. The documentation binders should be removed from the equipment room to reduce potential risks.

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Protecting people's lives should always be of highest priority in fire suppression activities. COz and halon both reduce the oxygen ratio in the atmosphere, which can induce serious personal hazards, in many countries installing or refilling halon fire suppression systems is not allowed. Although COz and halon are effective and appropriate for fires involving synthetic combustibles and electrical equipment, they are nearly totally ineffective on solid combustibles (wood and paper). Although not of highest priority, removal of the documentation would probably reduce some of the risks.

QUESTION 619
Which of the following would be BEST prevented by a raised floor in the computer machine room?

A. Damage of wires around computers and servers
B. A power failure from static electricity
C. Shocks from earthquakes
D. Water flood damage.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary reason for having a raised floor is to enable power cables and data cables to be installed underneath the floor. This eliminates the safety and damage risks posed when cables are placed in a spaghetti-like fashion on an open floor. Static electricity should be avoided in the machine room; therefore, measures such as specially manufactured carpet or shoes would be more appropriate for static prevention than a raised floor. Raised floors do not address shocks from earthquakes. To address earthquakes, anti-seismic architecture would be required to establish a quake-resistant structural framework. Computer equipment needs to be protected against water. However, a raised floor would not prevent damage to the machines in the event of overhead water pipe leakage.

QUESTION 620
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 621
Users are issued security tokens to be used in combination with a PIN to access the corporate virtual private network (VPN). Regarding the PIN, what is the MOST important rule to be included in a security policy?

A. Users should not leave tokens where they could be stolen
B. Users must never keep the token in the same bag as their laptop computer
C. Users should select a PIN that is completely random, with no repeating digits
D. Users should never write down their PIN

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If a user writes their PIN on a slip of paper, an individual with the token, the slip of paper, and the computer could access the corporate network. A token and the PIN is a two-factor authentication method. Access to the token is of no value without the PIN; one cannot work without the other. The PIN does not need to be random as long as it is secret.

QUESTION 622
Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

A. Wet-pipe sprinkler system
B. Dry-pipe sprinkler system
C. FM-200system

D. Carbon dioxide-based fire extinguishers

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
FM-200 is safer to use than carbon dioxide. It is considered a clean agent for use in gaseous fire suppression applications. A water-based fire extinguisher is suitable when sensitive computer equipment could be damaged before the fire department personnel arrive at the site. Manual firefighting (fire extinguishers) may not provide fast enough protection for sensitive equipment (e.g., network servers).

QUESTION 623
During the review of a biometrics system operation, an IS auditor should FIRST review the stage of:

A. enrollment.
B. identification.
C. verification.
D. storage.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The users of a biometrics device must first be enrolled in the device. The device captures a physical or behavioral image of the human, identifies the unique features and uses an algorithm to convert them into a string of numbers stored as a template to be used in the matching processes.

QUESTION 624
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 625
What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

A. Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
B. The contingency plan for the organization cannot effectively test controlled access practices.
C. Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.
D. Removing access for those who are no longer authorized is complex.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The concept of piggybacking compromises all physical control established. Choice B would be of minimal concern in a disaster recovery environment. Items in choice C are not easily duplicated. Regarding choice D, while technology is constantly changing, card keys have existed for some time and appear to be a viable option for the foreseeable future.

QUESTION 626
An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?

A. False-acceptance rate (FAR)
B. Equal-error rate (EER)
C. False-rejection rate (FRR)
D. False-identification rate (FIR)

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
FAR is the frequency of accepting an unauthorized person as authorized, thereby granting access when it should be denied, in an organization with high security requirements, user annoyance with a higher FRR is less important, since it is better to deny access to an authorized individual than to grant access to an unauthorized individual. EER is the point where the FAR equals the FRR; therefore, it does not minimize the FAR. FIR is the probability that an authorized person is identified, but is assigned a false ID.

QUESTION 627
The MOST effective control for addressing the risk of piggybacking is:

A. a single entry point with a receptionist.
B. the use of smart cards.
C. a biometric door lock.
D. a deadman door.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Deadman doors are a system of using a pair of (two) 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 reduces the risk of an unauthorized person following an authorized person through a secured entry (piggybacking). The other choices are all physical controls over entry to a secure area but do not specifically address the risk of piggybacking.

QUESTION 628
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 629
Which of the following is the MOST effective control over visitor access to a data center?

A. Visitors are escorted.
B. Visitor badges are required.
C. Visitors sign in.
D. Visitors are spot-checked by operators.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Escorting visitors will provide the best assurance that visitors have permission to access the data processing facility. Choices B and C are not reliable controls. Choice D is incorrect because visitors should be accompanied at all times while they are on the premises, not only when they are in the data processing facility.

QUESTION 630
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 631
A firm is considering using biometric fingerprint identification on all PCs that access critical datA. This requires:
A. that a registration process is executed for all accredited PC users.
B. the full elimination of the risk of a false acceptance.
C. the usage of the fingerprint reader be accessed by a separate password.
D. assurance that it will be impossible to gain unauthorized access to critical data.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The fingerprints of accredited users need to be read, identified and recorded, i.e., registered, before a user may operate the system from the screened PCs. Choice B is incorrect, as the false- acceptance risk of a biometric device may be optimized, but will never be zero because this would imply an unacceptably high risk of false rejection. Choice C is incorrect, as the fingerprint device reads the token (the user's fingerprint) and does not need to be protected in itself by a password. Choice Dis incorrect because the usage of biometric protection on PCs does not guarantee that other potential security weaknesses in the system may not be exploited to access protected data.

QUESTION 632

Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

A. Palm scan
B. Face recognition
C. Retina scan
D. Hand geometry

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Retina scan uses optical technology to map the capillary pattern of an eye's retina. This is highly reliable and has the lowest false-acceptance rate (FAR) among the current biometric methods. Use of palm scanning entails placing a hand on a scanner where a palm's physical characteristics are captured. Hand geometry, one of the oldest techniques, measures the physical characteristics of the user's hands and fingers from a three dimensional perspective. The palm and hand biometric techniques lack uniqueness in the geometry data. In face biometrics, a reader analyzes the images captured for general facial characteristics. Though considered a natural and friendly biometric, the main disadvantage of face recognition is the lack of uniqueness, which means that people looking alike can fool the device.

QUESTION 633
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 634
The purpose of a deadman door controlling access to a computer facility is primarily to:

A. prevent piggybacking.
B. prevent toxic gases from entering the data center.
C. starve a fire of oxygen.
D. prevent an excessively rapid entry to, or exit from, the facility.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The purpose of a deadman door controlling access to a computer facility is primarily intended to prevent piggybacking. Choices B and C could be accomplished with a single self-closing door. Choice D is invalid, as a rapid exit may be necessary in some circumstances, e.g., a fire.

QUESTION 635
An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

A. adequate fire insurance exists.
B. regular hardware maintenance is performed.
C. offsite storage of transaction and master files exists.
D. backup processing facilities are fully tested.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

QUESTION 636
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 637
Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

A. There are three individuals with a key to enter the area.
B. Paper documents are also stored in the offsite vault.
C. Data files that are stored in the vault are synchronized.
D. The offsite vault is located in a separate facility.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because an IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

QUESTION 638
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 639
To provide protection for media backup stored at an offsite location, the storage site should be:

A. located on a different floor of the building.
B. easily accessible by everyone.
C. clearly labeled for emergency access.
D. protected from unauthorized access.

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
The offsite storage site should always be protected against unauthorized access and have at least the same security requirements as the primary site. Choice A is incorrect because, if the backup is in the same building, it may suffer the same event and may be inaccessible. Choices B and C represent access risks.

QUESTION 640
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 641
IS management has decided to install a level 1 Redundant Array of Inexpensive Disks (RAID) system in all servers to compensate for the elimination of offsite backups. The IS auditor should recommend:

A. upgrading to a level 5 RAID.
B. increasing the frequency of onsite backups.
C. reinstating the offsite backups.
D. establishing a cold site in a secure location.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A RAID system, at any level, will not protect against a natural disaster. The problem will not be alleviated without offsite backups, more frequent onsite backups or even setting up a cold site. Choices A, B and D do not compensate for the lack of offsite backup.

QUESTION 642
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 643
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 644
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 645
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 646
In the event of a data center disaster, which of the following would be the MOST appropriate strategy to enable a complete recovery of a critical database?

A. Daily data backup to tape and storage at a remote site
B. Real-time replication to a remote site
C. Hard disk mirroring to a local server
D. Real-time data backup to the local storage area network (SAN)

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
With real-time replication to a remote site, data are updated simultaneously in two separate locations; therefore, a disaster in one site would not damage the information located in the remote site. This assumes that both sites were not affected by the disaster. Daily tape backup recovery could lose up to a day's work of data. Choices C and D take place in the same data center and could possibly be affected by the same disaster.

QUESTION 647
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 648
What is the BEST backup strategy for a large database with data supporting online sales?

A. Weekly full backup with daily incremental backup
B. Daily full backup
C. Clustered servers
D. Mirrored hard disks

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Weekly full backup and daily incremental backup is the best backup strategy; it ensures the ability to recover the database and yet reduces the daily backup time requirements. A full backup normally requires a couple of hours, and therefore it can be impractical to conduct a full back up every day. Clustered servers provide a redundant processing capability, but are not a backup. Mirrored hard disks will not help in case of disaster.

QUESTION 649
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 650

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 651
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 652
A structured walk-through test of a disaster recovery plan involves:

A. representatives from each of the functional areas coming together to go over the plan.
B. all employees who participate in the day-to-day operations coming together to practice executing the plan.
C. moving the systems to the alternate processing site and performing processing operations.
D. distributing copies of the plan to the various functional areas for review.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A structured walk-through test of a disaster recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete and can be implemented when required. Choice B is a simulation test to prepare and train the personnel who will be required to respond to disasters and disruptions. Choice C is a form of parallel testing to ensure that critical systems will perform satisfactorily in the alternate site. Choice D is a checklist test.

QUESTION 653
In a contract with a hot, warm or cold site, contractual provisions should cover which of the following considerations?

A. Physical security measures
B. Total number of subscribers
C. Number of subscribers permitted to use a site at one time
D. References by other users

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The contract should specify the number of subscribers permitted to use the site at any one time. Physical security measures are not a part of the contract, although they are an important consideration when choosing a third-party site. The total number of subscribers is not a consideration; what is important is whether the agreement limits the number of subscribers in a building or in a specific area. The references that other users can provide is a consideration taken before signing the contract; it is by no means part of the contractual provisions.

QUESTION 654
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 655
Which of the following recovery strategies is MOST appropriate for a business having multiple offices within a region and a limited recovery budget?

A. A hot site maintained by the business
B. A commercial cold site
C. A reciprocal arrangement between its offices
D. A third-party hot site

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
For a business having many offices within a region, a reciprocal arrangement among its offices would be most appropriate. Each office could be designated as a recovery site for some other office. This would be the least expensive approach to providing an acceptable level of confidence. A hot site maintained by the business would be a costly solution but would provide a high degree of confidence. Multiple cold sites leased for the multiple offices would lead to a costly solution with a high degree of confidence. A third-party facility for recovery is provided by a traditional hot site. This would be a costly approach providing a high degree of confidence.

QUESTION 656
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 657
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 658
Which of the following is the MOST reasonable option for recovering a noncritical system?

A. Warm site
B. Mobile site
C. Hot site
D. Cold site

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Generally, a cold site is contracted for a longer period at a lower cost. Since it requires more time to make a cold site operational, it is generally used for noncritical applications. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations. A mobile site is a vehicle ready with all necessary computer equipment that can be moved to any cold or warm site depending upon the need. The need for a mobile site depends upon the scale of operations. A hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.

QUESTION 659
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 660
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 661
Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?

A. Invite client participation.
B. involve all technical staff.
C. Rotate recovery managers.
D. install locally-stored backup.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Recovery managers should be rotated to ensure the experience of the recovery plan is spread among the managers. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or offsite backup should always be used.

QUESTION 662
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 663
An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

-The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
-The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting their attention.
- the plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The IS auditor's report should recommend that:

A. the deputy CEO be censured for their failure to approve the plan.
B. a board of senior managers is set up to review the existing plan.
C. the existing plan is approved and circulated to all key management and staff.
D. a manager coordinates the creation of a new or revised plan within a defined time limit.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary concern is to establish a workable disaster recovery plan, which reflects current processing volumes to protect the organization from any disruptive incident. Censuring the deputy CEO will not achieve this and is generally not within the scope of an IS auditor to recommend.
Establishing a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation, and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short time is to make an experienced manager responsible for coordinating the knowledge of other managers into a single, formal document within a defined time limit.

QUESTION 664
An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

-The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.

-The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his/her attention.

-The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The basis of an organization's disaster recovery plan is to reestablish live processing at an alternative site where a similar, but not identical, hardware configuration is already established. An IS auditor should:

A. take no action as the lack of a current plan is the only significant finding.
B. recommend that the hardware configuration at each site is identical.
C. perform a review to verify that the second configuration can support live processing.
D. report that the financial expenditure on the alternative site is wasted without an effective plan.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor does not have a finding unless it can be shown that the alternative hardware cannot support the live processing system. Even though the primary finding is the lack of a proven and communicated disaster recovery plan, it is essential that this aspect of recovery is included in the audit. If it is found to be inadequate, the finding will materially support the overall audit opinion. It is certainly not appropriate to take no action at all, leaving this important factor untested. Unless it is shown that the alternative site is inadequate, there can be no comment on the expenditure, even if this is considered a proper comment for the IS auditor to make. Similarly, there is no need for the configurations to be identical. The alternative site could actually exceed the recovery requirements if it is also used for other work, such as other processing or systems development and testing. The only proper course of action at this point would be to find out if the recovery site can actually cope with a recovery.

QUESTION 665
Disaster recovery planning (DRP) for a company's computer system usually focuses on:

A. operations turnover procedures.
B. strategic long-range planning.
C. the probability that a disaster will occur.
D. alternative procedures to process transactions.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
It is important that disaster recovery identifies alternative processes that can be put in place while the system is not available.

QUESTION 666
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 667
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 668
Facilitating telecommunications continuity by providing redundant combinations of local carrier T- 1 lines, microwaves and/or coaxial cables to access the local communication loop:

A. last-mile circuit protection.
B. long-haul network diversity.
C. diverse routing.
D. alternative routing.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The method of providing telecommunication continuity through the use of many recovery facilities, providing redundant combinations of local carrier T-ls, microwave and/or coaxial cable to access the local communication loop in the event of a disaster, is called last-mile circuit protection.
Providing diverse long-distance network availability utilizing T-l circuits among major long- distance carriers is called long-haul network diversity. This ensures longdistance access should any one carrier experience a network failure. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics.

QUESTION 669
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 670
Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization?

A. Built-in alternative routing
B. Completing full system backup daily
C. A repair contract with a service provider
D. A duplicate machine alongside each server

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Alternative routing would ensure the network would continue if a server is lost or if a link is severed as message rerouting could be automatic. System backup will not afford immediate protection. The repair contract is not as effective as perm a nentalte (native routing). Standby servers will not provide continuity if a link is severed.

QUESTION 671
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 672
There are several methods of providing telecommunications continuity. The method of routing traffic through split cable or duplicate cable facilities is called:

A. alternative routing.
B. diverse routing.
C. long-haul network diversity.
D. last-mile circuit protection.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
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. 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. Long-haul network diversity is a diverse, long-distance network utilizing T-l circuits among the major long-distance carriers. It ensures long-distance access should any carrier experience a network failure. Last-mile circuit protection is a redundant combination of local carrier T-ls, 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.

QUESTION 673
The responsibilities of a disaster recovery relocation team include:

A. obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule.
B. locating a recovery site, if one has not been predetermined, and coordinating the transport of company employees to the recovery site.
C. managing the relocation project and conducting a more detailed assessment of the damage to the facilities and equipment.
D. coordinating the process of moving from the hot site to a new location or to the restored original location.

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choice A describes an offsite storage team, choice B defines a transportation team and choice C defines a salvage team.

QUESTION 674
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 675
Which of the following disaster recovery/continuity plan components provides the GREATEST assurance of recovery after a disaster?

A. The alternate facility will be available until the original information processing facility is restored.
B. User management is involved in the identification of critical systems and their associated critical recovery times.
C. Copies of the plan are kept at the homes of key decision-making personnel.
D. Feedback is provided to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
The alternate facility should be made available until the original site is restored to provide the greatest assurance of recovery after a disaster. Without this assurance, the plan will not be successful. All other choices ensure prioritization or the execution pf the plan.

QUESTION 676
Which of the following must exist to ensure the viability of a duplicate information processing facility?

A. The site is near the primary site to ensure quick and efficient recovery.
B. The site contains the most advanced hardware available.
C. The workload of the primary site is monitored to ensure adequate backup is available.
D. The hardware is tested when it is installed to ensure it is working properly.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need. Testing the hardware when the site is established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.

QUESTION 677
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 678
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 679
A disaster recovery plan for an organization's financial system specifies that the recovery point objective (RPO) is no data loss and the recovery time objective (RTO) is 72 hours. Which of the following is the MOST cost-effective solution?

A. A hot site that can be operational in eight hours with asynchronous backup of the transaction logs
B. Distributed database systems in multiple locations updated asynchronously
C. Synchronous updates of the data and standby active systems in a hot site
D. Synchronous remote copy of the data in a warm site that can be operational in 48 hours

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The synchronous copy of the storage achieves the RPO objective and a warm site operational in 48 hours meets the required RTO. Asynchronous updates of the database in distributed locations do not meet the RPO. Synchronous updates of the data and standby active systems in a hot site meet the RPO and RTO requirements but are more costly than a warm site solution.

QUESTION 680
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 681
The cost of ongoing operations when a disaster recovery plan is in place, compared to not having a disaster recovery plan, will MOST likely:

A. increase.
B. decrease.
C. remain the same.
D. be unpredictable.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Due to the additional cost of disaster recovery planning (DRP) measures, the cost of normal operations for any organization will always increase after a DRP implementation, i.e., the cost of normal operations during a nondisaster period will be more than the cost of operations during a nondisaster period when no disaster recovery plan was in place.

QUESTION 682

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 683
Which of the following provides the BEST evidence of an organization's disaster recovery readiness?

A. A disaster recovery plan
B. Customer references for the alternate site provider
C. Processes for maintaining the disaster recovery plan
D. Results of tests and drills

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Plans are important, but mere plans do not provide reasonable assurance unless tested. References for the alternate site provider and the existence and maintenance of a disaster recovery plan are important, but only tests and drills demonstrate the adequacy of the plans and provide reasonable assurance of an organization's disaster recovery readiness.

QUESTION 684
Which of the following is the BEST method for determining the criticality of each application system in the production environment?

A. interview the application programmers.
B. Perform a gap analysis.

C. Review the most recent application audits.
D. Perform a business impact analysis.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A business impact analysis will give the impact of the loss of each application. Interviews with the application programmers will provide limited information related to the criticality of the systems. A gap analysis is only relevant to systems development and project management. The audits may not contain the required information or may not have been done recently.

QUESTION 685
A hot site should be implemented as a recovery strategy when the:
A. disaster tolerance is low.
B. recovery point objective (RPO) is high.
C. recovery time objective (RTO) is high.
D. disaster tolerance is high.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Disaster tolerance is the time gap during which the business can accept nonavailability of IT facilities. If this time gap is low, recovery strategies that can be implemented within a short period of time, such as a hot site, should be used. The RPO is the earliest point in time at which it is acceptable to recover the data. A high RPO means that the process can wait for a longer time. In such cases, other recovery alternatives, such as warm or cold sites, should be considered. A high RTO means that additional time would be available for the recovery strategy, thus making other recovery alternatives-such as warm or cold sites- viable alternatives.

QUESTION 686
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 687
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 688
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 689
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 690
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 691
If the recovery time objective (RTO) increases:

A. the disaster tolerance increases.
B. the cost of recovery increases.
C. a cold site cannot be used.
D. the data backup frequency increases.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The longer the recovery time objective (RTO), the higher disaster tolerance and the lower the recovery cost. It cannot be concluded that a cold site is inappropriate or that the frequency of data backup would increase.

QUESTION 692
Due to changes in IT, the disaster recovery plan of a large organization has been changed. What is the PRIMARY risk if the new plan is not tested?

A. Catastrophic service interruption
B. High consumption of resources
C. Total cost of the recovery may not be minimized
D. Users and recovery teams may face severe difficulties when activating the plan

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choices B, C and D are all possible problems that might occur, and would cause difficulties and financial losses or waste of resources. However, if a new disaster recovery plan is not tested, the possibility of a catastrophic service interruption is the most critical of all risks.

QUESTION 693
When developing a disaster recovery plan, the criteria for determining the acceptable downtime should be the:

A. annualized loss expectancy (ALE).
B. service delivery objective.
C. quantity of orphan data.
D. maximum tolerable outage.

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
The recovery time objective is determined based on the acceptable downtime in case of a disruption of operations, it indicates the maximum tolerable outage that an organization considers to be acceptable before a system or process must resume following a disaster. Choice A is incorrect, because the acceptable downtime would not be determined by the annualized loss expectancy (ALE). Choices B and C are relevant to business continuity, but they are not determined by acceptable downtime.

QUESTION 694
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 695
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 696
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 697
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 698
Which of the following issues should be the GREATEST concern to the IS auditor when reviewing an IT disaster recovery test?
A. Due to the limited test time window, only the most essential systems were tested. The other systems were tested separately during the rest of the year.
B. During the test it was noticed that some of the backup systems were defective or not working, causing the test of these systems to fail.
C. The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
D. Every year, the same employees perform the test. The recovery plan documents are not used since every step is well known by all participants.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A disaster recovery test should test the plan, processes, people and IT systems. Therefore, if the plan is not used, its accuracy and adequacy cannot be verified. Disaster recovery should not rely on key staff since a disaster can occur when they are not available. It is common that not all systems can be tested in a limited test time frame. It is important, however, that those systems which are essential to the business are tested, and that the other systems are eventually tested throughout the year. One aim of the test is to identify and replace defective devices so that all systems can be replaced in the case of a disaster. Choice B would only be a concern if the number of discovered problems is systematically very high, in a real disaster, there is no need for a clean shutdown of the original production environment since the first priority is to bring the backup site up.

QUESTION 699

The frequent updating of which of the following is key to the continued effectiveness of a disaster recovery plan (DRP)?

A. Contact information of key personnel
B. Server inventory documentation
C. individual roles and responsibilities
D. Procedures for declaring a disaster

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In the event of a disaster, it is important to have a current updated list of personnel who are key to the operation of the plan. Choices B, C and D would be more likely to remain stable overtime.

QUESTION 700
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 701
To address an organization's disaster recovery requirements, backup intervals should not exceed the:

A. service level objective (SLO).
B. recovery time objective (RTO).

C. recovery point objective (RPO).
D. maximum acceptable outage (MAO).

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The recovery point objective (RPO) defines the point in time to which data must be restored after a disaster so as to resume processing transactions. Backups should be performed in a way that the latest backup is no older than this maximum time frame. If service levels are not met, the usual consequences are penalty payments, not cessation of business. Organizations will try to set service level objectives (SLOs) so as to meet established targets. The resulting time for the service level agreement (SLA) will usually be longer than the RPO. The recovery time objective (RTO) defines the time period after the disaster in which normal business functionality needs to be restored. The maximum acceptable outage (MAO) is the maximum amount of system downtime that is tolerable. It can be used as a synonym for RTO. However, the RTO denotes an objective/target, while the MAO constitutes a vital necessity for an organization's survival.

QUESTION 702
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 703
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 704
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 705
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 706
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 707
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 708
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 709
Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?

A. A hot site contracted and available as needed.
B. A business continuity manual is available and current.
C. insurance coverage is adequate and premiums are current.
D. Media backups are performed on a timely basis and stored offsite.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.

QUESTION 710
The PRIMARY objective of business continuity and disaster recovery plans should be to:

A. safeguard critical IS assets.
B. provide for continuity of operations.
C. minimize the loss to an organization.
D. protect human life.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people. All other priorities are important but are secondary objectives of a business continuity and disaster recovery plan.

QUESTION 711
After a full operational contingency test, an IS auditor performs a review of the recovery steps. The auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the auditor recommend?
A. Perform an integral review of the recovery tasks.
B. Broaden the processing capacity to gain recovery time.
C. Make improvements in the facility's circulation structure.
D. increase the amount of human resources involved in the recovery.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Performing an exhaustive review of the recovery tasks would be appropriate to identify the way these tasks were performed, identify the time allocated to each of the steps required to accomplish recovery, and determine where adjustments can be made. Choices B, C and D could be actions after the described review has been completed.

QUESTION 712
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 713
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 714
During a business continuity audit an IS auditor found that the business continuity plan (BCP) covered 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 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 715
An IS auditor noted that an organization had adequate business continuity plans (BCPs) for each individual process, but no comprehensive BCP. Which would be the BEST course of action for the IS auditor?

A. Recommend that an additional comprehensive BCP be developed.
B. Determine whether the BCPs are consistent.
C. Accept the BCPs as written.
D. Recommend the creation of a single BCP.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Depending on the complexity of the 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 should be consistent with other plans to have a viable business continuity planning strategy.

QUESTION 716
When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?

A. Business continuity self-audit
B. Resource recovery analysis
C. Risk assessment
D. Gap analysis

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Risk assessment and business impact assessment are tools for understanding business- for- business continuity planning. Business continuity self-audit is a tool for evaluating the adequacy of the BCP, resource recovery analysis is a tool for identifying a business resumption strategy, while the role gap analysis can play in business continuity planning is to identify deficiencies in a plan. Neither of these is used for gaining an understanding of the business.

QUESTION 717
During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?

A. Evacuation plan
B. Recovery priorities
C. Backup storages
D. Call tree

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Protecting human resources during a disaster-related event should be addressed first. Having separate BCPs could result in conflicting evacuation plans, thus jeopardizing the safety of staff and clients. Choices B, C and D may be unique to each department and could be addressed separately, but still should be reviewed for possible conflicts and/or the possibility of cost reduction, but only after the issue of human safety has been analyzed.

QUESTION 718
Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:

A. downtime costs.
B. resumption costs.
C. recovery costs.
D. walkthrough costs.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since the recovery time is longer in plan B, resumption and recovery costs can be expected to be lower. Walkthrough costs are not a part of disaster recovery. Since the management considered a higher window for recovery in plan B, downtime costs included in the plan are likely to be higher.

QUESTION 719
The optimum business continuity strategy for an entity is determined by the:

A. lowest downtime cost and highest recovery cost.
B. lowest sum of downtime cost and recovery cost.
C. lowest recovery cost and highest downtime cost.
D. average of the combined downtime and recovery cost.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Both costs have to be minimized, and the strategy for which the costs are lowest is the optimum strategy. The strategy with the highest recovery cost cannot be the optimum strategy. The strategy with the highest downtime cost cannot be the optimum strategy. The average of the combined downtime and recovery cost will be higher than the lowest combined cost of downtime and recovery.

QUESTION 720
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 721
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 722
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 723
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 724
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 725
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 726

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 727
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 728

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 729

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 730
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 731
Talking about biometric authentication, physical characteristics typically include (Choose five.):

A. fingerprints

B. eye retinas
C. irises
D. facial patternsE. hand measurements F. None of the choices.

Correct Answer: ABCDE
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Biometric authentication refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes. Physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while behavioral characteristics include signature, gait and typing patterns. Voice is often considered as a mix of both physical and behavioral characteristics.

QUESTION 732
Talking about biometric authentication, which of the following is often considered as a mix of both physical and behavioral characteristics?

A. Voice
B. Finger measurement
C. Body measurement
D. Signature
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Biometric authentication refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes. Physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while behavioral characteristics include signature, gait and typing patterns. Voice is often considered as a mix of both physical and behavioral characteristics.

QUESTION 733
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 734
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 735
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 736
As part of the IEEE 802.11 standard ratified in September 1999, WEP uses which stream cipher for confidentiality?

A. CRC-32
B. CRC-64
C. DES
D. 3DES
E. RC4
F. RC5
G. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference: Explanation:
As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.

QUESTION 737
As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the CRC- 32 checksum for:

A. integrity.
B. validity.
C. accuracy.
D. confidentiality.

E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. Many WEP systems require a key in hexadecimal format. If one chooses keys that spell words in the limited 0-9, A-F hex character set, these keys can be easily guessed.

QUESTION 738
Many WEP systems require a key in a relatively insecure format. What format is this?

A. binary format.
B. hexadecimal format.
C. 128 bit format.
D. 256 bit format.
E. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. Many WEP systems require a key in hexadecimal format. If one chooses keys that spell words in the limited 0-9, A-F hex character set, these keys can be easily guessed.

QUESTION 739
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 740
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 741
Which of the following refers to a symmetric key cipher which operates on fixedlength groups of bits with an unvarying transformation?

A. stream cipher
B. block cipher
C. check cipher
D. string cipher

E. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation.
A stream cipher, on the other hand, operates on individual digits one at a time.

QUESTION 742
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 743
Which of the following is a tool you can use to simulate a big network structure on a single computer?

A. honeymoon
B. honeytrap
C. honeytube
D. honeyd

E. None of the choices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
honeyd is a GPL licensed software you can use to simulate a big network structure on a single computer.

QUESTION 744
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 745
What would be the major purpose of rootkit?

A. to hide evidence from system administrators.
B. to encrypt files for system administrators.
C. to corrupt files for system administrators.
D. to hijack system sessions.
E. None of the choices.

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
rootkit originally describes those recompiled Unix tools that would hide any trace of the intruder.
You can say that the only purpose of rootkit is to hide evidence from system administrators so there is no way to detect malicious special privilege access attempts.

QUESTION 746
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 747
The Trojan.Linux.JBellz Trojan horse runs as a malformed file of what format?

A. e-mails.
B. MP3.
C. MS Office.
D. Word template.
E. None of the choices.

Correct Answer: B

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 748
Which of the following types of spyware was originally designed for determining the sources of error or for measuring staff productivity?

A. Keywords logging
B. Keystroke logging
C. Directory logging
D. Password logging
E. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Keystroke logging (in the form of spyware) was originally a function of diagnostic tool deployed by software developers for capturing user's keystrokes. This is done for determining the sources of error or for measuring staff productivity.

QUESTION 749
You should know the difference between an exploit and a vulnerability. Which of the following refers to a weakness in the system?

A. exploit
B. vulnerability
C. both

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
You should know the difference between an exploit and a vulnerability. An exploit refers to software, data, or commands capable of taking advantage of a bug, glitch or vulnerability in order to cause unintended behavior. Vulnerability in this sense refers to a weakness in the system.

QUESTION 750
Which of the following is a rewrite of ipfwadm?

A. ipchains
B. iptables
C. Netfilter
D. ipcook
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
ipchains is a free software based firewall running on earlier Linux. It is a rewrite of ipfwadm but is superseded by iptables in Linux 2.4 and above. Iptables controls the packet filtering and NAT components within the Linux kernel. It is based on Netfilter, a framework which provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.

QUESTION 751
Iptables is based on which of the following frameworks?

A. Netfilter
B. NetDoom
C. NetCheck
D. NetSecure
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
ipchains is a free software based firewall running on earlier Linux. It is a rewrite of ipfwadm but is superseded by iptables in Linux 2.4 and above.
Iptables controls the packet filtering and NAT components within the Linux kernel. It is based on Netfilter, a framework which provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.

QUESTION 752
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 753
Which of the following correctly describe the potential problem of deploying Wi-Fi Protected Access to secure your wireless network?

A. potential compatibility problems with wireless network interface cards.
B. potential compatibility problems with wireless access points.
C. potential performance problems with wireless network interface cards.
D. potential performance problems with wireless access points.
E. None of the choices.

Correct Answer: B
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).

QUESTION 754
The Federal Information Processing Standards (FIPS) were developed by:

A. the United States Federal government
B. ANSI
C. ISO
D. IEEE
E. IANA
F. None of the choices.

Correct Answer: A
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 755
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 756
Sophisticated database systems provide many layers and types of security, including (Choose three.):

A. Access control
B. Auditing
C. Encryption
D. Integrity controls
E. Compression controls

Correct Answer: ABCD
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Sophisticated database systems 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 757
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 758
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 759
Creating which of the following is how a hacker can insure his ability to return to the hacked system at will?

A. rootsec
B. checksum
C. CRC
D. backdoors
E. None of the choices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A backdoor refers to a generally undocumented means of getting into a system, mostly for programming and maintenance/troubleshooting needs. Most real world programs have backdoors. Creating backdoors is how a hacker can insure his ability to return to the hacked system at will.

QUESTION 760

A trojan horse simply cannot operate autonomously.

A. true
B. false

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
As a common type of Trojan horses, a legitimate software might have been corrupted with malicious code which runs when the program is used. The key is that the user has to invoke the program in order to trigger the malicious code. In other words, a trojan horse simply cannot operate autonomously. You would also want to know that most but not all trojan horse payloads are harmful - a few of them are harmless.

QUESTION 761
Which of the following refers to the collection of policies and procedures for implementing controls capable of restricting access to computer software and data files?

A. Binary access control
B. System-level access control
C. Logical access control
D. Physical access controlE. Component access control
F. None of the choices.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:
Explanation:
Logical access control is about the use of a collection of policies, procedures, and controls to restrict access to computer software and data files. Such control system should provide reasonable assurance that an organization's objectives are being properly achieved securely and reliably.

QUESTION 762
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 763
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:
Section: Protection of Information Assets
Explanation

Explanation/Reference:
A

QUESTION 764
An IS auditor plans to review all access attempts to a video-monitored and proximity-card controlled communications room. Which of the following would be **MOST** useful to the auditor?

A. System electronic log
B. Security incident log
C. Manual sign-in and sign-out log
D. Alarm system with CCTV

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Reference: https://www.slideshare.net/desmond.devendran/chap5-2007-cisa-review-course

QUESTION 765
A company uses a standard form to document and approve all changes in production programs. To ensure that the forms are properly authorized, which of the following is the **MOST** effective sampling method?

A. Attribute
B. Variable
C. Discovery
D. Monetary

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 766

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 767

During the review of a business process reengineering project, the **PRIMARY** concern of an IS auditor is to determine whether the new business model:

A. is aligned with industry best practices.
B. is aligned with organizational goals.
C. leverages benchmarking results.
D. meets its key performance measures.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 768

The **PRIMARY** purpose of reviewing the IT strategic plan is to identify risks that may:

A. limit the ability to deliver customer requirements.
B. limit the organization's ability to achieve its objectives.
C. impact operational efficiency of the IT department.

Correct Answer:
Section: Protection of Information Assets
Explanation

Explanation/Reference:
D. impact financial resourcing to implement the plan.

B

QUESTION 769
An IS auditor finds that intellectual property is not being protected to the level specified in the organization's data classification and protection policy. The business owner is aware of this issue and chooses to accept the risk. Which of the following is the auditor's **BEST** course of action?

A. Note the finding and request formal acceptance.
B. Include the finding in the follow-up audit.
C. Amend the data classification policy.
D. Form a committee and further investigate the issue.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 770
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 771
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 772
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 773
Which of the following could be determined by entity-relationship diagram?

A. Links between data objects
B. How the system behaves as a consequence of external events

Correct Answer:
Section: Protection of Information Assets
Explanation

Explanation/Reference:
C. How data are transformed as they move through the system
D. Modes of behavior of data objects

A

QUESTION 774
Which of the following is a method to prevent disclosure of classified documents printed on a shared printer?

A. Requiring a key code to be entered on the printer to produce hardcopy
B. Producing a header page with classification level for printed documents
C. Encrypting the data stream between the user's computer and the printer
D. Using passwords to allow authorized users to send documents to the printer

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 775
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 776
A database is denormalized in order to:

Explanation

Explanation/Reference:
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 777
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 778
When removing a financial application system from production, which of the following is **MOST** important?

A. Media used by the retired system has been sanitized.
B. Data retained for regulatory purposes can be retrieved.
C. End-user requests for changes are recorded and tracked.
D. Software license agreements are retained.

B

QUESTION 779
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 780
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 781
An organization is currently replacing its accounting system. Which of the following strategies will **BEST** minimize risk associated with the loss of data integrity from the upgrade?
A. Pilot implementation
B. Functional integration testing
C. Fallback contingency
D. Parallel implementation

Correct Answer: B
Correct Answer:
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 782
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 783
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

A

QUESTION 784
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 785
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 786
An IS auditor finds the log management system is overwhelmed with false positive alerts. The auditor's **BEST** recommendation would be to:
A. recruit more monitoring personnel.
B. fine tune the intrusion detection system (IDS).
C. reduce the firewall rules.
D. establish criteria for reviewing alerts.

Correct Answer: D

Correct Answer:
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 787
Which of the following is the **BEST** reason for an organization to develop a business continuity plan?

A. To develop a detailed description of information systems and processes
B. To identify the users of information systems and processes
C. To avoid the costs resulting from the failure of key systems and processes
D. To establish business unit prioritization of systems, projects, and strategies

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Reference: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Business-Continuity-Management-Audit-Assurance-Program.aspx

QUESTION 788
One advantage of managing an entire collection of projects as a portfolio is that it highlights the need to:

A. identify dependencies between projects.
B. inform users about all ongoing projects.
C. manage the risk of each individual project.
D. manage the quality of each project.

D

QUESTION 789
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 790
Which of the following should be an IS auditor's **BEST** recommendation to prevent installation of unlicensed software on employees' company-provided devices?

A. Enforce audit logging of software installation activities.
B. Restrict software installation authority to administrative users only.
C. Implement software blacklisting.
D. Remove unlicensed software from end-user devices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 791
Which of the following is the **MOST** reliable way for an IS auditor to evaluate the operational effectiveness of an organization's data loss prevention (DLP)

controls? A. Verify that confidential files cannot be transmitted to a personal USB device.

Correct Answer:
Section: Protection of Information Assets

B. Conduct interviews to identify possible data protection vulnerabilities.
C. Review data classification levels based on industry best practice.
D. Verify that current DLP software is installed on all computer systems.

Correct Answer: C
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 792
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 793
Which of the following is the **MOST** effective method of destroying sensitive data stored on electronic media?

A. Physical destruction
B. Degaussing
C. Random character overwrite
D. Low-level formatting

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
Reference: https://www.isaca.org/Journal/archives/2010/Volume-6/Pages/An-Introduction-to-Digital-Records-Management.aspx

QUESTION 794
Email required for business purposes is being stored on employees' personal devices. Which of the following is an IS auditor's **BEST** recommendation?

A. Implement an email containerization solution on personal devices B. Prohibit employees from storing company email on personal devices.
C. Ensure antivirus to utilize passwords on personal devices.
D. Require employees to utilize passwords on personal devices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 795
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 796
Which of the following IS functions can be performed by the same group or individual while still providing the proper segregation of duties?

A. Computer operations and application programming
B. Database administration and computer operations
C. Security administration and application programming
D. Application programming and systems analysis

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Reference: https://www.isaca.org/Journal/archives/2016/volume-3/Pages/implementing-segregation-of-duties.aspx

QUESTION 797
An organization wants to reuse company-provided smartphones collected from staff leaving the organization. Which of the following would be the **BEST** recommendation?

A. The memory cards of the smartphones should be replaced.
B. Smartphones should not be reused, but physically destroyed.
C. Data should be securely deleted from the smartphones.
D. The SIM card and telephone number should be changed.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 798
During a review of information security procedures for disabling user accounts, an IS auditor discovers that IT is only disabling network access for terminated employees. IT management maintains if terminated users cannot access the network, they will not be able to access any applications. Which of the following is the **GREATEST** risk associated with application access?

A. Unauthorized access to data
B. Inability to access data
C. Lack of segregation of duties
D. Loss of non-repudiation

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:

QUESTION 799
Adopting a service-oriented architecture would **MOST** likely:

A. inhibit integration with legacy systems.
B. compromise application software security.
C. facilitate connectivity between partners.
D. streamline all internal processes.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 800
An organization has established three IS processing environments: development, test, and production. The **MAJOR** reason for separating the development and test environments is to:

A. obtain segregation of duties between IS staff and end users.
B. limit the user's access rights to the test environment.
C. perform testing in a stable environment.
D. protect the programs under development from unauthorized testing.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 801
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 802
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 803
The use of symmetric key encryption controls to protect sensitive data transmitted over a communications network requires that:

A. primary keys for encrypting the data be stored in encrypted form.
B. encryption keys be changed only when a compromise is detected at both ends.
C. encryption keys at one end be changed on a regular basis.
D. public keys be stored in encrypted form.

Correct Answer: A
Section: Protection of Information Assets Explanation

Explanation/Reference:
QUESTION 804
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 805
Which of the following should be the **PRIMARY** basis for prioritizing follow-up audits?

A. Complexity of management's actions plans
B. Recommendation from executive management
C. Audit cycle defined in the audit plan
D. Residual risk from the findings of previous audits

Correct Answer: D
Section: Protection of Information Assets Explanation

Explanation/Reference:

QUESTION 806
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
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 807
Which of the following controls can **BEST** detect accidental corruption during transmission of data across a network?

A. Sequence checking
B. Parity checking
C. Symmetric encryption
D. Check digit verification

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Parity check is used to detect transmission errors in the data. When a parity check is applied to a single character, it is called vertical or column check. In addition, if a parity check is applied to all the data it is called vertical or row check. By using both types of parity check simultaneously can greatly increase the error detection possibility, which may not be possible when only one type of parity check is used.

QUESTION 808
An IS auditor is asked to identify risk within an organization's software development project. The project manager tells the auditor that an agile development methodology is being used to minimize the lengthy development process. Which of the following would be of **GREATEST** concern to the auditor?

A. Each team does its own testing.
B. The needed work has not yet been fully identified.
C. Some of the developers have not attended recent training.
D. Elements of the project have not been documented.

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:

QUESTION 809
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 810
An organization transmits large amounts of data from one internal system to another. The IS auditor is reviewing the quality of the data at the originating point. Which of the following should the auditor verify **FIRST**?

A. The data has been encrypted.
B. The data transformation is accurate.
C. The data extraction process is completed.
D. The source data is accurate.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference: