CISA.exam.650q

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

CISA

Certified Information Systems Auditor

Sections

1. Information System Acquisition, Development and Implementation
2. Information System Operations, Maintenance and Support

3. Protection of Information Assets

Exam A

QUESTION 1

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 are 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 2
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 are 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 3
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

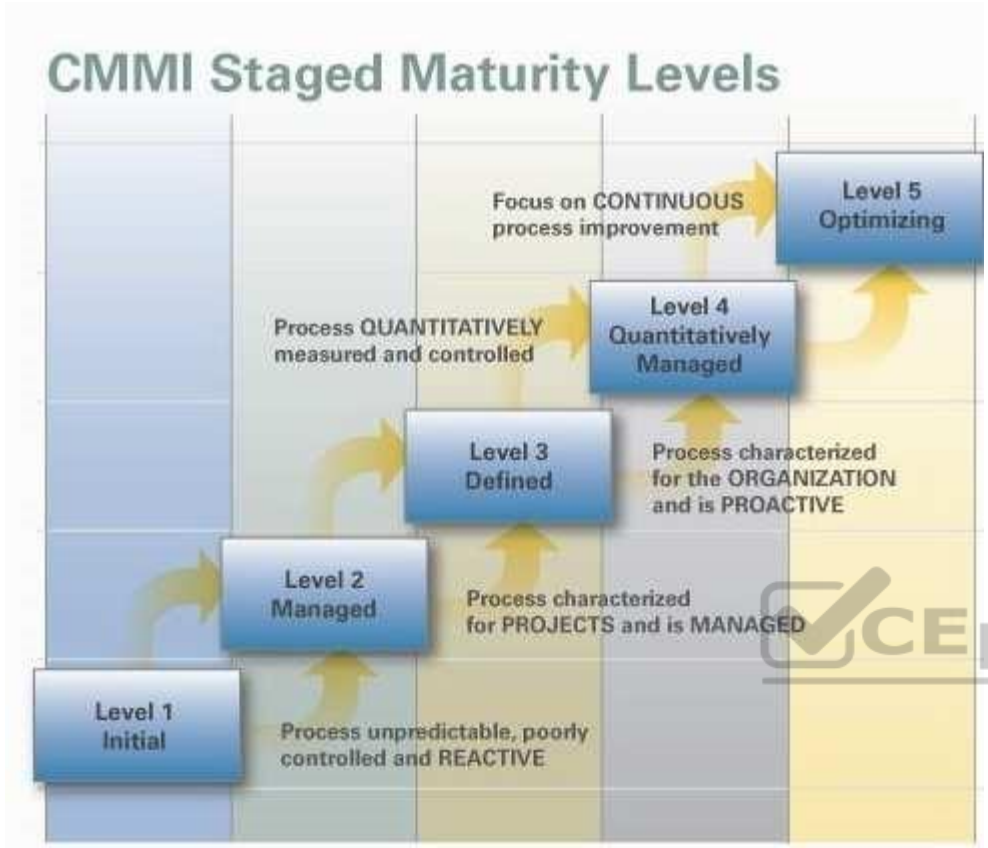
Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

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 4
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

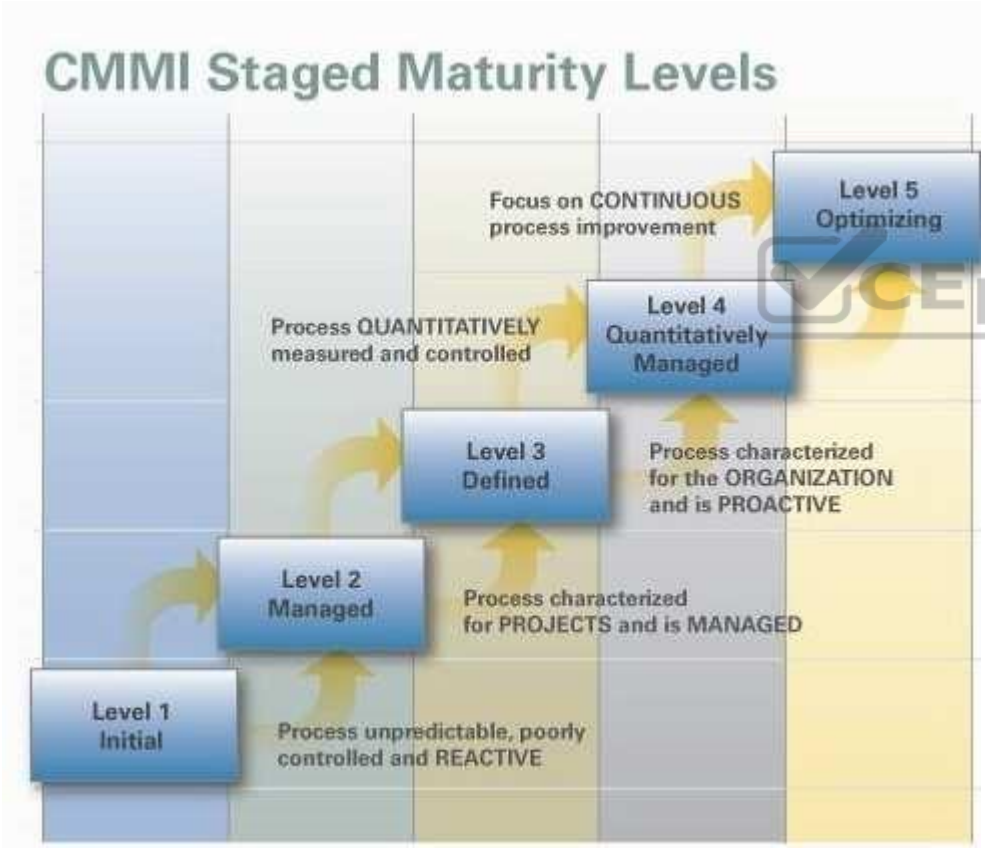
Correct Answer: C
Section: Information System Acquisition, Development and Implementation
Explanation

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 5
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

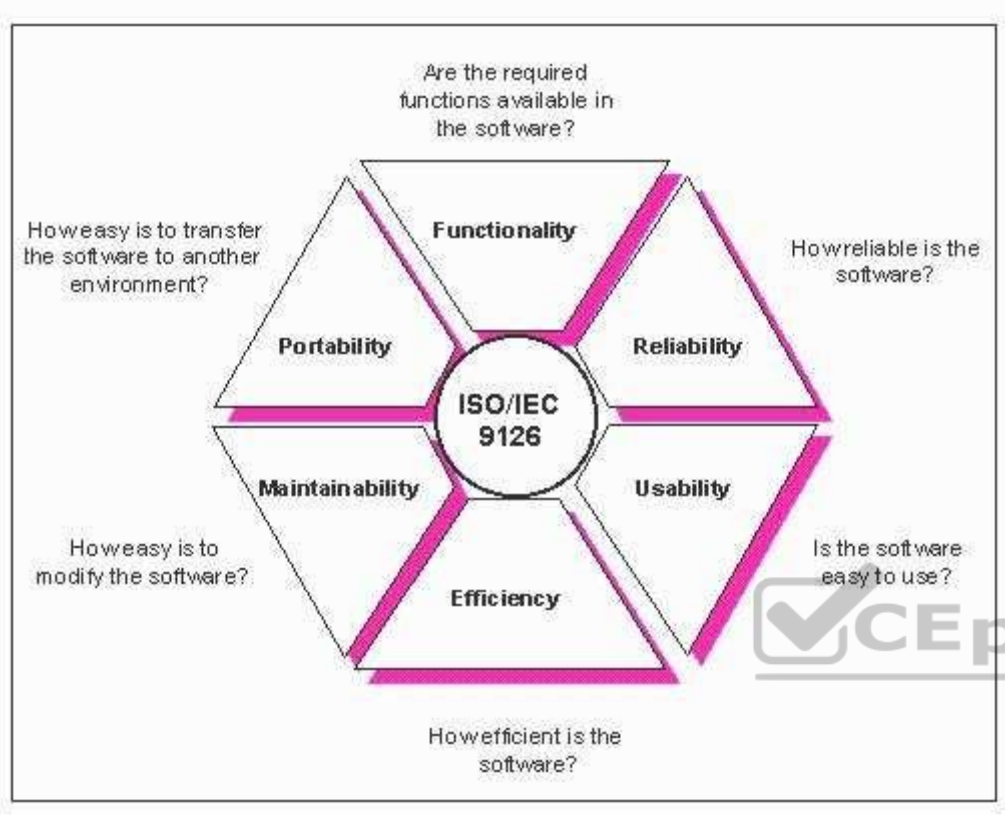


Image above from: http://www.cse.dcu.ie/essiscope/sm2/9126ref1.gif

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 6
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 7
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 8
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 9
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 10
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?

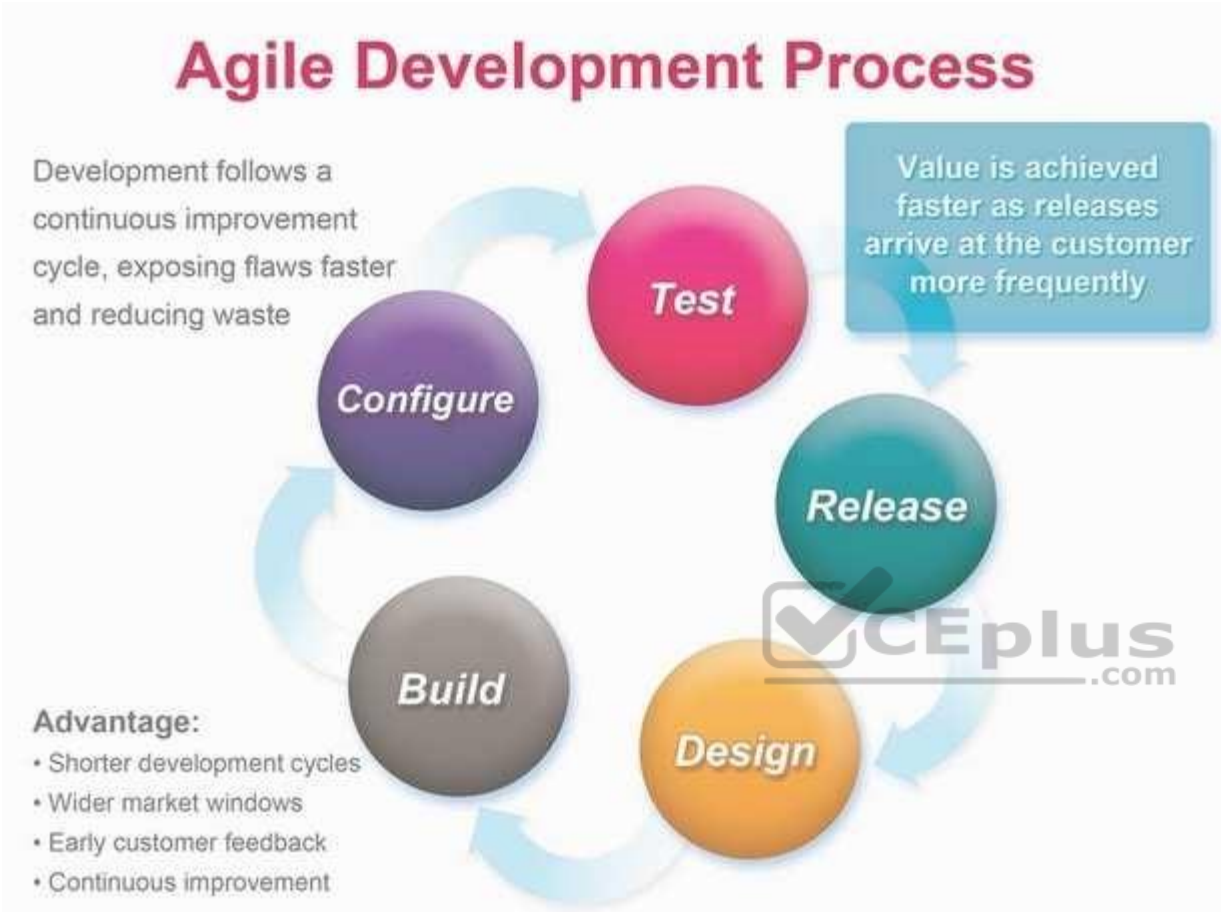
A. Agile Development
B. Software prototyping
C. Rapid application development
D. Component based development

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



Source: http://computertrainingcenters.com/wp-content/uploads/2012/10/what-is-agile-development.jpg

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 11

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:

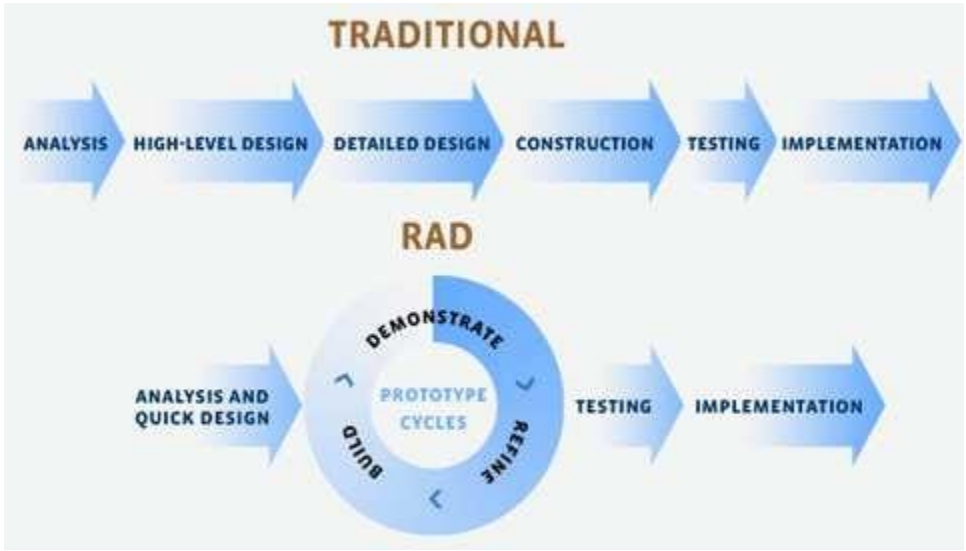
CISA review manual 2014 Page number 194

QUESTION 12
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



Click Here for original image

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 13
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 14
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 15
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 16
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 17
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 18
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 19
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 20
Which of the following attacks could capture network user passwords?

A. Data diddling
B. Sniffing
C. IP Spoofing
D. Surfing

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

Explanation/Reference:
A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.
Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.

A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.

Another method for sniffing is to use a network tap—a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.

The packets captured by sniffer are decoded and then displayed by the sniffer. Therefore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).

Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.

The following answers are incorrect:
Data did dlinginvolves changing data before, as it is entered into a computer, or after it is extracted.

Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.

Surfing would refer to the surf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

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

CISA Review manual 2014 Page number 321
Official ISC2 Guide to the CISSP 3rd edition Page Number 153

QUESTION 21
Most access violations are:

A. Accidental
B. Caused by internal hackers
C. Caused by external hackers
D. Related to Internet

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

Explanation/Reference:
The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 192).

QUESTION 22
Which of the following is NOT a component of IPSec?
A. Authentication Header
B. Encapsulating Security Payload
C. Key Distribution Center
D. Internet Key Exchange

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

Explanation/Reference:
AH, ESP and IKE are the three main components of IPSec. A KDC (Key Distribution Center) is a component of Kerberos, not IPSec.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 217).

QUESTION 23
Which of the following statements pertaining to IPSec is incorrect?

A. A security association has to be defined between two IPSec systems in order for bi-directional communication to be established.
B. Integrity and authentication for IP datagrams are provided by AH.
C. ESP provides for integrity, authentication and encryption to IP datagram's.
D. In transport mode, ESP only encrypts the data payload of each packet.

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

Explanation/Reference:
This is incorrect, there would be a pair of Security Association (SA) needed for bi directional communication and NOT only one SA. The sender and the receiver would both negotiate an SA for inbound and outbound connections.

The two main concepts of IPSec are Security Associations (SA) and tunneling. A Security Association (SA) is a simplex logical connection between two IPSec systems. For bi-directional communication to be established between two IPSec systems, two separate Security Associations, one in each direction, must be defined.

The security protocols can either be AH or ESP.

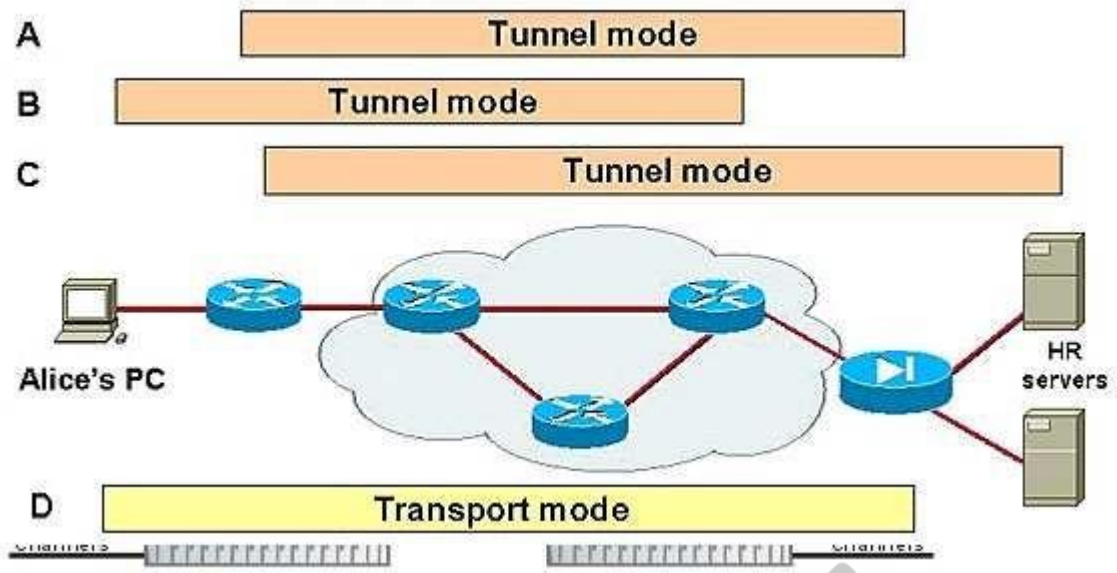
NOTE FROM CLEMENT:
The explanations below are a bit more thorough than what you need to know for the exam. However, they always say a picture is worth one thousand words, I think it is very true when it comes to explaining IPSEC and it's inner working. I have found a great article from CISCO PRESS and DLINK covering this subject, see references below.

Tunnel and Transport Modes
IPSec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:

Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.

Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.

As you can see in the Figure 1 graphic below, basically transport mode should be used for end-to-end sessions and tunnel mode should be used for everything else.
FIGURE: 1



IPSEC Transport Mode versus Tunnel Mode

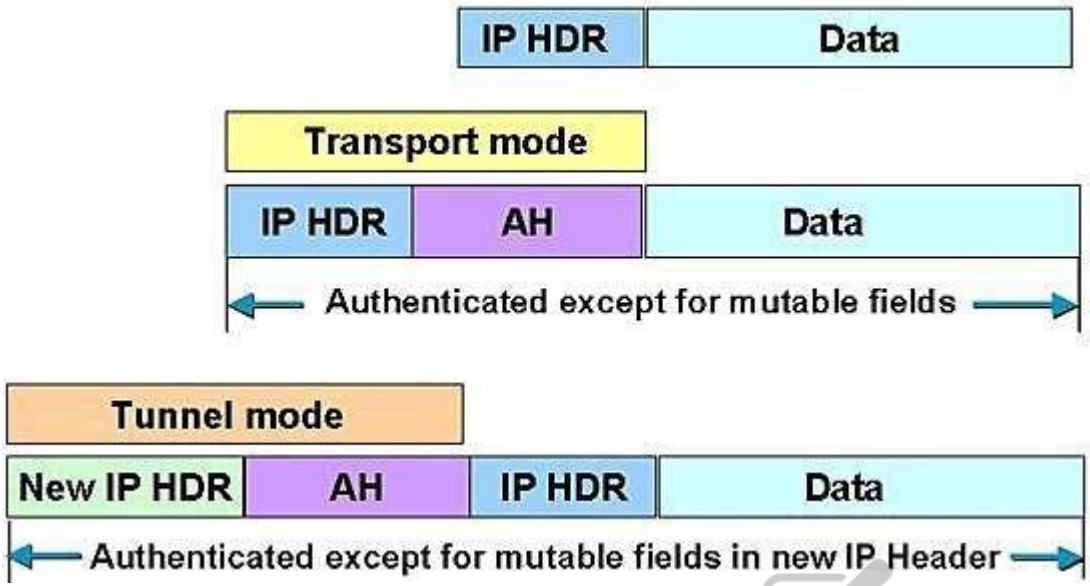
Tunnel and transport modes in IPSec.

Figure 1 above displays some examples of when to use tunnel versus transport mode:
Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall (as shown in example A in Figure 1). The IPSec gateways proxy IPSec for the devices behind them, such as Alice's PC and the HR servers in Figure 1. In example A, Alice connects to the HR servers securely through the IPSec tunnel set up between the gateways.

Tunnel mode is also used to connect an end-station running IPSec software, such as the Cisco Secure VPN Client, to an IPSec gateway, as shown in example B.

In example C, tunnel mode is used to set up an IPSec tunnel between the Cisco router and a server running IPSec software. Note that Cisco IOS software and the PIX Firewall sets tunnel mode as the default IPSec mode.

Transport mode is used between end-stations supporting IPSec, or between an end-station and a gateway, if the gateway is being treated as a host. In example D, transport mode is used to set up an encrypted Telnet session from Alice's PC running Cisco Secure VPN Client software to terminate at the PIX Firewall, enabling Alice to remotely configure the PIX Firewall securely.
FIGURE: 2

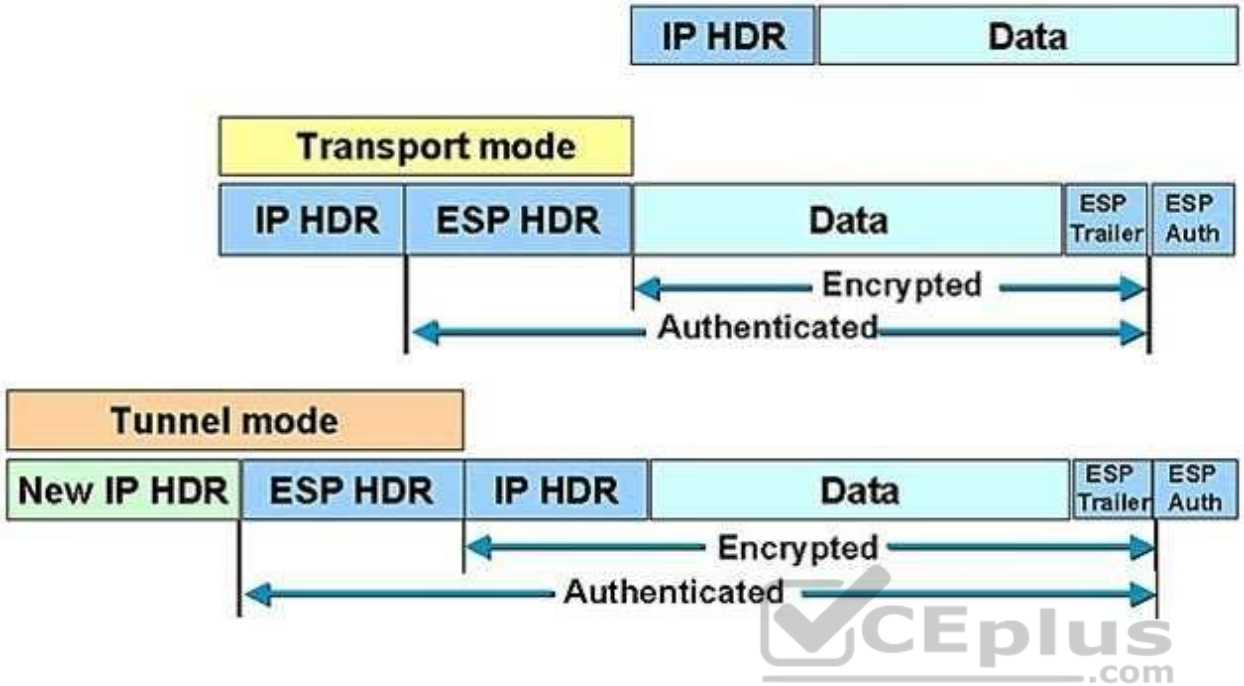


IPSEC AH Tunnel and Transport mode

AH Tunnel Versus Transport Mode
Figure 2 above, shows the differences that the IPSec mode makes to AH. In transport mode, AH services protect the external IP header along with the data payload. AH services protect all the fields in the header that don't change in transport. The header goes after the IP header and before the ESP header, if present, and other higher-layer protocols.

As you can see in Figure 2 above, In tunnel mode, the entire original header is authenticated, a new IP header is built, and the new IP header is protected in the same way as the IP header in transport mode.
AH is incompatible with Network Address Translation (NAT) because NAT changes the source IP address, which breaks the AH header and causes the packets to be rejected by the IPSec peer. FIGURE: 3

IPSEC ESP Tunnel versus Transport modes



ESP Tunnel Versus Transport Mode

Figure 3 above shows the differences that the IPSec mode makes to ESP. In transport mode, the IP payload is encrypted and the original headers are left intact. The ESP header is inserted after the IP header and before the upper-layer protocol header. The upper-layer protocols are encrypted and authenticated along with the ESP header. ESP doesn't authenticate the IP header itself.

NOTE: Higher-layer information is not available because it's part of the encrypted payload.

When ESP is used in tunnel mode, the original IP header is well protected because the entire original IP datagram is encrypted. With an ESP authentication mechanism, the original IP datagram and the ESP header are included; however, the new IP header is not included in the authentication.

When both authentication and encryption are selected, encryption is performed first, before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can detect the problem and potentially reduce the impact of denial-of-service attacks.

ESP can also provide packet authentication with an optional field for authentication. Cisco IOS software and the PIX Firewall refer to this service as ESP hashed message authentication code (HMAC). Authentication is calculated after the encryption is done. The current IPSec standard specifies which hashing algorithms have to be supported as the mandatory HMAC algorithms.

The main difference between the authentication provided by ESP and AH is the extent of the coverage. Specifically, ESP doesn't protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode).

The following were incorrect answers for this question:

Integrity and authentication for IP datagrams are provided by AH This is correct, AH provides integrity and authentication and ESP provides integrity, authentication and encryption.

ESP provides for integrity, authentication and encryption to IP datagram's. ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

In transport mode, ESP only encrypts the data payload of each packet. ESP can be operated in either tunnel mode (where the original packet is encapsulated into a new one) or transport mode (where only the data payload of each packet is encrypted, leaving the header untouched).

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6986-6989). Acerbic Publications. Kindle Edition.

and
http://www.ciscopress.com/articles/article.asp?p=25477 and
http://documentation.netgear.com/reference/sve/vpn/VPNBasics-3-05.html

QUESTION 24
As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains a significant change or addition of new functionality?

A. Major software Release

B. Minor software Release
C. Emergency software release
D. General software Release

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

Explanation/Reference:
A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

For CISA exam you should know below information about software release management:

Software Release Management is the process of ensuring releases can be reliably planned, scheduled and successfully transitioned (deployed) to Test and Live Environments. Software Release Management is not just about "automating the path to production" although that is certainly an important part. It also about adopting a holistic view of application changes, using the "Release" as the container to ensure that changes are packaged, released and tested in a repeatable and controlled manner.

Release Management is often likened to the conductor of an orchestra, with the individual changes to be implemented the various instruments within it. Software Release Management is intrinsically linked with the more well understood and adopted Software Change and Configuration Management disciplines.

Software Release management is a process through which software is made available to user. Each update or upgrade of a Configuration Item is referred to as a release.

There are three levels of releases. These levels related to releasing hardware or software into your IT infrastructure. Some may be a single change, others may implement many changes at a time.
Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.
Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

The following were incorrect answers:
Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

General software Release – Not a valid type of software release.

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

CISA review manual 2014 Page number 244

QUESTION 25
As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains small enhancements and fixes?

A. Major software Release
B. Minor software Release
C. Emergency software release
D. General software Release

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

Explanation/Reference:
Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

For CISA exam you should know below information about software release management:

Software Release Management is the process of ensuring releases can be reliably planned, scheduled and successfully transitioned (deployed) to Test and Live Environments. Software Release Management is not just about "automating the path to production" although that is certainly an important part. It also about adopting a holistic view of application changes, using the "Release" as the container to ensure that changes are packaged, released and tested in a repeatable and controlled manner. Release Management is often likened to the conductor of an orchestra, with the individual changes to be implemented the various instruments within it. Software Release Management is intrinsically linked with the more well understood and adopted Software Change and Configuration Management disciplines.

Software Release management is a process through which software is made available to user. Each update or upgrade of a Configuration Item is referred to as a release.

There are three levels of releases. These levels related to releasing hardware or software into your IT infrastructure. Some may be a single change, others may implement many changes at a time.

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.
Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.
Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

The following were incorrect answers:
Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

General software Release – Not a valid type of software release.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 244

QUESTION 26
In which of the following database model is the data organized into a tree-like structure, implying a single parent for each record?

A. Hierarchical database model
B. Network database model
C. Relational database model
D. Object-relational database model

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

Explanation/Reference:
In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:

Hierarchical database model
Network model
Relational model
Object-relational database models

Hierarchical database model
In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.

This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.

Hierarchical database model

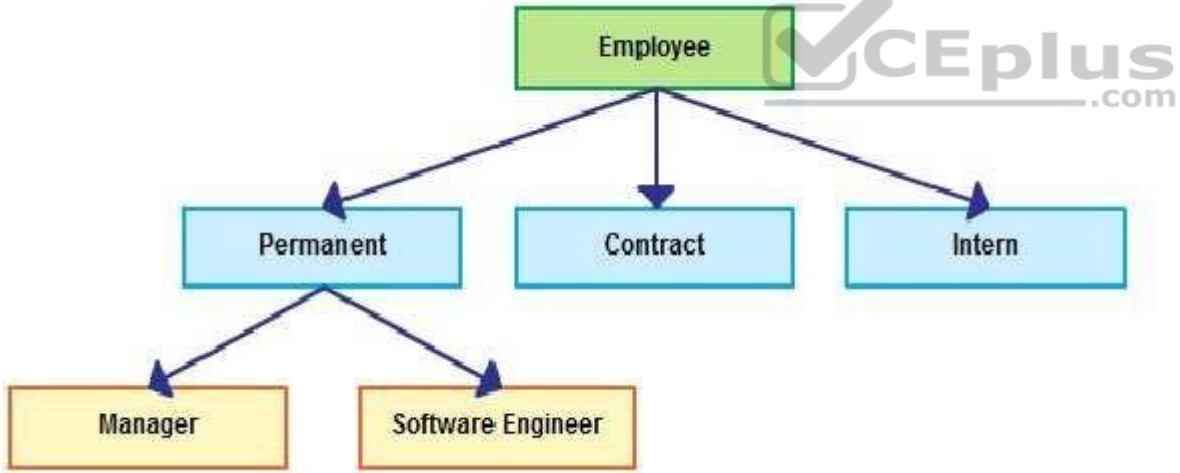


Image source: http://creately.com/blog/wp-content/uploads/2012/06/hierarchical-database-model.png

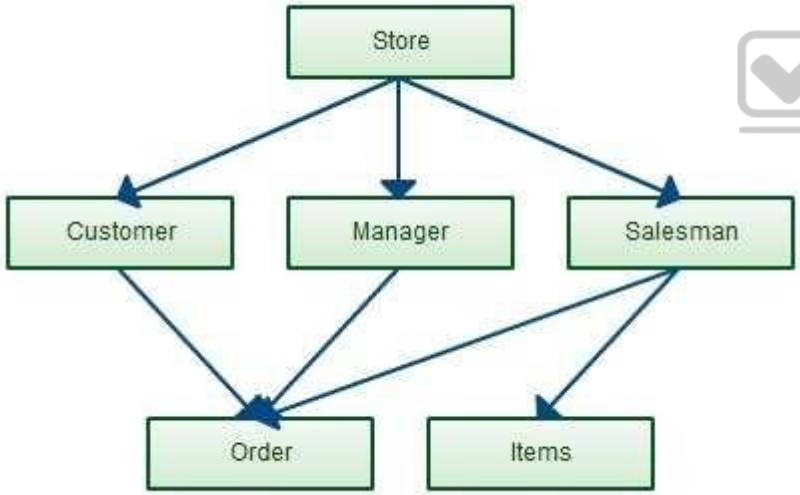
Network database model

The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.

The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of B. At the same time another set may be defined where B is the owner of A. Thus all the sets comprise a general directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.

The network model is able to represent redundancy in data more efficiently than in the hierarchical model, and there can be more than one path from an ancestor node to a descendant. The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values. Network Database model



Source of Image:http://creately.com/blog/wp-content/uploads/2012/06/database-design-network-model.png

Relational database model

In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

In the relational model, related records are linked together with a "key".

The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.

Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.
Relational database model

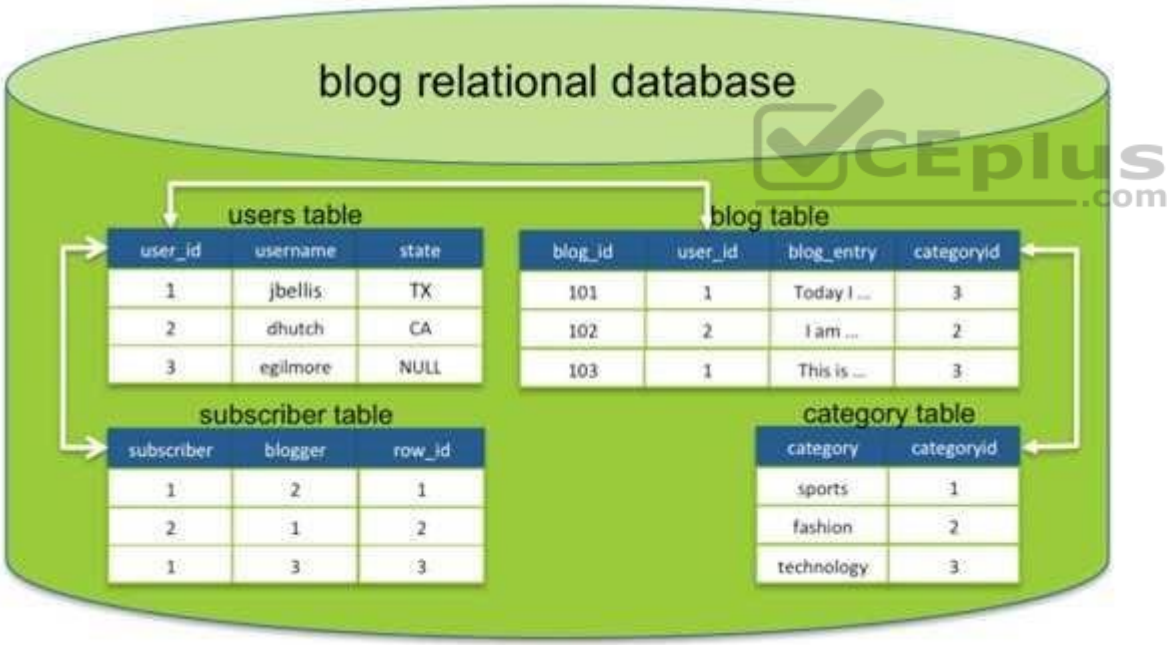


Image Source: http://www.datastax.com/docs/_images/relational_model.png

Object-relational database Model
An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.

Example of an object-oriented database model
An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:
Network model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.
Relational model- In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database. In the relational model, related records are linked together with a "key".
Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

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

CISA review manual 2014 Page number 254

QUESTION 27
Which of the following database model allow many-to-many relationships in a tree-like structure that allows multiple parents?

A. Hierarchical database model
B. Network database model
C. Relational database model
D. Object-relational database model

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

Explanation/Reference:

Network database model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:
Hierarchical database model
Network model
Relational model
Object-relational database models

Hierarchical database model
In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.

This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.

Hierarchical database model

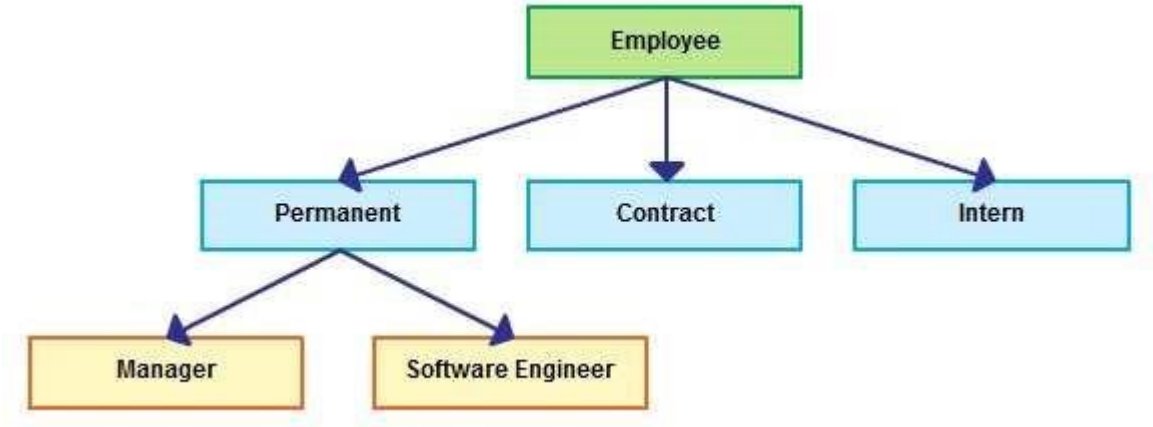


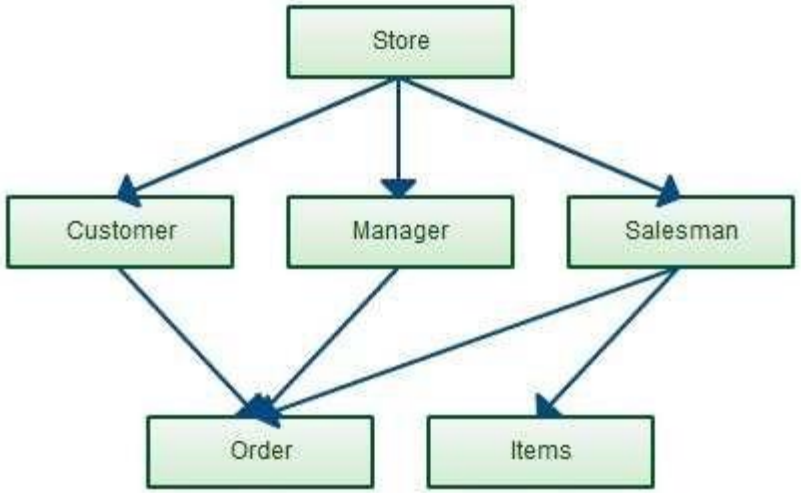
Image source: http://creately.com/blog/wp-content/uploads/2012/06/hierarchical-database-model.png

Network database model
The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.

The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of B. At the same time another set may be defined where B is the owner of A. Thus all the sets comprise a general directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.

The network model is able to represent redundancy in data more efficiently than in the hierarchical model, and there can be more than one path from an ancestor node to a descendant. The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values.
Network Database model



Source of Image:http://creately.com/blog/wp-content/uploads/2012/06/database-design-network-model.png

Relational database model
In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

In the relational model, related records are linked together with a "key".

The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.

Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.
Relational database model

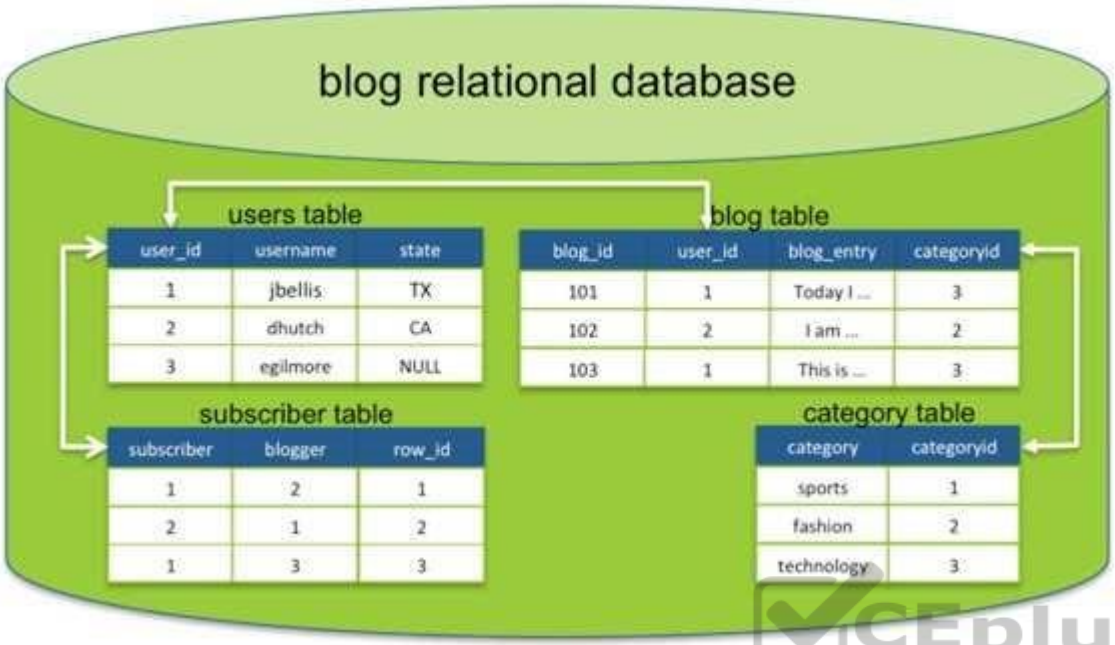


Image Source: http://www.datastax.com/docs/_images/relational_model.png

Object-relational database Model
An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.
Example of an object-oriented database model
An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:
Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.
Relational model- In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database. In the relational model, related records are linked together with a "key".

Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 254

QUESTION 28
In which of the following database models is the data represented in terms of tulles and grouped into relations?

A. Hierarchical database model
B. Network database model
C. Relational database model
D. Object-relational database model

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

Explanation/Reference:
In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:
Hierarchical database model
Network model
Relational model
Object-relational database models

Hierarchical database model
In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and

now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.

This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.

Hierarchical database model

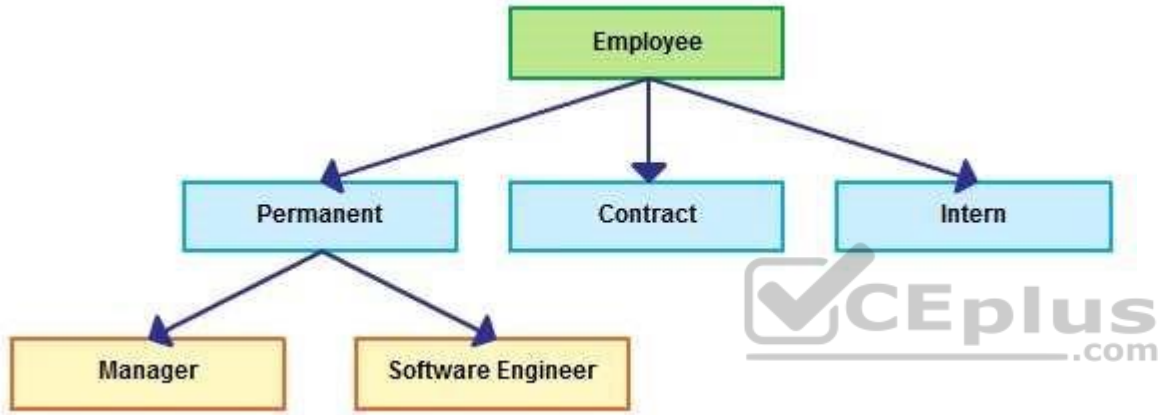


Image source: http://creately.com/blog/wp-content/uploads/2012/06/hierarchical-database-model.png

Network database model

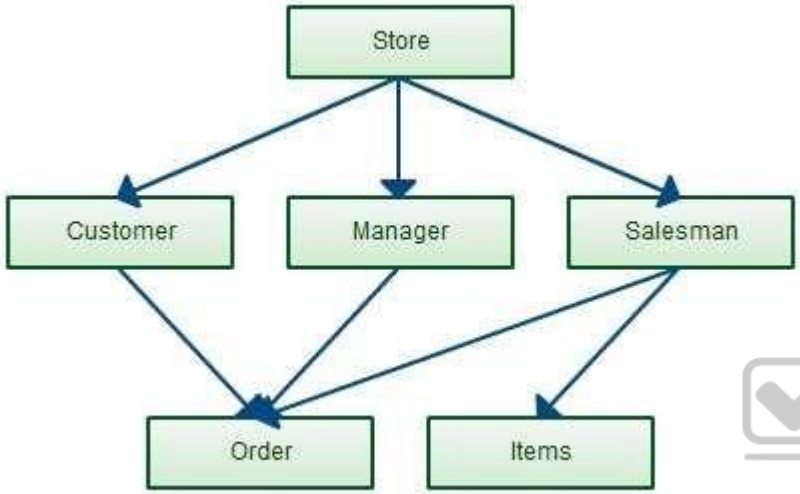
The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.

The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of B. At the

same time another set may be defined where B is the owner of A. Thus all the sets comprise a general directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.

The network model is able to represent redundancy in data more efficiently than in the hierarchical model, and there can be more than one path from an ancestor node to a descendant. The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values. Network Database model



Source of Image:http://creately.com/blog/wp-content/uploads/2012/06/database-design-network-model.png

Relational database model
In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

In the relational model, related records are linked together with a "key".

The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.

Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.

Relational database model

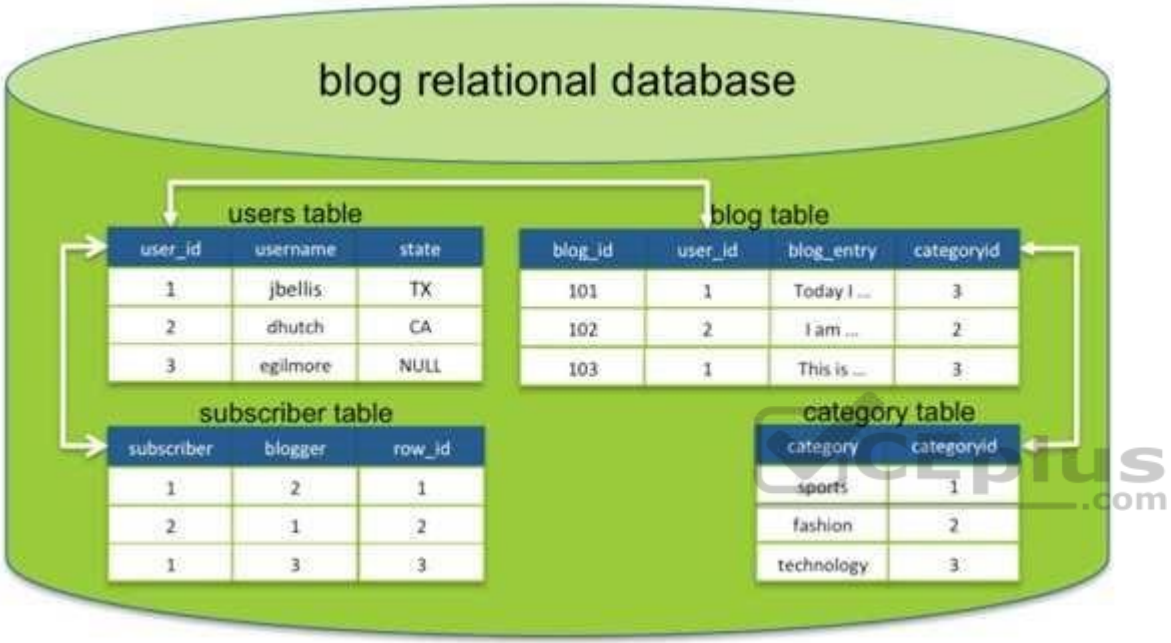


Image Source: http://www.datastax.com/docs/_images/relational_model.png

Object-relational database Model

An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.

Example of an object-oriented database model

An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:
Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.
Network database model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.
Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

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

CISA review manual 2014 Page number 254

QUESTION 29
Which of the following is a type of computer network used for data transmission among devices such as computers, telephones and personal digital assistants?

A. LAN
B. WAN
C. SAN
D. PAN

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

Explanation/Reference:

QUESTION 30
Which of the following type of a computer network covers a limited area such as a home, office or campus?

A. LAN
B. WAN
C. SAN
D. PAN

Correct Answer: A

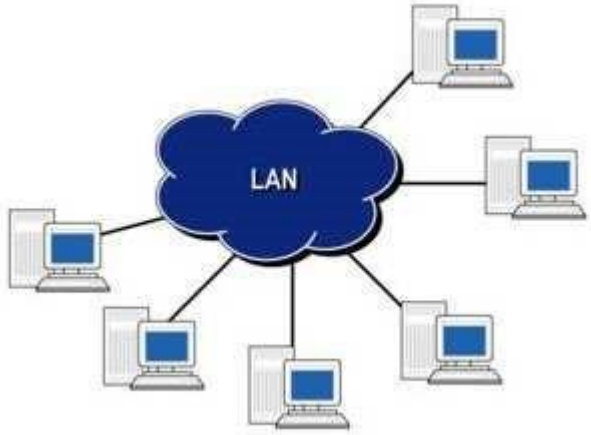
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

For your exam you should know below information about computer networks:
Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

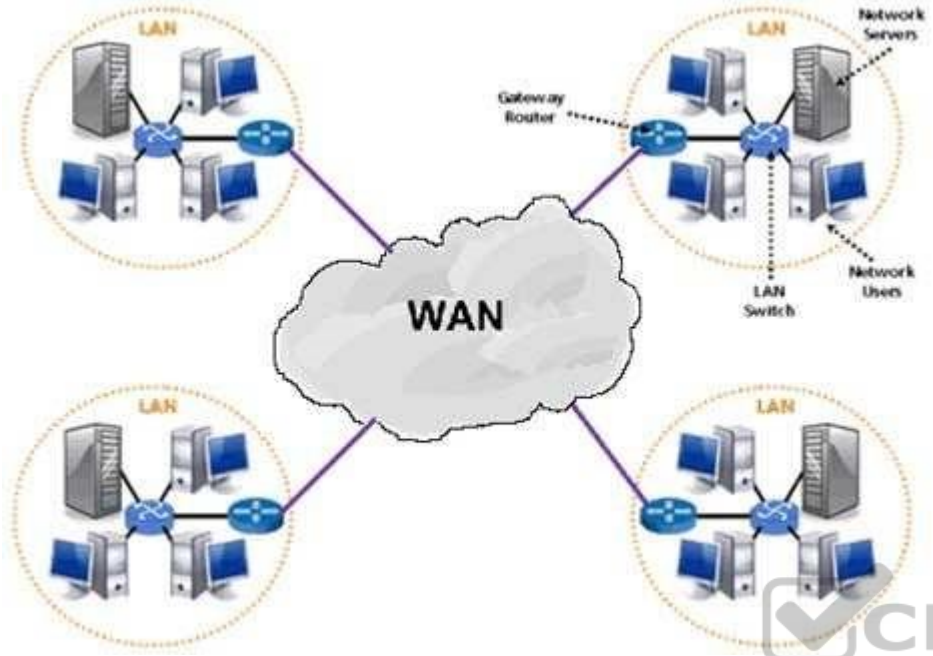
Local Area Network



Click HERE for original source of image

Wide Area Network
A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

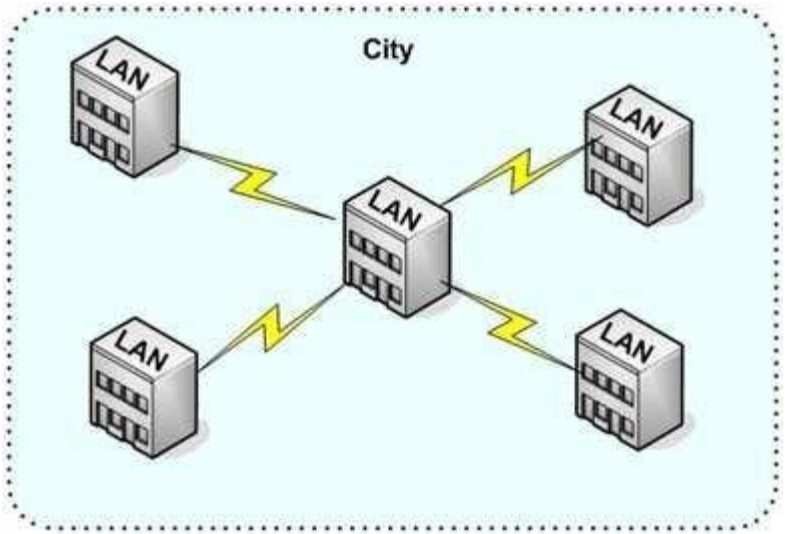
Wide Area Network



Source of image: http://www.netprivateer.com/images/lanwan.gif

Metropolitan Area Network
A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

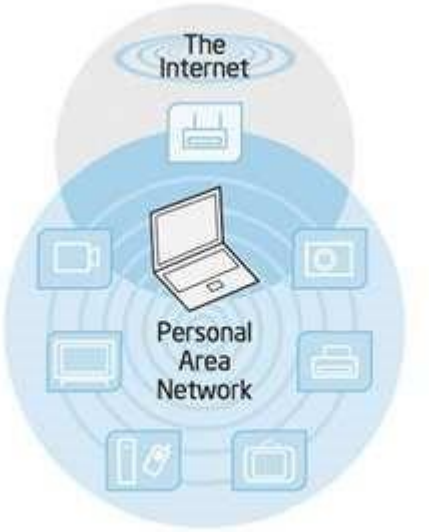
Metropolitan Area Network



Source of image: http://cis.msjc.edu/courses/images/MAN.jpg

Personal Area Network
A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Click HERE for original image

Storage Area Network
A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

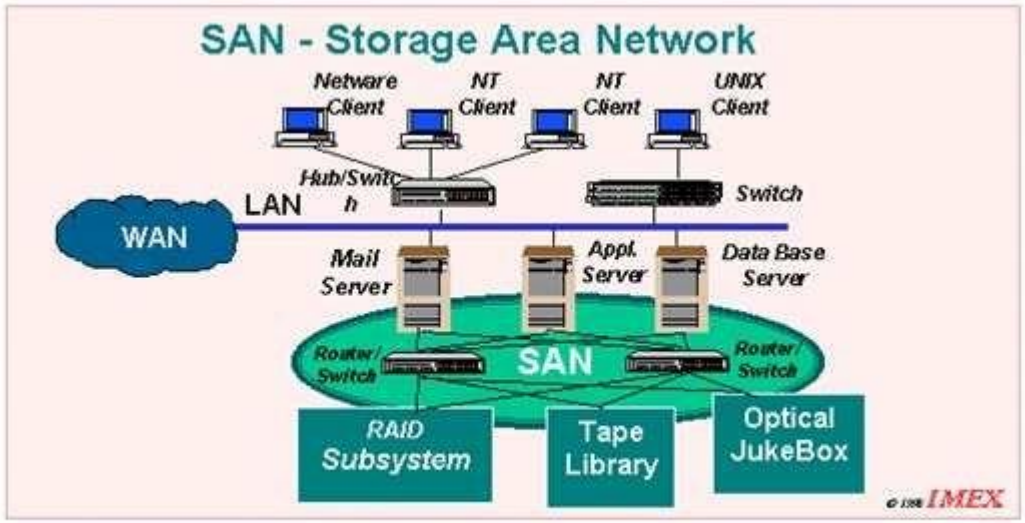


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

Source of image: http://www.imexresearch.com/images/sasnassan-3.gif

The following were incorrect answers:
PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).
WAN - A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.
SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

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

CISA review manual 2014 Page number 258

QUESTION 31
Which of the following type of a computer network covers a broad area such as city, region, nation or international link?

A. LAN
B. WAN
C. SAN
D. PAN

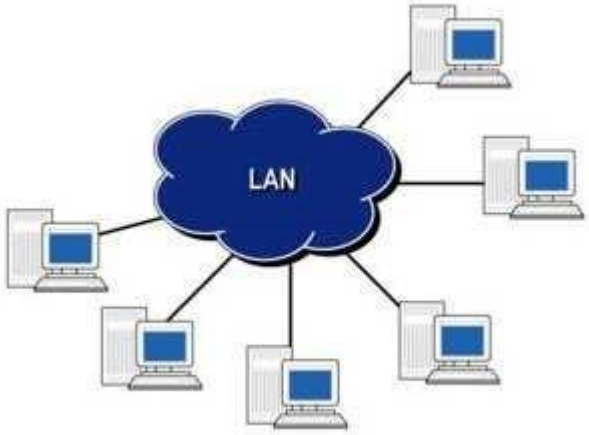
Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

For your exam you should know below information about computer networks:

Local Area Network (LAN)
A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

Local Area Network

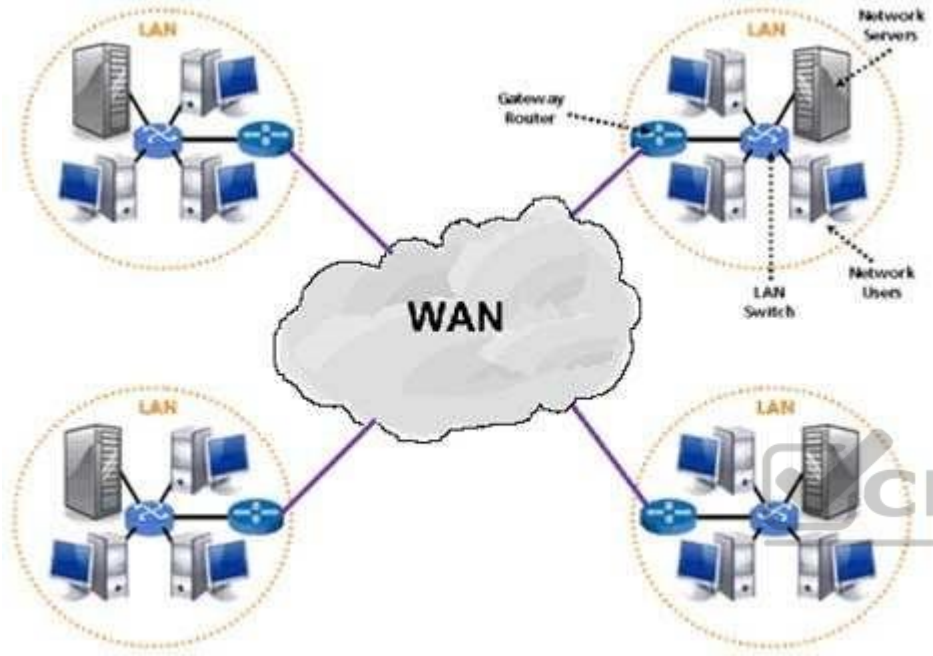


Click HERE for original source of image

Wide Area Network

A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

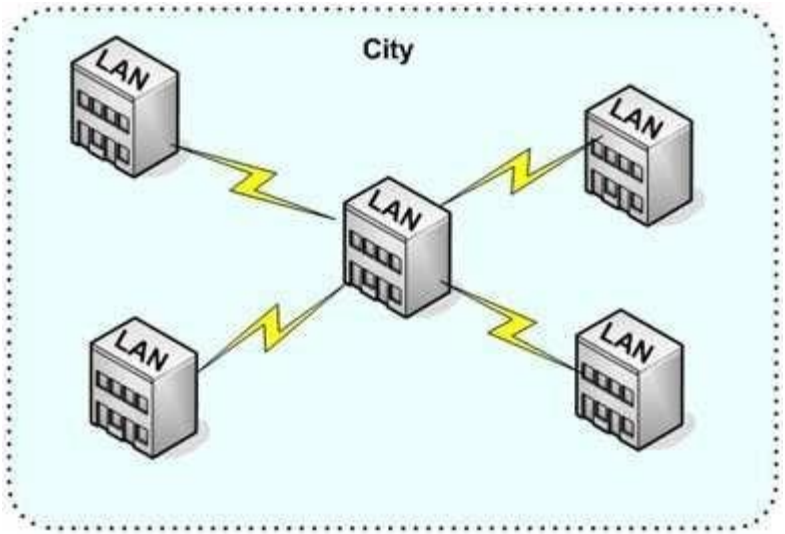
Wide Area Network



Source of image: http://www.netprivateer.com/images/lanwan.gif

Metropolitan Area Network
A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

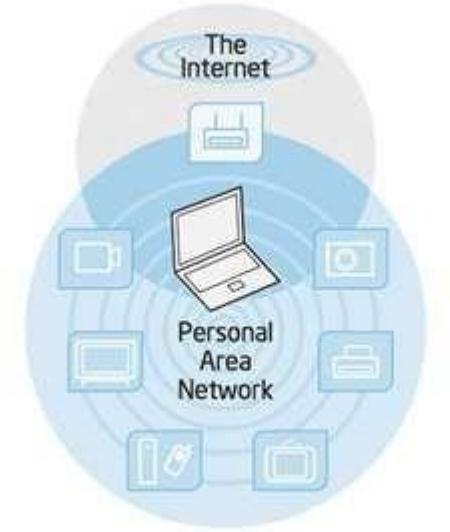


Metropolitan Area Network (MAN)

Source of image: http://cis.msjc.edu/courses/images/MAN.jpg

Personal Area Network
A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Click HERE for original image

Storage Area Network
A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

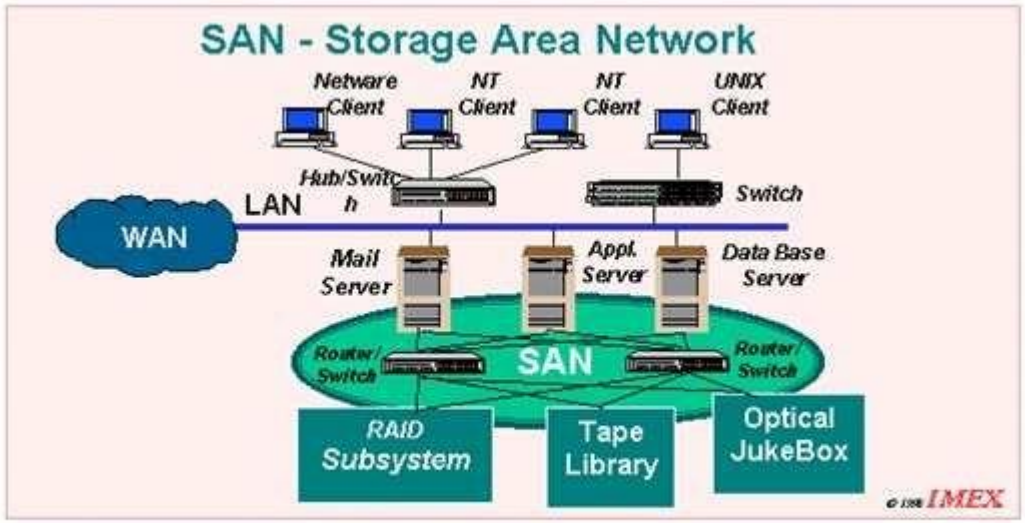


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

Source of image: http://www.imexresearch.com/images/sasnassan-3.gif

The following were incorrect answers:
PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

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

CISA review manual 2014 Page number 258

QUESTION 32

Which of the following type of a computer network is a WAN that are limited to a city?

A. LAN
B. MAN
C. SAN
D. PAN

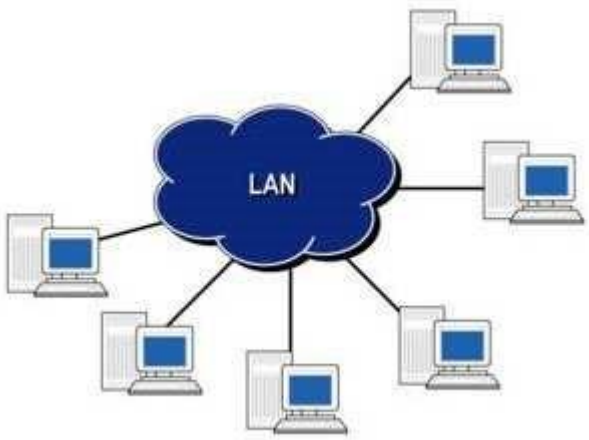
Correct Answer: B
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
MAN - A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN.

For your exam you should know below information about computer networks:

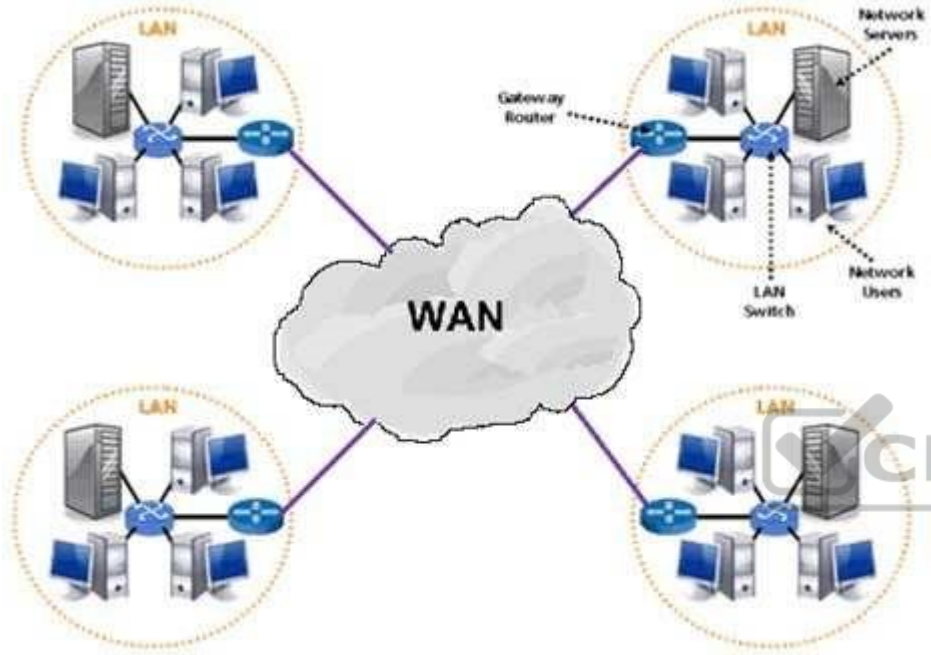
Local Area Network (LAN)
A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

Local Area Network



Wide Area Network
A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

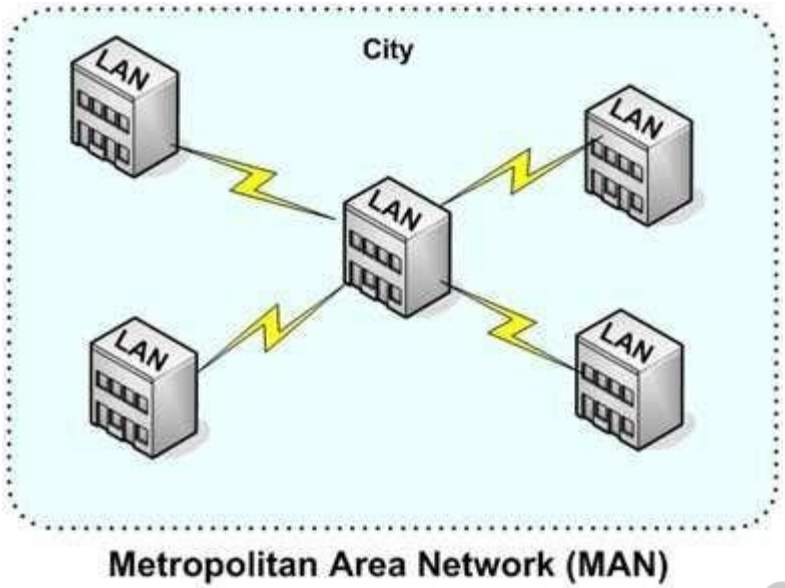
Wide Area Network



Source of image: http://www.netprivateer.com/images/lanwan.gif

Metropolitan Area Network
A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

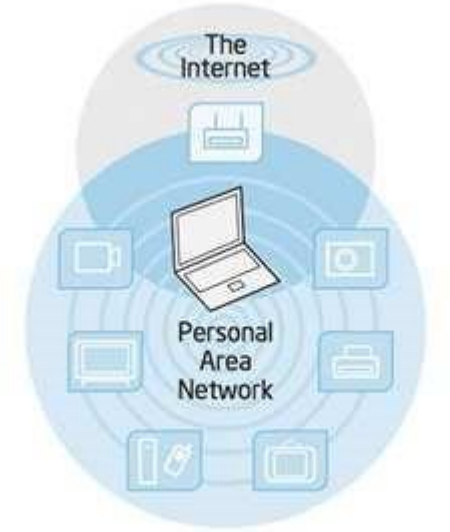


Source of image: http://cis.msjc.edu/courses/images/MAN.jpg

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Click HERE for original image

Storage Area Network
A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

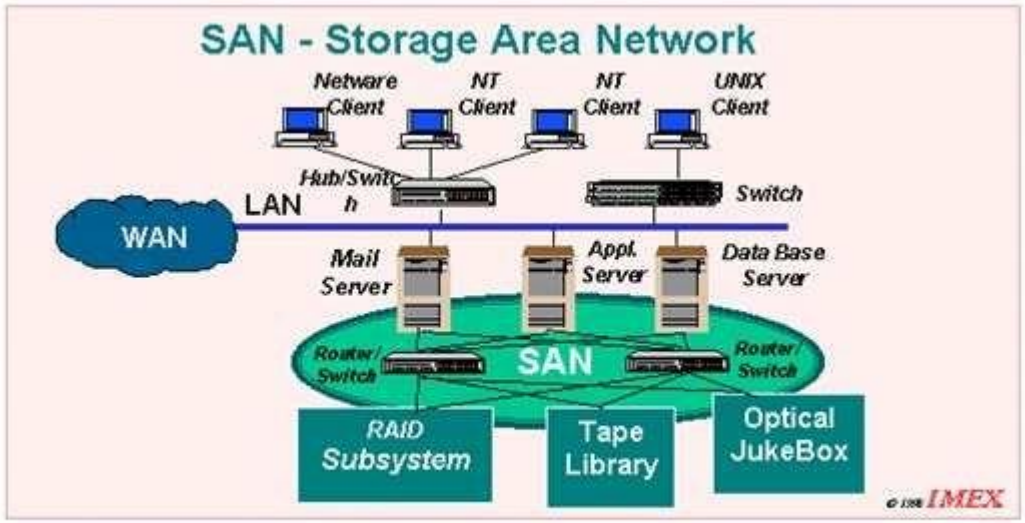


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

Source of image: http://www.imexresearch.com/images/sasnassan-3.gif

The following were incorrect answers:
PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

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

CISA review manual 2014 Page number 258

QUESTION 33
Which of the following type of a computer network are variation of LAN and are dedicated to connecting storage devices to servers and other computing devices?

A. LAN
B. MAN
C. SAN
D. PAN

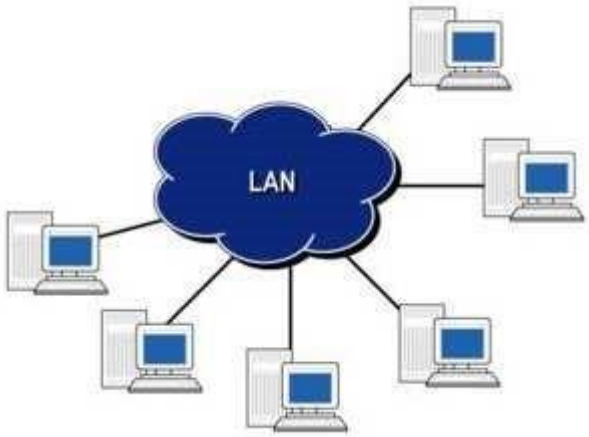
Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

For your exam you should know below information about computer networks:

Local Area Network (LAN)
A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

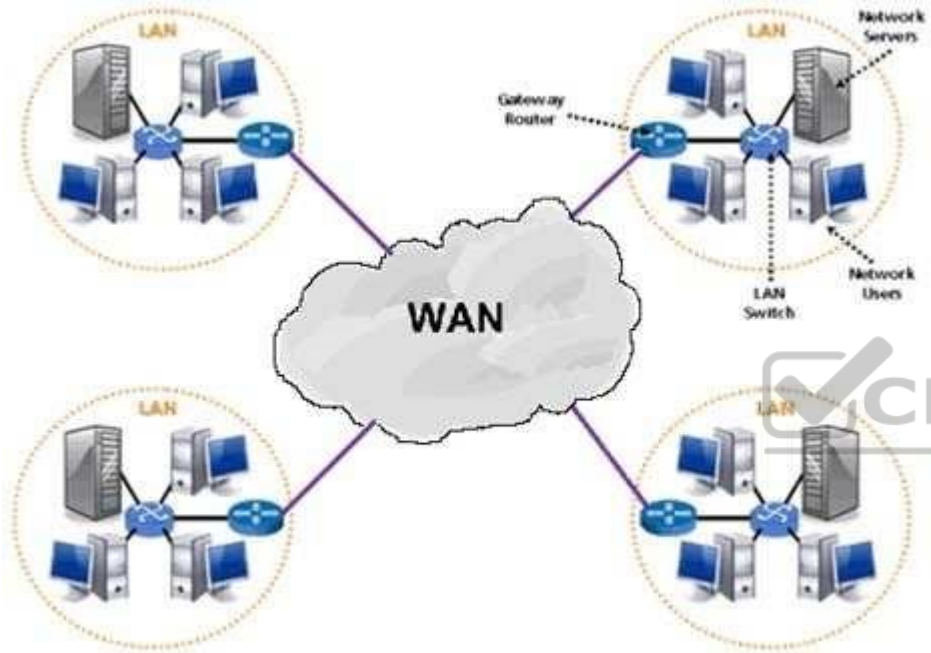
Local Area Network



Click HERE for original source of image

Wide Area Network
A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

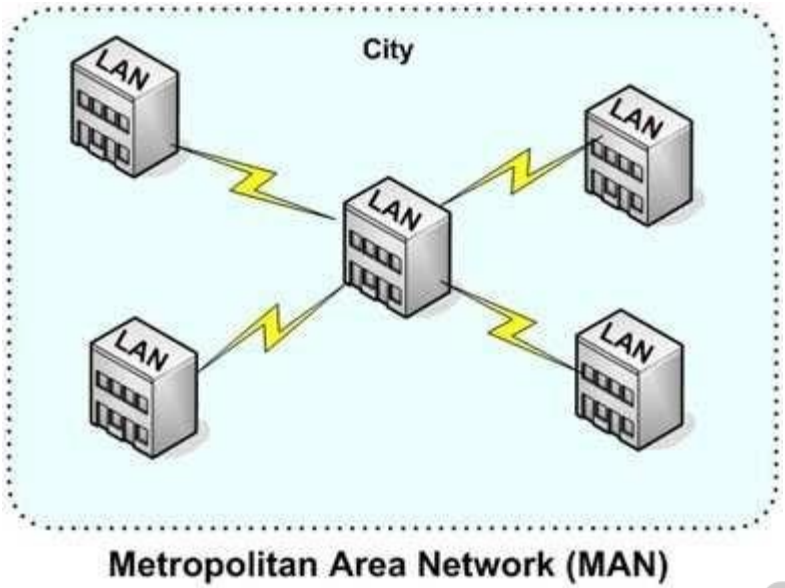
Wide Area Network



Source of image: http://www.netprivateer.com/images/lanwan.gif

Metropolitan Area Network
A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

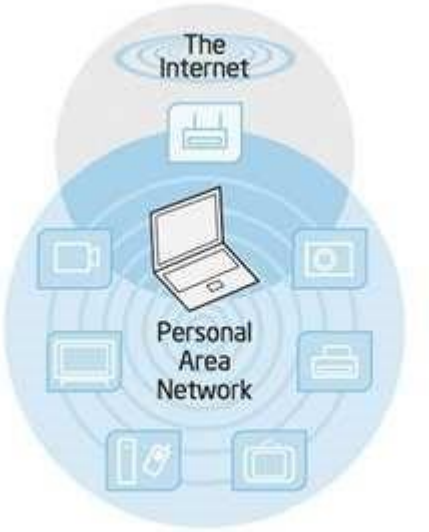


Source of image: http://cis.msjc.edu/courses/images/MAN.jpg

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Click HERE for original image

Storage Area Network
A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

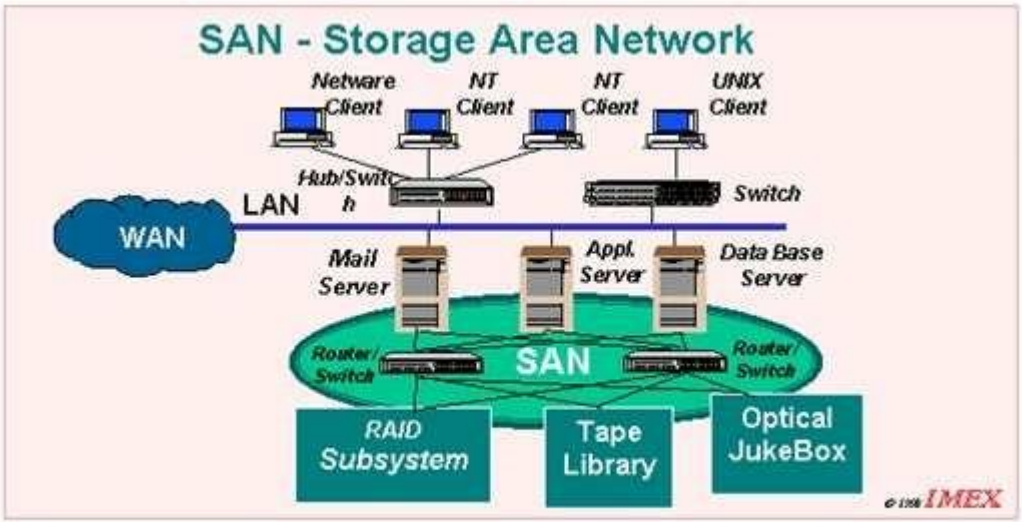


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

Source of image: http://www.imexresearch.com/images/sasnassan-3.gif

The following were incorrect answers:
PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

MAN - A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

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

CISA review manual 2014 Page number 258

QUESTION 34
Which of the following type of network service maps Domain Names to network IP addresses or network IP addresses to Domain Names?
A. DHCP
B. DNS
C. Directory Service
D. Network Management

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

Explanation/Reference:
Domain Name System(DNS) - Translates the names of network nodes into network IP address.

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.
Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine. Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:
Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.
Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP

addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.
Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network
Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

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

CISA review manual 2014 Page number 258

QUESTION 35
Which of the following type of network service stores information about the various resources in a central database on a network and help network devices locate services?

A. DHCP
B. DNS
C. Directory Service
D. Network Management

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

Explanation/Reference:
A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.
Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.
Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:
Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.
Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.
Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network
Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP

addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Domain Name System(DNS) - Translates the names of network nodes into network IP address.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 258

QUESTION 36

Which of the following type of network service is used by network computer to obtain an IP addresses and other parameters such as default gateway, subnet mask?

A. DHCP
B. DNS
C. Directory Service
D. Network Management

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

Explanation/Reference:
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.
Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine. Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:

Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.
Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.
Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.
Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network
Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:
Directory Service - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
Domain Name System(DNS) - Translates the names of network nodes into network IP address.
Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

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

CISA review manual 2014 Page number 258

QUESTION 37
Which of the following layer of the OSI model provides a standard interface for applications to communicate with devices on a network?

A. Application layer

B. Presentation layer
C. Session layer
D. Transport layer

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

Explanation/Reference:
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals

For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal. OSI Model

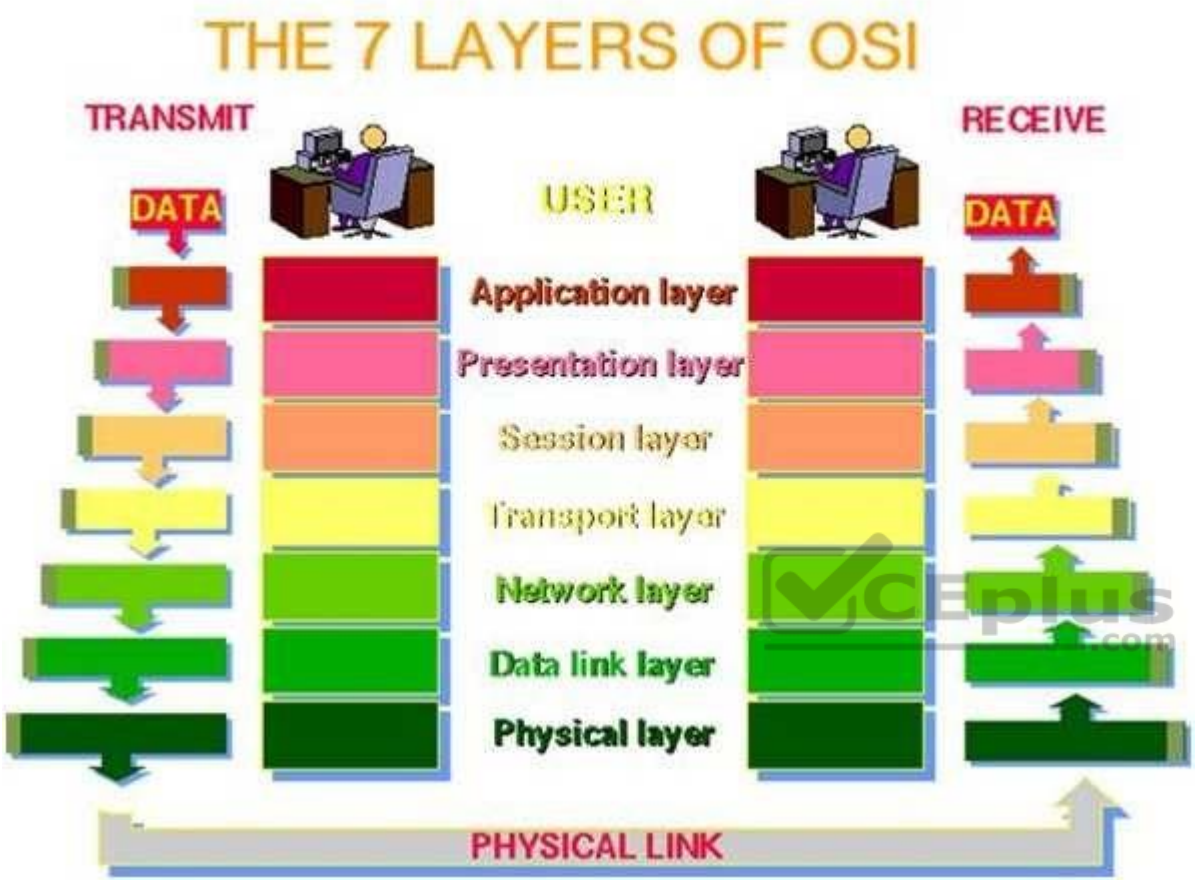


Image source: http://www.petri.co.il/images/osi_model.JPG

PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts
How the receiving station delimits a frame

DATA LINK LAYER
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.
Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
Frame sequencing: transmits/receives frames sequentially.
Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet
The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER
The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER
The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:
Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals

The following were incorrect answers:
Presentation layer - The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

Session layer - The session layer allows session establishment between processes running on different stations.

Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

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

CISA review manual 2014 Page number 260

QUESTION 38
Which of the following layer of an OSI model controls dialog between computers?

A. Application layer
B. Presentation layer
C. Session layer

D. Transport layer

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

Explanation/Reference:
The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.
For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal. OSI Model

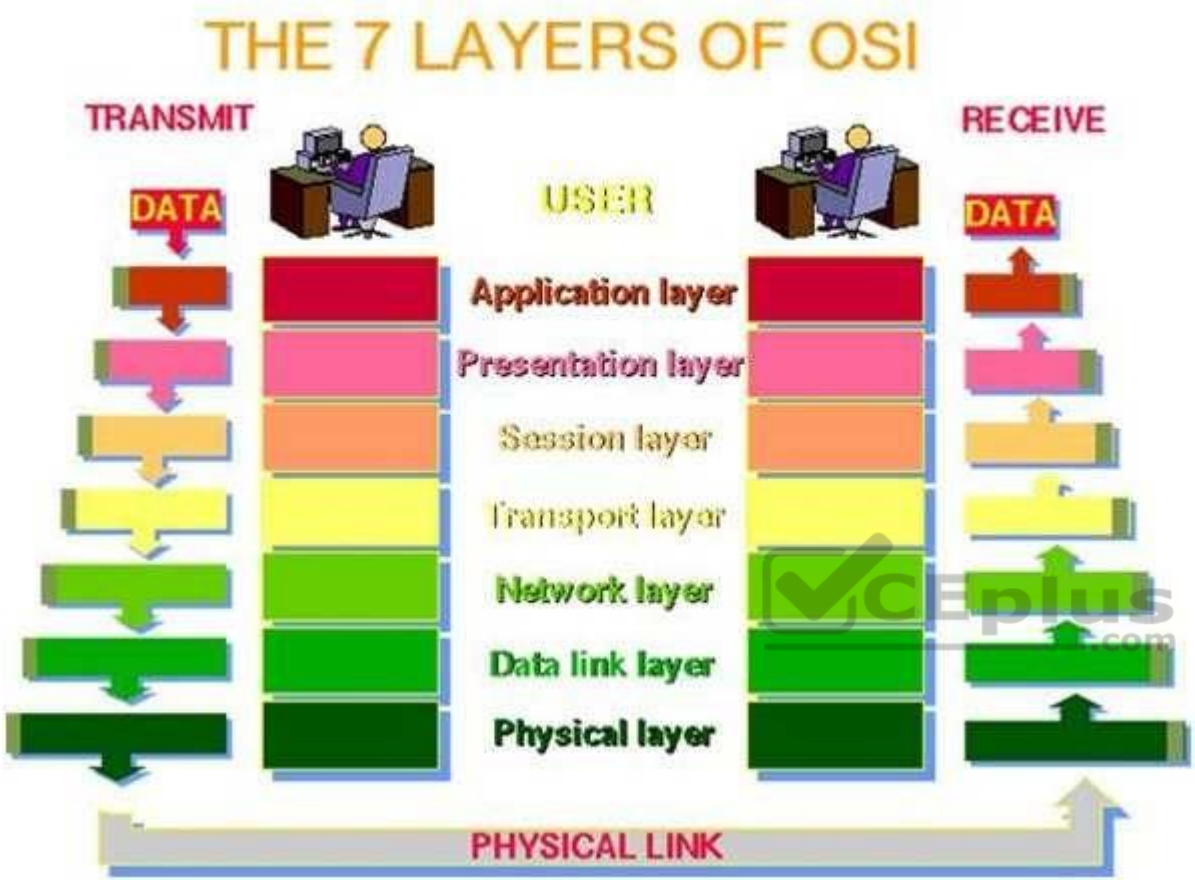


Image source: http://www.petri.co.il/images/osi_model.JPG

PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1
How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.
Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
Frame sequencing: transmits/receives frames sequentially.
Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet
The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER
The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals

The following were incorrect answers:
Application Layer - The application layer serves as the window for users and application processes to access network services.

Presentation layer - The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

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

CISA review manual 2014 Page number 260

QUESTION 39
Which of the following layer of an OSI model ensures that messages are delivered error-free, in sequence, and with no losses or duplications?

A. Application layer
B. Presentation layer
C. Session layer
D. Transport layer

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

Explanation/Reference:
The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal. OSI Model

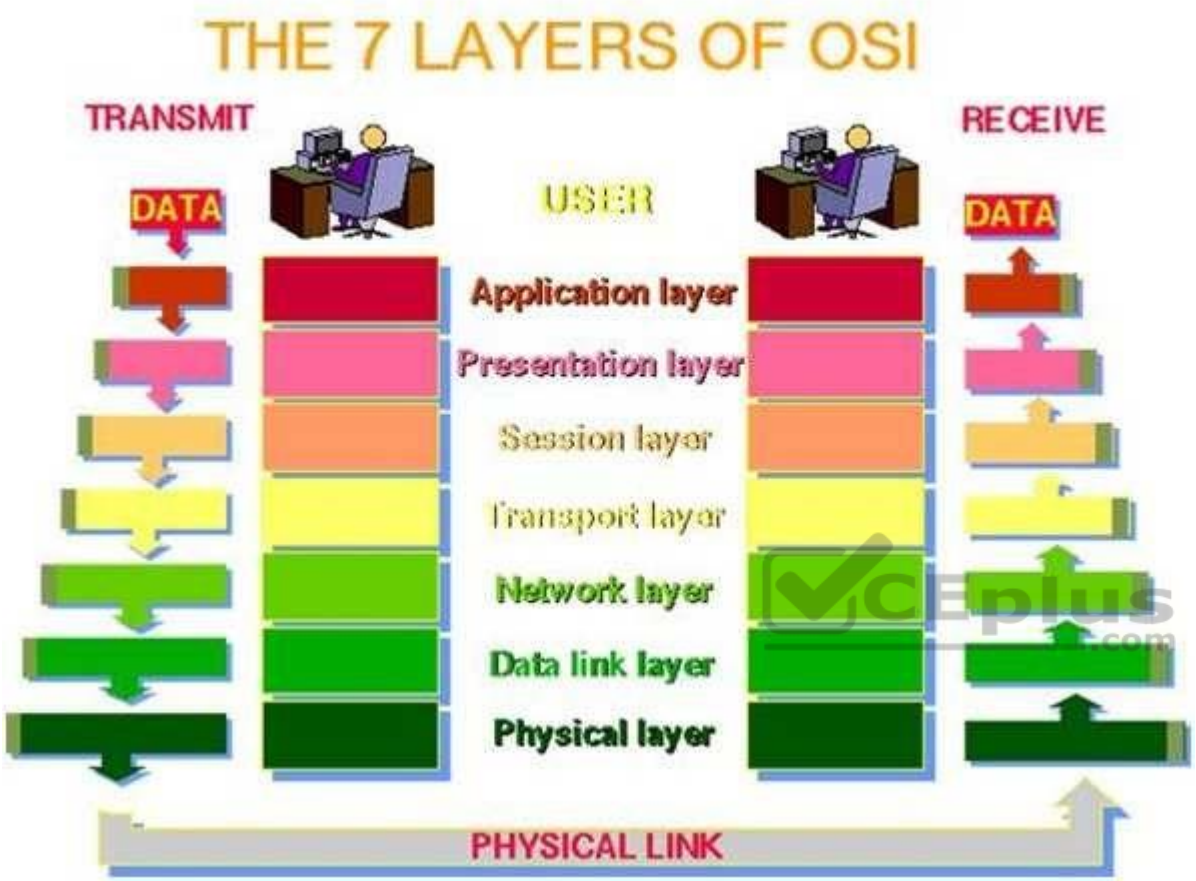


Image source: http://www.petri.co.il/images/osi_model.JPG

PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts
How the receiving station delimits a frame

DATA LINK LAYER
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.
Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
Frame sequencing: transmits/receives frames sequentially.
Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet
The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER
The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER
The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:
Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals

The following were incorrect answers:
Application Layer - The application layer serves as the window for users and application processes to access network services.

Presentation layer - The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

Session layer - The session layer allows session establishment between processes running on different stations.

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

CISA review manual 2014 Page number 260

QUESTION 40
Which of the following layer of an OSI model responsible for routing and forwarding of a network packets?

A. Transport Layer
B. Network Layer
C. Data Link Layer
D. Physical Layer

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

Explanation/Reference:
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.

For CISA exam you should know below information about OSI model:
The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.OSI Model

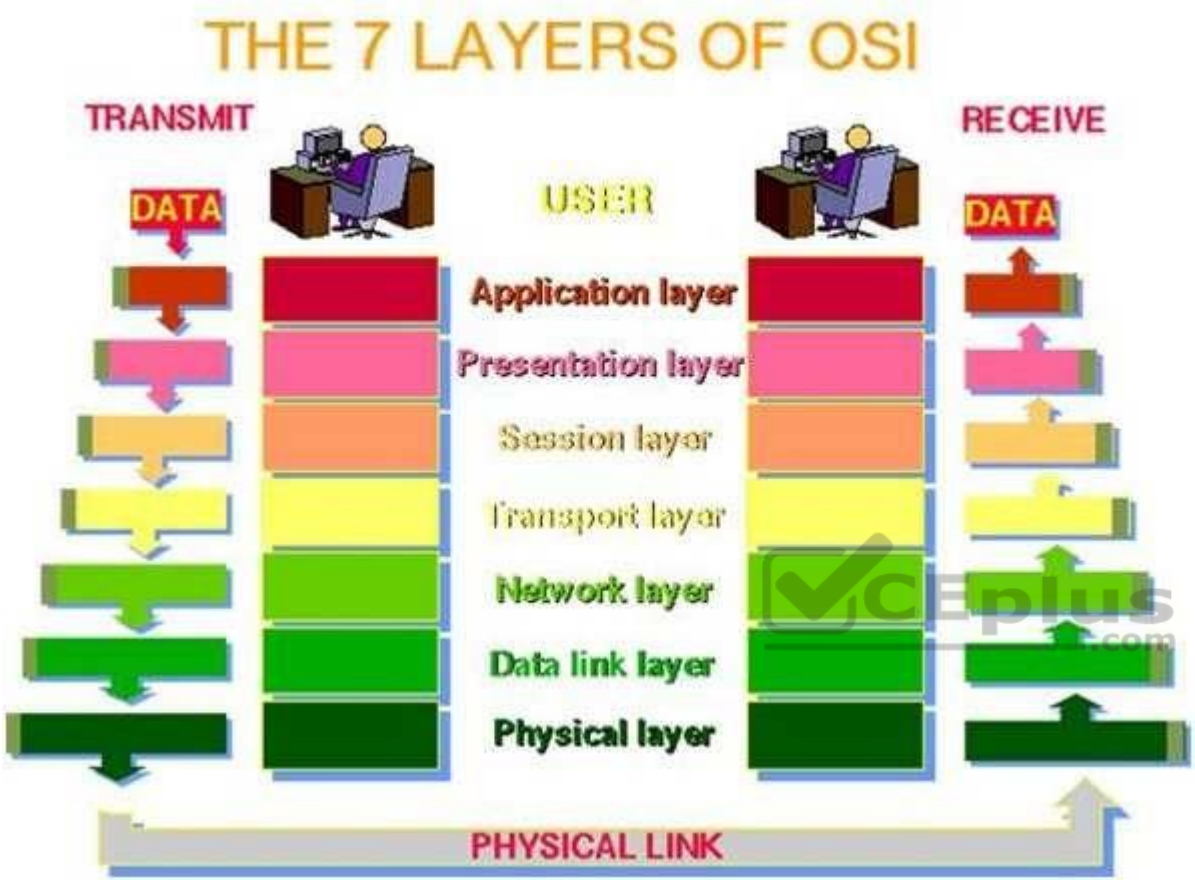


Image source: http://www.petri.co.il/images/osi_model.JPG
PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts
How the receiving station delimits a frame

DATA LINK LAYER
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.
Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
Frame sequencing: transmits/receives frames sequentially.
Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet
The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).
In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER
The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.
The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals

The following were incorrect answers:
Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.
Data link layer - The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.
Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

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

CISA review manual 2014 Page number 260

QUESTION 41
Which of the following layer of an OSI model encapsulates packets into frames?

A. Transport Layer
B. Network Layer
C. Data Link Layer
D. Physical Layer
.

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

Explanation/Reference:
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link.

For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal. OSI Model

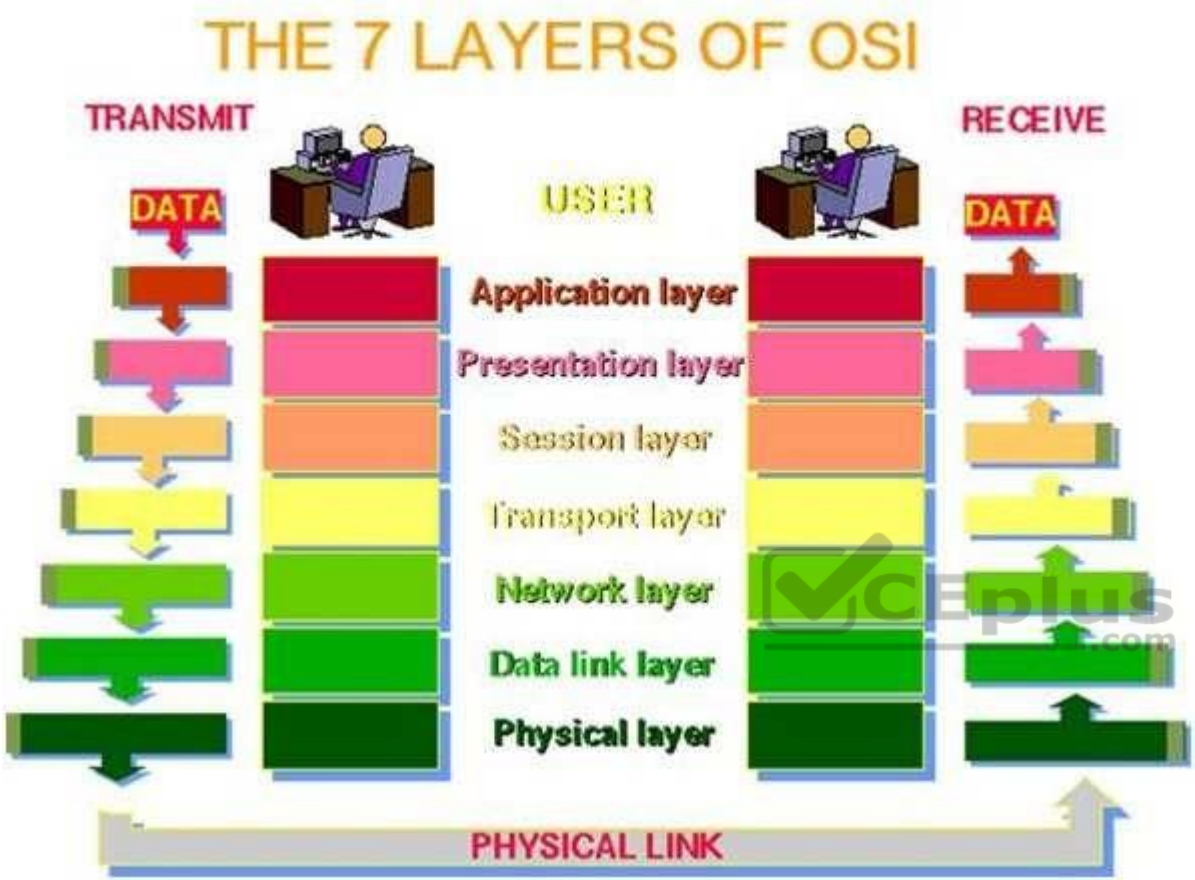


Image source: http://www.petri.co.il/images/osi_model.JPG

PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts
How the receiving station delimits a frame

DATA LINK LAYER
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.
Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
Frame sequencing: transmits/receives frames sequentially.
Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet
The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER
The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:
Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals

The following were incorrect answers:
Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.
Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.
Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

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

CISA review manual 2014 Page number 260

QUESTION 42
Which of the following layer of an OSI model transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier?

A. Transport Layer
B. Network Layer
C. Data Link Layer
D. Physical Layer

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

Explanation/Reference:
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

For your exam you should know below information about OSI model:
The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal. OSI Model

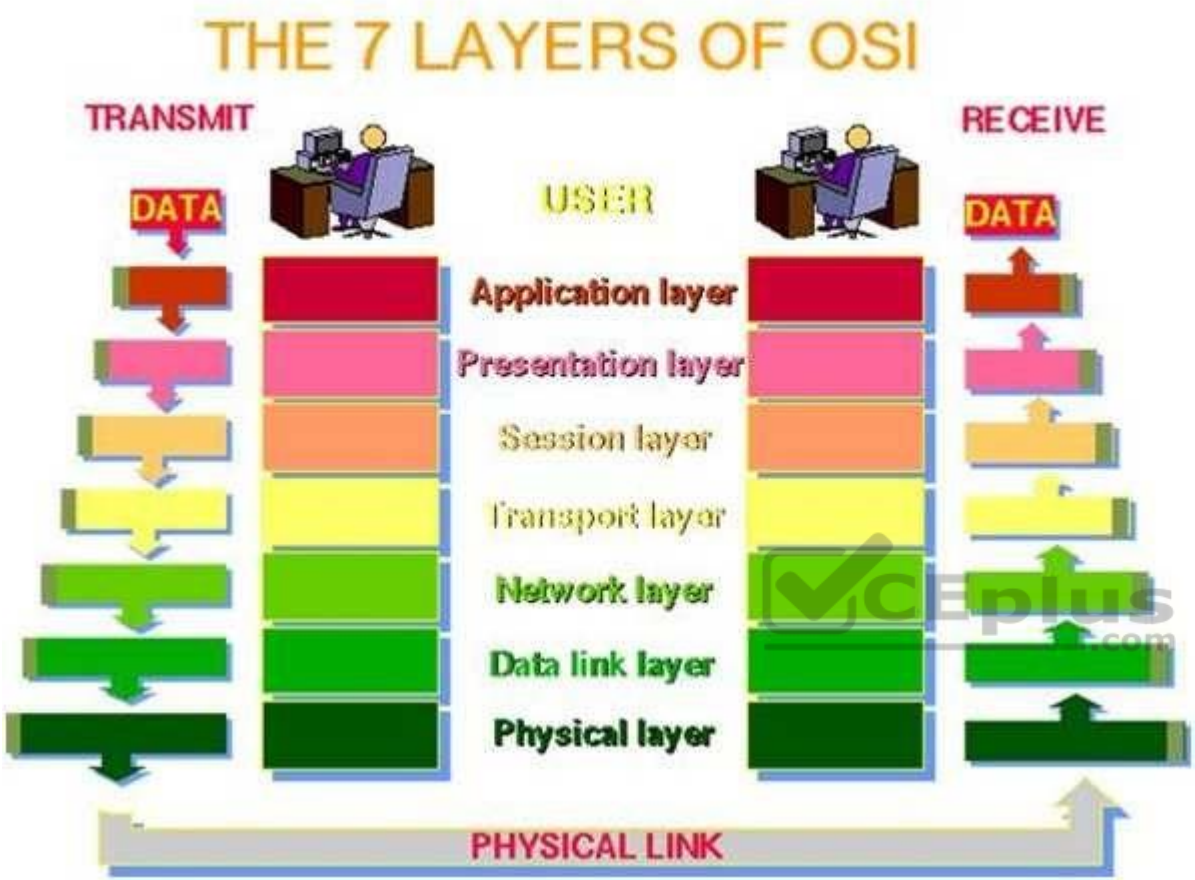


Image source: http://www.petri.co.il/images/osi_model.JPG
PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1
How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.
Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
Frame sequencing: transmits/receives frames sequentially.
Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet
The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).
In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:
Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals

The following were incorrect answers:
Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.
Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.
Data link layer - The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.

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

CISA review manual 2014 Page number 260

QUESTION 43
Which of the following statement INCORRECTLY describes network device such as a Router?

A. Router creates a new header for each packet
B. Router builds a routing table based on MAC address
C. Router does not forward broadcast packet
D. Router assigns a different network address per port

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

Explanation/Reference:
The INCORRECTLY keyword is used in the question. You need to find out a statement which is not valid about router. Router builds a routing table based on IP address and not on MAC address.

Difference between Router and Bridge:
Router
Bridge

Creates a new header for each packet
Does not alter header. Only reads the header
Builds routing table based on IP address
Build forwarding table based on MAC address
Assigns a different network address per port

Use the same network address for all ports

Filters traffic based on IP address
Filter traffic based on MAC address

Does not forward broadcast packet

Forward broadcast packet
Does not forward traffic that contain destination address unknown to the router

Forward traffic if destination address is unknown to bridge

For your exam you should know below information about network devices:

Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.
A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Repeater

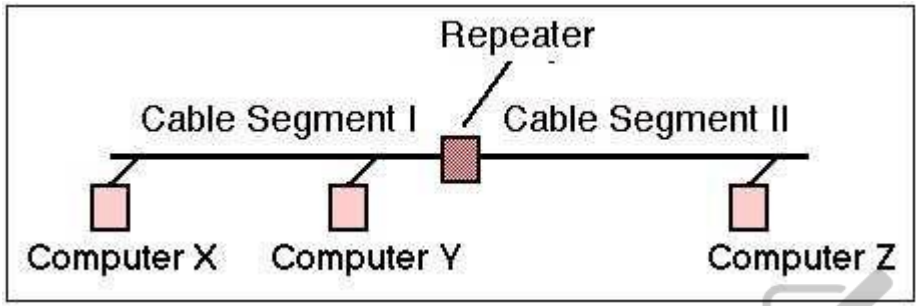


Image from: http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif

Bridges
A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge

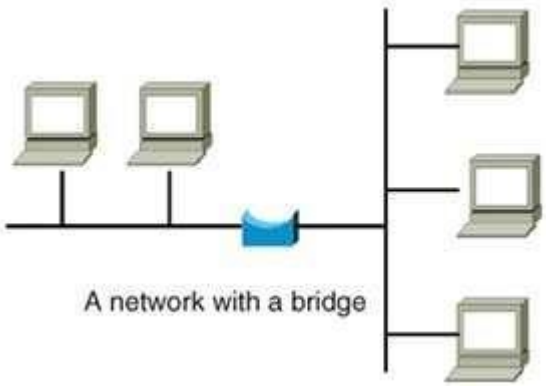


Image from: http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg

Routers

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch

Image from: http://www.computer-networking-success.com/images/router-switch.jpg

Switches

Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways
Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions.

Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server

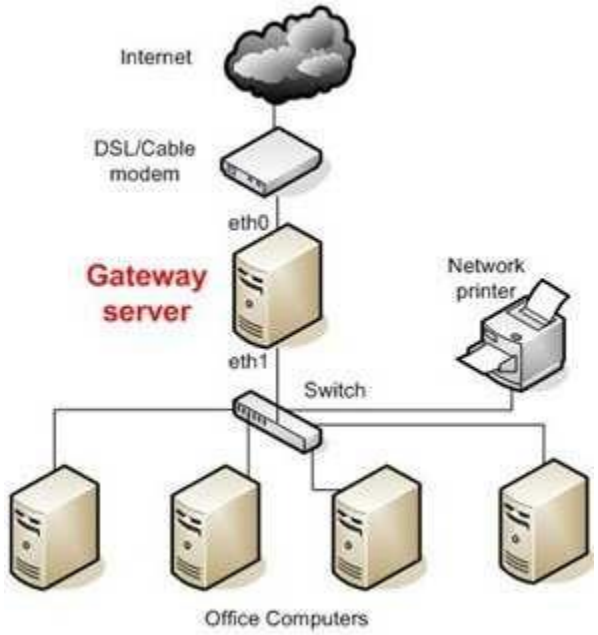
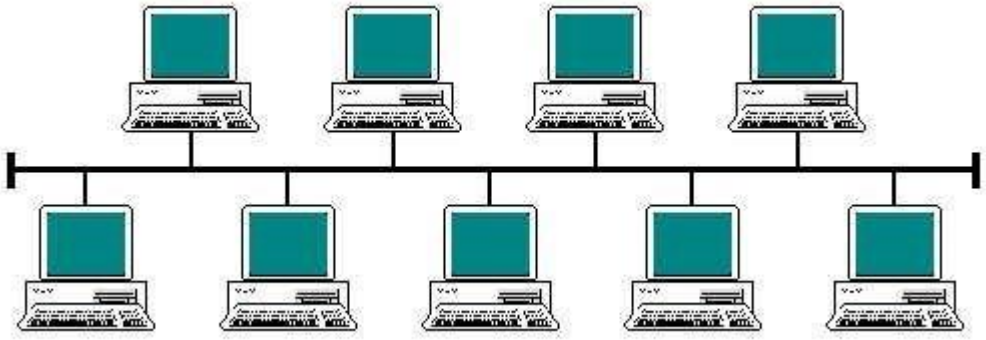


Image from: http://static.howtoforge.com/

The following were incorrect answers:
The other options presented correctly describes about Router.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 263

QUESTION 44
Identify the LAN topology from below diagram presented below:



bus topology

A. Bus
B. Star
C. Ring
D. Mesh

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

Explanation/Reference:
For your exam you should know the information below related to LAN topologies:

LAN Topologies
Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

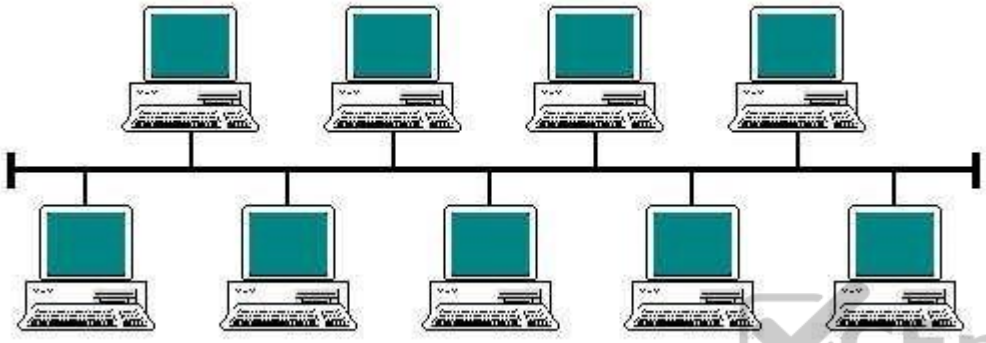
Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

Bus topology



Graphic from: http://www.technologyuk.net/telecommunications/networks/images/bus_topology.gif

Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Star

In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure. Star Topology

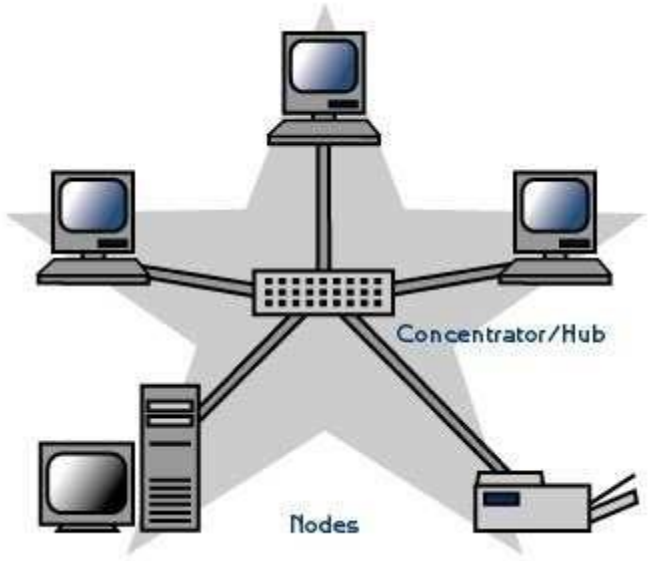


Image from: http://fcit.usf.edu/network/chap5/pics/star.gif

Ring
A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

Ring Topology

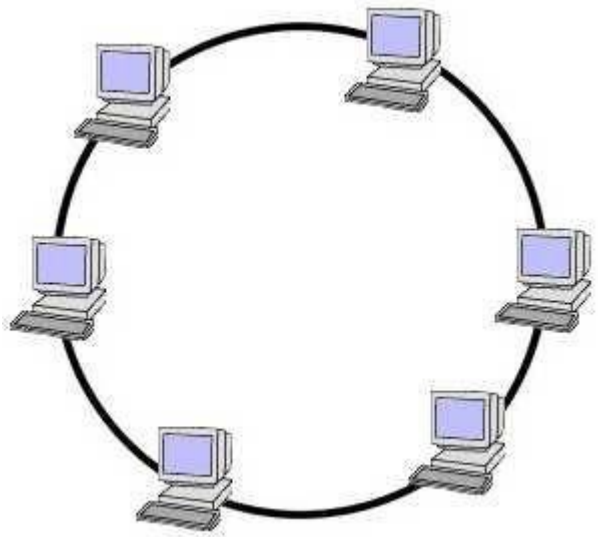


Image from: https://forrester-infosystems.wikispaces.com/

Mesh
The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.
Mesh Topology

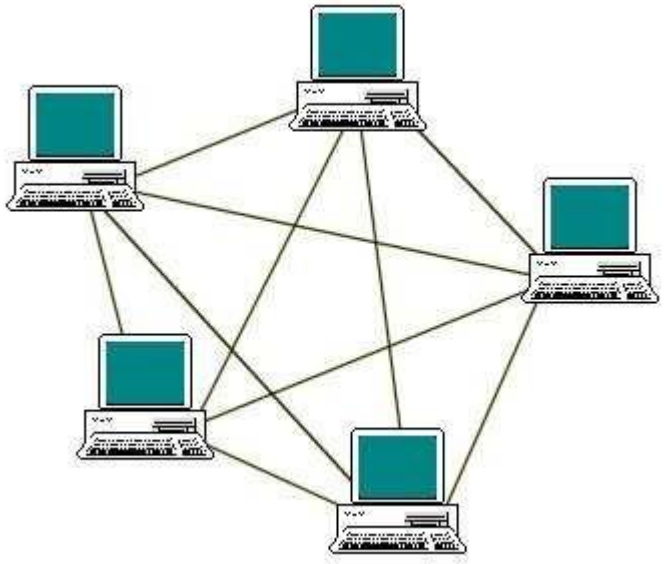


Image from: http://www.technologyuk.net/telecommunications/networks/images/mesh_topology.gif

Fully connected mesh topology
A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

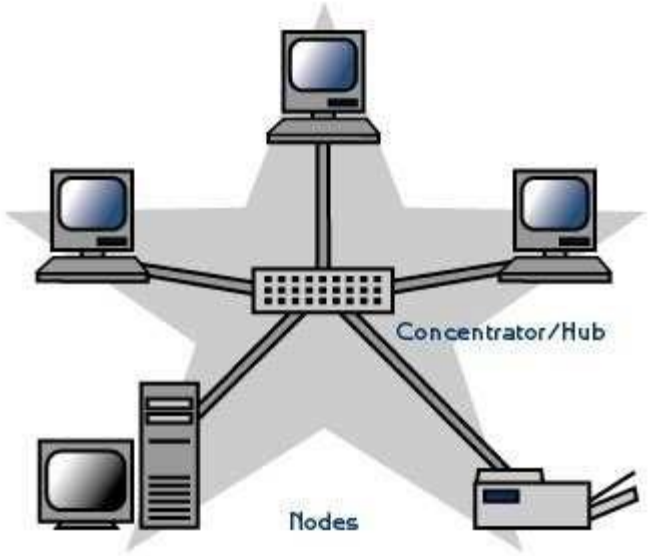
Partially connected mesh topology
The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:

The other options presented are not valid.

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

CISA review manual 2014, Page number 262
QUESTION 45
Identify the network topology from below diagram presented below:



Network Topology

A. Bus
B. Star
C. Ring
D. Mesh

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

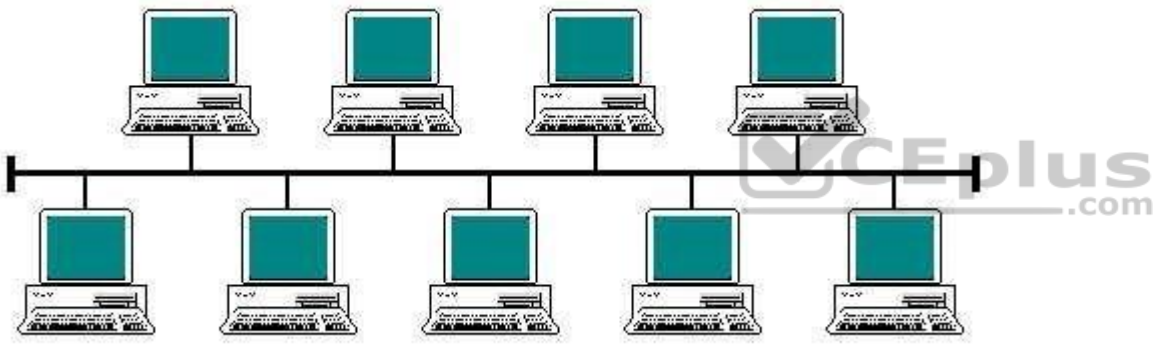
Explanation/Reference:
For your exam you should know the information below related to LAN topologies:

LAN Topologies
Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus
In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down. Bus topology Graphic from:



http://www.technologyuk.net/telecommunications/networks/images/bus_topology.gif

Linear bus
The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus
The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Star

In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure.

Star Topology

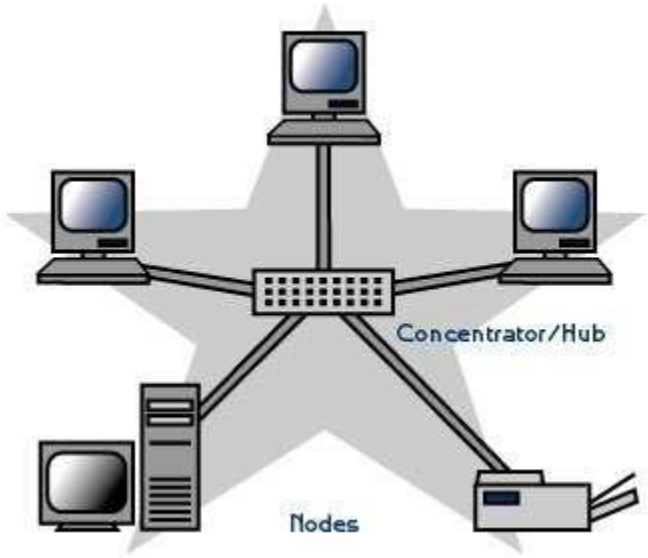


Image from: http://fcit.usf.edu/network/chap5/pics/star.gif

Ring

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

Ring Topology

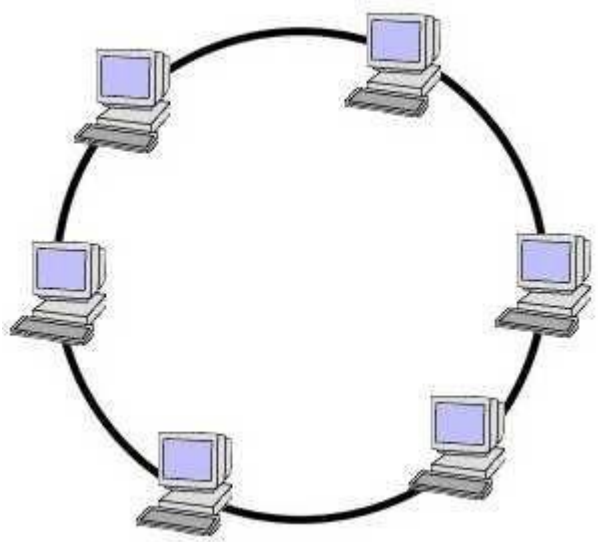


Image from: https://forrester-infosystems.wikispaces.com/

Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.
Mesh Topology

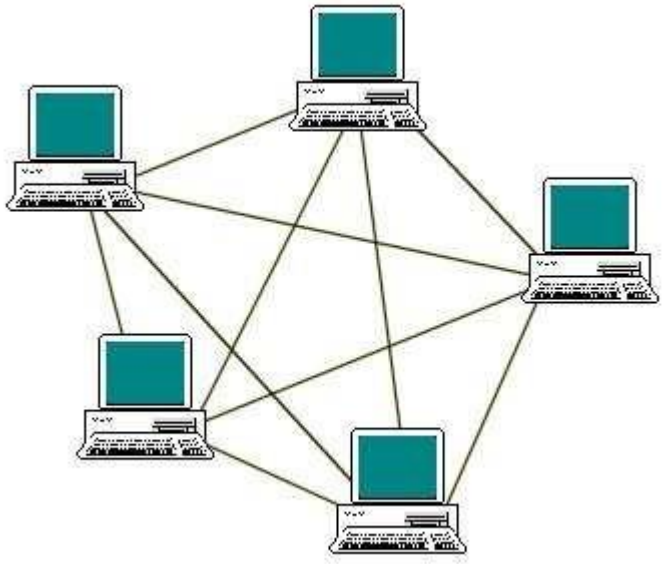


Image from: http://www.technologyuk.net/telecommunications/networks/images/mesh_topology.gif

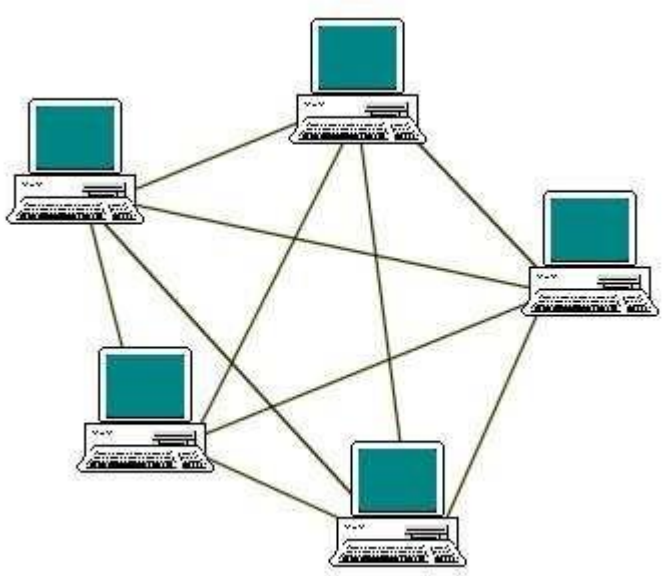
Fully connected mesh topology
A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology
The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:
The other options presented are not valid.

The following reference(s) were/was used to create this question:
CISA review manual 2014, Page number 262

QUESTION 46
Identify the network topology from below diagram presented below:



Network Topology

A. Bus
B. Star
C. Ring
D. Mesh

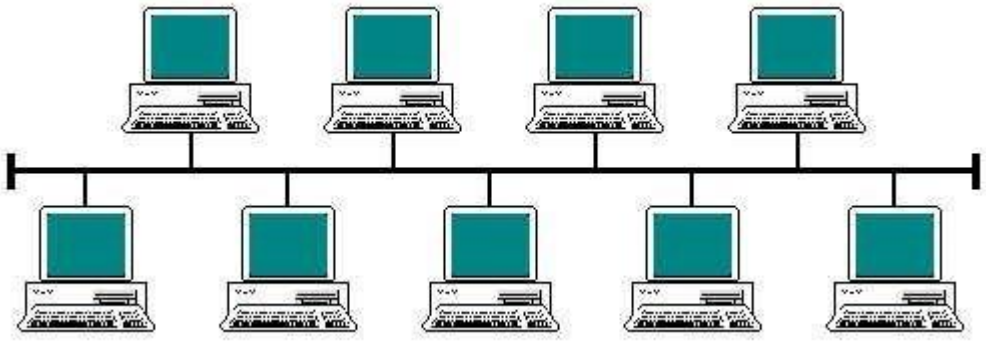
Correct Answer: D
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
For your exam you should know the information below related to LAN topologies:
LAN Topologies
Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus
In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down. Bus topology



Graphic from: http://www.technologyuk.net/telecommunications/networks/images/bus_topology.gif

Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus
The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).
Star

In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure.
Star Topology

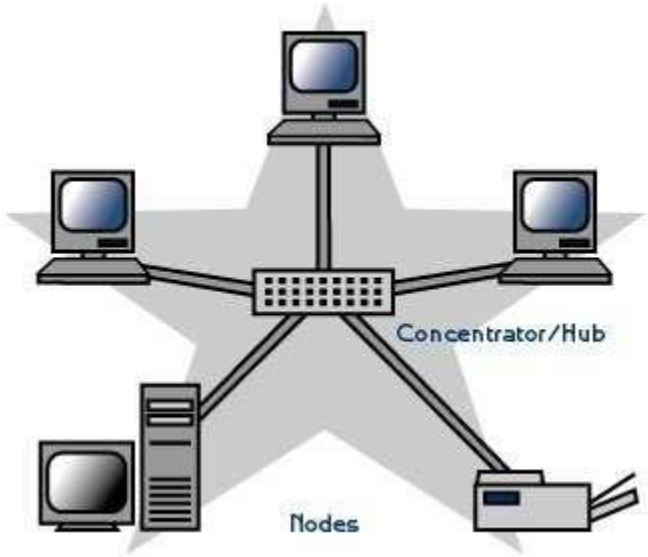


Image from: http://fcit.usf.edu/network/chap5/pics/star.gif

Ring

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

Ring Topology

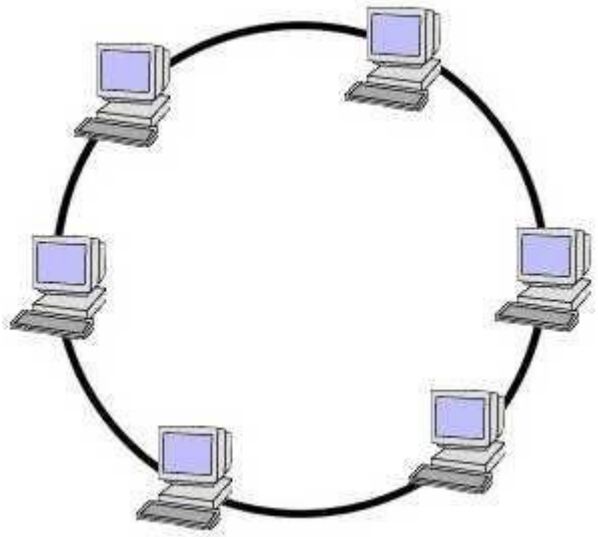


Image from: https://forrester-infosystems.wikispaces.com/

Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.
Mesh Topology

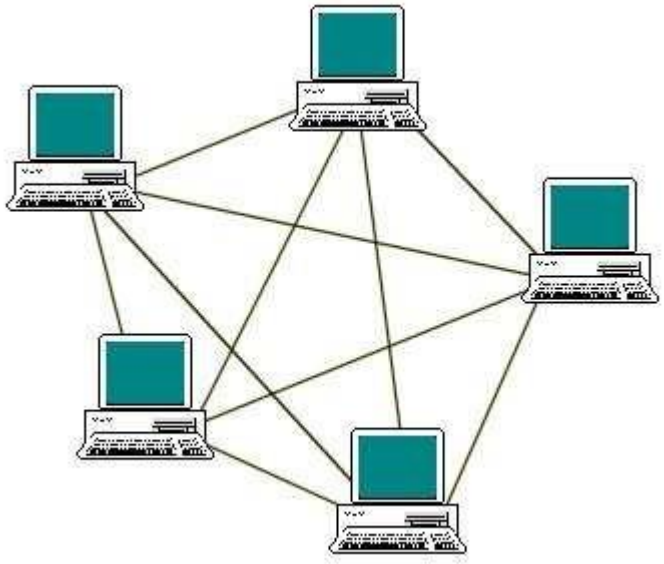


Image from: http://www.technologyuk.net/telecommunications/networks/images/mesh_topology.gif

Fully connected mesh topology
A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology
The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:
The other options presented are not valid.

The following reference(s) were/was used to create this question:
CISA review manual 2014, Page number 262

QUESTION 47

Identify the WAN message switching technique being used from the description presented below:
“Data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, this WAN switching technology stores and delays the message until ample resources become available for effective transmission of the message. “

A. Message Switching
B. Packet switching
C. Circuit switching
D. Virtual Circuits

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

Explanation/Reference:
For your exam you should know below information about WAN message transmission technique:

Message Switching
Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

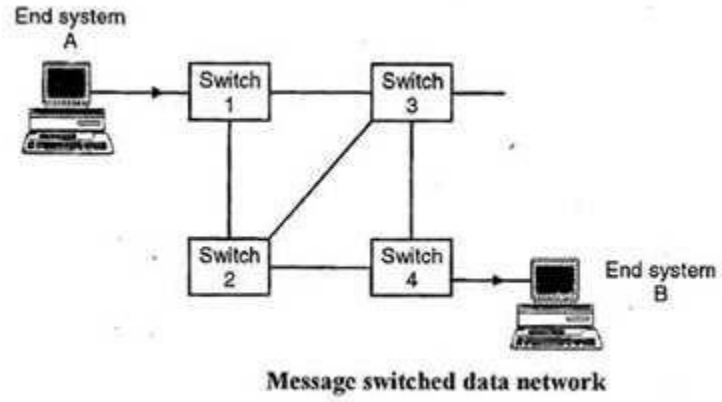


Image from: http://ecomputernotes.com/images/Message-Switched-data-Network.jpg

Packet Switching
Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Packet Switching

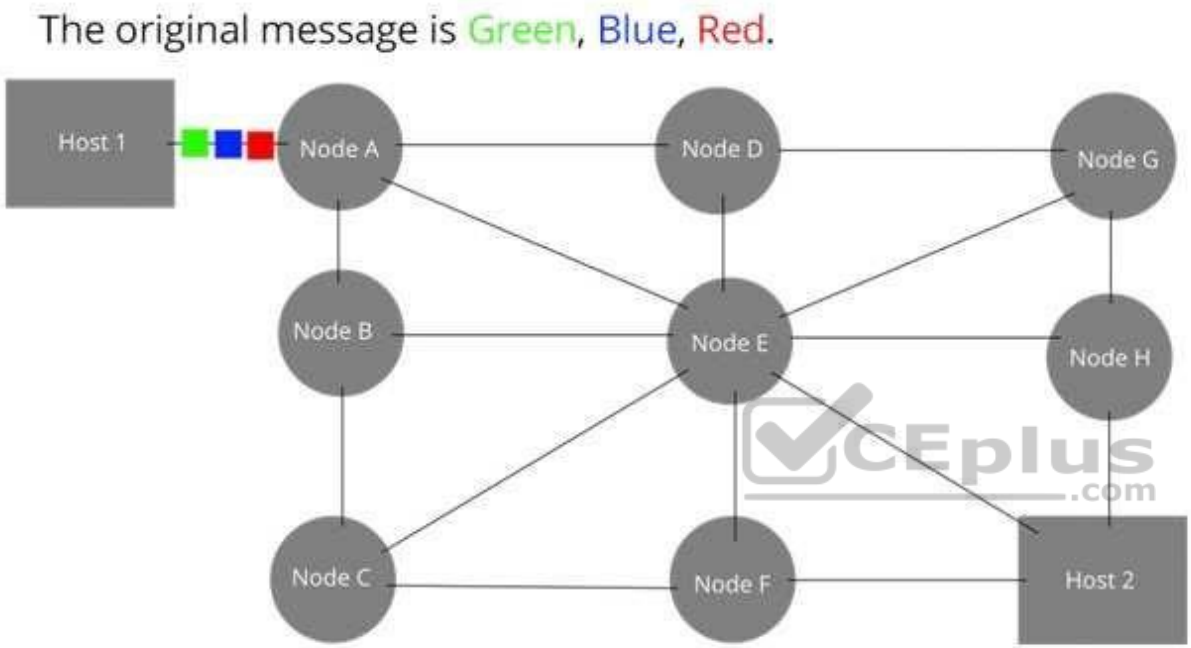


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

Circuit Switching
Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.
The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching

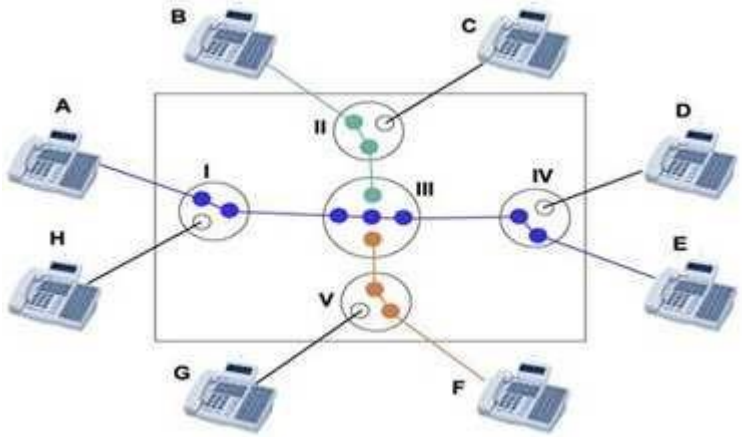


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

See a table below comparing Circuit Switched versus Packet Switched networks:
Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Image from:http://www.hardware-one.com/reviews/network-guide-2/images/packet-vs-circuit.gif

Virtual circuit
In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes, varying bit rate generated by the application, varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:
The other options presented are not valid choices.

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

QUESTION 48
In which of the following WAN message transmission technique messages are divided into packets before they are sent and each packet is then transmitted individually and can even follow different routes to its destination?

A. Message Switching
B. Packet switching
C. Circuit switching
D. Virtual Circuits

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

Explanation/Reference:
For your exam you should know below information about WAN message transmission technique:
Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

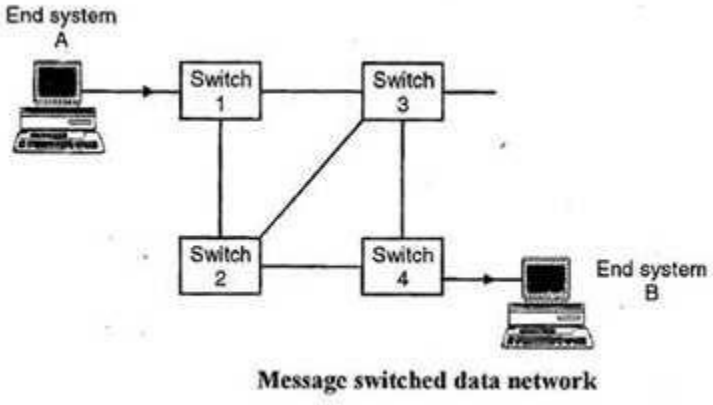


Image from: http://ecomputernotes.com/images/Message-Switched-data-Network.jpg

Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Packet Switching

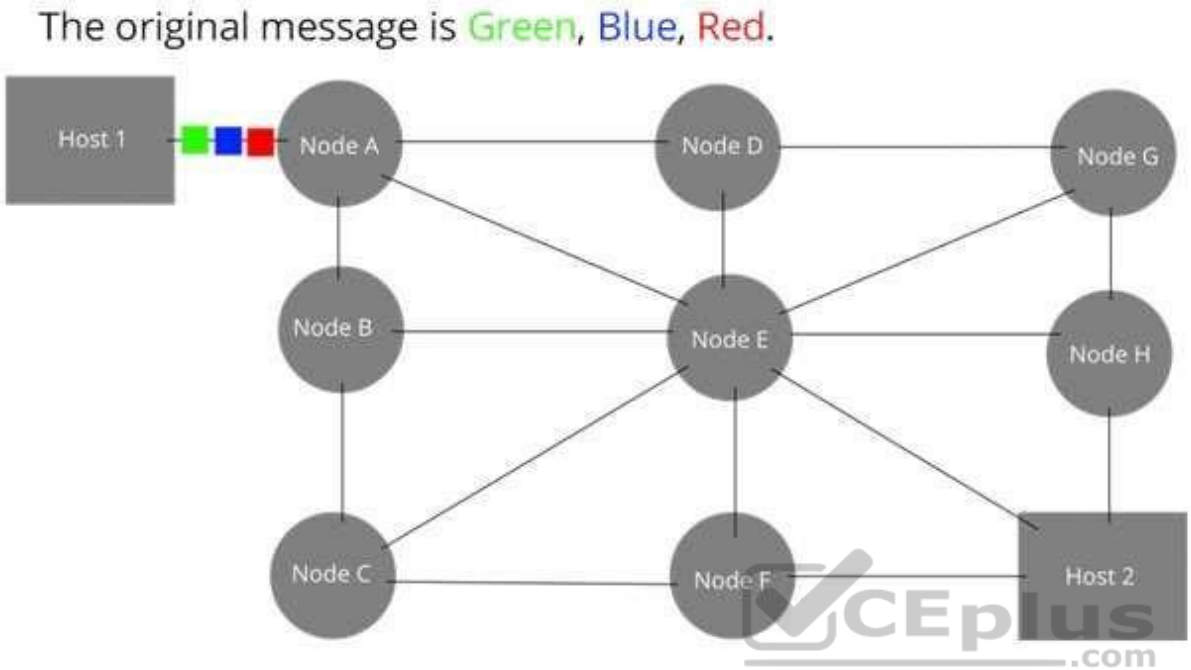


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

Circuit Switching
Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching

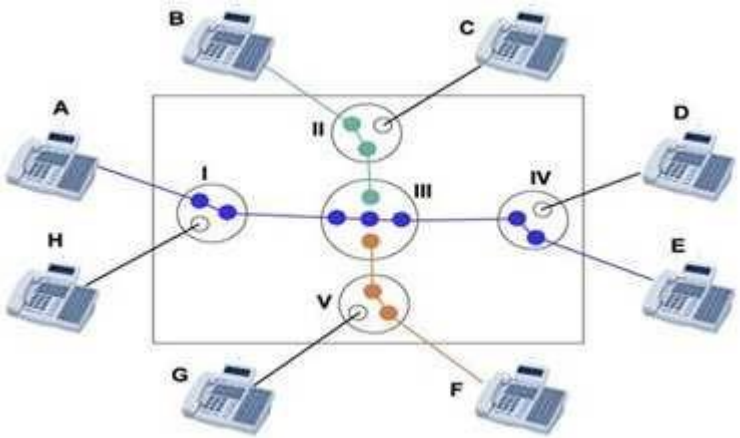


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

See a table below comparing Circuit Switched versus Packet Switched networks:
Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Image from:http://www.hardware-one.com/reviews/network-guide-2/images/packet-vs-circuit.gif

Virtual circuit
In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes, varying bit rate generated by the application, varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:
The other options presented are not valid choices.

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

QUESTION 49
In which of the following WAN message transmission technique does two network nodes establish a dedicated communications channel through the network before the nodes may communicate?

A. Message Switching
B. Packet switching
C. Circuit switchingD. Virtual Circuits

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

Explanation/Reference:
For your exam you should know below information about WAN message transmission technique:
Message Switching
Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

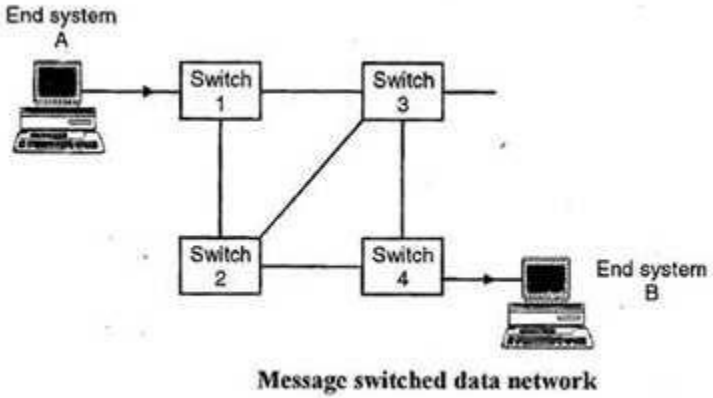


Image from: http://ecomputernotes.com/images/Message-Switched-data-Network.jpg

Packet Switching
Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Packet Switching

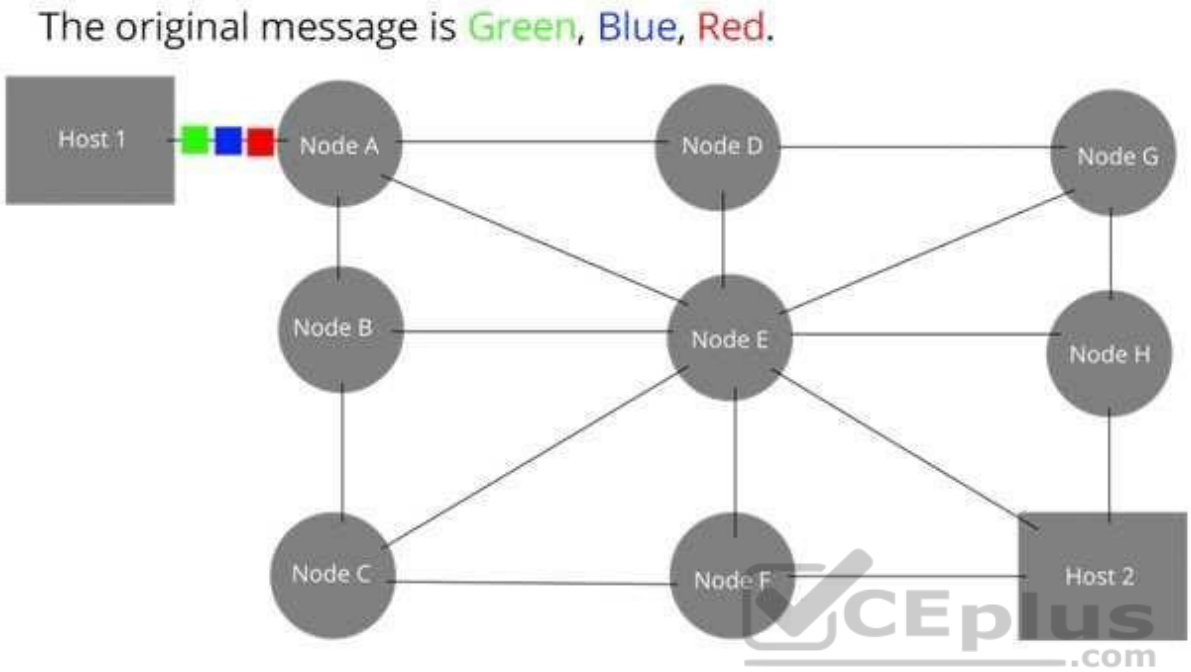


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

Circuit Switching
Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching

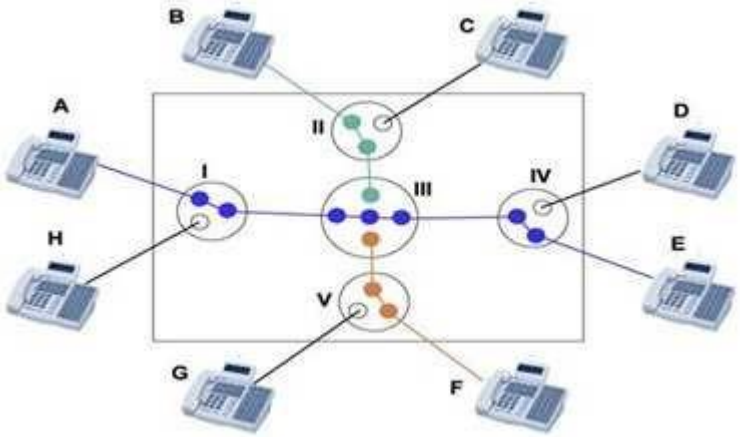


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

See a table below comparing Circuit Switched versus Packet Switched networks:
Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Image from:http://www.hardware-one.com/reviews/network-guide-2/images/packet-vs-circuit.gif

Virtual circuit
In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes, varying bit rate generated by the application, varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:
The other options presented are not valid choices.

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

QUESTION 50
Which of the following statement INCORRECTLY describes circuit switching technique?

A. Packet uses many different dynamic paths to get the same destination
B. Connection oriented virtual links
C. Fixed delays
D. Traffic travels in a predictable and constant manner

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

Explanation/Reference:
The word INCORRECTLY is the keyword used in the question. You need to find out a statement which is not valid about circuit switching.

For your exam you should know below information about WAN message transmission technique:

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

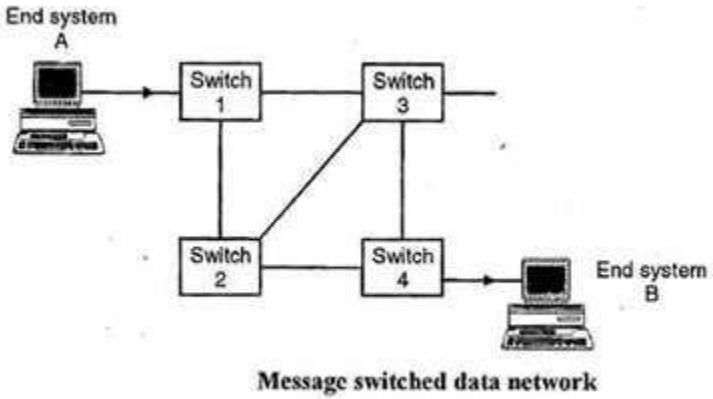


Image from: http://ecomputernotes.com/images/Message-Switched-data-Network.jpg

Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Packet Switching

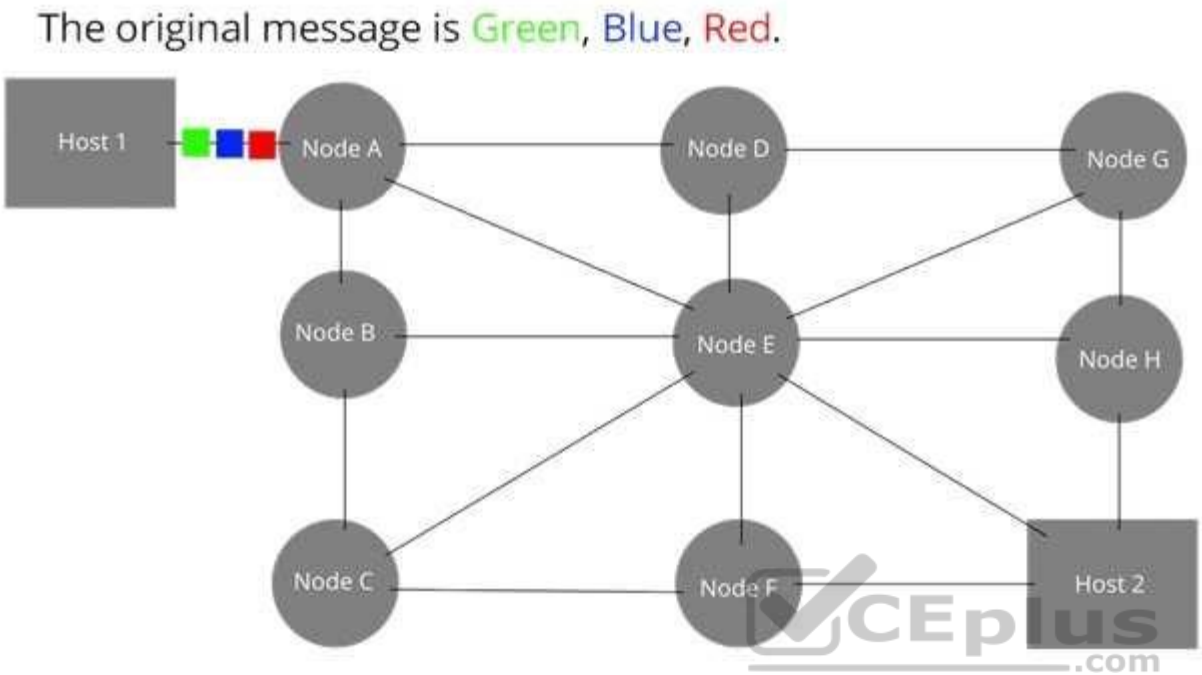


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

Circuit Switching
Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching

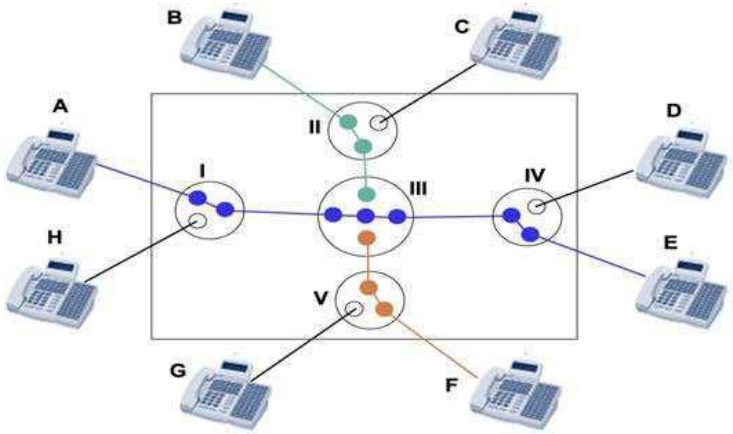


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

See a table below comparing Circuit Switched versus Packet Switched networks:
Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Image from:http://www.hardware-one.com/reviews/network-guide-2/images/packet-vs-circuit.gif

Virtual circuit
In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes, varying bit rate generated by the application, varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:
The other options presented correctly describes about circuit switching.

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

QUESTION 51
Which of the following statement INCORRECTLY describes packet switching technique?

A. Packet uses many different dynamic paths to get the same destination
B. Traffic is usually burst in nature
C. Fixed delays to reach each packet to destination
D. Usually carries data-oriented data

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

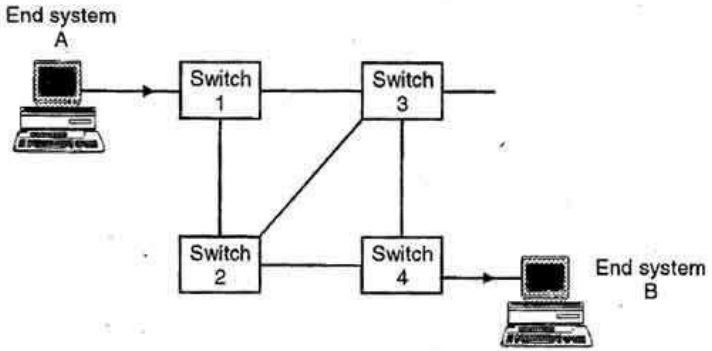
Explanation/Reference:
The word INCORRECTLY is the keyword used in the question. You need to find out a statement which is not valid about packet switching. As in the network switching, packet traverse different path, there will be always variable delay for each packet to reach to destination.

For your exam you should know below information about WAN message transmission technique:

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching



Message switched data network

Image from: http://ecomputernotes.com/images/Message-Switched-data-Network.jpg

Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Packet Switching

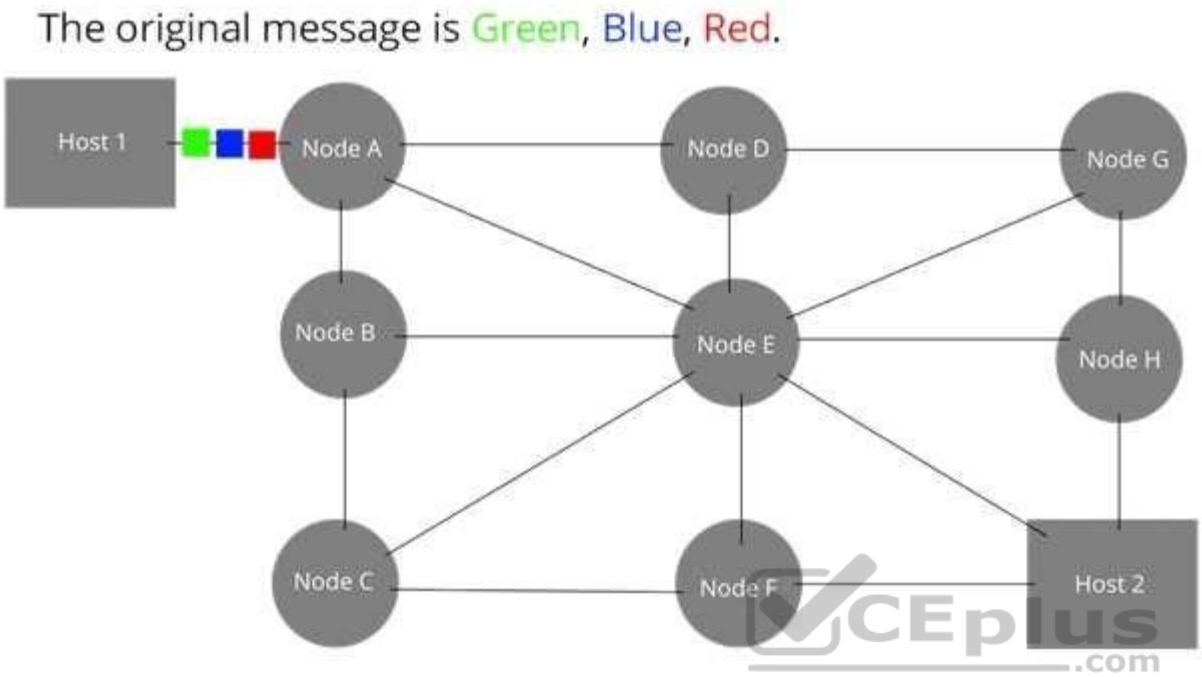


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

Circuit Switching

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching

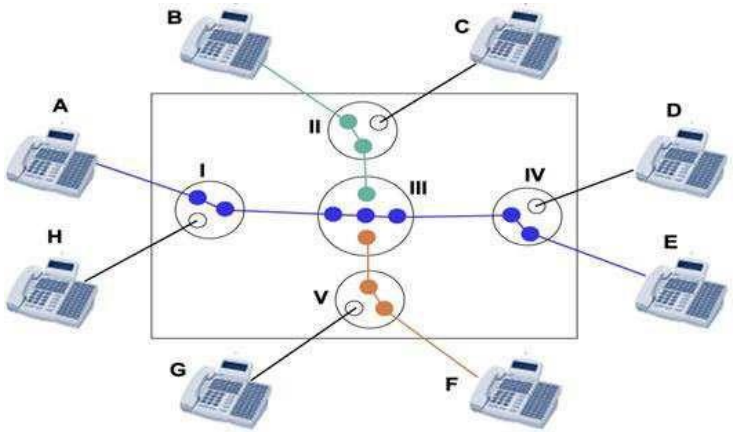


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

See a table below comparing Circuit Switched versus Packet Switched networks:
Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Image from:http://www.hardware-one.com/reviews/network-guide-2/images/packet-vs-circuit.gif

Virtual circuit
In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.
Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes, varying bit rate generated by the application, varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:
The other options presented correctly describes about packet switching.

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

QUESTION 52
Which of the following protocol uses serial interface for communication between two computers in WAN technology?

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

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

Explanation/Reference:
PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer using a MODEM connected by phone line to a server.

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

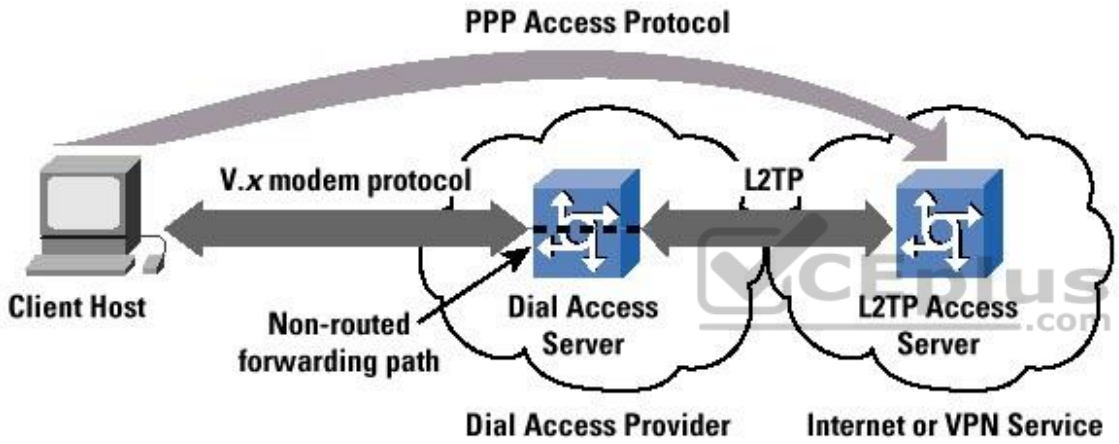
Point-to-point protocol
PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's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

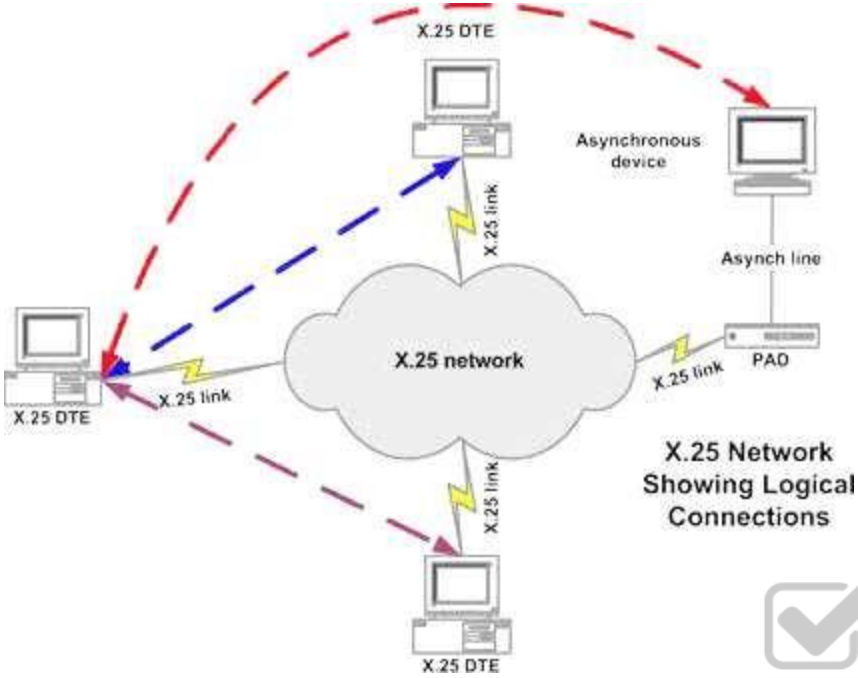
PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

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

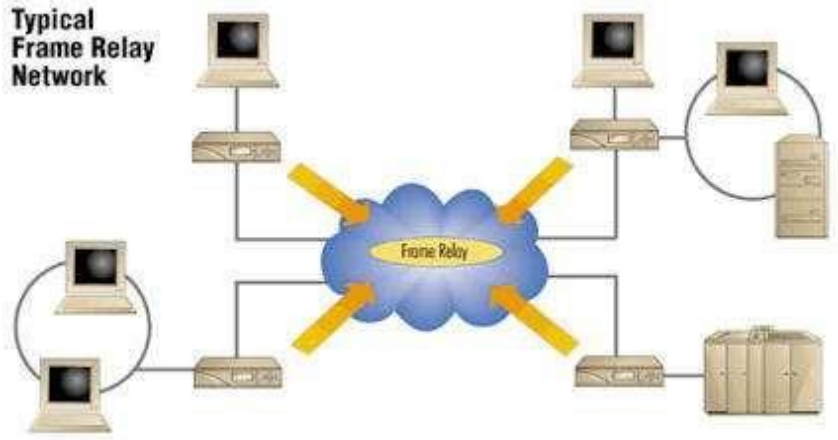
Works on a packet switching
Operates at data link layer of an OSI model
Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

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.

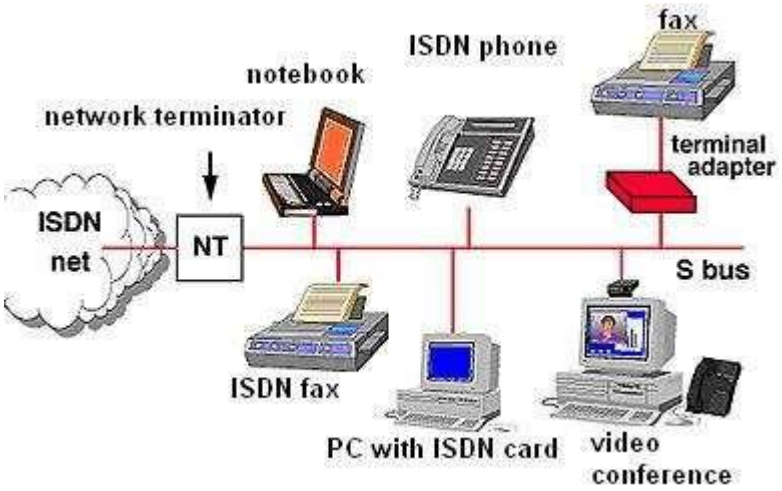


Frame Relay

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



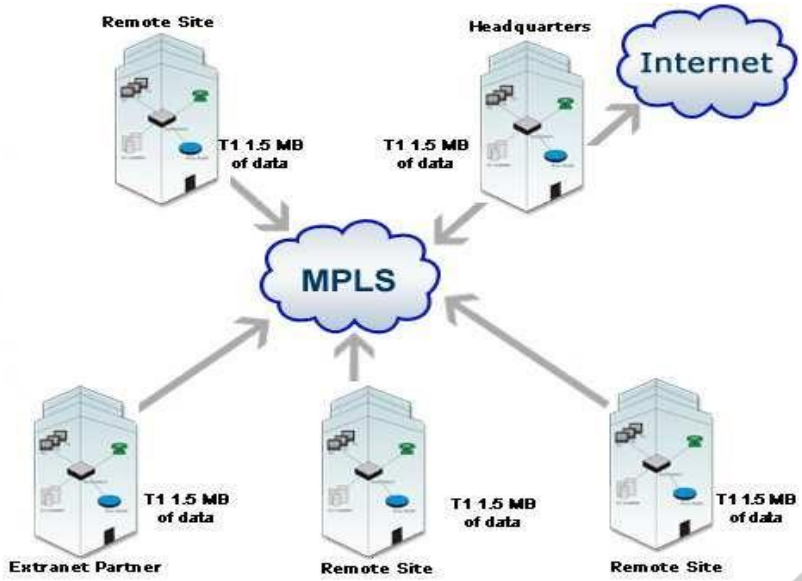
Asynchronous Transfer Mode (ATM)

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:

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.

Frame Relay - 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.

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. Same copper telephone wire is used. Provide digital point-to-point circuit switching medium.

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

QUESTION 53
Which of the following is a ITU-T standard protocol suite for packet switched wide area network communication?

A. Point-to-point protocol
B. X.25
C. Frame Relay

D. ISDN

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

Explanation/Reference:
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.

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

The following answers are incorrect:
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.
Frame Relay - 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.

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. Same copper telephone wire is used. Provide digital point-to-point circuit switching medium.

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

QUESTION 54
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

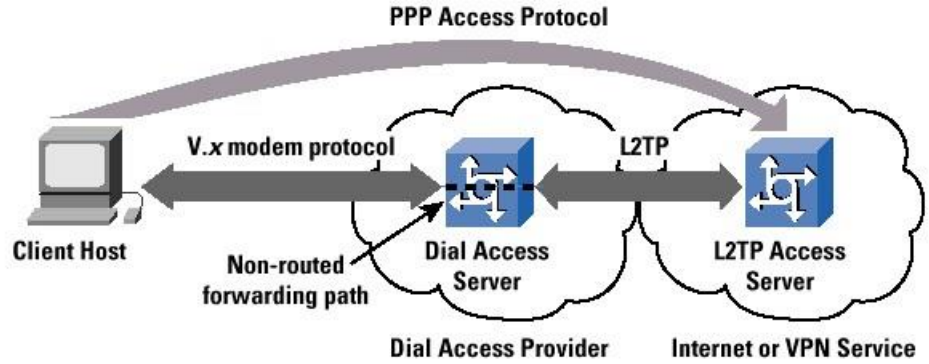


Image from:http://withfriendship.com/images/g/31728/a-pointtopoint-protocol.png

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

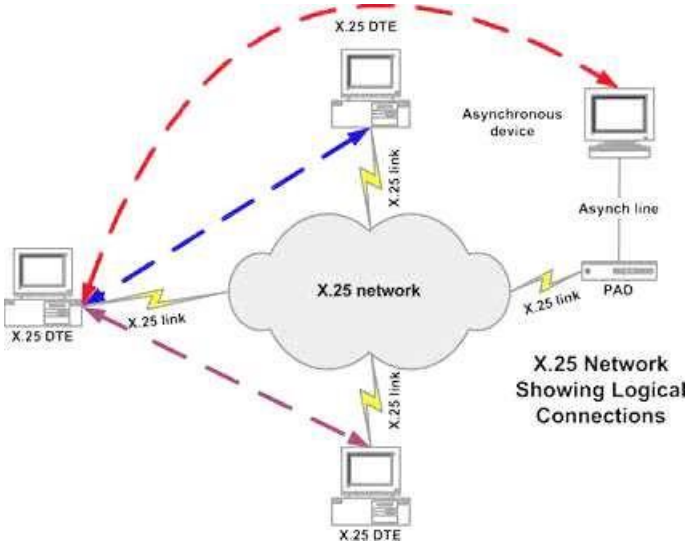


Image from:http://www.sangoma.com/assets/images/content/tutorials_x25_1.gif

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

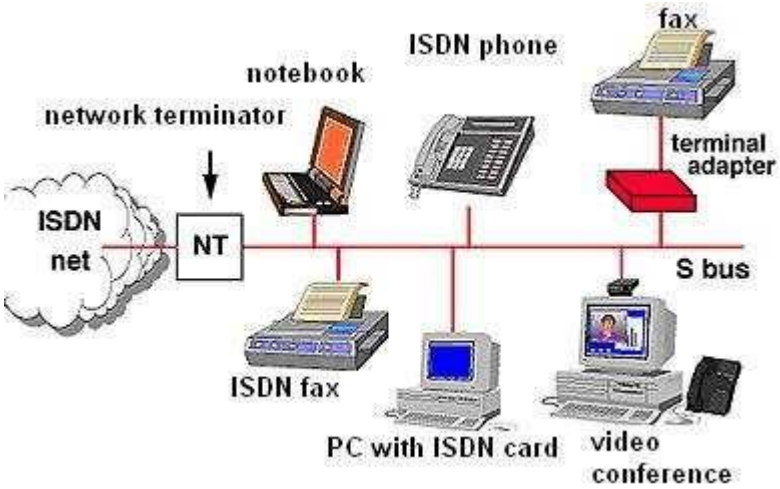


Image from: http://www.cpcstech.com/images/frame-2.jpg

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

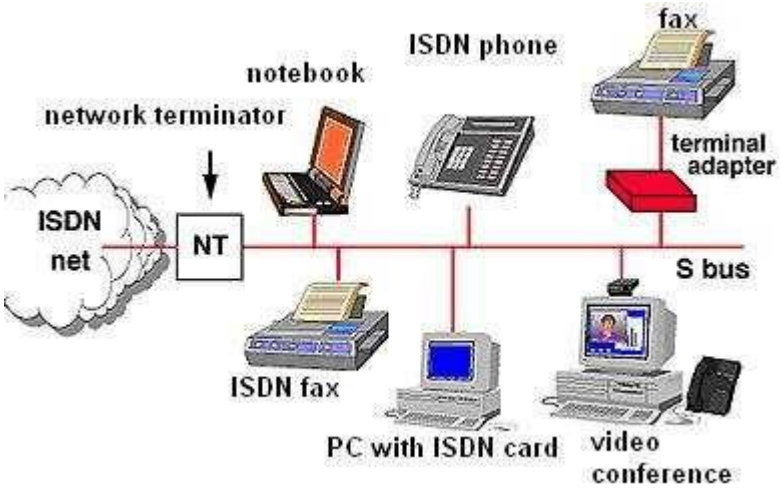


Image from: http://www.hw-server.com/obrazek/network_topology

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

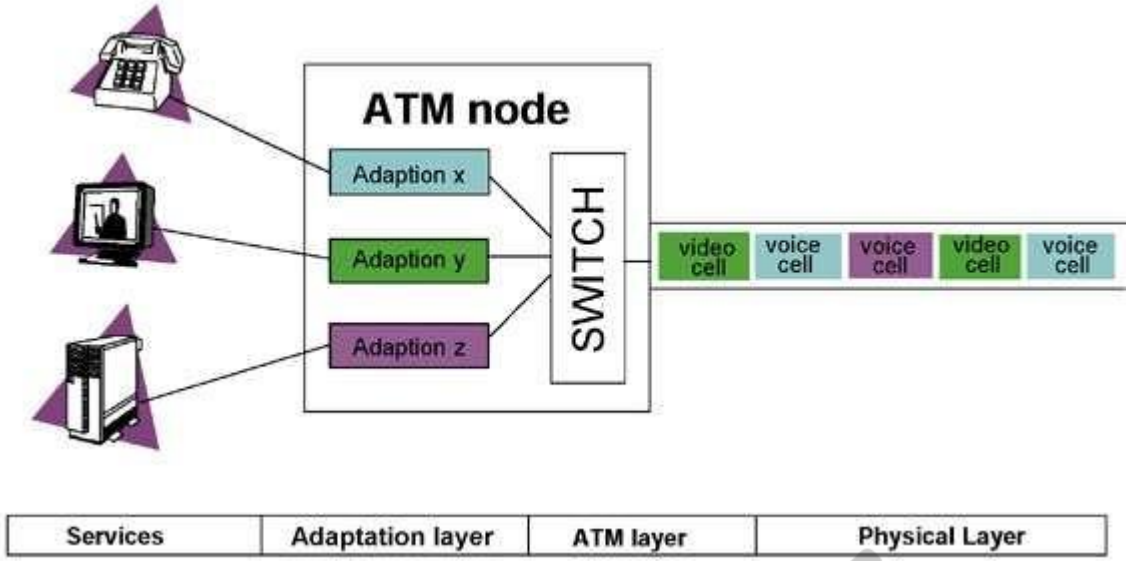


Image from: http://html.rincondelvago.com/000050700.png

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

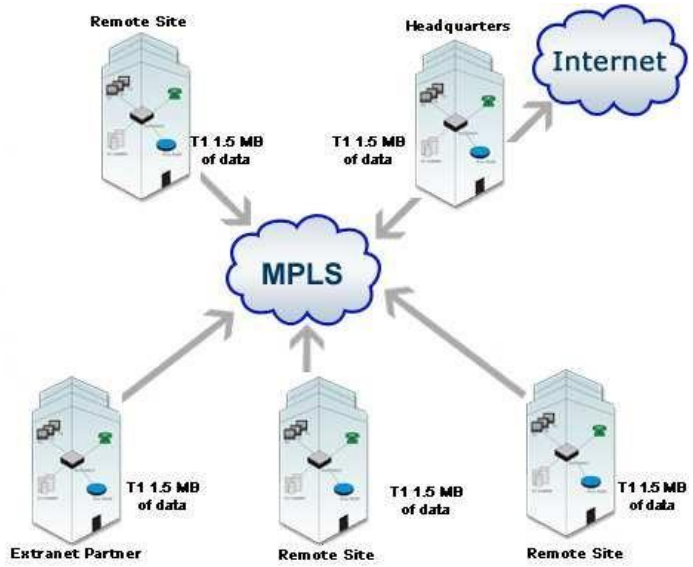


Image from: http://www.carrierbid.com/wp-content/uploads/2011/01/mpls1.gif

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 55
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

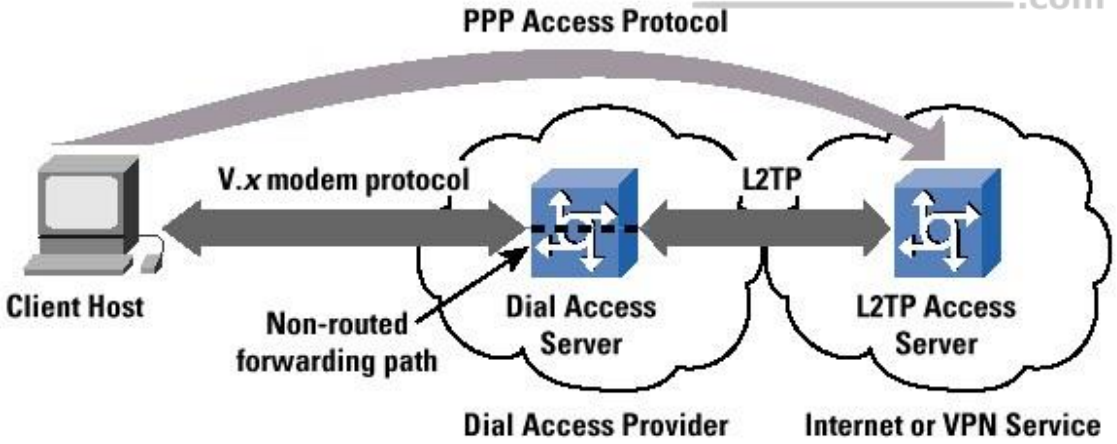
Explanation/Reference:
Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

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.

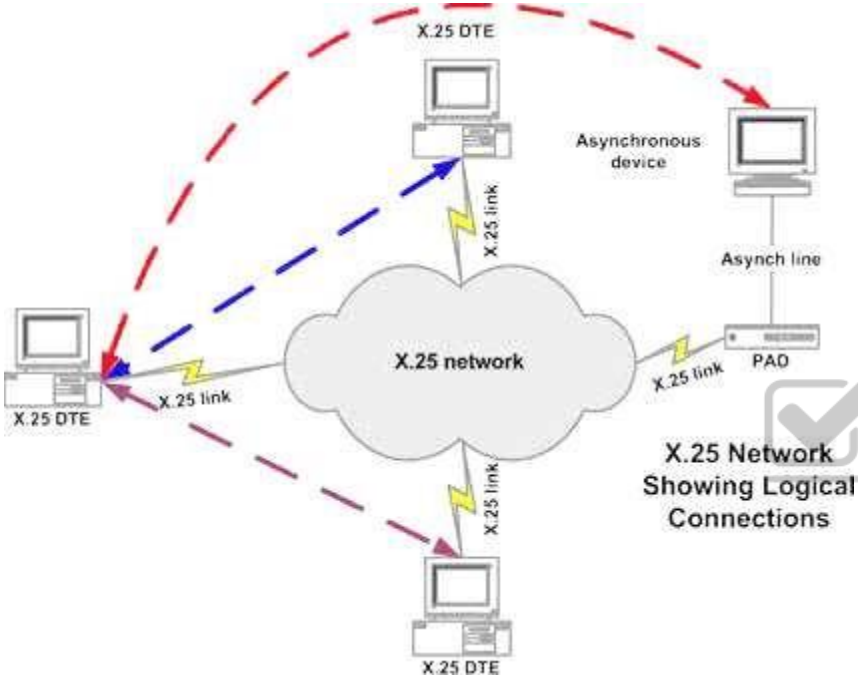


Point-to-point protocol

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.

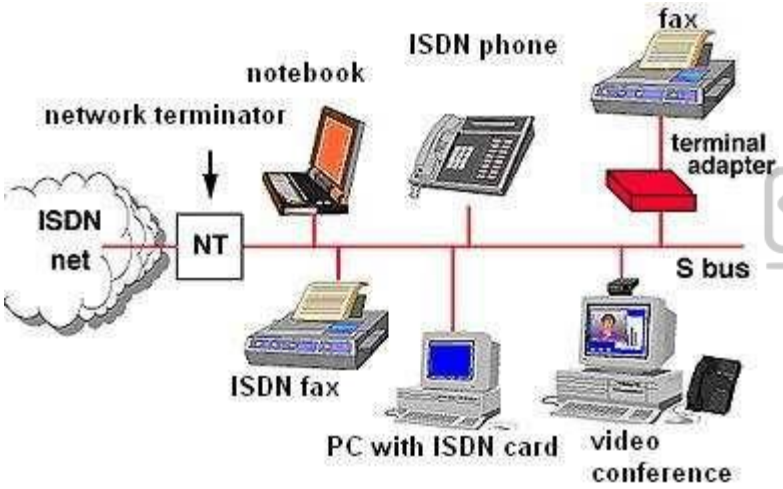
2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

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

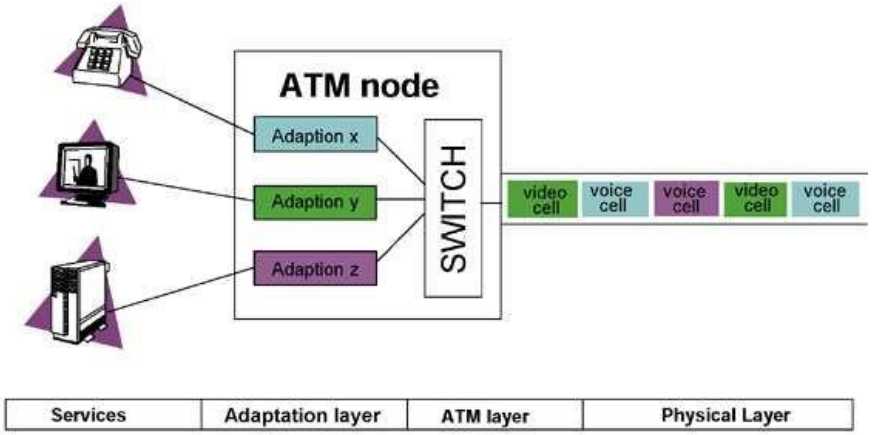
ISDN



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

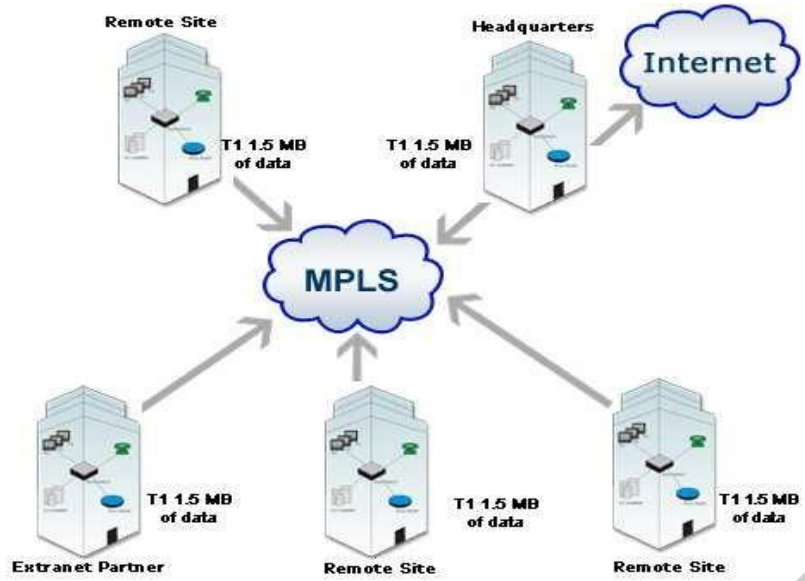
Asynchronous Transfer Mode



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 56
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

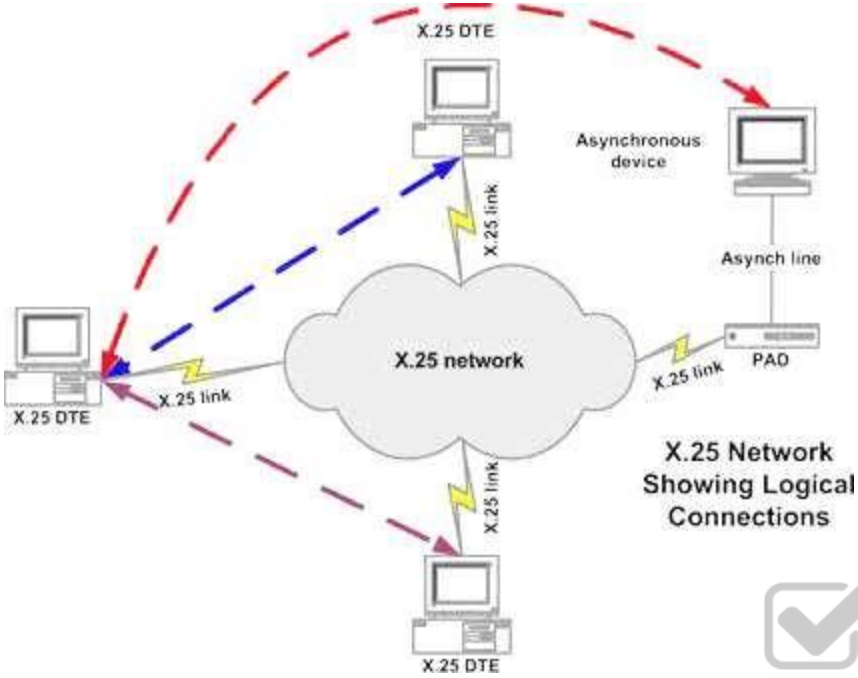
For your exam you should know below information about WAN Technologies:

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

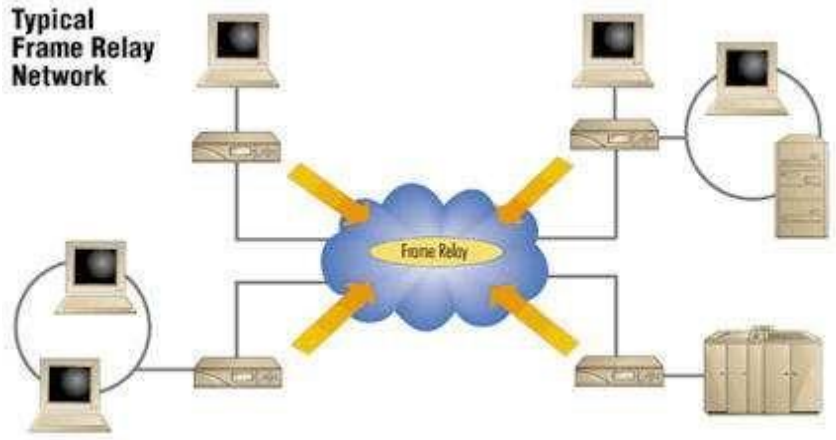
Works on a packet switching
Operates at data link layer of an OSI model
Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

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.

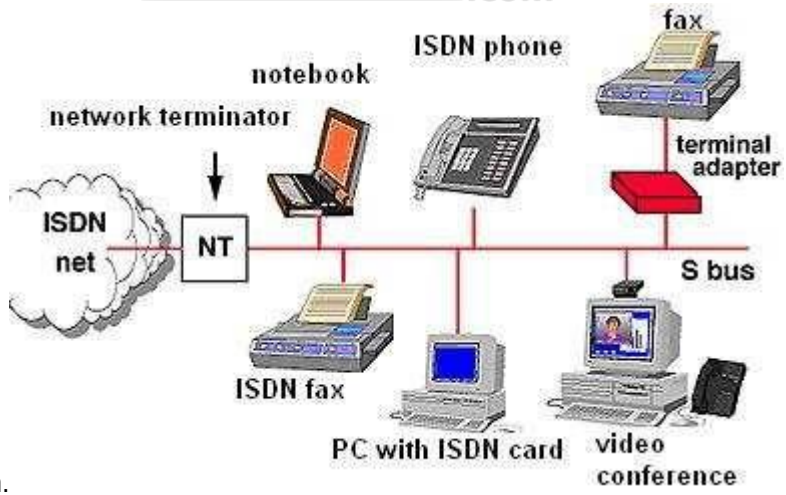
The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.



Frame Relay

Integrated Service Digital Network

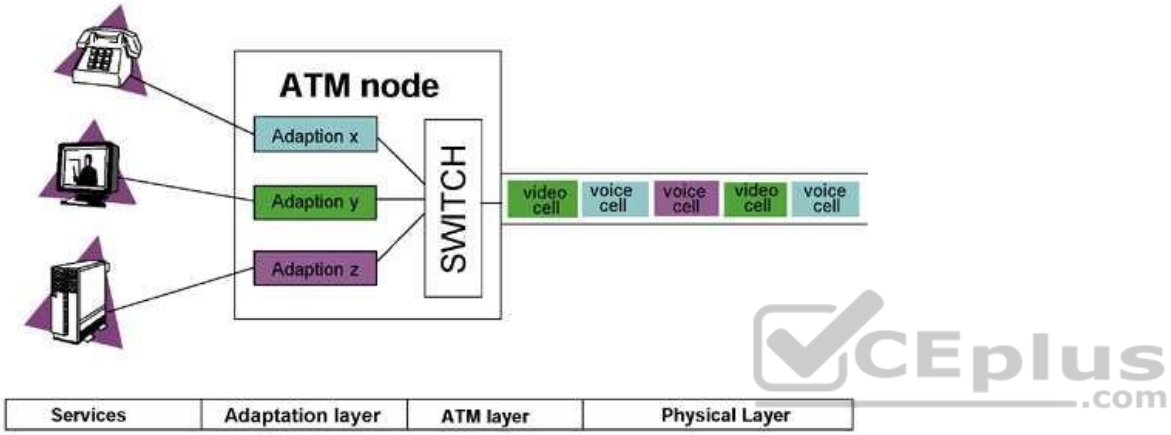
Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission. Same copper telephone wire is used.



Provide digital point-to-point circuit switching medium.

ISDN
Asynchronous Transfer Mode (ATM)

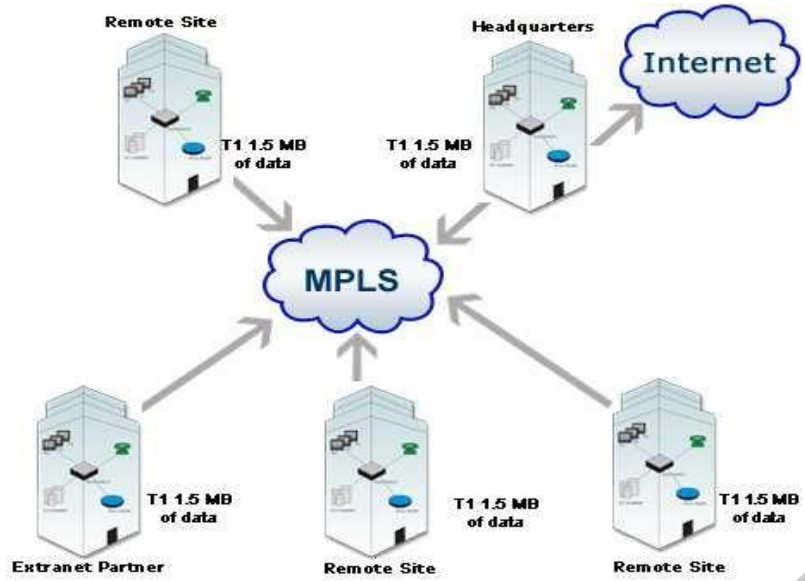
Uses Cell switching method
High speed network technology used for LAN, MAN and WAN
Like a frame relay it is connection oriented technology which creates and uses fixed channel
Data are segmented into fixed size cell of 53 bytes
Some companies have replaces FDDI back-end with ATM



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 57
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.

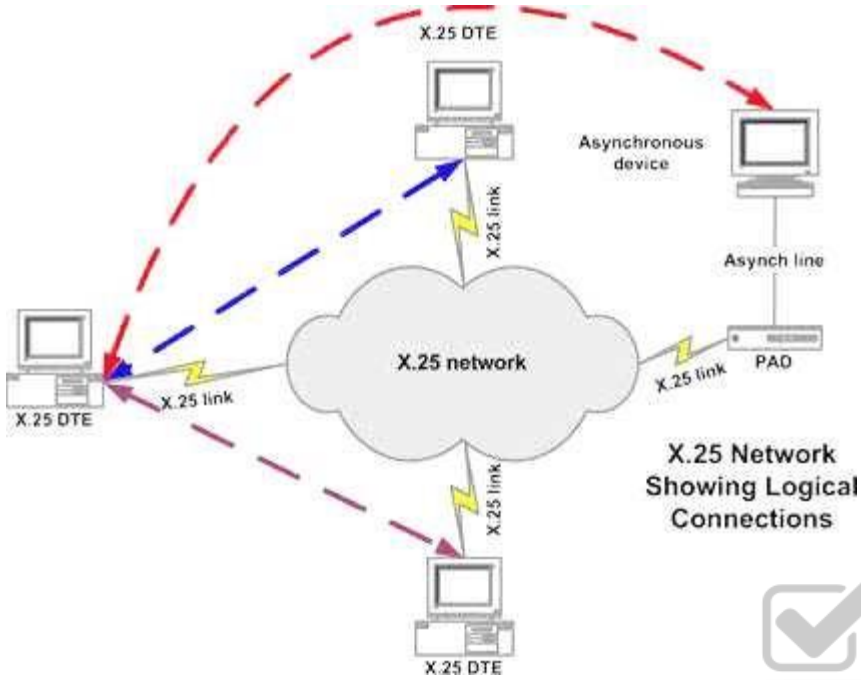
PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

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 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

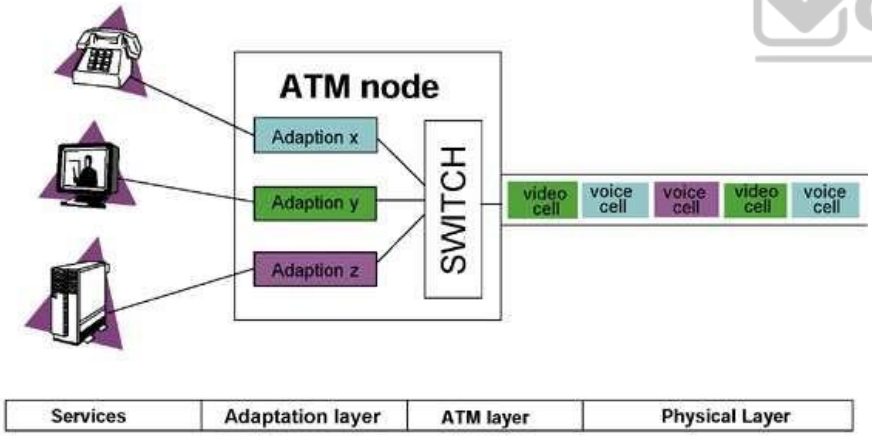
Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.
Same copper telephone wire is used.
Provide digital point-to-point circuit switching medium.

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

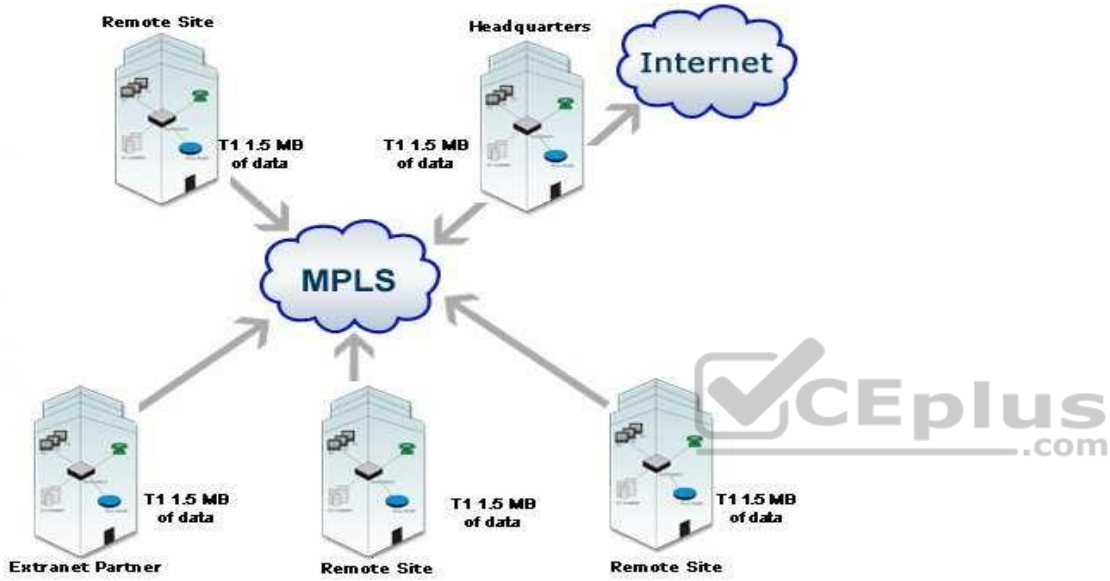
Asynchronous Transfer Mode



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:

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 58
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.

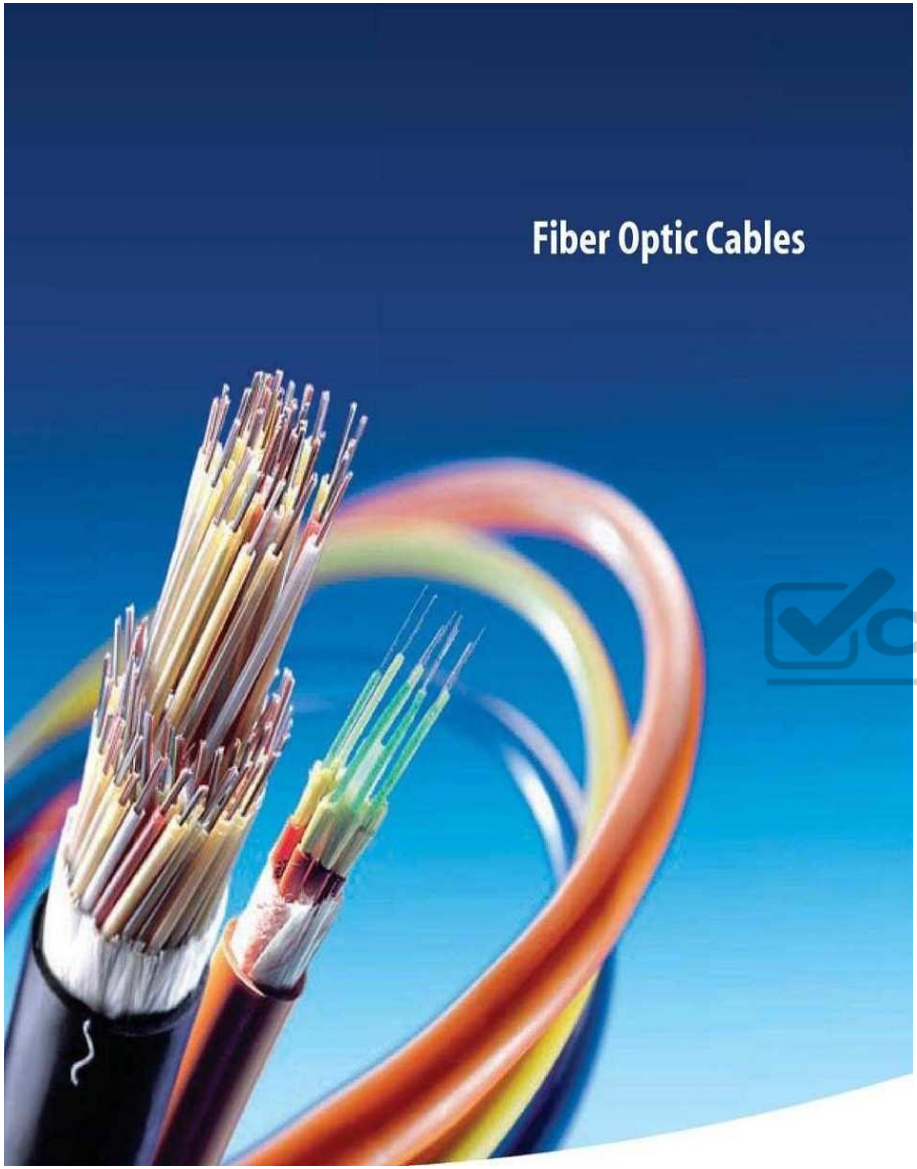
Coaxial Cable

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 59

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 60
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.

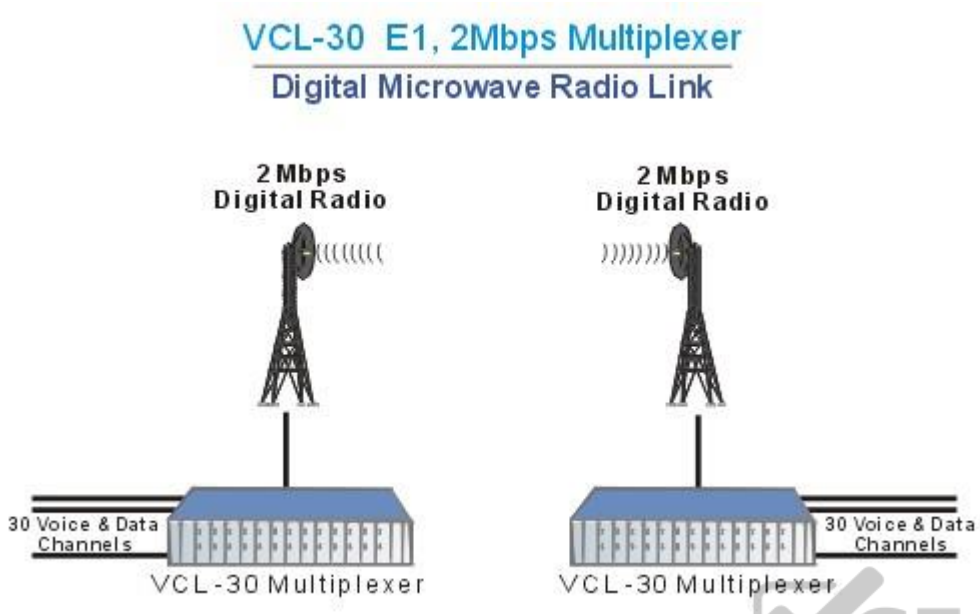
Fiber Optics

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 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.

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.

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.
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 61
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.

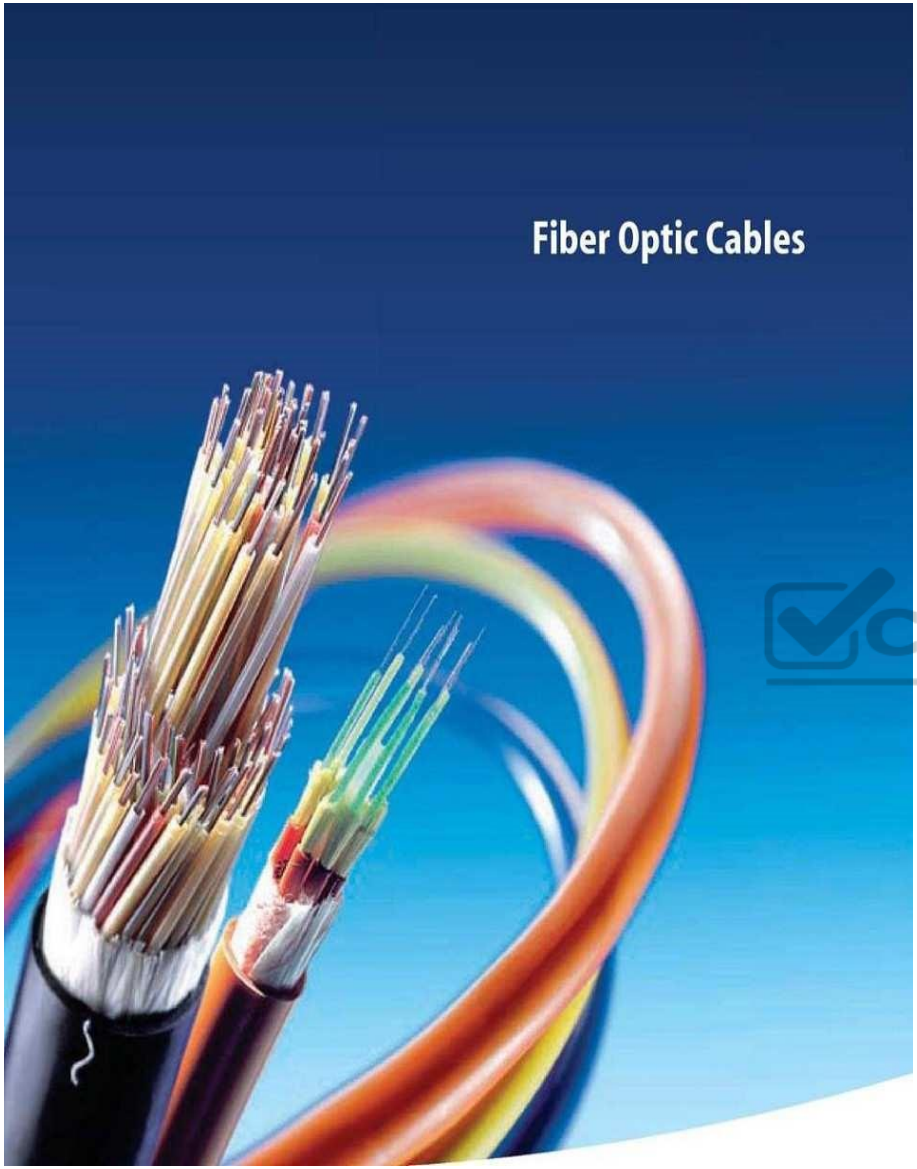
Coaxial cable is expensive and does not support many LAN's. It supports data and video.

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



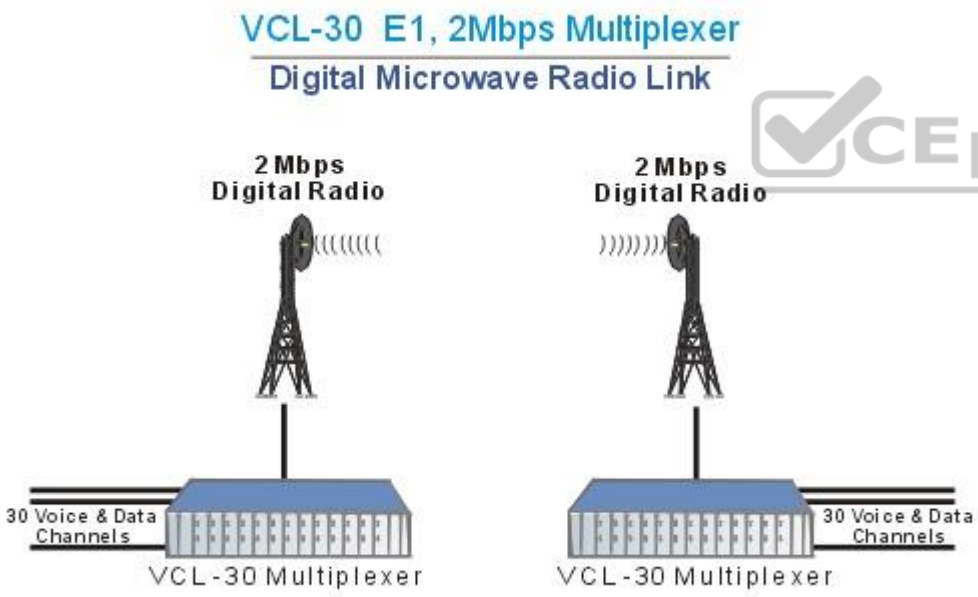
Microwave radio system

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 62
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.

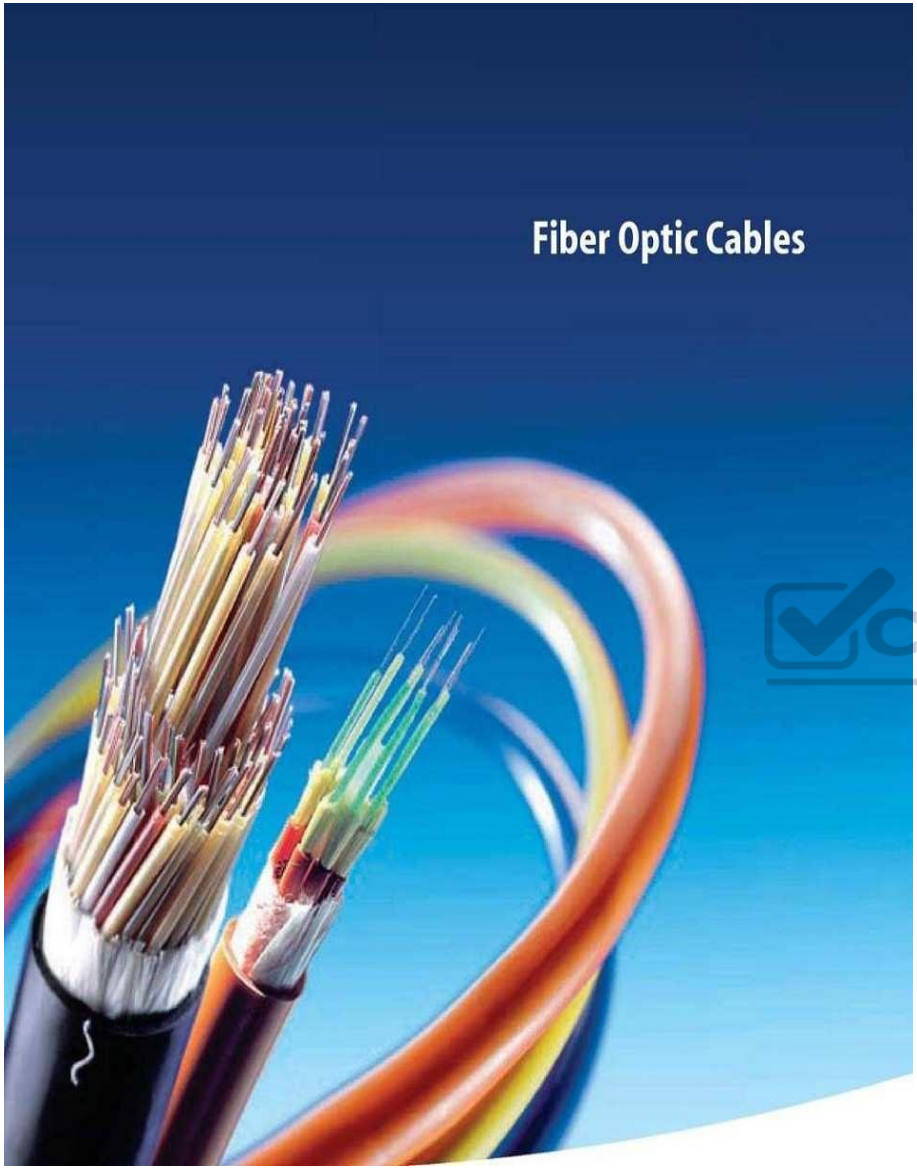
Coaxial Cable

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



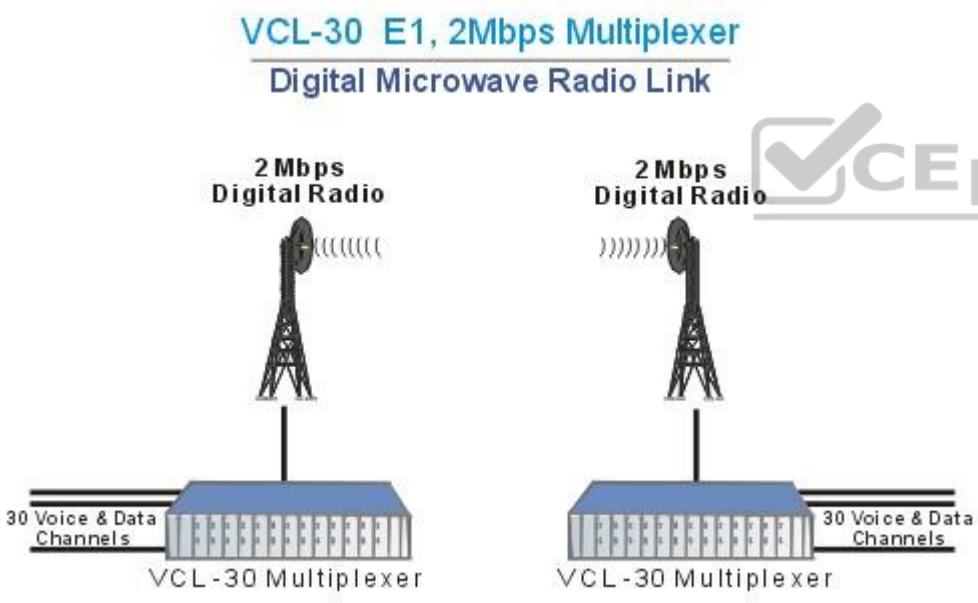
Microwave radio system

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 63
Which of the following is the INCORRECT Layer to Protocol mapping used in the DOD TCP/IP model?

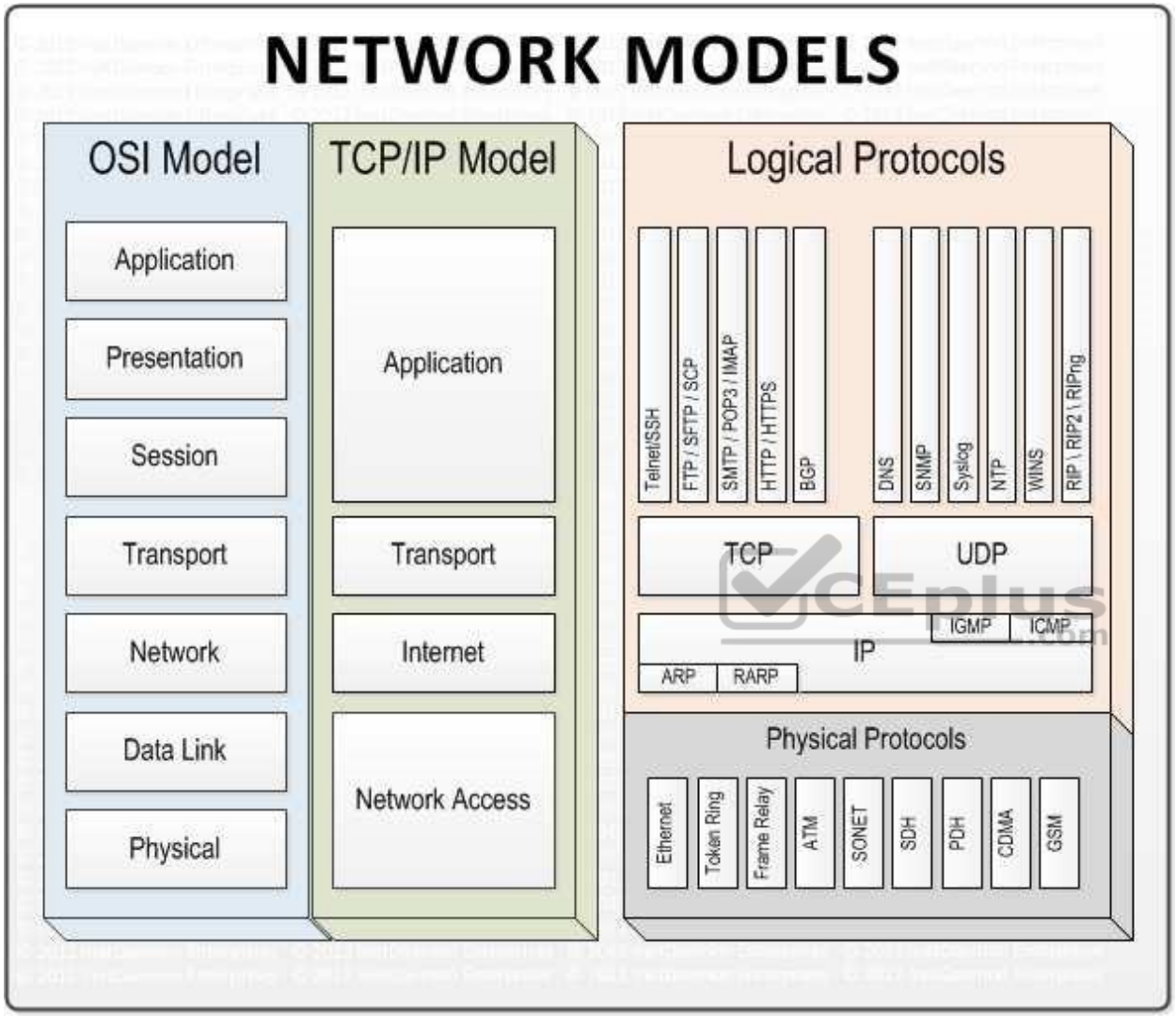
A. Application layer – Telnet
B. Transport layer – ICMP
C. Internet layer – IP
D. Network Access layer – Ethernet

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.

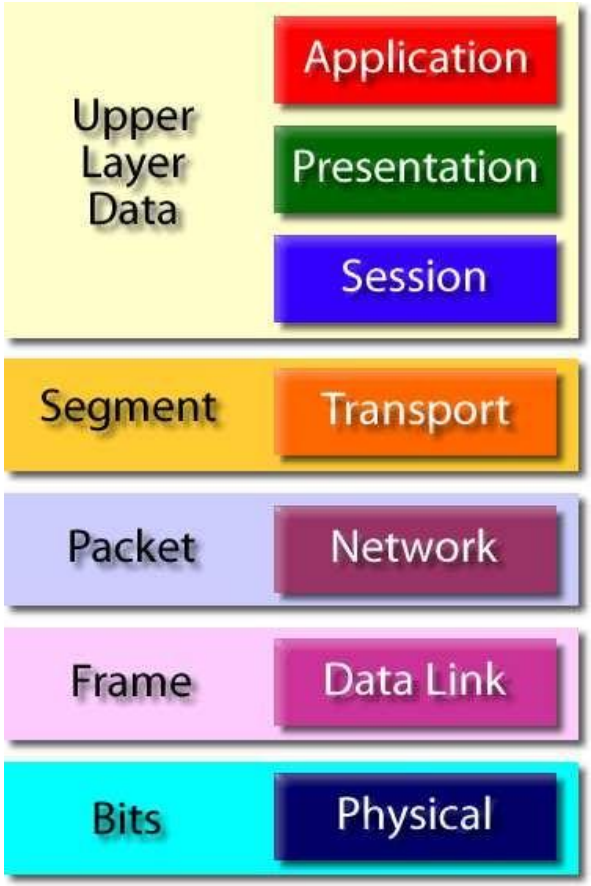
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 describes 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

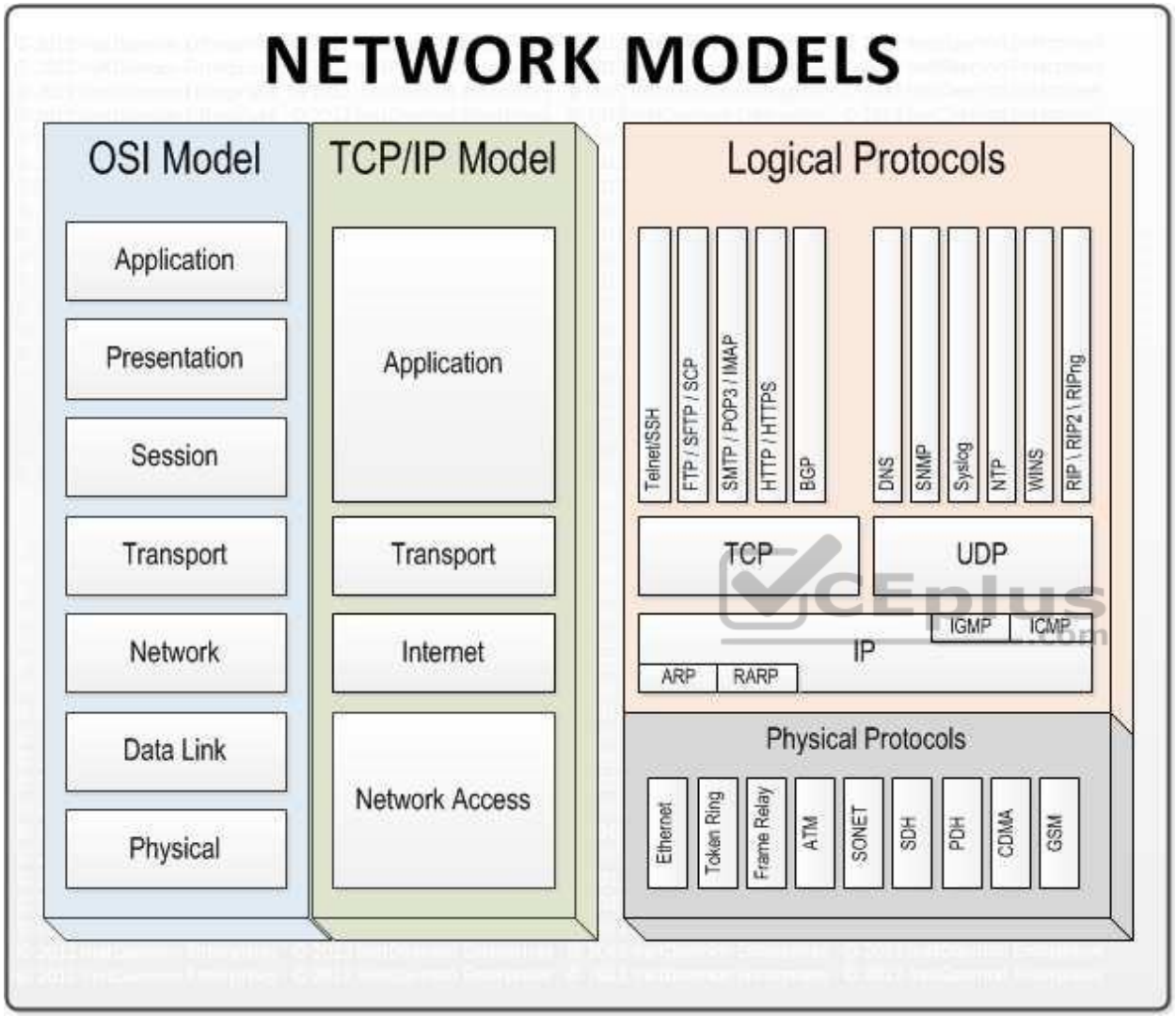
QUESTION 64
Which of the following protocol does NOT work at the Application layer of the TCP/IP Models?
A. HTTP
B. FTP
C. NTP
D. TCP

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

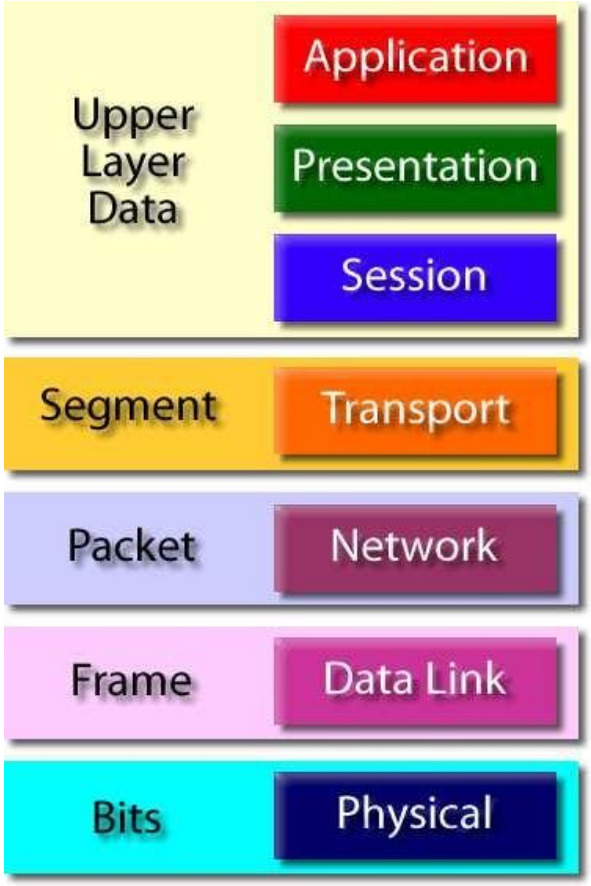
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial 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 65
Which of the following statement INCORRECTLY describes device and where they sit within the TCP/IP model?

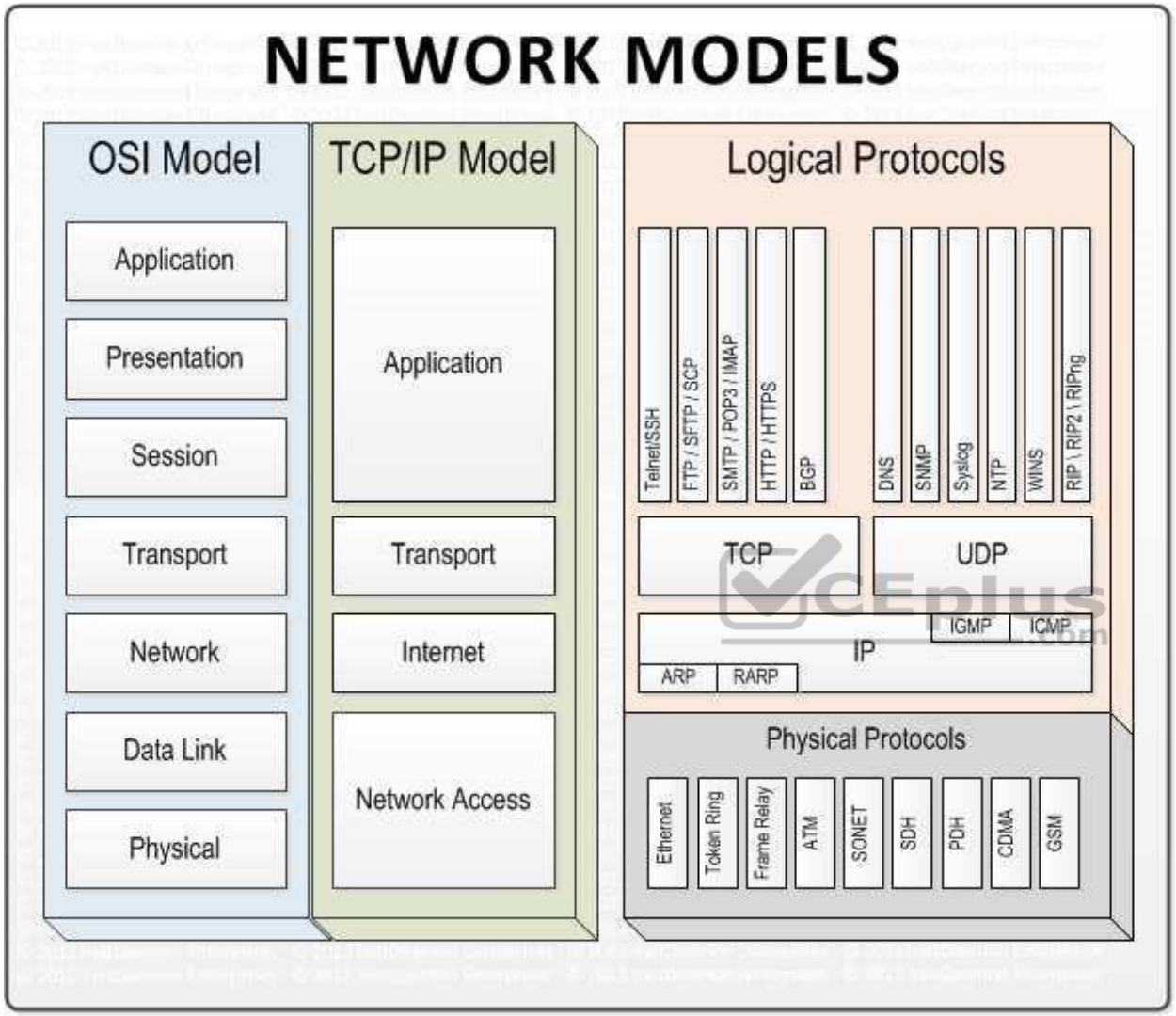
A. Layer 4 switch work at Network interface layer in TCP/IP model
B. Router works at Network interface layer in TCP/IP model
C. Layer 3 switch work at Network interface layer in TCP/IP model
D. Hub works at LAN or WAN interface layer of a TCP/IP model

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).

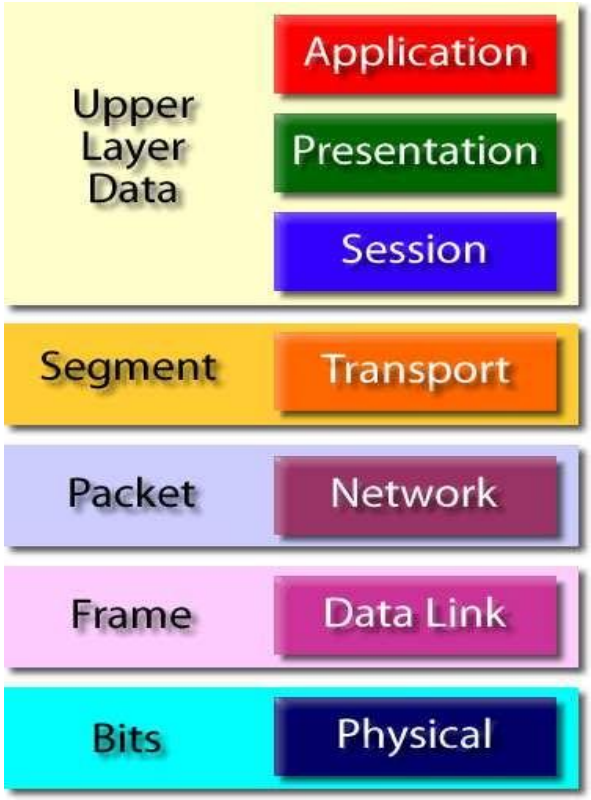
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network 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 describes 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 66
Which of the following protocol does NOT work at Network interface layer in TCP/IP model?
A. ICMP

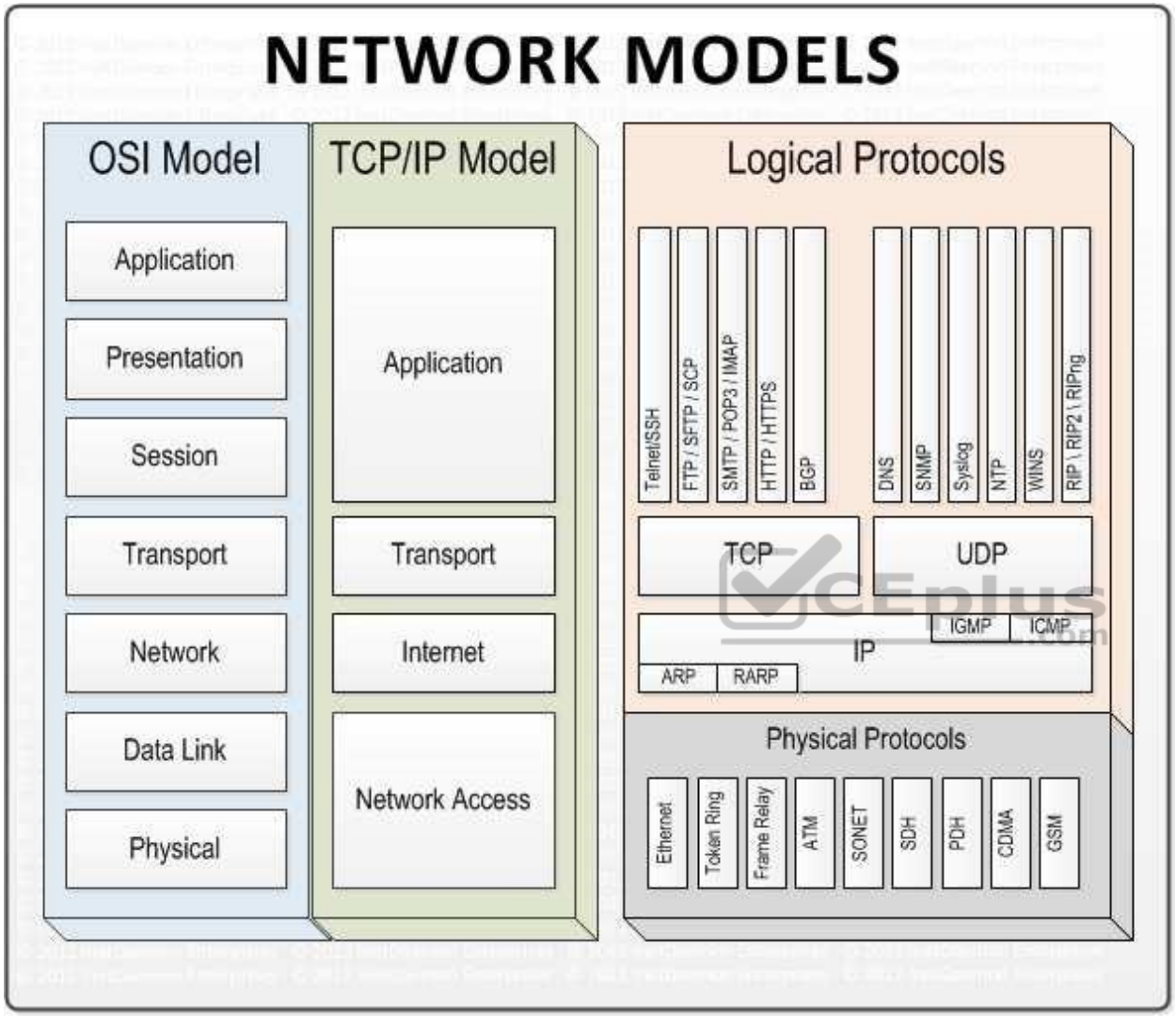
B. DNS
C. ARP
D. Internet protocol

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).

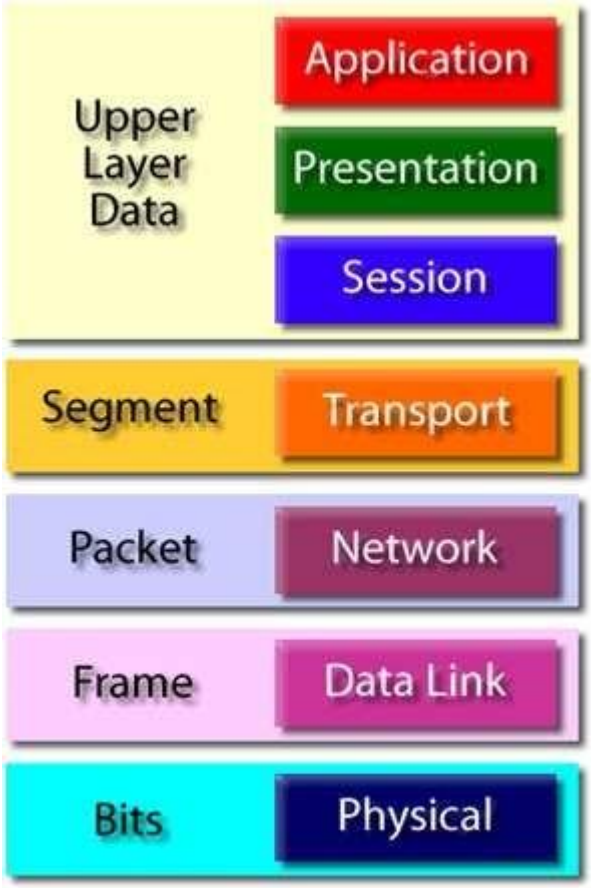
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network 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 67

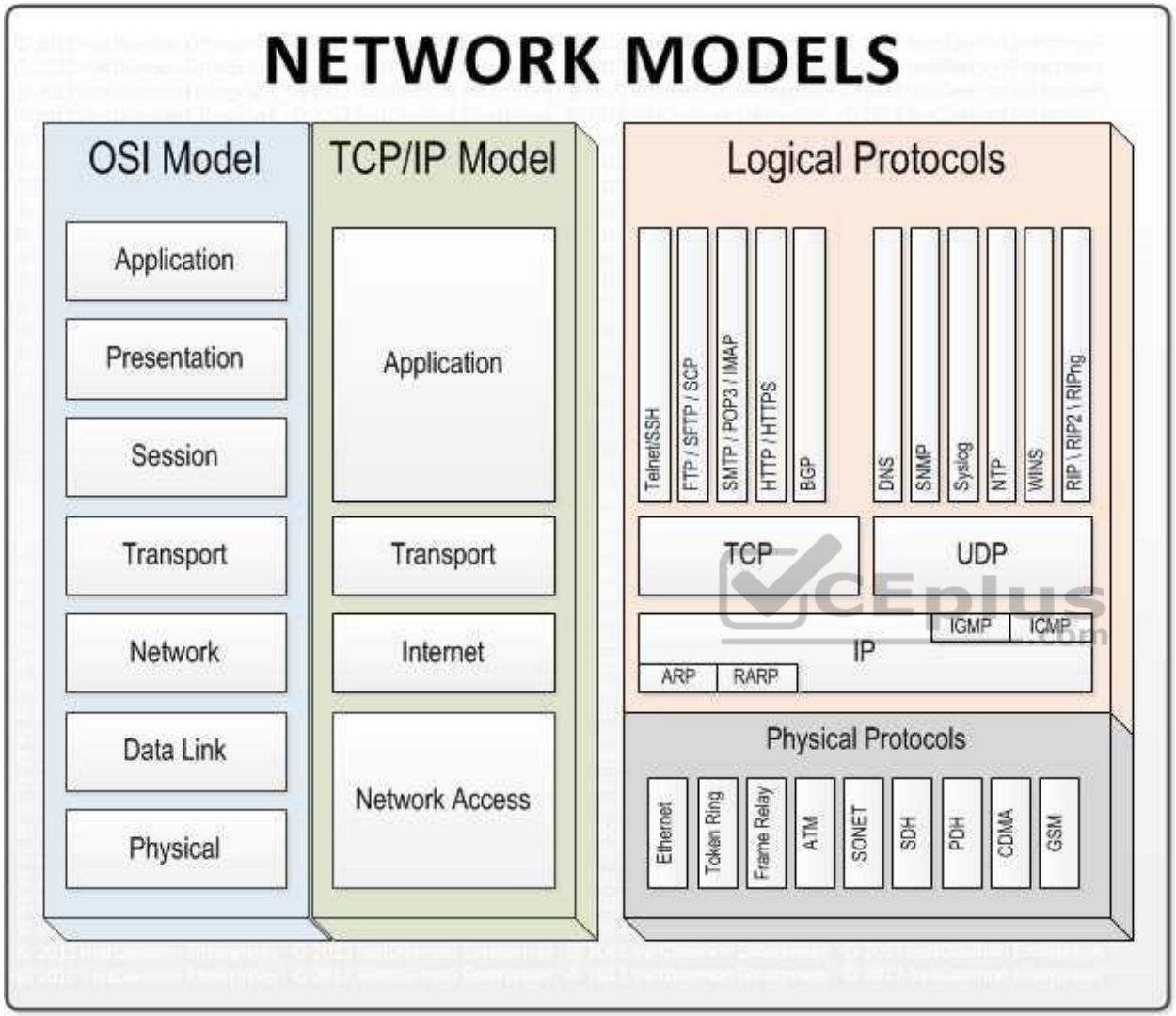
Which of the following is the protocol data unit (PDU) of application layer in TCP/IP model?

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.

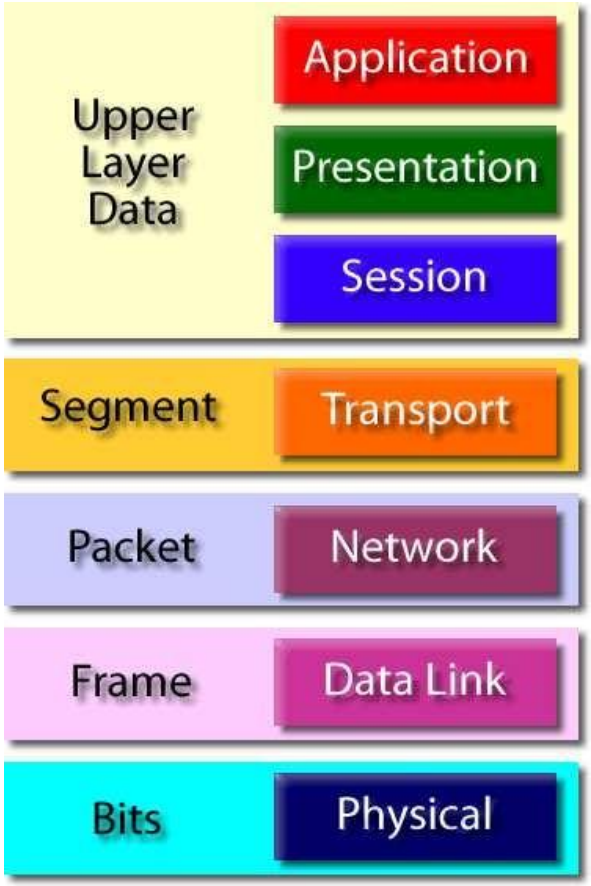
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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

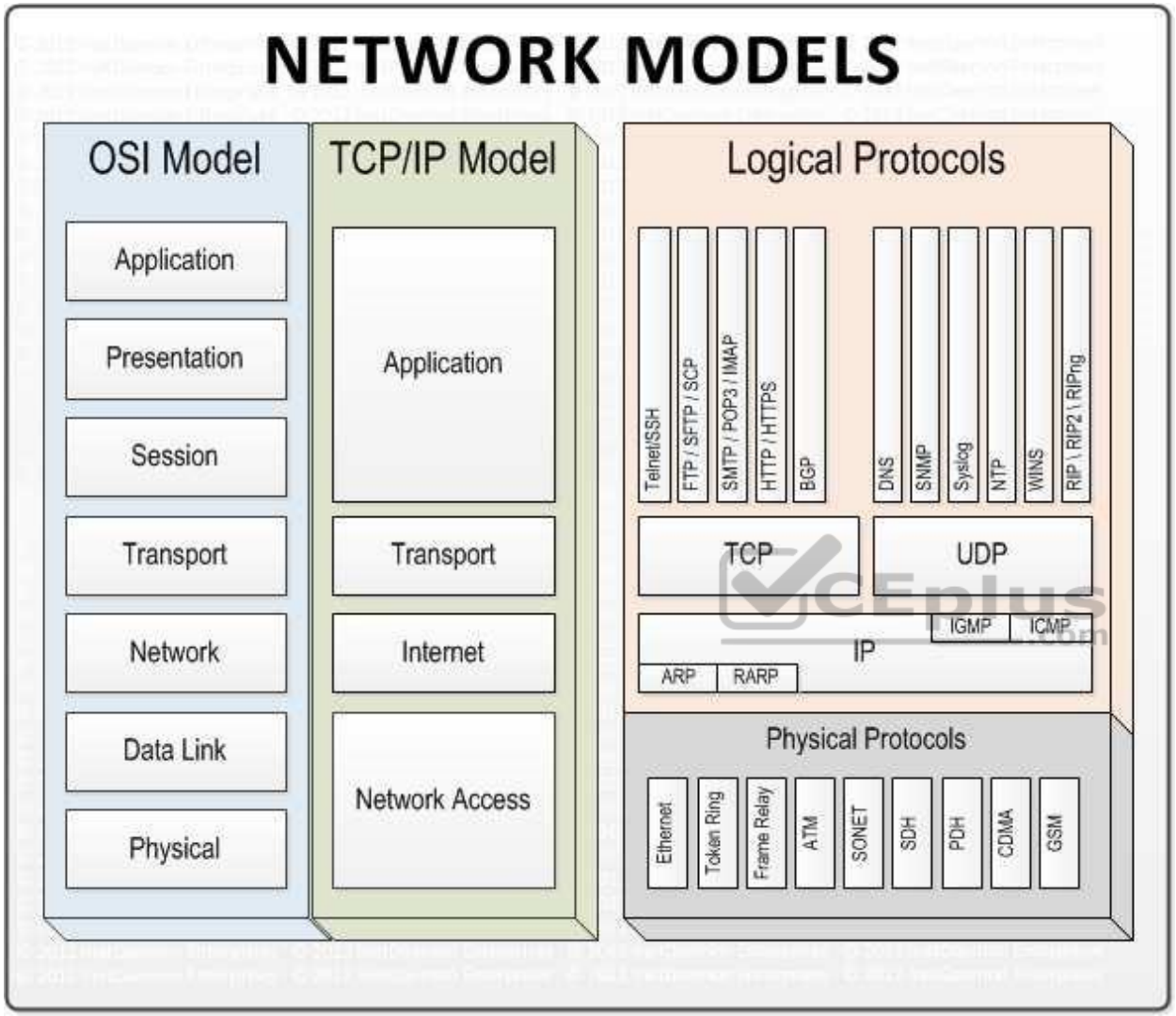
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 272

QUESTION 68
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.

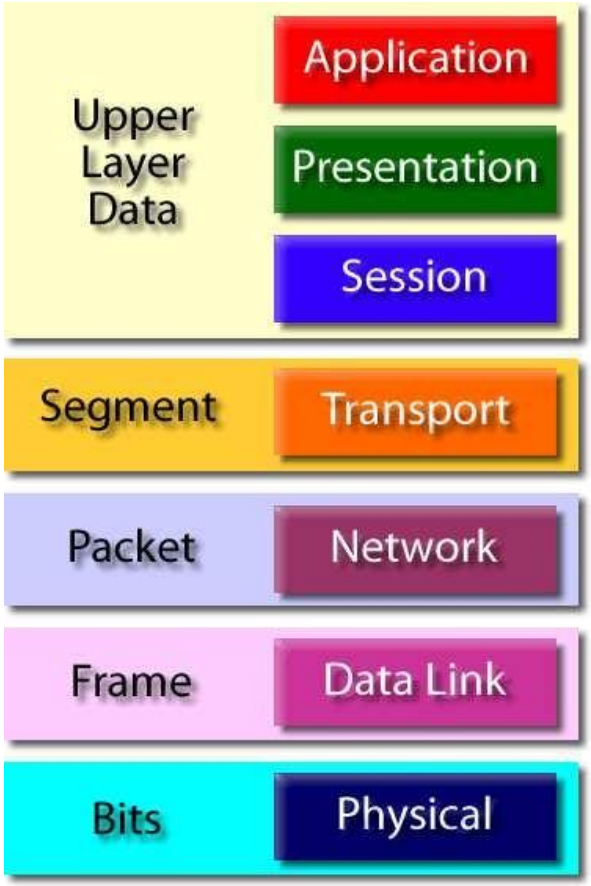
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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

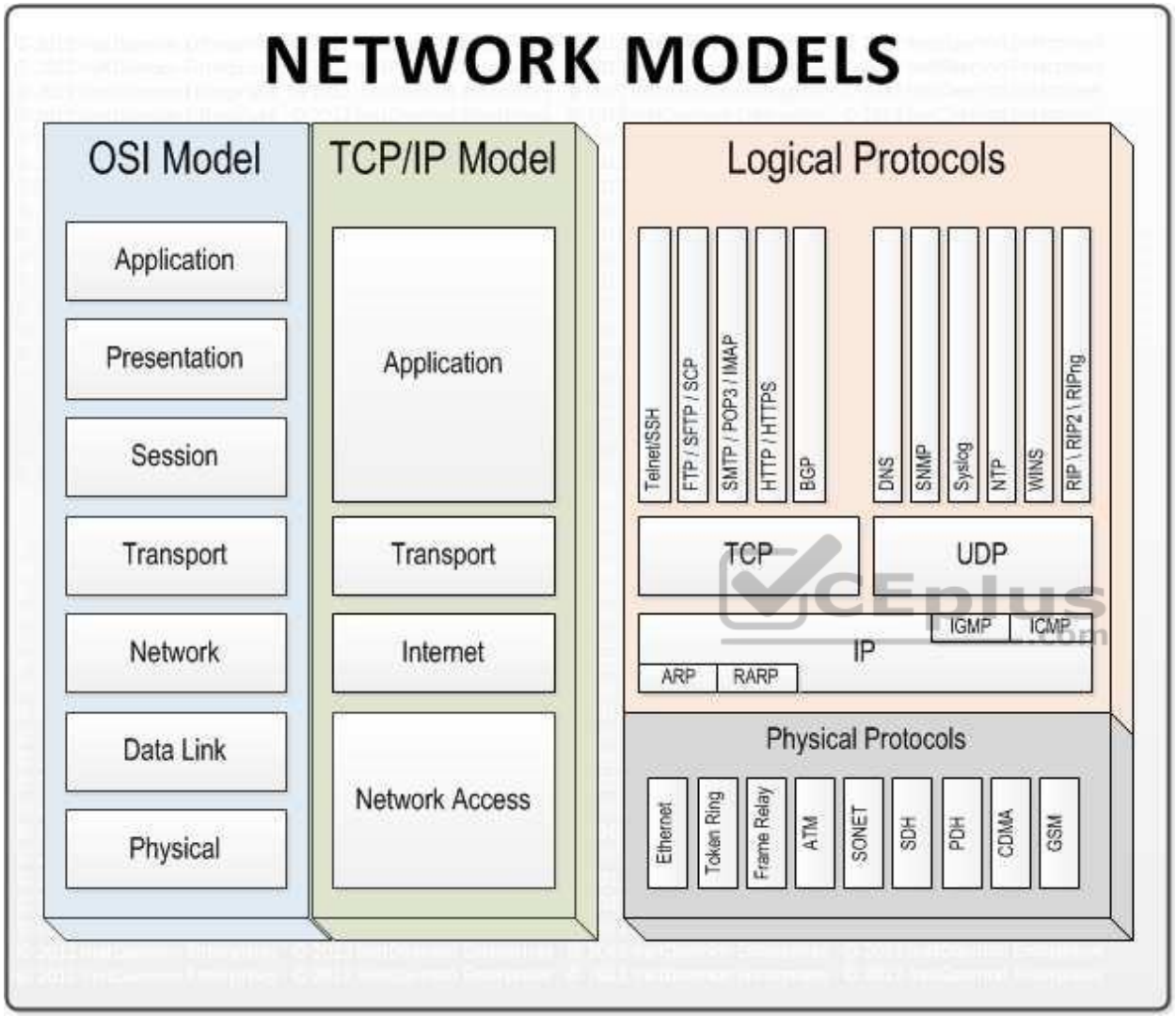
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 272

QUESTION 69
Which of the following is protocol data unit (PDU) of network interface layer in TCP/IP model?

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

Correct Answer: C
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.

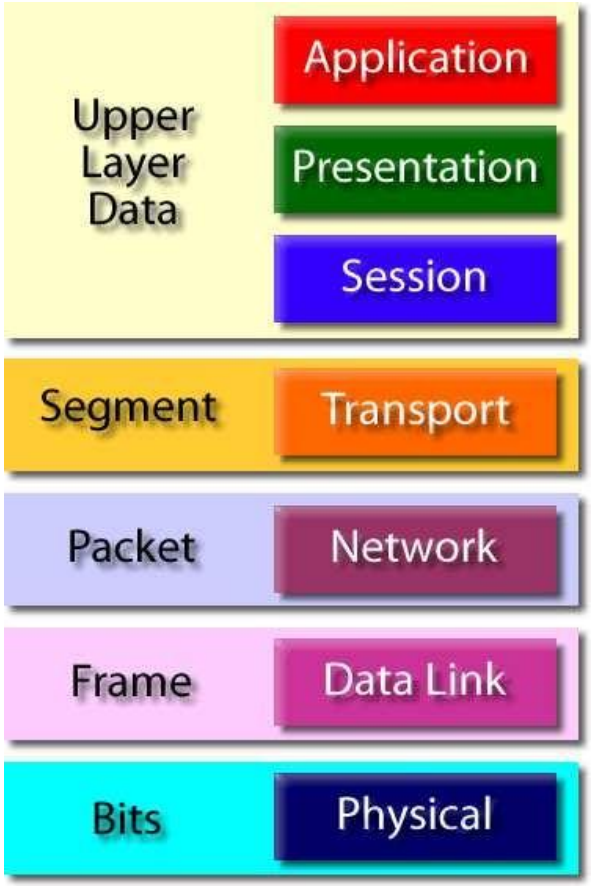
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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:

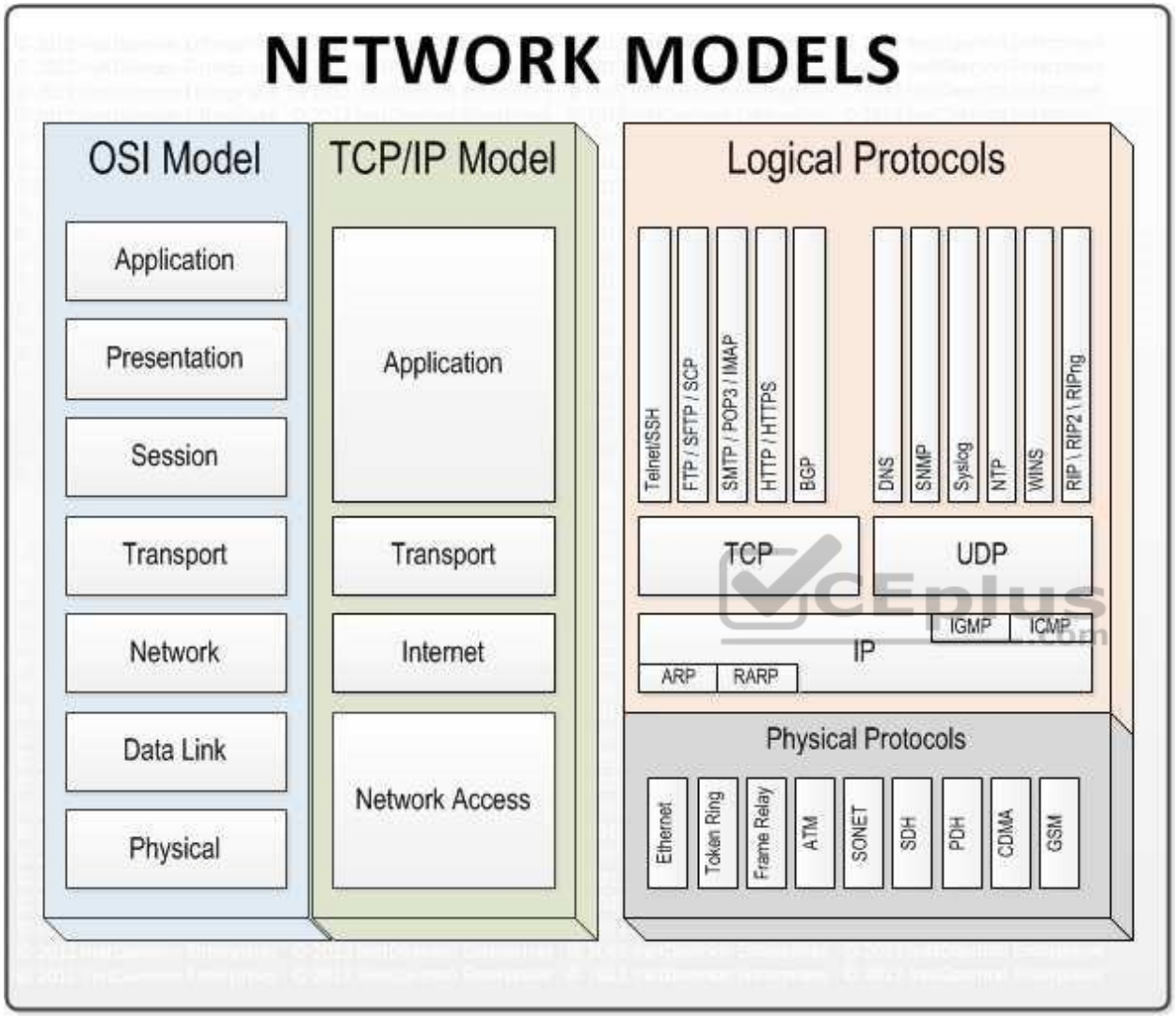
Data – Application layer PDU
Segment – Transport layer PDU
Frame/bit – LAN or WAN interface layer PDU

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

QUESTION 70
Which of the following is protocol data unit (PDU) of data at LAN or WAN interface layer in TCP/IP model?
A. Data
B. Segment
C. Packet
D. Frame and bits

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

Explanation/Reference:
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.

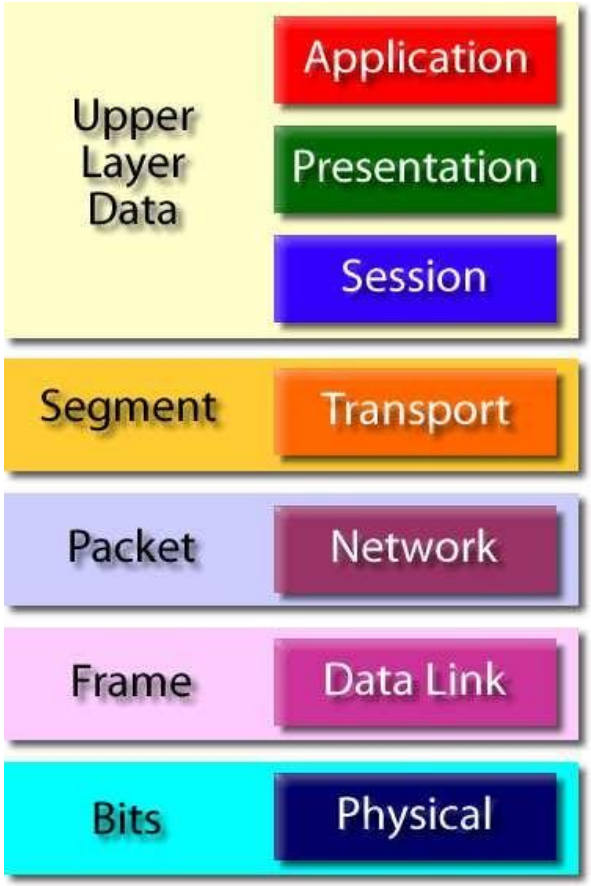
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 data PDU
Segment – Transport layer data PDU
Packet – Network interface layer data PDU

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

QUESTION 71
Which of the following INCORRECTLY describes the layer function of the Application Layer within the TCP/IP model?
A. Provides user interface
B. Perform data processing such as encryption, encoding, etc
C. Provides reliable delivery
D. Keeps separate the data of different applications

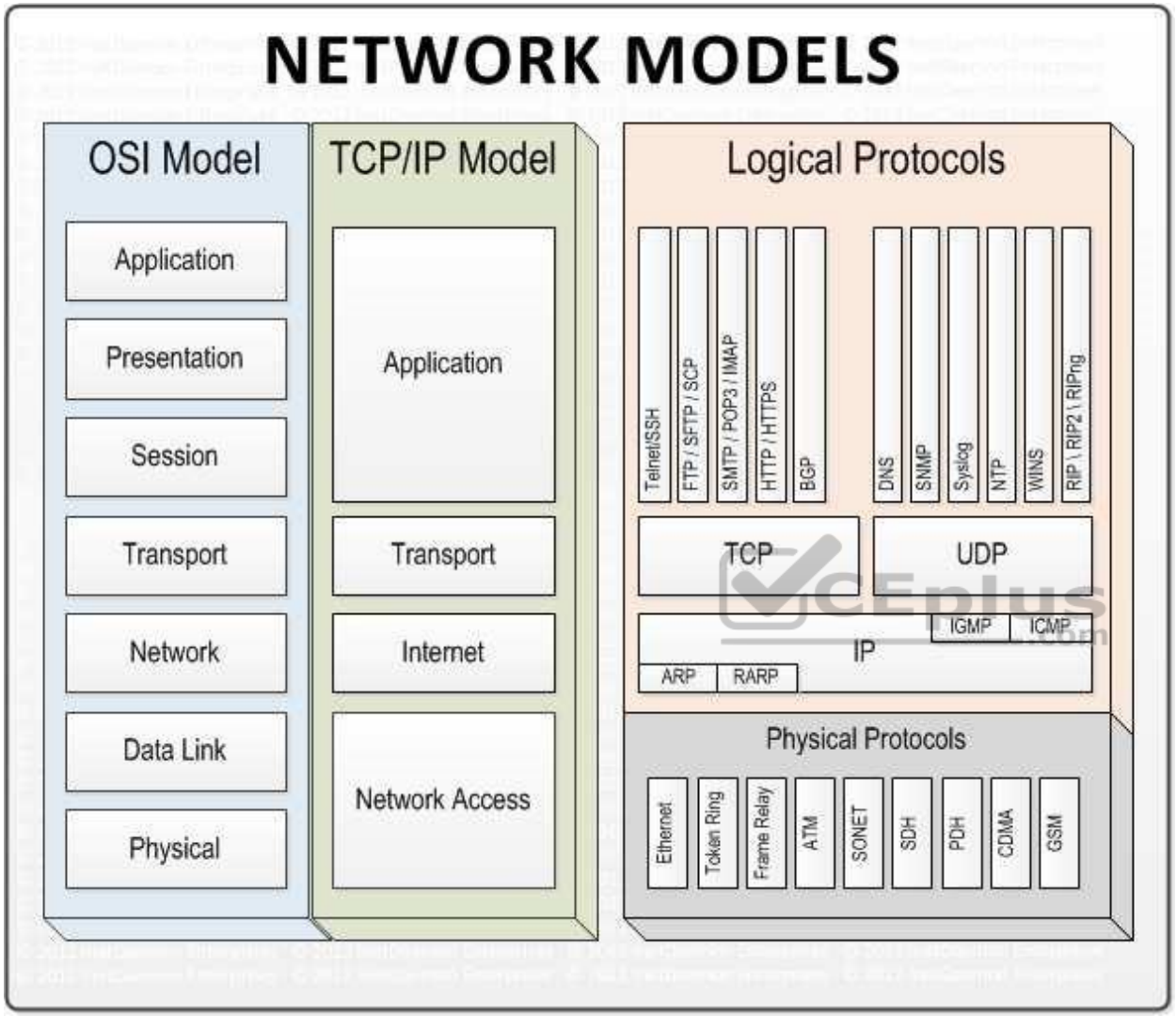
Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
The word INCORRECTLY keyword is used in the question.

You need to find out the service or functionality which is not performed by application layer of a TCP/IP model.

The reliable or unreliable delivery of a message is the functionality of transport 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.

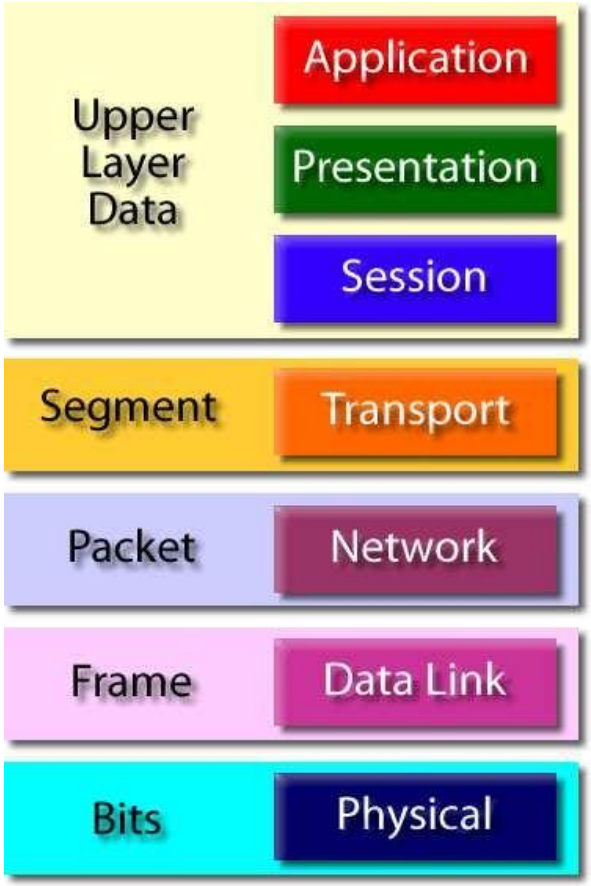
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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:
The other options correctly describe functionalities of 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 72
Which of the following INCORRECTLY describes the layer functions of the LAN or WAN Layer of the TCP/IP model?

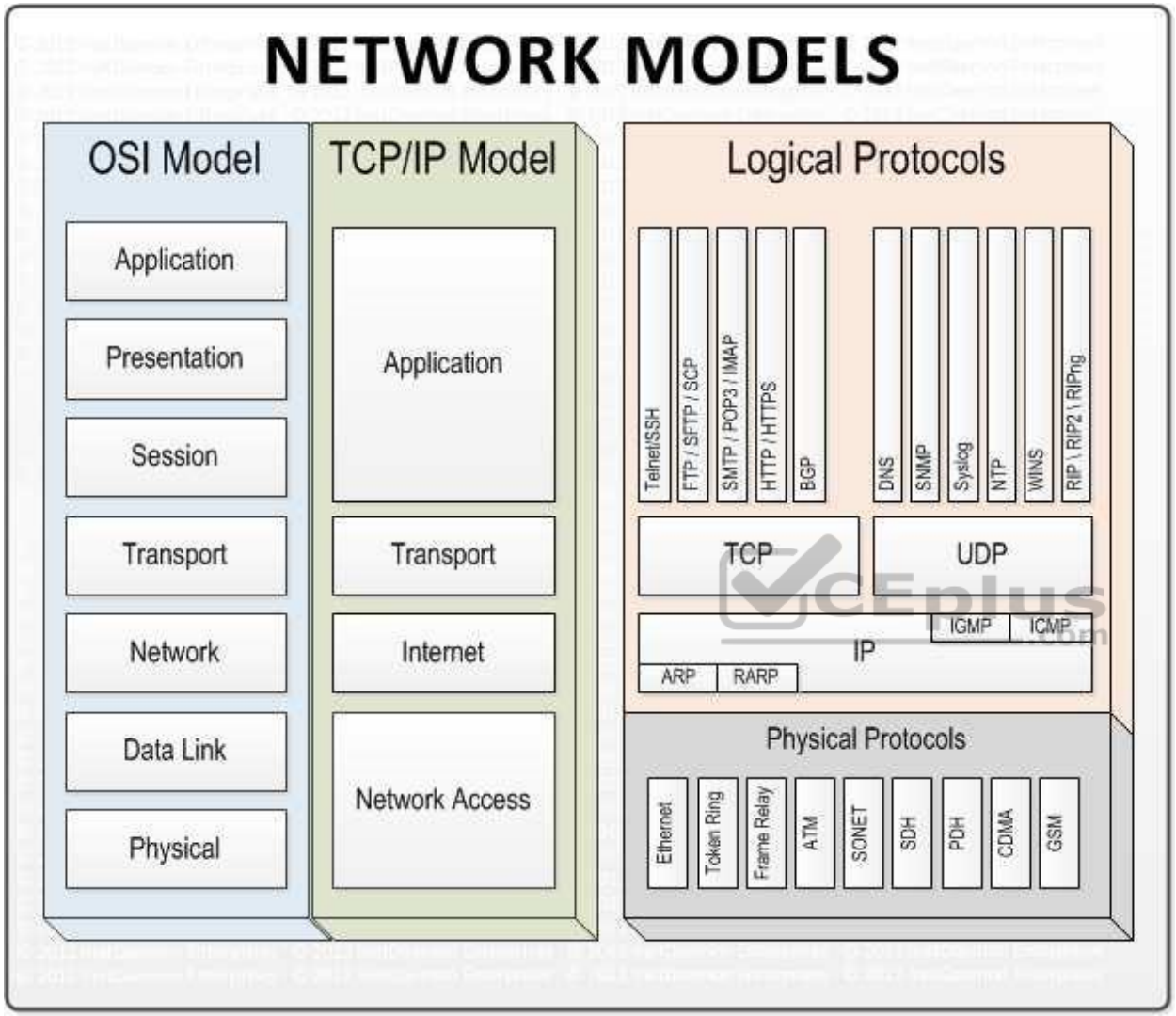
A. Combines packets into bytes and bytes into frame
B. Providers logical addressing which routers use for path determination
C. Provide address to media using MAC address
D. Performs only error detection

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

Explanation/Reference:
The word INCORRECTLY is the keyword used in the question. You need to find out the functionality that is not performed by LAN or WAN layer in TCP/IP model.

The Network layer of a TCP/IP model provides logical addressing which routers use for path determination.

For your exam you should know below information about TCP/IP model:
Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer
Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

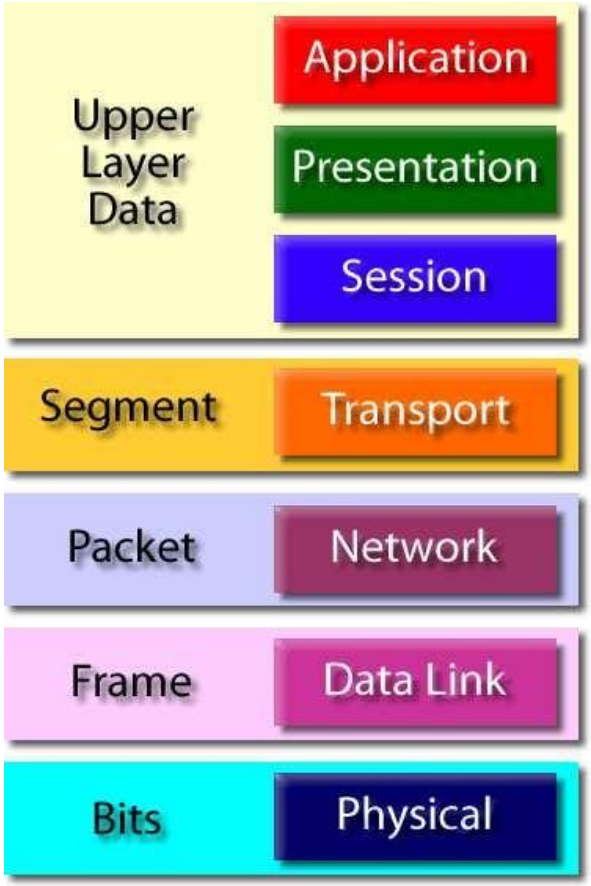
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:
The other options correctly describe functionalities of 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 73
Which of the following functionality is NOT performed by the application layer of a TCP/IP model?

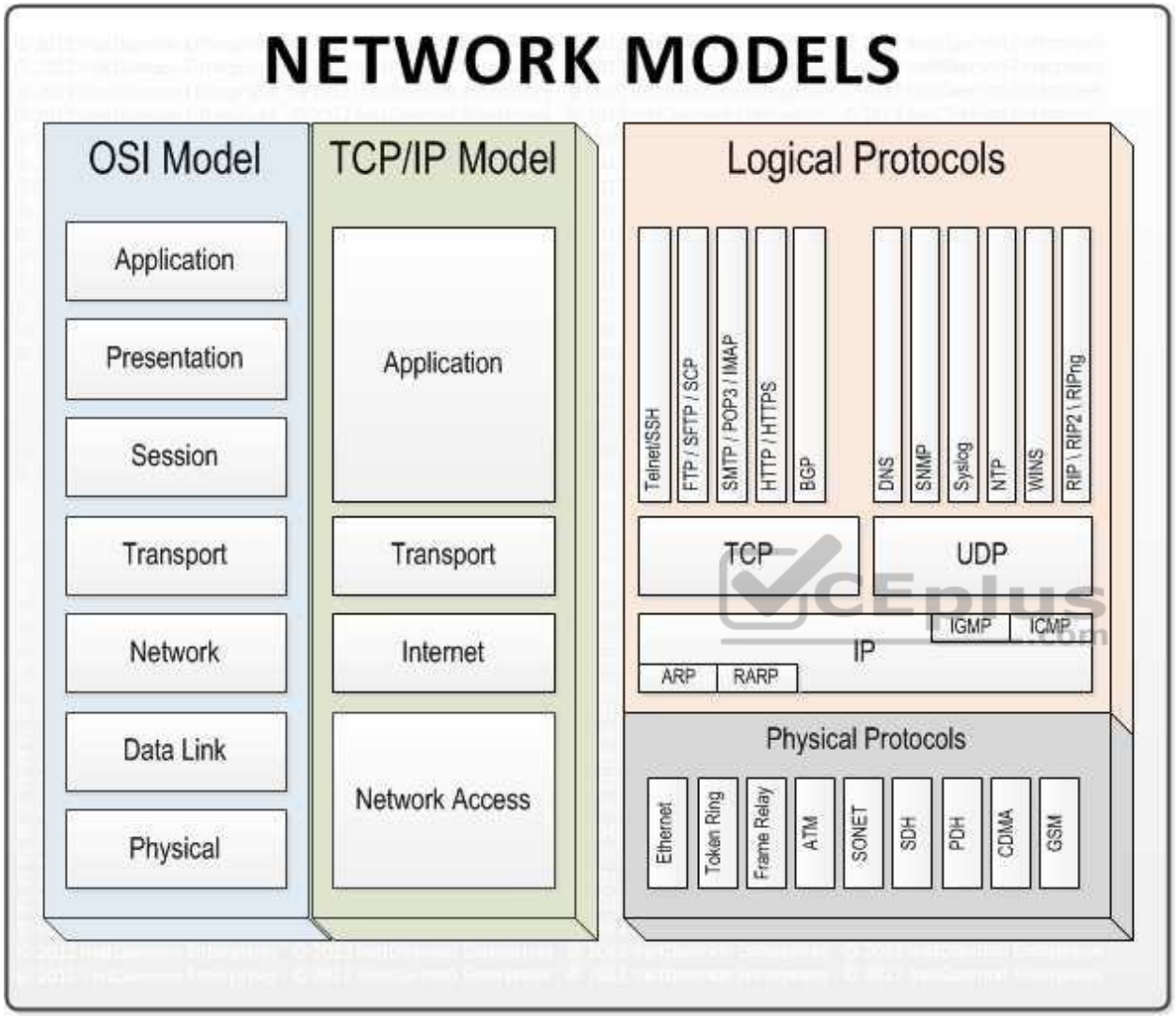
A. Print service, application services
B. Data encryption and compression
C. Dialog management
D. End-to-end connection

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

Explanation/Reference:
The word NOT is the keyword used in the question, You need to find out a functionality which is not performed by application layer of a TCP/IP model.

End-to-end connection is the Transport layer functionality in TCP/IP model.

For your exam you should know below information about TCP/IP model:
Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer
Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

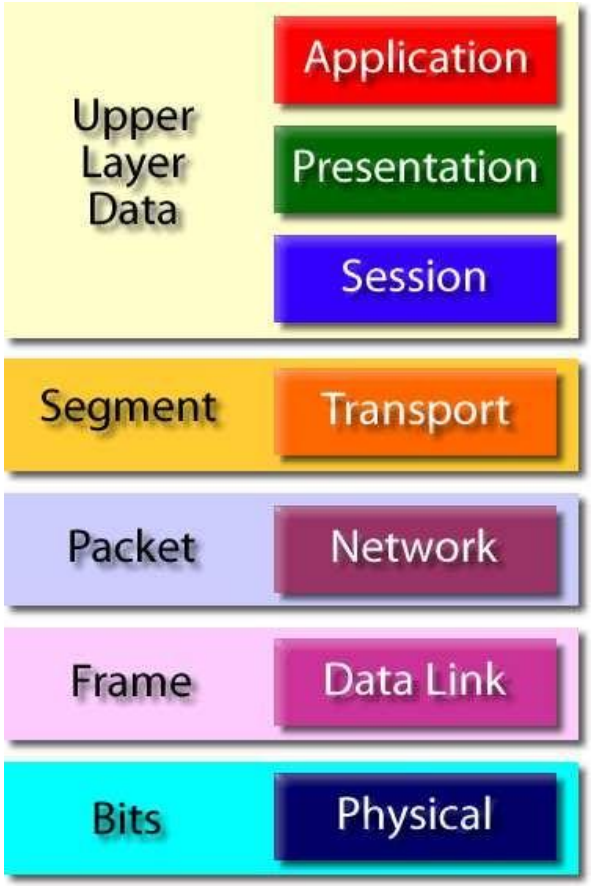
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:
The other functionalities described in the options are performed by application layer in TCP/IP model.

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

QUESTION 74
Which of the following is the INCORRECT “layer - protocol" mapping within the TCP/IP model?

A. Application layer – NFS
B. Transport layer – TCP
C. Network layer – UDP
D. LAN or WAN interface layer – point-to-point protocol

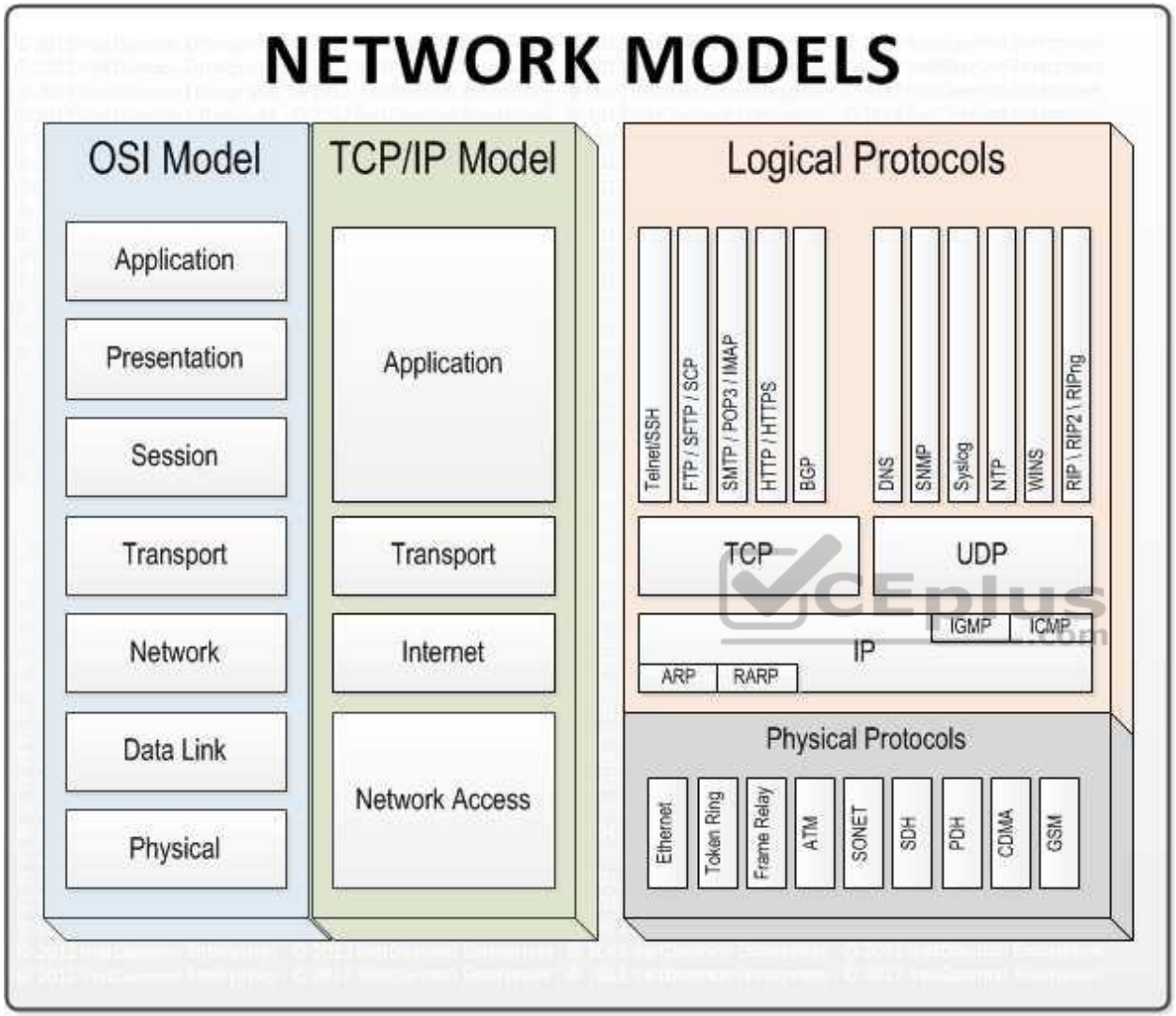
Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
The word INCORRECT is the keyword used in the question.

You need to find out invalid layer-protocol mapping.

The UDP protocol works at Transport 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.

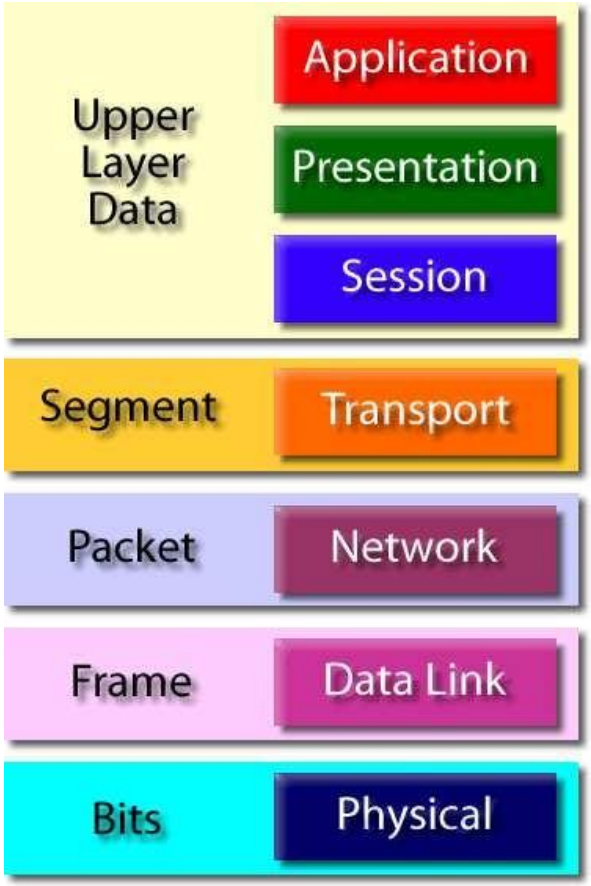
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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:
The other options correctly describe layer-protocol mapping in TCP/IP protocol.

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

QUESTION 75
Which of the following is the INCORRECT “layer - protocol data unit (PDU)" mapping within the TCP/IP model?

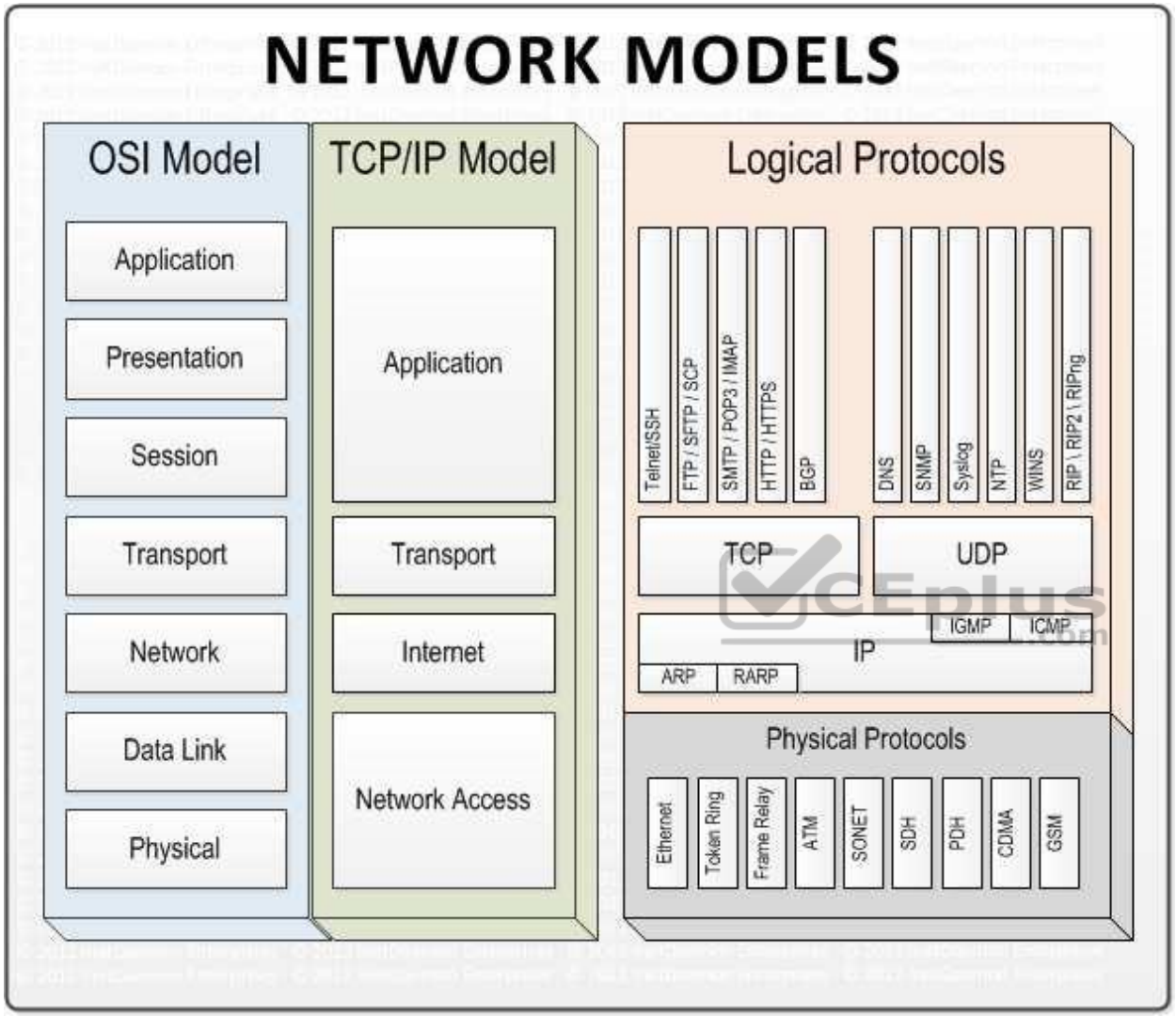
A. Application layer – Data
B. Transport layer – Segment
C. Network layer – Frame
D. Physical layer – bits

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

Explanation/Reference:
The word INCORRECT is the keyword used in the question. You need to find out incorrect layer-protocol mapping from give options.

The correct mapping is Network layer – Packet.
The LAN or WAN interface layer creates frame.

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.

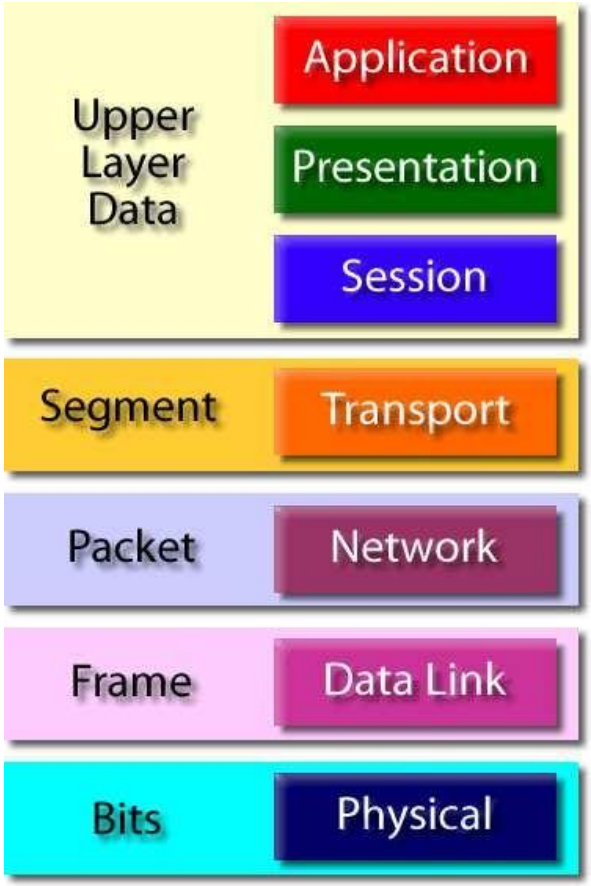
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 layer-PDU mapping in TCP/IP protocol.

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

QUESTION 76
Which of the following protocol is used for electronic mail service?

A. DNS
B. FTP
C. SSH
D. SMTP

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

Explanation/Reference:
SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

For your exam you should know below information general Internet terminology:

Network access point -Internet service providers access internet using net access point. A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.
File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

The following answers are incorrect:

DNS - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/ server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 273 and 274

QUESTION 77
Which of the following service is a distributed database that translate host name to IP address to IP address to host name?

A. DNS
B. FTP

C. SSH
D. SMTP

Correct Answer: A
Section: Information System Operations, Maintenance and Support
Explanation
Explanation/Reference:
The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Network access point -Internet service providers access internet using net access point. A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

The following answers are incorrect:
SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/ server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 273 and 274

QUESTION 78
Which of the following term related to network performance refers to the maximum rate that information can be transferred over a network?

A. Bandwidth
B. Throughput
C. Latency
D. Jitter

Correct Answer: A

Section: Information System Operations, Maintenance and Support
Explanation

Explanation/Reference:
In computer networks, bandwidth is often used as a synonym for data transfer rate - it is the amount of data that can be carried from one point to another in a given time period (usually a second).

This kind of bandwidth is usually expressed in bits (of data) per second (bps). Occasionally, it's expressed as bytes per second (Bps). A modem that works at 57,600 bps has twice the bandwidth of a modem that works at 28,800 bps. In general, a link with a high bandwidth is one that may be able to carry enough information to sustain the succession of images in a video presentation.
It should be remembered that a real communications path usually consists of a succession of links, each with its own bandwidth. If one of these is much slower than the rest, it is said to be a bandwidth bottleneck.

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 275

QUESTION 79
Which of the following term related to network performance refers to the actual rate that information is transferred over a network?
A. Bandwidth
B. Throughput
C. Latency
D. Jitter

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

Explanation/Reference:
Throughput the actual rate that information is transferred. In data transmission, throughput is the amount of data moved successfully from one place to another in a given time period.

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:
Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 275

QUESTION 80
Which of the following term related to network performance refers to the delay that packet may experience on their way to reach the destination from the source?

A. Bandwidth
B. Throughput
C. Latency
D. Jitter

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

Explanation/Reference:

Latency the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses.

In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. In some usages (for example, AT&T), latency is measured by sending a packet that is returned to the sender and the round-trip time is considered the latency.

The latency assumption seems to be that data should be transmitted instantly between one point and another (that is, with no delay at all). The contributors to network latency include:

Propagation: This is simply the time it takes for a packet to travel between one place and another at the speed of light.
Transmission: The medium itself (whether optical fiber, wireless, or some other) introduces some delay. The size of the packet introduces delay in a round trip since a larger packet will take longer to receive and return than a short one.
Router and other processing: Each gateway node takes time to examine and possibly change the header in a packet (for example, changing the hop count in the time-to-live field).
Other computer and storage delays: Within networks at each end of the journey, a packet may be subject to storage and hard disk access delays at intermediate devices such as switches and bridges. (In backbone statistics, however, this kind of latency is probably not considered.)

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred Jitter -
Jitter is the variation in the time of arrival at the receiver of the information

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 275

QUESTION 81
Which of the following term related to network performance refers to the variation in the time of arrival of packets on the receiver of the information?

A. Bandwidth
B. Throughput
C. Latency
D. Jitter

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

Explanation/Reference:
Simply said, the time difference in packet inter-arrival time to their destination can be called jitter. Jitter is specific issue that normally exists in packet switched networks and this phenomenon is usually not causing any communication problems.TCP/IP is responsible for dealing with the jitter impact on communication.

On the other hand, in VoIP network environment, or better say in any bigger environment today where we use IP phones on our network this can be a bigger problem. When someone is sending VoIP communication at a normal interval (let's say one frame every 10 ms) those packets can stuck somewhere in between inside the packet network and not arrive at expected regular peace to the destined station. That's the whole jitter phenomenon all about so we can say that the anomaly in tempo with which packet is expected and when it is in reality received is jitter.
jitter

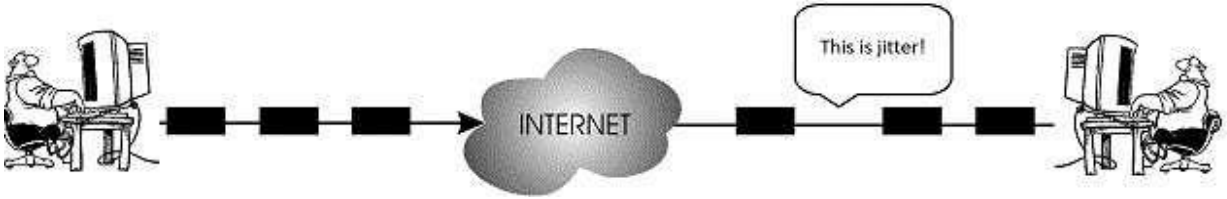


Image from: http://howdoesinternetwork.com/wp-content/uploads/2013/05/jitter.gif

In this image above, you can notice that the time it takes for packets to be send is not the same as the period in which the will arrive on the receiver side. One of the packets encounters some delay on his way and it is received little later than it was asumed. Here are the jitter buffers entering the story. They will mitigate packet delay if required. VoIP packets in networks have very changeable packet inter-arrival intervals because they are usually smaller than normal data packets and are therefore more numerous with bigger chance to get some delay along the way.

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

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

CISA review manual 2014 page number 275
and
http://howdoesinternetwork.com/2013/jitter

QUESTION 82
Which of the following term related to network performance refers to the number of corrupted bits expressed as a percentage or fraction of the total sent?

A. Bandwidth
B. Throughput
C. Latency
D. Error Rate

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

Explanation/Reference:
Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sent

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 275

QUESTION 83
Identify the INCORRECT statement related to network performance below?
A. Bandwidth - Bandwidth commonly measured in bits/second is the maximum rate that information can be transferred
B. Latency - Latency the actual rate that information is transferred
C. Jitter - Jitter variation in the time of arrival at the receiver of the information
D. Error Rate - Error rate the number of corrupted bits expressed as a percentage or fraction of the total sent

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

Explanation/Reference:
The word INCORRECT is the keyword used within the question. You need to find out a statement which is incorrectly describe about network performance. Throughput the actual rate that information is transferred and Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred
Throughput - Throughput is the actual rate that information is transferred
Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
Jitter - Jitter is the variation in the time of arrival at the receiver of the information
Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sent

The following answers are incorrect:
The other options correctly describe network performance parameters.

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

CISA review manual 2014 page number 275

QUESTION 84
Which of the following term in business continuity determines the maximum acceptable amount of data loss measured in time?

A. RPO
B. RTO
C. WRT
D. MTD

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

Explanation/Reference:
A recovery point objective, or “RPO”, is defined by business continuity planning. It is the maximum tolerable period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit to work to. For instance, if the RPO is set to four hours, then in practice, off-site mirrored backups must be continuously maintained – a daily off-site backup on tape will not suffice. Care must be taken to avoid two common mistakes around the use and definition of RPO. Firstly, BC staff use business impact analysis to determine RPO for each service – RPO is not determined by the existent backup regime. Secondly, when any level of preparation of off-site data is required, rather than at the time the backups are offsite, the period during which data is lost very often starts near the time of the beginning of the work to prepare backups which are eventually offsite.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual
Business as usual

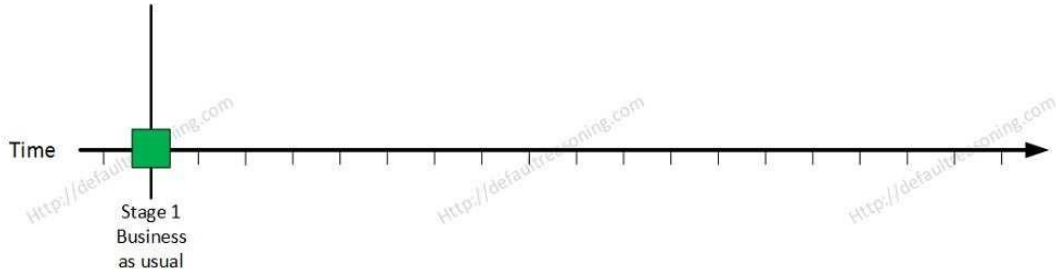


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png

At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs

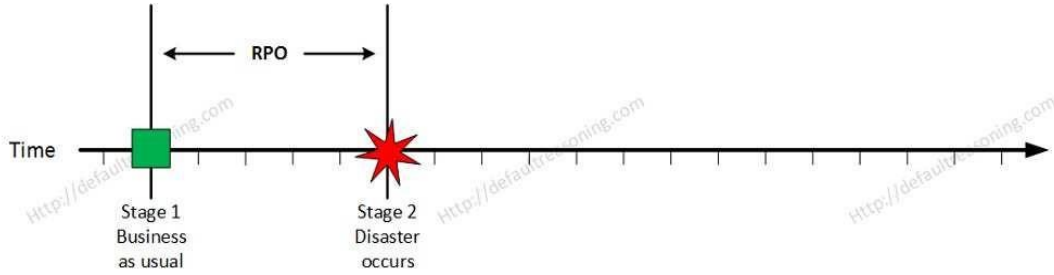


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery
Recovery

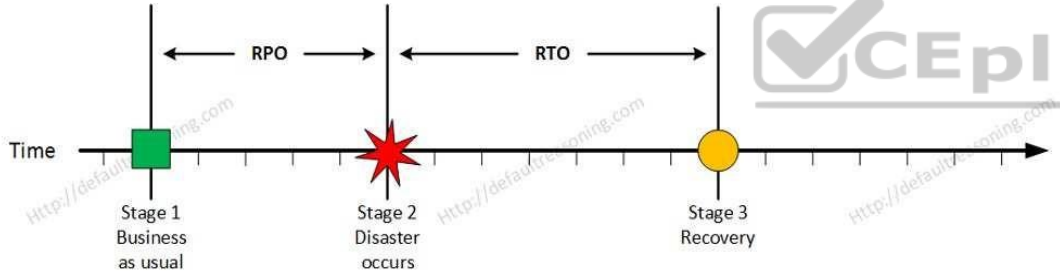


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.
Stage 4: Resume Production
Resume Production

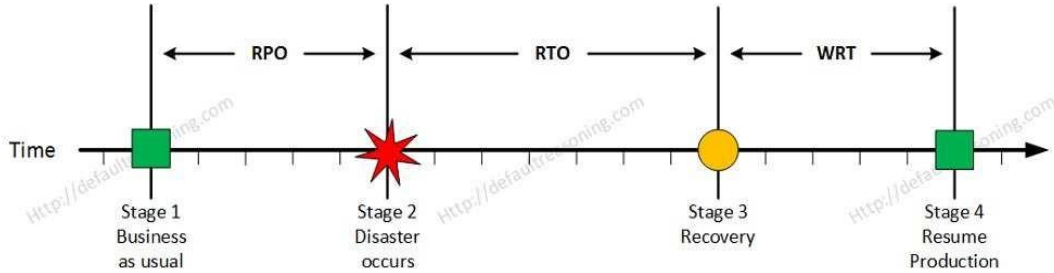


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.
MTD

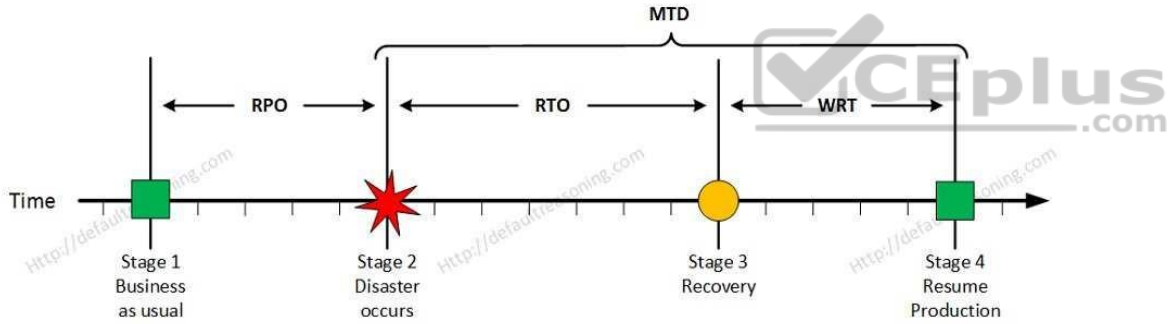


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png

The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

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

CISA review manual 2014 page number 284
http://en.wikipedia.org/wiki/Recovery_point_objective
http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

QUESTION 85
Which of the following term in business continuity determines the maximum tolerable amount of time needed to bring all critical systems back online after disaster occurs?

A. RPO
B. RTO
C. WRT
D. MTD

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

Explanation/Reference:
The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

It can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users. Decision time for users representative is not included.

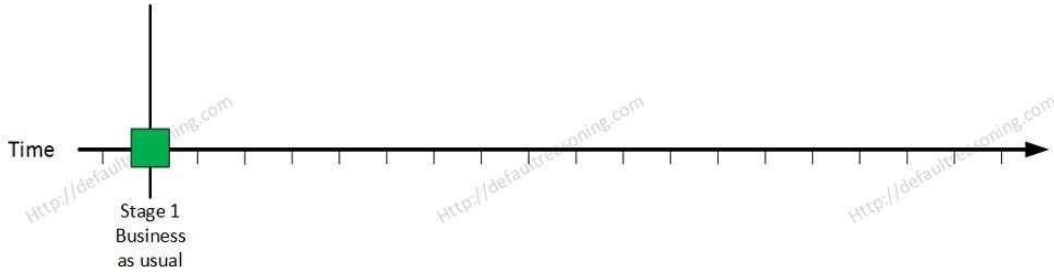
The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points.

In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance.

The RTO attaches to the business process and not the resources required to support the process.
The RTO and the results of the BIA in its entirety provide the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs.

For your exam you should know below information about RPO, RTO, WRT and MTD :

Stage 1: Business as usual



Business as usual
Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png

At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs

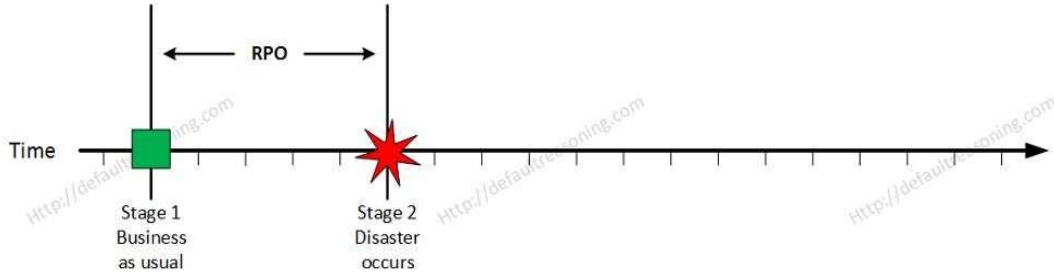


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery
Recovery

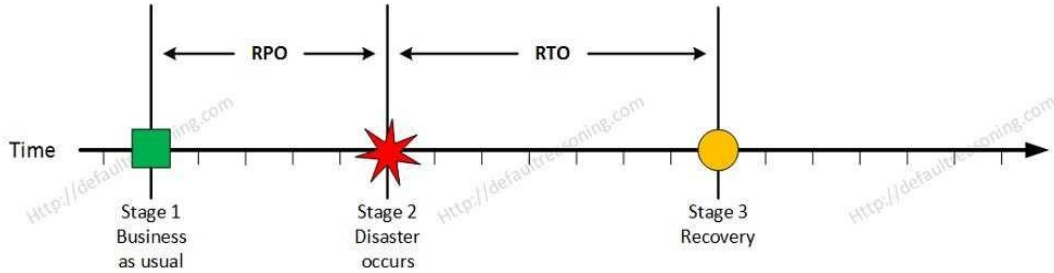


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.
Stage 4: Resume Production
Resume Production

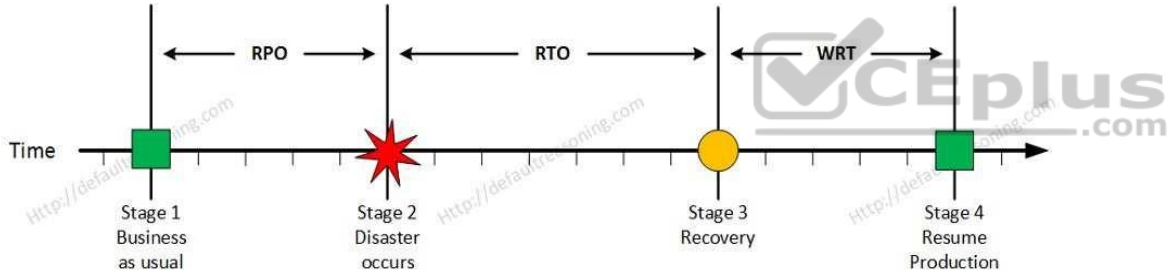


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.
MTD

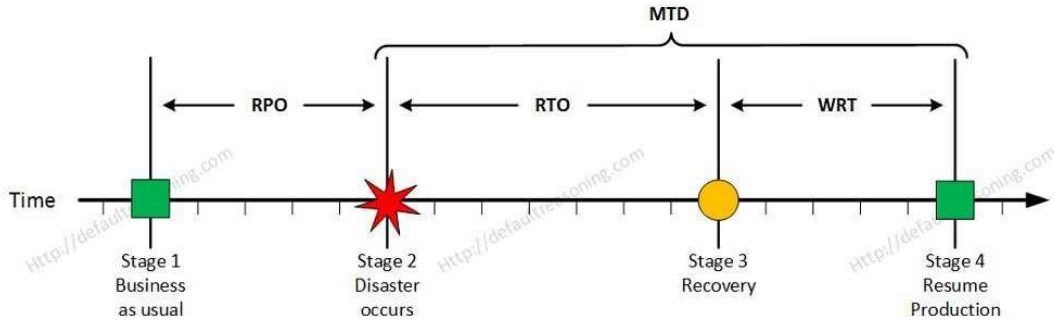


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

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

CISA review manual 2014 page number 284
http://en.wikipedia.org/wiki/Recovery_time_objective
http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

QUESTION 86
Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?

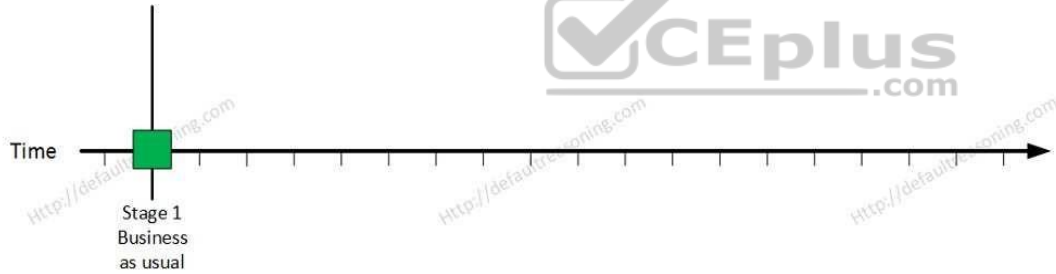
A. RPO
B. RTO
C. WRT
D. MTD

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

Explanation/Reference:
The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual



Business as usual
Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png

At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs

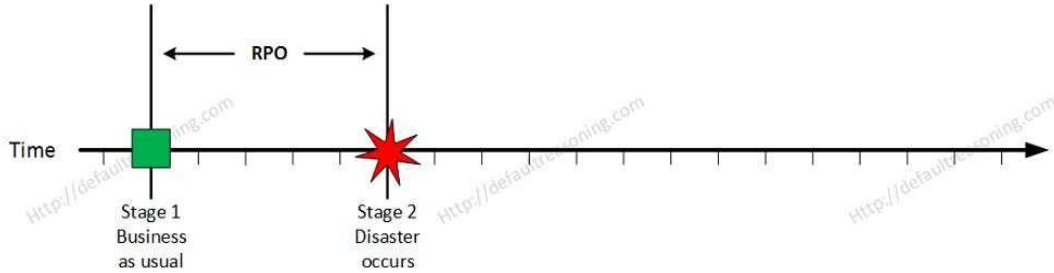


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery
Recovery

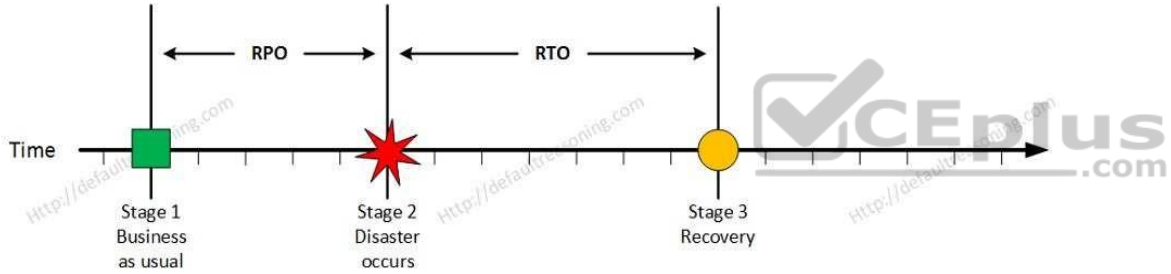


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production
Resume Production

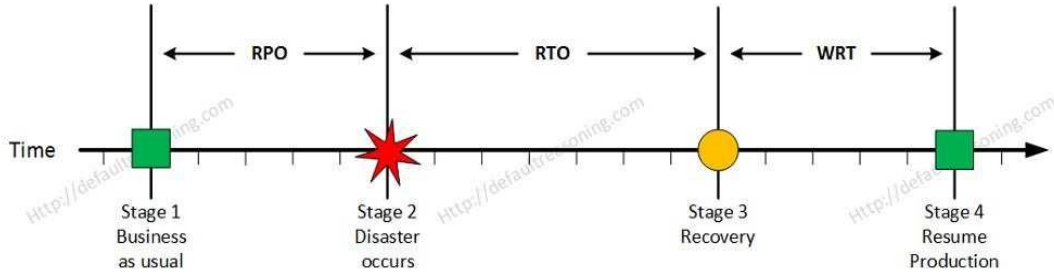


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.
MTD

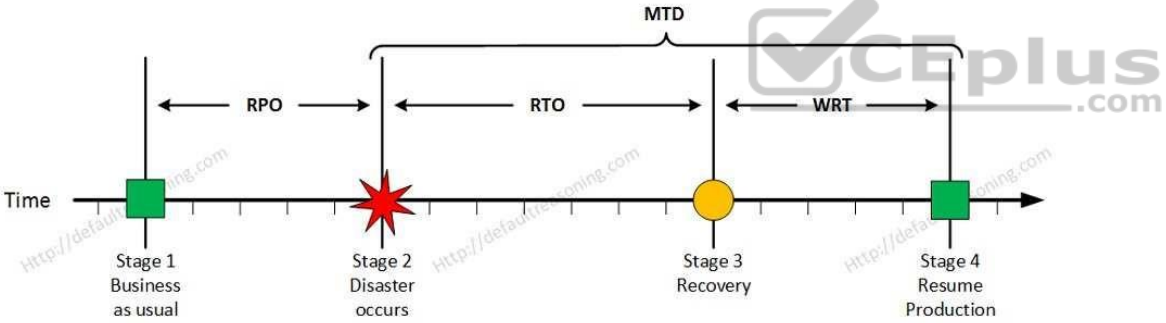


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png

The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

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

CISA review manual 2014 page number 284 http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

QUESTION 87
Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

A. RPO
B. RTO
C. WRT
D. MTD

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

Explanation/Reference:
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual
Business as usual

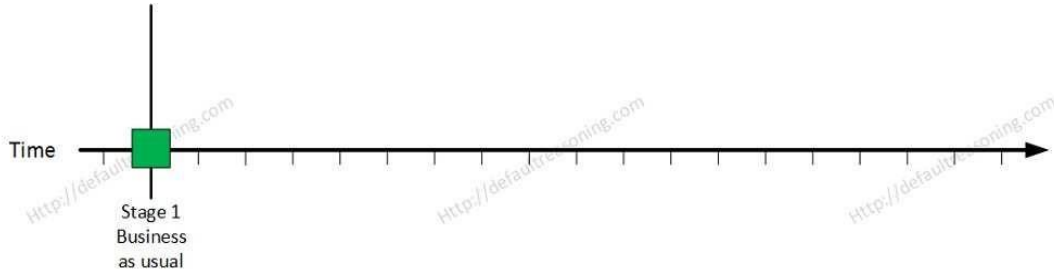


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png

At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs

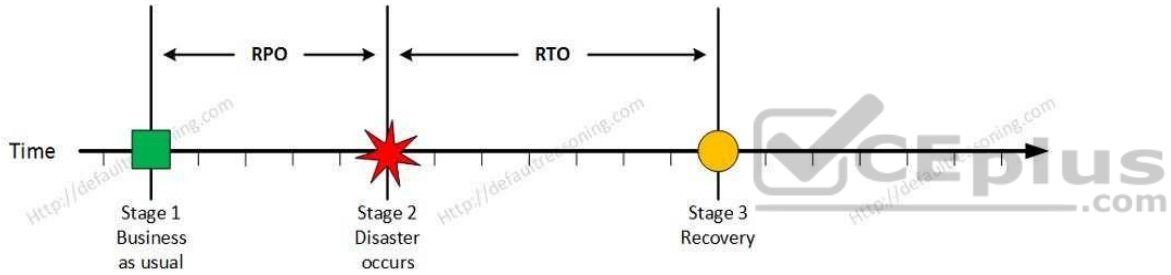


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery
Recovery

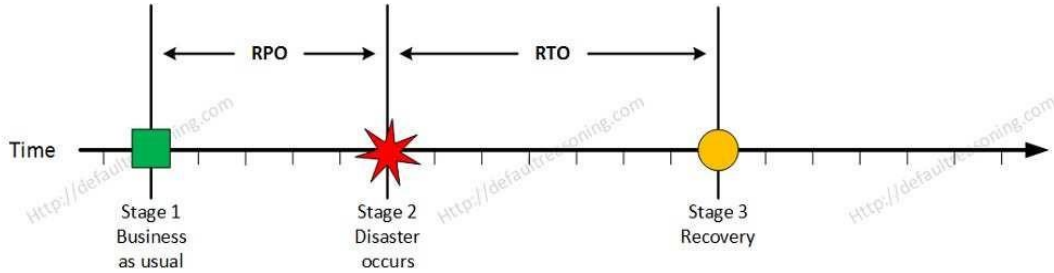


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production
Resume Production

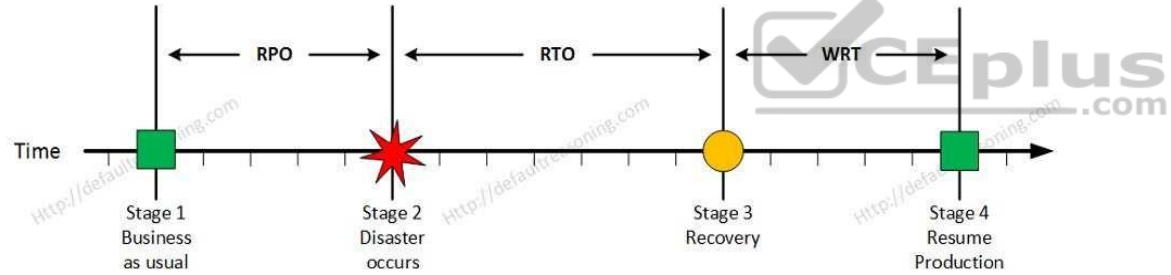


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.
MTD

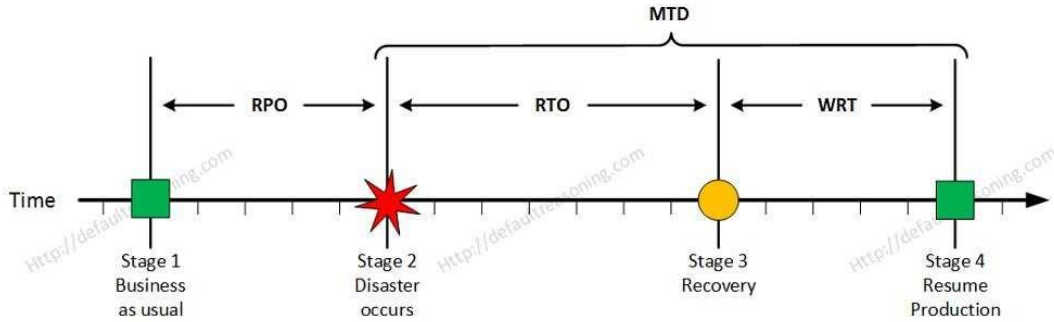


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

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

CISA review manual 2014 page number 284 http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

QUESTION 88
Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

A. RPO
B. RTO C. WRT
D. MTD

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

Explanation/Reference:
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual
Business as usual

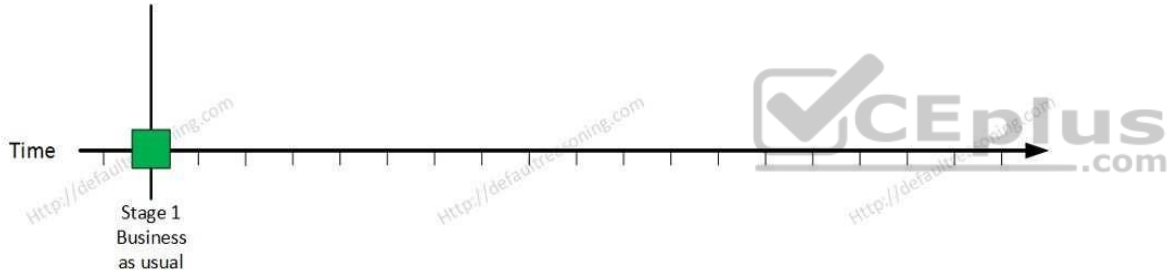


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png

At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs

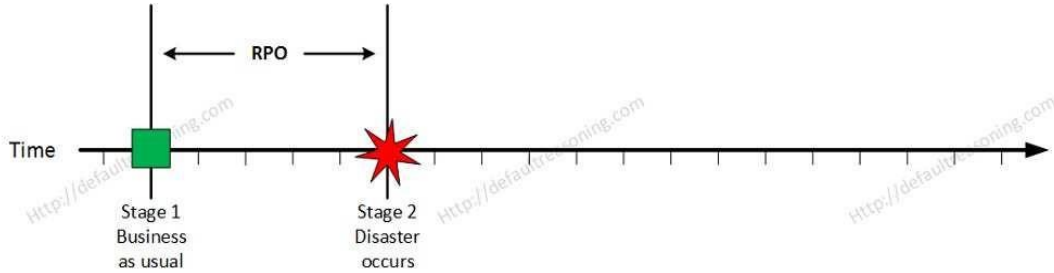


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery
Recovery

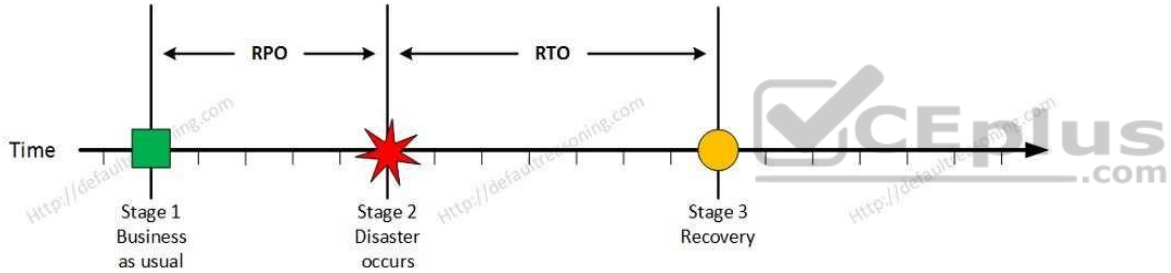


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production
Resume Production

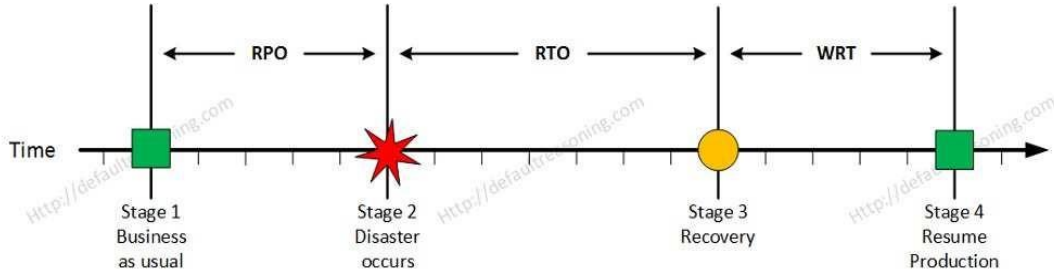


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.
MTD

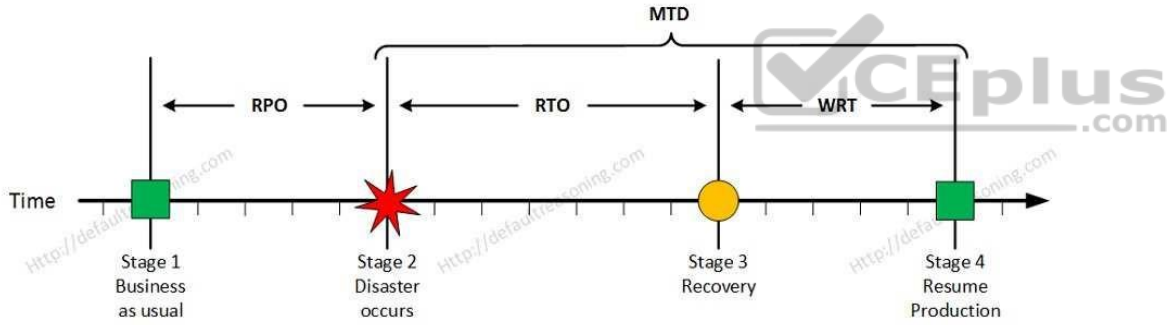


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

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

CISA review manual 2014 page number 284 http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

QUESTION 89
As an IS auditor it is very important to understand the importance of job scheduling. Which of the following statement is NOT true about job scheduler or job scheduling software?

A. Job information is set up only once, which increase the probability of an error.
B. Records are maintained of all job success and failures.
C. Reliance on operator is reduced.
D. Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

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

Explanation/Reference:
The NOT keyword is used in this question. You need to find out an option which is not true about job scheduling.

Below are some advantages of job scheduling or using job scheduling software.

Job information is set up only once, reduce the probability of an error.
Records are maintained of all job success and failures.
Reliance on operator is reduced.
Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

For your exam you should know the information below:

A job scheduler is a computer application for controlling unattended background program execution (commonly called batch processing).

Synonyms are batch system, Distributed Resource Management System (DRMS), and Distributed Resource Manager (DRM). Today's job schedulers, often termed workload automation, typically provide a graphical user interface and a single point of control for definition and monitoring of background executions in a distributed network of computers. Increasingly, job schedulers are required to orchestrate the integration of real-time business activities with traditional background IT processing across different operating system platforms and business application environments.

Job scheduling should not be confused with process scheduling, which is the assignment of currently running processes to CPUs by the operating system.

Basic features expected of job scheduler software include:

interfaces which help to define workflows and/or job dependencies
automatic submission of executions interfaces to monitor the
executions priorities and/or queues to control the execution order of
unrelated jobs

If software from a completely different area includes all or some of those features, this software is consider to have job scheduling capabilities.

Most operating systems (such as Unix and Windows) provide basic job scheduling capabilities, for example: croon. Web hosting services provide job scheduling capabilities through a control panel or a webcron solution. Many programs such as DBMS, backup, ERPs, and BPM also include relevant job-scheduling capabilities. Operating system ("OS") or point program supplied job-scheduling will not usually provide the ability to schedule beyond a single OS instance or outside the remit of the specific program. Organizations needing to automate unrelated IT workload may also leverage further advanced features from a job scheduler, such as:

real-time scheduling based on external, unpredictable
events automatic restart and recovery in event of failures
alerting and notification to operations personnel generation
of incident reports audit trails for regulatory compliance
purposes

The following answers are incorrect:
The other options are correctly defined about job scheduling

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

CISA review manual 2014 page number 242
http://en.wikipedia.org/wiki/Job_scheduler

QUESTION 90

Which of the following type of computer has highest processing speed?

A. Supercomputers
B. Midrange servers
C. Personal computers
D. Thin client computers

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

Explanation/Reference:
Supercomputers are very large and expensive computers with the highest processing speed, designed to be used for specialized purpose or fields that require extensive processing power.

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations.

A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS.

An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

For your exam you should know the information below:

Common Types of computers

Supercomputers
A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations. A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Mainframes
The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

Mid-range servers
Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM). They can also take the form of powerful technical workstations for computer-aided design (CAD) and other computation and graphics-intensive applications. Midrange system are also used as front-end servers to assist mainframe computers in telecommunications processing and network management.

Personal computers
A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Laptop computers
A laptop is a portable personal computer with a clamshell form factor, suitable for mobile use.[1] They are also sometimes called notebook computers or notebooks. Laptops are commonly used in a variety of settings, including work, education, and personal multimedia.

A laptop combines the components and inputs as a desktop computer; including display, speakers, keyboard, and pointing device (such as a touchpad), into a single device. Most modern-day laptop computers also have a webcam and a mice (microphone) pre-installed. [citation needed] A laptop can be powered either from a rechargeable battery, or by mains electricity via an AC adapter. Laptops are a diverse category of devices, and other more specific terms, such as ultrabooks or net books, refer to specialist types of laptop which have been optimized for certain uses. Hardware specifications change vastly between these classifications, forgoing greater and greater degrees of processing power to reduce heat emissions.

Smartphone, tablets and other handheld devices
A mobile device (also known as a handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard.
A handheld computing device has an operating system (OS), and can run various types of application software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.

Early pocket-sized devices were joined in the late 2000s by larger but otherwise similar tablet computers. Much like in a personal digital assistant (PDA), the input and output of modern mobile devices are often combined into a touch-screen interface.

Smartphone's and PDAs are popular amongst those who wish to use some of the powers of a conventional computer in environments where carrying one would not be practical. Enterprise digital assistants can further extend the available functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers.

Thin Client computers
A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following answers are incorrect:

Mid-range servers- Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM).

Personal computers - A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models

which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Thin Client computers- A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

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

CISA review manual 2014 page number 246
http://en.wikipedia.org/wiki/Thin_client
http://en.wikipedia.org/wiki/Mobile_device
http://en.wikipedia.org/wiki/Personal_computer
http://en.wikipedia.org/wiki/Classes_of_computers
http://en.wikipedia.org/wiki/Laptop

QUESTION 91
Which of the following type of computer is a large, general purpose computer that are made to share their processing power and facilities with thousands of internal or external users?

A. Thin client computer
B. Midrange servers
C. Personal computers
D. Mainframe computers

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

Explanation/Reference:
Mainframe computer is a large, general purpose computer that are made to share their processing power and facilities with thousands of internal or external users. The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

For your exam you should know the information below:

Common Types of computers

Supercomputers

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations. A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Mainframes

The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

Mid-range servers

Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM). They can also take the form of powerful technical workstations for computer-aided design (CAD) and other computation and graphics-intensive applications. Midrange system are also used as front-end servers to assist mainframe computers in telecommunications processing and network management.

Personal computers

A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Laptop computers

A laptop is a portable personal computer with a clamshell form factor, suitable for mobile use.[1] They are also sometimes called notebook computers or notebooks. Laptops are commonly used in a variety of settings, including work, education, and personal multimedia.

A laptop combines the components and inputs as a desktop computer; including display, speakers, keyboard, and pointing device (such as a touchpad), into a single device. Most modern-day laptop computers also have a webcam and a mice (microphone) pre-installed. [citation needed] A laptop can be powered either from a rechargeable battery, or by mains electricity via an AC adapter. Laptops are a diverse category of devices, and other more specific terms, such as ultrabooks or net books, refer to specialist types of laptop which have been optimized for certain uses. Hardware specifications change vastly between these classifications, forgoing greater and greater degrees of processing power to reduce heat emissions.

Smartphone, tablets and other handheld devices

A mobile device (also known as a handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard.

A handheld computing device has an operating system (OS), and can run various types of application software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.

Early pocket-sized devices were joined in the late 2000s by larger but otherwise similar tablet computers. Much like in a personal digital assistant (PDA), the input and output of modern mobile devices are often combined into a touch-screen interface.

Smartphone's and PDAs are popular amongst those who wish to use some of the powers of a conventional computer in environments where carrying one would not be practical. Enterprise digital assistants can further extend the available functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers.

Thin Client computers

A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following answers are incorrect:

Mid-range servers- Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM).

Personal computers - A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models

which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.
Thin Client computers- A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 246
http://en.wikipedia.org/wiki/Thin_client
http://en.wikipedia.org/wiki/Mobile_device
http://en.wikipedia.org/wiki/Personal_computer
http://en.wikipedia.org/wiki/Classes_of_computers
http://en.wikipedia.org/wiki/Laptop

QUESTION 92
Diskless workstation is an example of:

A. Handheld devices
B. Thin client computer
C. Personal computer
D. Midrange server

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

Explanation/Reference:
Diskless workstations are example of Thin client computer.
A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

For your exam you should know the information below:

Common Types of computers

Supercomputers

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations. A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Mainframes

The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

Mid-range servers

Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM). They can also take the form of powerful technical workstations for computer-aided design (CAD) and other computation and graphics-intensive applications. Midrange system are also used as front-end servers to assist mainframe computers in telecommunications processing and network management.

Personal computers

A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Laptop computers

A laptop is a portable personal computer with a clamshell form factor, suitable for mobile use.[1] They are also sometimes called notebook computers or notebooks. Laptops are commonly used in a variety of settings, including work, education, and personal multimedia.

A laptop combines the components and inputs as a desktop computer; including display, speakers, keyboard, and pointing device (such as a touchpad), into a single device. Most modern-day laptop computers also have a webcam and a mice (microphone) pre-installed. [citation needed] A laptop can be powered either from a rechargeable battery, or by mains electricity via an AC adapter. Laptops are a diverse category of devices, and other more specific terms, such as

ultrabooks or net books, refer to specialist types of laptop which have been optimized for certain uses. Hardware specifications change vastly between these classifications, forgoing greater and greater degrees of processing power to reduce heat emissions.

Smartphone, tablets and other handheld devices

A mobile device (also known as a handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard.
A handheld computing device has an operating system (OS), and can run various types of application software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.

Early pocket-sized devices were joined in the late 2000s by larger but otherwise similar tablet computers. Much like in a personal digital assistant (PDA), the input and output of modern mobile devices are often combined into a touch-screen interface.

Smartphone's and PDAs are popular amongst those who wish to use some of the powers of a conventional computer in environments where carrying one would not be practical. Enterprise digital assistants can further extend the available functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers.

Thin Client computers
A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following answers are incorrect:
The other types of computers are not example of diskless workstation.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 246
http://en.wikipedia.org/wiki/Thin_client
http://en.wikipedia.org/wiki/Mobile_device
http://en.wikipedia.org/wiki/Personal_computer
http://en.wikipedia.org/wiki/Classes_of_computers
http://en.wikipedia.org/wiki/Laptop

QUESTION 93
In RFID technology which of the following risk could represent a threat to non-RFID networked or collocated systems, assets, and people?

A. Business Process Risk
B. Business Intelligence Risk
C. Privacy Risk
D. Externality Risk

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

Explanation/Reference:
RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

RFID systems typically are not isolated from other systems and assets in the enterprise. Every connection point between the RFID system and something outside the RFID system represents a potential vulnerability for the entity on the other side of the connection, whether that is an application process, a valued asset, or a person.

Externality risks are present for both the RF and enterprise subsystems of an RFID system.
The main externality risk for the RF subsystem is hazards resulting from electromagnetic radiation, which could possibly range from adverse human health effects to ignition of combustible material, such as fuel or ordnance.

The main externality risk for the enterprise subsystem is successful computer network attacks on networked devices and applications. Computer network attacks can involve malware (e.g., worms and viruses) or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage.
The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application. Because the externality risk by definition involves risks outside of the RFID system, it is distinct from both the business process and business intelligence risks; externality risks can be realized without having any effect on RFID-supported business processes or without revealing any information to adversaries.

For your exam you should know the information below:

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal.

RFID RISKS

RFID technology enables an organization to significantly change its business processes to:

Increase its efficiency, which results in lower costs, Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk.

For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics. This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments.

The risks are as follows:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people. An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users.

The following answers are incorrect:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 248
NIST SP 800-98 RFID 2007 - http://www.csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

QUESTION 94
In which of the following RFID risks competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system?

A. Business Process Risk
B. Business Intelligence Risk
C. Privacy Risk
D. Externality Risk

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

Explanation/Reference:
An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

RFID is a powerful technology, in part, because it supports wireless remote access to information about assets and people that either previously did not exist or was difficult to create or dynamically maintain. While this wireless remote access is a significant benefit, it also creates a risk that unauthorized parties could also have similar access to that information if proper controls are not in place. This risk is distinct from the business process risk because it can be realized even when business processes are functioning as intended.
A competitor or adversary can gain information from the RFID system in a number of ways, including eavesdropping on RF links between readers and tags, performing independent queries on tags to obtain relevant data, and obtaining unauthorized access to a back-end database storing information about tagged items. Supply chain applications may be particularly vulnerable to this risk because a variety of external entities may have read access to the tags or related databases.

The risk of unauthorized access is realized when the entity engaging in the unauthorized behavior does something harmful with that information. In some cases, the information may trigger an immediate response. For example, someone might use a reader to determine whether a shipping container holds expensive

electronic equipment, and then break into the container when it gets a positive reading. This scenario is an example of targeting. In other cases, data might also be aggregated over time to provide intelligence regarding an organization's operations, business strategy, or proprietary methods.

For instance, an organization could monitor the number of tags entering a facility to provide a reasonable indication of its business growth or operating practices. In this case, if someone determined that a warehouse recently received a number of very large orders, then that might trigger an action in financial markets or prompt a competitor to change its prices or production schedule.

For your exam you should know the information below:

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal.

RFID RISKS

RFID technology enables an organization to significantly change its business processes to:

Increase its efficiency, which results in lower costs, Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk.

For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics. This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments.

The risks are as follows:
Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.
An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users.

The following answers are incorrect:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 248
NIST SP 800-98 RFID 2007 - http://www.csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

QUESTION 95
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 96
Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

A. Alternative routing
B. Diverse routing
C. Long haul network diversity
D. Last mile circuit protection

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Diverse routing routes traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. This type of access is time-consuming and costly. Long haul network diversity is a diverse long-distance network utilizing T1 circuits among the major long-distance carriers. It ensures long-distance access should any one carrier experience a network failure. Last mile circuit protection is a redundant combination of local carrier T1s microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also utilized.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 259).

QUESTION 97
During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?

A. Measurement of accuracy
B. Elapsed time for completion of critical tasks
C. Quantitatively measuring the results of the test
D. Evaluation of the observed test results

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
It is important to have ways to measure the success of the plan and tests against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation based only on observation. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices A and B are also quantitative, they relate to specific areas, or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 5: Disaster Recovery and Business Continuity (page 269).

QUESTION 98
Which of the following statements regarding an off-site information processing facility is TRUE?

A. It should have the same amount of physical access restrictions as the primary processing site.
B. It should be located in proximity to the originating site so that it can quickly be made operational.

C. It should be easily identified from the outside so in the event of an emergency it can be easily found.
D. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
It is very important that the offsite has the same restrictions in order to avoided misuse.

The following answers are incorrect because:

It should be located in proximity to the originating site so that it can quickly be made operational is incorrect as the offsite is also subject to the same disaster as of the primary site.

It should be easily identified from the outside so in the event of an emergency it can be easily found is also incorrect as it should not be easily identified to prevent intentional sabotage.

Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive is also incorrect as it should be like its primary site.

Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 265).

QUESTION 99
Business Continuity Planning (BCP) is not defined as a preparation that facilitates:

A. the rapid recovery of mission-critical business operations
B. the continuation of critical business functions
C. the monitoring of threat activity for adjustment of technical controls
D. the reduction of the impact of a disaster

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The following answers are incorrect:
All of the other choices are facilitated by a BCP:

the continuation of critical business functions the rapid
recovery of mission-critical business operations the
reduction of the impact of a disaster

QUESTION 100
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 101
Which key is used by the sender of a message to create a digital signature for the message being sent?
A. Sender's public key B.
Sender's private key
C. Receiver's public key
D. Receiver's private key

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The sender private key is used to calculate the digital signature

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 (signing) of the message and receiver need to decrypt the same using sender's public key to validate the signature.

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 are easily transportable, cannot be imitated by someone else, and can 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.
How It 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. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in 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 grave 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 signature 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 these authentication, non-repudiation etc. 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". Very roughly 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. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purposes.

Tip for the exam:

Digital Signature does not provide confidentiality. The sender's private key is used for calculating digital

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

encryption The following were incorrect answers:

Sender's Public key – This is incorrect as receiver will require sender's private key to verify digital signature.

Receiver's Public Key – The digital signature provides non-repudiation. The receiver's public key is known to every one. So it can not be used for digital-signature. Receiver's public key can be used for encryption.
Receiver's Private Key – The sender does not know the receiver's private key. So this option is incorrect.

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

CISA review manual 2014 Page number 348
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 102
Which of the following cryptography is based on practical application of the characteristics of the smallest “grains” of light, the photon, the physical laws governing their generation and propagation and detection?

A. Quantum Cryptography
B. Elliptical Curve Cryptography (ECC)
C. Symmetric Key Cryptography
D. Asymmetric Key Cryptography

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Quantum cryptography is based on a practical application of the characteristics of the smallest “grain” of light, photons and on physical laws governing their generation, propagation and detection.
Quantum cryptography is the next generation of cryptography that may solve some of the existing problem associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. Initial commercial usage has already started now that the laboratory research phase has been completed.

Quantum cryptography is based on a practical application of the characteristics of the smallest “grain” of light, photons and on physical laws governing their generation, propagation and detection.
Quantum cryptography is the next generation of cryptography that may solve some of the existing problem associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. Initial commercial usage has already started now that the laboratory research phase has been completed.

The following were incorrect answers: Elliptic Key Cryptography(ECC) - A variant and more efficient form of a public key cryptography (how to manage more security out of minimum resources) gaining prominence is the ECC. ECC works well on a network computer requires strong cryptography but have some limitation such as bandwidth and processing power. This is even more important with devices such as smart cards, wireless phones and other mobile devices. It is believed that ECC demands less computational power and, therefore offers more security per bit. For example, an ECC with a 160-bit key offer the same security as an RSA based system with a 1024-bit key.

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.

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.

Asymmetric encryption -In which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using 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.

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

CISA review manual 2014 Page number 349 and 350
http://support.microsoft.com/kb/246071

QUESTION 103
Which of the following cryptography demands less computational power and offers more security per bit?

A. Quantum cryptography
B. Elliptic Curve Cryptography (ECC)
C. Symmetric Key Cryptography
D. Asymmetric Key Cryptography

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
ECC demands less computational power and, therefore offers more security per bit. For example, an ECC with a 160-bit key offer the same security as an RSA based system with a 1024-bit key.

ECC is a variant and more efficient form of a public key cryptography (how tom manage more security out of minimum resources) gaining prominence is the ECC. ECC works well on a network computer requires strong cryptography but have some limitation such as bandwidth and processing power. This is even more important with devices such as smart cards, wireless phones and other mobile devices.

The following were incorrect answers:

Quantum Cryptography - Quantum cryptography is based on a practical application of the characteristics of the smallest “grain” of light, photons and on physical laws governing their generation, propagation and detection. Quantum cryptography is the next generation of cryptography that may solve some of the existing problem associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. Initial commercial usage has already started now that the laboratory research phase has been completed.

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.
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 asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using 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.

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

CISA review manual 2014 Page number 349 and 350
http://support.microsoft.com/kb/246071

QUESTION 104
Which of the following is a form of Hybrid Cryptography where the sender encrypts the bulk of the data using Symmetric Key cryptography and then communicates securely a copy of the session key to the receiver?

A. Digital Envelope
B. Digital Signature
C. Symmetric key encryption

D. Asymmetric

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
A Digital Envelope is used to send encrypted information using symmetric keys, and the relevant session key along with it. It is a secure method to send electronic document without compromising the data integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.

A Digital envelope mechanism works as follows:

The symmetric key, which is used to encrypt the bulk of the date or message can be referred to as session key. It is simply a symmetric key picked randomly in the key space.
In order for the receiver to have the ability to decrypt the message, the session key must be sent to the receiver.
This session key cannot be sent in clear text to the receiver, it must be protected while in transit, else anyone who have access to the network could have access to the key and confidentiality can easily be compromised.
Therefore, it is critical to encrypt and protect the session key before sending it to the receiver. The session key is encrypted using receiver's public key. Thus providing confidentiality of the key.
The encrypted message and the encrypted session key are bundled together and then sent to the receiver who, in turn opens the session key with the receiver matching private key.
The session key is then applied to the message to get it in plain text.

The process of encrypting bulk data using symmetric key cryptography and encrypting the session key with a public key algorithm is referred as a digital envelope. Sometimes people refer to it as Hybrid Cryptography as well.

The following were incorrect answers:

Digital-signature – A digital signature is an electronic identification of a person or entity created by using public key algorithm and intended to verify to recipient the integrity of the data and the identity of the sender. Applying a digital signature consist of two simple steps, first you create a message digest, then you encrypt the message digest with the sender's private key. Encrypting the message digest with the private key is the act of signing the message.

Symmetric Key Encryption - Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Asymmetric Key Encryption - The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both. Public-key algorithms are based on mathematical problems

which currently admit no efficient solution that are inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to generate their own public and private key-pair and to use them for encryption and decryption. The strength lies in the fact that it is "impossible" (computationally unfeasible) for a properly generated private key to be determined from its corresponding public key. Thus the public key may be published without compromising security, whereas the private key must not be revealed to anyone not authorized to read messages or perform digital signatures. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of one (or more) secret keys between the parties.

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

CISA review manual 2014 Page number 350 and 351 http://en.wikipedia.org/wiki/Public-key_cryptography

QUESTION 105
How does the digital envelop work? What are the correct steps to follow?

A. You encrypt the data using a session key and then encrypt session key using private key of a sender
B. You encrypt the data using the session key and then you encrypt the session key using sender's public key
C. You encrypt the data using the session key and then you encrypt the session key using the receiver's public key
D. You encrypt the data using the session key and then you encrypt the session key using the receiver's private key

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The process of encrypting bulk data using symmetric key cryptography and then encrypting the session key using public key algorithm is referred as a digital envelope.

A Digital Envelope is used to send encrypted information using symmetric crypto cipher and then key session along with it. It is secure method to send electronic document without compromising the data integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.

A Digital envelope mechanism works as follows:

The symmetric key used to encrypt the message can be referred to as session key. The bulk of the message would take advantage of the high speed provided by Symmetric Cipher.
The session key must then be communicated to the receiver in a secure way to allow the receiver to decrypt the message.
If the session key is sent to receiver in the plain text, it could be captured in clear text over the network and anyone could access the session key which would lead to confidentiality being compromised.

Therefore it is critical to encrypt the session key with the receiver public key before sending it to the receiver. The receiver's will use their matching private key to decrypt the session key which then allow them to decrypt the message using the session key.

The encrypted message and the encrypted session key are sent to the receiver who, in turn decrypts the session key with the receiver's private key. The session key is then applied to the message cipher text to get the plain text.

The following were incorrect answers:

You encrypt the data using a session key and then encrypt session key using private key of a sender - If the session key is encrypted using sender's private key, it can be decrypted only using sender's public key. The sender's public key is know to everyone so anyone can decrypt session key and message.

You encrypt the data using the session key and then you encrypt the session key using sender's public key - If the session key is encrypted by using sender's public key then only sender can decrypt the session key using his/her own private key and receiver will not be able to decrypt the same.

You encrypt the data using the session key and then you encrypt the session key using the receiver's private key - Sender should not have access to receiver's private key. This is not a valid option.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 350 and 351

QUESTION 106
Which of the following is NOT a true statement about public key infrastructure (PKI)?

A. The Registration authority role is to validate and issue digital certificates to end users
B. The Certificate authority role is to issue digital certificates to end users
C. The Registration authority (RA) acts as a verifier for Certificate Authority (CA)
D. Root certificate authority's certificate is always self-signed

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The word NOT is the keyword used in the question. We need to find out the invalid statement from the options.

A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)

A public key infrastructure consists of:

A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requester A Subscriber is the end user who wish to get digital certificate from certificate authority.

The following were incorrect answers:

The Certificate authority role is to issue digital certificates to end users - This is a valid statement as the job of a certificate authority is to issue a digital certificate to end user.

The Registration authority (RA) acts as a verifier for Certificate Authority (CA) - This is a valid statement as registration authority acts as a verifier for certificate authority

Root certificate authority's certificate is always self-signed - This is a valid statement as the root certificate authority's certificate is always self-signed.

The following reference(s) were/was used to create this question:
http://searchsecurity.techtarget.com/definition/PKI

QUESTION 107
Which of the following functionality is NOT supported by SSL protocol?

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

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The NOT is a keyword used in this question. You need to find out the functionality which is NOT provided by SSL protocol. The SSL protocol provides:

Confidentiality
Integrity
Authentication, e.g. between client and server
Non-repudiation

For CISA exam you should know the information below about Secure Socket Layer (SSL) and Transport Layer Security (TLS)

These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.

SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases
Peer negotiation for algorithm support
Public-key, encryption based key exchange and certificate based authentication
Symmetric cipher based traffic encryption.

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.

The following were incorrect answers:
Confidentiality - It is supported by the SSL Protocol

Integrity -It is supported by the SSL Protocol
Authentication - It is supported by the SSL protocol

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 352

QUESTION 108
Which of the following statement correctly describes one way SSL authentication between a client (e.g. browser) and a server (e.g. web server)?

A. Only the server is authenticated while client remains unauthenticated
B. Only the client is authenticated while server remains authenticated
C. Client and server are authenticated
D. Client and server are unauthenticated

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
In one way authentication only server needs to be authenticated where as in mutual authentication both the client and the server needs to be authenticated.

For CISA exam you should know the information below about Secure Socket Layer (SSL) and Transport Layer Security (TLS)

These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.

SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases
Peer negotiation for algorithm support
Public-key, encryption based key exchange and certificate based authentication
Symmetric cipher based traffic encryption.

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.
SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.

The following were incorrect answers:

The other choices presented in the options are not valid as in one way authentication only server needs to be authenticated where as client will remain unauthenticated.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 352

QUESTION 109
Which of the following statement correctly describes difference between SSL and S/HTTP?

A. Both works at application layer of OSI model
B. SSL works at transport layer where as S/HTTP works at application layer of OSI model
C. Both works at transport layer
D. S/HTTP works at transport layer where as SSL works at the application layer of OSI model

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
For your exam you should know below information about S/HTTP and SSL protocol:

Secure Hypertext Transfer Protocol (S/HTTP) -As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

Secure Socket Layer (SSL) and Transport Layer Security (TLS) - These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.
SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.
SSL involves a number of basic phases
Peer negotiation for algorithm support
Public-key, encryption based key exchange and certificate based authentication
Symmetric cipher based traffic encryption.

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.

The following were incorrect answers:

The other choices presented in the options are not valid asSSL works at transport layer where as S/HTTP works at application layer of OSI model.

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

CISA review manual 2014 Page number 352

QUESTION 110
Which of the following is a standard secure email protection protocol?

A. S/MIME
B. SSH
C. SET
D. S/HTTP

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Secure Multipurpose Internet Mail Extension (S/MIME) is a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of message's content's, including attachments.

The following were incorrect answers:

SSH –A client server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data, including password, binary files and administrative commands, transmitted between system on a network. SSH is typically implemented between two parties by validating each other's credential via digital certificates. SSH is useful in securing Telnet and FTP services, and is implemented at the application layer, as opposed to operating at network layer (IPSec Implementation)

SET – SET is a protocol developed jointly by VISA and Master Card to secure payment transaction among all parties involved in credit card transactions among all parties involved in credit card transactions on behalf of cardholders and merchants. As an open system specification, SET is a application-oriented protocol that

uses trusted third party's encryption and digital-signature process, via PKI infrastructure of trusted third party institutions, to address confidentiality of information, integrity of data, cardholders authentication, merchant authentication and interoperability.

Secure Hypertext Transfer Protocol (S/HTTP) -As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 352 and 353

QUESTION 111
Which of the following statement correctly describes the differences between tunnel mode and transport mode of the IPSec protocol?

A. In transport mode the ESP is encrypted where as in tunnel mode the ESP and its header's are encrypted
B. In tunnel mode the ESP is encrypted where as in transport mode the ESP and its header's are encrypted
C. In both modes (tunnel and transport mode) the ESP and its header's are encrypted
D. There is no encryption provided when using ESP or AH

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology. For you exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.
In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/ Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

The other options presented are invalid as the transport mode encrypts ESP and the tunnel mode encrypts ESP and its header's.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number353

QUESTION 112
Which of the following is the unique identifier within and IPSec packet that enables the sending host to reference the security parameter to apply?

A. SPI
B. SA
C. ESP
D. AH

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The Security Parameter Index (SPI) is the unique identifier that enables the sending host to reference the security parameter to apply in order to decrypt the packet.

For you exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.
In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established

when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/ Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

SA – Security Association (SA) defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc.
ESP – Encapsulation Security Payload (ESP) is used to support authentication of sender and encryption of data
AH – Authentication Header allows authentication of a sender of a data.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number353

QUESTION 113
Within IPSEC which of the following defines security parameters which should be applied between communicating parties such as encryption algorithms, key initialization vector, life span of keys, etc?

A. Security Parameter Index (SPI)
B. Security Association (SA)
C. Encapsulation Security Payload (ESP)
D. Authentication Header (AH)

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Security Association (SA)s defines which security parameters should be applied between communication parties as encryption algorithms, key initialization vector, life span of keys, etc.

For you exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.
In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/ Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

Security Parameter Index (SPI) – A Security Parameter Index (SPI) is an unique identifier that enables the sending host to reference the security parameters to apply.

Encapsulation Security Payload (ESP) – Encapsulation Security Payload (ESP) is used support authentication of sender and encryption of data.

Authentication Header(AH) – Authentication Header allows authentication of a sender of a data.

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

CISA review manual 2014 Page number 353

QUESTION 114
Which of the following statement correctly describes the difference between IPSec and SSH protocols?

A. IPSec works at the transport layer where as SSH works at the network layer of an OSI Model
B. IPSec works at the network layer where as SSH works at the application layer of an OSI Model
C. IPSec works at the network layer and SSH works at the transport layer of an OSI Model
D. IPSec works at the transport layer and SSH works at the network layer of an OSI Model

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
For CISA exam you should know below information about SSH and IPSec protocol

SSH -A client server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data, including password, binary files and administrative commands, transmitted between system on a network. SSH is typically implemented between two parties by validating each other's credential via digital certificates. SSH is useful in securing Telnet and FTP services, and is implemented at the application layer, as opposed to operating at network layer (IPSec Implementation)

IPSec -The IP network layer packet security protocol establishes VPNsvia transport and tunnel mode encryption methods. For the transport method, the data portion of each packet referred to as the encapsulation security payload(ESP) is encrypted, achieving confidentiality over a process. In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied. In establishing IPSec sessions in either mode, Security Association (SAs) are established. SAs defines which security parameters should be applied between communication parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAsis established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host. IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and those of the cryptographic keys.

The following were incorrect answers:

The other options presented are invalid as IPSec works at network layer where as SSH works at application layer of an OSI Model.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number352 and 353

QUESTION 115
Which of the following protocol is developed jointly by VISA and Master Card to secure payment transactions among all parties involved in credit card transactions on behalf of cardholders and merchants?

A. S/MIME
B. SSH
C. SET
D. S/HTTP

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Secure Electronic Transaction(SET) is a protocol developed jointly by VISA and Master Card to secure payment transaction among all parties involved in credit card transactions among all parties involved in credit card transactions on behalf of cardholders and merchants. As an open system specification, SET is an applicationoriented protocol that uses trusted third party's encryption and digital-signature process, via PKI infrastructure of trusted third party institutions, to address confidentiality of information, integrity of data, cardholders authentication, merchant authentication and interoperability.

The following were incorrect answers:

S/MIME - Secure Multipurpose Internet Mail Extension (S/MIME) is a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of message's content's, including attachments.

SSH –A client server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data, including password, binary files and administrative commands, transmitted between system on a network. SSH is typically implemented between two parties by validating each other's credential via digital certificates. SSH is useful in securing Telnet and FTP services, and is implemented at the application layer, as opposed to operating at network layer (IPSec Implementation)

Secure Hypertext Transfer Protocol (S/HTTP) -As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 352 and 353

QUESTION 116
An auditor needs to be aware of technical controls which are used to protect computer from malware. Which of the following technical control interrupts DoS and ROM BIOS call and look for malware like action?

A. Scanners
B. Active Monitors
C. Immunizer

D. Behavior blocker

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Active monitors interpret DoS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.
For CISA exam you should know below mentioned different kinds of malware Controls

A. Scanners Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present). Scanners examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are

malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

The following were incorrect answers:

Scanners -Look for sequences of bit called signature that are typical malware programs.

Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior.

Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.
The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 354 and 355

QUESTION 117
Which are the two primary types of scanner used for protecting against Malware?

Malware mask/signatures and Heuristic Scanner
Active and passive Scanner
Behavioral Blockers and immunizer Scanner
None of the above

A. Malware mask/signatures and Heuristic Scanner
B. Active and passive Scanner
C. Behavioral Blockers and immunizer Scanner
D. None of the above

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Scanners Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.
2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)

Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

For CISA exam you should know below mentioned different kinds of malware Controls

A. Active Monitors - Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.
B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker - Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

The following were incorrect answers:

The other options presented are not a valid primary types of scanner.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 354 and 355

QUESTION 118

Which of the following malware technical fool's malware by appending section of themselves to files – somewhat in the same way that file malware append themselves?

A. Scanners
B. Active Monitors
C. Immunizer
D. Behavior blocker

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Immunizers defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

For you exam you should know below mentioned different kinds of malware Controls

A. Scanners- Look for sequences of bit called signature that are typical malware programs.
The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.
2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)

Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

E. Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

The following were incorrect answers:

Scanners -Look for sequences of bit called signature that are typical malware programs.
Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.
Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 354 and 355

QUESTION 119
Which of the following statement INCORRECTLY describes anti-malware?

A 2
B 14
C. 2 andD. None of the choices listed ..... **Error! Bookmark not defined.**

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

The word INCORRECT is the keyword used in the question. All the terms presented in options correctly describes some type of anti-malware related activities.

For your exam you should know below mentioned different kinds of malware Controls

A. Scanners Look for sequences of bit called signature that are typical malware programs.
The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.
2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)

Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

E. Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

The following were incorrect answers:

All of the choices presented other than one were describing Anti-Malware related activities

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 354 and 355

QUESTION 120
Which of the following statement is NOT true about Voice-Over IP (VoIP)?

VoIP uses circuit switching technology
Lower cost per call or even free calls, especially for long distance call
Lower infrastructure cost
VoIP is a technology where voice traffic is carried on top of existing data infrastructure

A. VoIP uses circuit switching technology
B. Lower cost per call or even free calls, especially for long distance call
C. Lower infrastructure cost
D. VoIP is a technology where voice traffic is carried on top of existing data infrastructure

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The NOT is a keyword used in the question. You need to find out invalid statement about VoIP. VoIP uses packet switching and not circuit switching.
For your exam you should know below information about VoIP:

Voice-Over-IP
IP telephony, internet telephony, is the technology that makes it possible to have a voice conversation over the Internet or over any dedicated IP network instead of dedicated transmission lines. The protocol is used to carry the signal over the IP network are commonly referred as Voice-Over-IP (VoIP).VoIP is a technology where voice traffic is carried on top of existing data infrastructure. Sounds are digitalized into IP packets and transferred through the network layer before being decode back into the original voice.

VoIP allows the elimination of circuit switching and the associated waste of bandwidth. Instead, packet switching is used, where IP packets with voice data are sent over the network only when data needs to be sent.

It has advantages over traditional telephony:

Unlike traditional telephony, VoIP innovation progresses at market rates rather than at the rates of multilateral committee process of the International Telecommunication Union (ITU)

Lower cost per call or even free calls, especially for long distance call

Lower infrastructure costs. Once IP infrastructure is installed, no or little additional telephony infrastructure is needed

VoIP Security Issues
With the introduction of VoIP, the need for security is more important because it is needed to protect two assets – the data and the voice.

Protecting the security of conversation is vital now.
In VoIP, packets are sent over the network from the user's computer or VoIP phone to similar equipment at other end. Packets may pass through several intermediate systems that are not under the control of the user's ISP.The current Internet architecture does not provide same physical wire security as phone line.

The main concern of VoIP solution is that while, in the case of traditional telephones, if data system is disrupted, then the different sites of the organization could still be reached via telephone. Thus a backup communication facility should be planned for if the availability of communication is vital to organization.
Another issue might arises with the fact that IP telephones and their supporting equipment require the same care and maintenance as computer system do.
To enhance the protection of the telephone system and data traffic, the VoIP infrastructure should be segregated using Virtual Local Area Network (VLAN).
In many cases, session border controllers (SBCs) are utilized to provide security features for VoIP traffic similar to that provided by firewalls.

The following were incorrect answers:

Lower cost per call or even free calls, especially for long distance call - This is a valid statement about VoIP. In fact it is an advantage of VoIP.

Lower infrastructure cost - This is a valid statement and advantage of using VoIP as compare to traditional telephony system.

VoIP is a technology where voice traffic is carried on top of existing data infrastructure – This is also valid statement about VoIP.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number355

QUESTION 121
Private Branch Exchange(PBX) environment involves many security risks, one of which is the people both internal and external to an organization. Which of the following risks are NOT associated with Private Branch Exchange?

1. Theft of service
2. Disclosure of information
3. Data Modifications
4. Denial of service
5. Traffic Analysis

A. 3 and 4
B. 4 and 5
C. 1-4

D. They are ALL risks associated with PBX

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The NOT is a keyword used in the question. You need to find out the risks which are NOT associated with PBX. All the risk listed within the options are associated with PBX.

The threat of the PBX telephone system are many, depending on the goals of these attackers, and include:

Theft of service - Toll fraud, probably the most common of motives for attacker.

Disclosure of Information -Data disclosed without authorization, either by deliberate actionably accident. Examples includes eavesdropping on conversation and unauthorized access to routing and address data.

Data Modification -Data altered in some meaningful way by recording, deleting or modifying it. For example, an intruder may change billing information or modify system table to gain additional services.

Unauthorized access – Actions that permit an unauthorized user to gain access to system resources or privileges.

Denial of service -Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

Traffic Analysis – A form of passive attack in which an intruder observes information about calls and make inferences, e.g. from the source and destination number or frequency and length of messages. For example, an intruder observes a high volume of calls between a company's legal department and patent office, and conclude that a patent is being filed.

The following were incorrect answers:

All the risks presented in options are associated with PBX. So other options are not valid.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number356

QUESTION 122
Which of the following is a sophisticated computer based switch that can be thought of as essentially a small in-house phone company for the organization?

A. Private Branch Exchange

B. Virtual Local Area Network
C. Voice over IP
D. Dial-up connection

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
A Private Branch Exchange(PBX) is a sophisticated computer based switch that can be thought of as essentially a small in-house phone company for the organization that operates it. Protection of PBX is thus a height priority. Failure to secure PBX can result in exposing the organization to toll fraud, theft of proprietary or confidential information, loss of revenue or legal entanglements.
PBX environment involves many security risks, presented by people both internal and external to an organization. The threat of the PBX telephone system are many, depending on the goals of these attackers, and include:

Theft of service - Toll fraud, probably the most common of motives for attacker.

Disclosure of Information -Data disclosed without authorization, either by deliberate actionably accident. Examples includes eavesdropping on conversation and unauthorized access to routing and address data.

Data Modification -Data altered in some meaningful way by recording, deleting or modifying it. For example, an intruder may change billing information or modify system table to gain additional services.

Unauthorized access – Actions that permit an unauthorized user to gain access to system resources or privileges.

Denial of service -Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.
Traffic Analysis – A form of passive attack in which an intruder observes information about calls and make inferences, e.g. from the source and destination number or frequency and length of messages. For example, an intruder observes a high volume of calls between a company's legal department and patent office, and conclude that a patent is being filed.

The following were incorrect answers:

Virtual Local Area Network - A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to change in network requirements and relocation of workstations and server nodes.

Voice over IP - VoIP is a technology where voice traffic is carried on top of existing data infrastructure. Sounds are digitalized into IP packets and transferred through the network layer before being decode back into the original voice.

Dial-up connection - Dial-up refers to an Internet connection that is established using a modem. The modem connects the computer to standard phone lines, which serve as the data transfer medium. When a user initiates a dial-up connection, the modem dials a phone number of an Internet Service Provider (ISP) that is designated to receive dial-up calls. The ISP then establishes the connection, which usually takes about ten seconds and is accompanied by several beeping an buzzing sounds.

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

CISA review manual 2014 Page number356

QUESTION 123
Which of the following PBX feature provides the possibility to break into a busy line to inform another user of an important message?

A. Account Codes
B. Access Codes
C. Override
D. Tenanting

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Override feature of PBS provides for the possibility to break into a busy line to inform another user an important message.

For CISA exam you should know below mentioned PBS features and Risks
System Features
Description
Risk
Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic
Call forwarding

Allow specifying an alternate number to which calls will be forwarded based on certain condition User tracking Account codes

Used to:
Track calls made by certain people or for certain projects for appropriate billing
Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes
Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features
Silent Monitoring
Silently monitors other calls
Eavesdropping
Conferencing

Allows for conversation among several users

Eavesdropping, by adding unwanted/unknown parties to a conference
override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message
Eavesdropping
Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose
Tenanting
Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail

Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release
Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping
No busy extension
Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress
Diagnostics
Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage

Camp-on or call waiting
When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections
Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility Eavesdropping on a line

The following were incorrect answers:

Account Codes - that are use to:
Track calls made by certain people or for certain projects for appropriate billing
Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Access Codes - Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Tenanting - Limits system user access to only those users who belong to the same tenant group useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

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

CISA review manual 2014 Page number358

QUESTION 124
Which of the following PBX feature allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available?

A. Automatic Call distribution
B. Call forwarding
C. Tenanting
D. Voice mail

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Automatic Call distribution allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

For your exam you should know below mentioned PBX features and Risks:

System Features
Description
Risk

Automatic Call distribution
Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic
Call forwarding

Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking

Account codes

Used to:
Track calls made by certain people or for certain projects for appropriate billing
Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes
Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features
Silent Monitoring

Silently monitors other calls

Eavesdropping
Conferencing

Allows for conversation among several users
Eavesdropping, by adding unwanted/unknown parties to a conference
override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping
Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting
Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail
Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release
Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping
No busy extension
Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics
Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage
Camp-on or call waiting
When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections
Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:

Call forwarding - Allow specifying an alternate number to which calls will be forwarded based on certain condition

Tenanting - Limits system user access to only those users who belong to the same tenant group useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Voice Mail - Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 358

QUESTION 125
Which of the following PBX feature supports shared extensions among several devices, ensuring that only one device at a time can use an extension?

A. Call forwarding
B. Privacy release
C. Tenanting
D. Voice mail

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Privacy release supports shared extensions among several devices, ensuring that only one device at a time can use an extension.

For you exam you should know below mentioned PBX features and Risks:

System Features
Description
Risk

Automatic Call distribution
Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding
Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking
Account codes

Used to:
Track calls made by certain people or for certain projects for appropriate billing

Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes
Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features
Silent Monitoring

Silently monitors other calls
Eavesdropping
Conferencing

Allows for conversation among several users
Eavesdropping, by adding unwanted/unknown parties to a conference
override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping
Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting
Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail
Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release
Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping
No busy extension
Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics
Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage
Camp-on or call waiting
When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections
Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:

Call forwarding - Allow specifying an alternate number to which calls will be forwarded based on certain condition

Tenanting -Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Voice Mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

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

CISA review manual 2014 Page number358

QUESTION 126
Which of the following option INCORRECTLY describes PBX feature?

A. Voice mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
B. Tenanting-Provides for the possibility to break into a busy line to inform another user an important message
C. Automatic Call Distribution - Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available
D. Diagnostics -Allows for bypassing normal call restriction procedures

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The word INCORRECTLY was the keyword used in the question. You need to find out the incorrectly described PBX feature from given options. The Tenanting feature is incorrectly described.

Tenanting limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

For your exam you should know below mentioned PBX features and Risks:

System Features
Description
Risk

Automatic Call distribution
Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding
Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking
Account codes

Used to:

Track calls made by certain people or for certain projects for appropriate billing

Dial-In system access (user dials from outside and gain access to normal feature of the PBX)
Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes
Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features
Silent Monitoring

Silently monitors other calls

Eavesdropping
Conferencing

Allows for conversation among several users
Eavesdropping, by adding unwanted/unknown parties to a conference
override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping

Auto-answer
Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting
Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail
Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release
Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension
Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics
Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage

Camp-on or call waiting
When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections
Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:
The other options presented correctly describes PBX features thus not the right choice.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number358

QUESTION 127
Which of the following technique is NOT used by a preacher against a Private Branch Exchange (PBX)?

A. Eavesdropping
B. Illegal call forwarding
C. Forwarding a user's to an unused or disabled number
D. SYN Flood

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
The word NOT the keyword used in the question. You need to find out the technique which preacher do not use to exploit PBX.

SYN Flood -Sends a flood of TCP/SYN packets with forged sender address, causing half-open connections and saturates available connection capacity on the target machine.

For CISA Exam you should know below mentioned techniques used by preacher for illegal purpose of PBX.

Eavesdropping on conversation, without the other parties being aware of it
Eavesdropping on conference call
Illegal forwarding calls from specific equipment to remote numbers
Forwarding a user's to an unused or disabled number, thereby making it unreachable by external calls.

The following were incorrect answers:

The other options presented correctly describes the techniques used preacher for illegal purpose of PBX.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 357

QUESTION 128

Who is primarily responsible for storing and safeguarding the data?

A. Data Owner
B. Data User
C. Data Steward
D. Security Administrator

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Data Steward or data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

For CISA exam you should know below roles in an organization

Data Owners – These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.
Data Custodian or Data Steward – These people are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Data Owner- These peoples are generally managers and directors responsible for using information for running and controlling the business.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.

Security Administrator - Security administrator is responsible for providing adequate and logical security for IS programs, data and equipment.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number361

QUESTION 129
Who is responsible for providing adequate physical and logical security for IS program, data and equipment?

A. Data Owner
B. Data User
C. Data Custodian
D. Security Administrator

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Security administrator are responsible for providing adequate physical and logical security for IS programs, data and equipment.

For CISA exam you should know below roles in an organization

Data Owners – These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward – These people are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Data Owner- These peoples are generally managers and directors responsible for using information for running and controlling the business.
Data Users – Data users, including internal and external user community, are the actual user of computerized data.
Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number361

QUESTION 130
Who is responsible for restricting and monitoring access of a data user?

A. Data Owner

B. Data User
C. Data Custodian
D. Security Administrator

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Security administrator are responsible for providing adequate and logical security for IS programs, data and equipment.

For CISA exam you should know below roles in an organization

Data Owners – These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward – These people are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator-Security administrator are responsible for providing adequate physical and logical security for IS programs, data and equipment.
Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Data Owner - These peoples are generally managers and directors responsible for using information for running and controlling the business.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.

Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number361

QUESTION 131
Who is responsible for authorizing access level of a data user?

A. Data Owner

B. Data User
C. Data Custodian
D. Security Administrator

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Data owners are responsible for authorizing access level of a data user. These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

For your exam you should know below roles in an organization

Data Owners – Data Owners are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward –are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.
Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Security Administrator -Security administrator is responsible for providing adequate and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.
Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number361

QUESTION 132
During Involuntary termination of an employee, which of the following is the MOST important step to be considered?

A. Get a written NDA agreement from an employee
B. Terminate all physical and logical access
C. Provide compensation in lieu of notice period
D. Do not communicate to the respective employee about the termination

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
For CISA exam you should know below information about Terminated Employee Access

Termination of employment can occur in the following circumstances:

On the request of the employee (Voluntary resignation from service)
Scheduled (On retirement or completion of contract)
Involuntary (forced by management in special circumstances)

In case of an involuntary termination of employment, the logical and physical access rights of employees to the IT infrastructure should either be withdrawn completely or highly restricted as early as possible, before the employee become aware of termination or its likelihood.

This ensures that terminated employees cannot continue to access potentially confidential or damaging information from the IT resources or perform any action that would result in damage of any kind of IT infrastructure, applications and data. Similar procedure in place to terminate access for third parties upon terminating their activities with the organization.
When it is necessary for employee to continue to have accesses, such access must be monitored carefully and continuously and should take place with senior management's knowledge and authorization.

In case of a voluntary or scheduled termination of employment, it is management's prerogative to decide whether access is restricted or withdrawn. This depends on:

The specific circumstances associated with each case
The sensitivity of employee's access to the IT infrastructure and resources
The requirement of the organization's information security policies, standards and procedure.

The following were incorrect answers:
The other options presented are incorrectly describes about involuntary termination.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 361 and 362

QUESTION 133
While evaluating logical access control the IS auditor should follow all of the steps mentioned below EXCEPT one?

1. Obtain general understanding of security risk facing information processing, through a review of relevant documentation, inquiry and observation,etc
2. Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness
3. Test Control over access paths to determine whether they are functioning and effective by applying appropriate audit technique
4. Evaluate the access control environment to determine if the control objective are achieved by analyzing test result and other audit evidence
5. Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standard or practice and procedures used by other organization.
6. Evaluate and deploy technical controls to mitigate all identified risks during audit.

A. 2
B. 3
C. 1
D. 6

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
The word EXCEPT is the keyword used in the question. You need find out the item an IS auditor should not perform while evaluating logical access control. It is not an IT auditor's responsibility to evaluate and deploy technical controls to mitigate all identified risks during audit.
For CISA exam you should know below information about auditing logical access:

Obtain general understanding of security risk facing information processing, through a review of relevant documentation, inquiry and observation,etc
Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness
Test Control over access paths to determine whether they are functioning and effective by applying appropriate audit technique
Evaluate the access control environment to determine if the control objective are achieved by analyzing test result and other audit evidence
Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standard or practice and procedures used by other organization.

The following were incorrect answers:

The other options presented are valid choices which IS auditor needs to follow while evaluating logical access control.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number362

QUESTION 134
Identify the correct sequence which needs to be followed as a chain of event in regards to evidence handling in computer forensics?

A. Identify, Analyze, preserve and Present
B. Analyze, Identify, preserve and present
C. Preserve, Identify, Analyze and Present
D. Identify, Preserve, Analyze and Present

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
There are 4 major considerations in the chain of event in regards to evidence in computer forensics:

Identify -Refers to identification of information that is available and might form evidence of an accident

Preserve -Refers to the practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain-of-custody so that it can be established in a court law.

Analyze – Involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. Interpreting the data requires an in-depth knowledge of how different pieces of evidences may fit together. The analysis should be performed using an image of media and not the original.

Present -Involves a presentation of the various audiences such as management, attorneys, court, etc.Acceptance of evidence depends upon the manner of presentation, qualification of the presenter, and credibility of the process used to preserve and analyze the evidence.

The following were incorrect answers:

The other options presented are not a valid sequence which needs to be followed in the chain of events in regards to evidence in computer forensic.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number367

QUESTION 135
In computer forensics, which of the following is the process that allows bit-for-bit copy of a data to avoid damage of original data or information when multiple analysis may be performed?

A. Imaging

B. Extraction
C. Data Protection
D. Data Acquisition

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Imaging is the process that allows one to obtain a bit-for bit copy of a data to avoid damage to the original data or information when multiple analysis may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

For CISA exam you should know below mentioned key elements of computer forensics during audit planning.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Imaging -The Imaging is a process that allows one to obtain bit-for bit copy of a data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Extraction - This process consist of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

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

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Reporting- The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis. The report should achieve the following goals

Accurately describes the details of an incident.

Be understandable to decision makers.
Be able to withstand a barrage of legal security Be
unambiguous and not open to misinterpretation.
Be easily referenced
Contains all information required to explain conclusions reached
Offer valid conclusions, opinions or recommendations when needed
Be created in timely manner.

The following were incorrect answers:

Extraction - This process consist of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number367 and 368

QUESTION 136
In computer forensic which of the following describe the process that converts the information extracted into a format that can be understood by investigator?

A. Investigation
B. Interrogation
C. Reporting
D. Extraction

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Investigation is the process that converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

For CISA exam you should know below mentioned key elements of computer forensics during audit planning.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Imaging -The Imaging is a process that allows one to obtain bit-for bit copy of a data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Extraction - This process consist of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

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

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Reporting- The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis. The report should achieve the following goals

Accurately describes the details of an incident.

Be understandable to decision makers.
Be able to withstand a barrage of legal security Be
unambiguous and not open to misinterpretation.
Be easily referenced
Contains all information required to explain conclusions reached
Offer valid conclusions, opinions or recommendations when needed
Be created in timely manner.

The following were incorrect answers:

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

Extraction - This process consist of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability.

Reporting -The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number367 and 368

QUESTION 137
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 consist 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 number367 and 368 **QUESTION**
138
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 139
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 140
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 141
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 142
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 143
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

These system are 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 number373 and 374

QUESTION 144
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 number376
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 145
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 number376

QUESTION 146
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 147
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 148
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 149

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

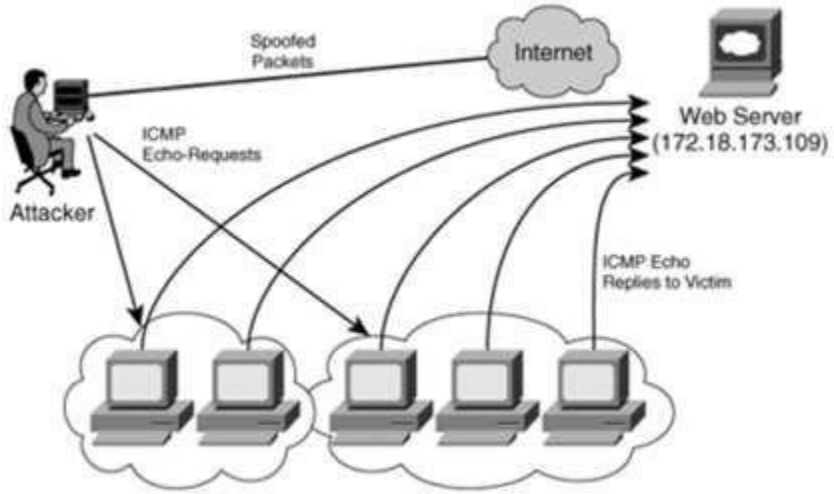


Image reference - http://resources.infosecinstitute.com/wp-content/uploads/012813_1439_HaveYouEver2.png

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 150
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 151
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 152
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 analysisC. 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 issue 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 153
Which of the following attack includes social engineering, link manipulation or web site forgery techniques?

A. surf attack
B. Traffic analysisC. 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 154
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 analysisC. 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 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 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 155
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 156
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 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 157
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.

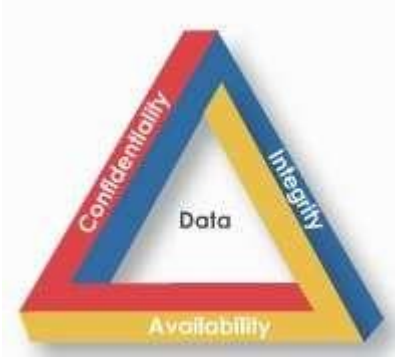
The two primary areas affecting the availability of systems are:
1. Denial-of-Service attacks and
2. Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (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 number350

QUESTION 158
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 159
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 160
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

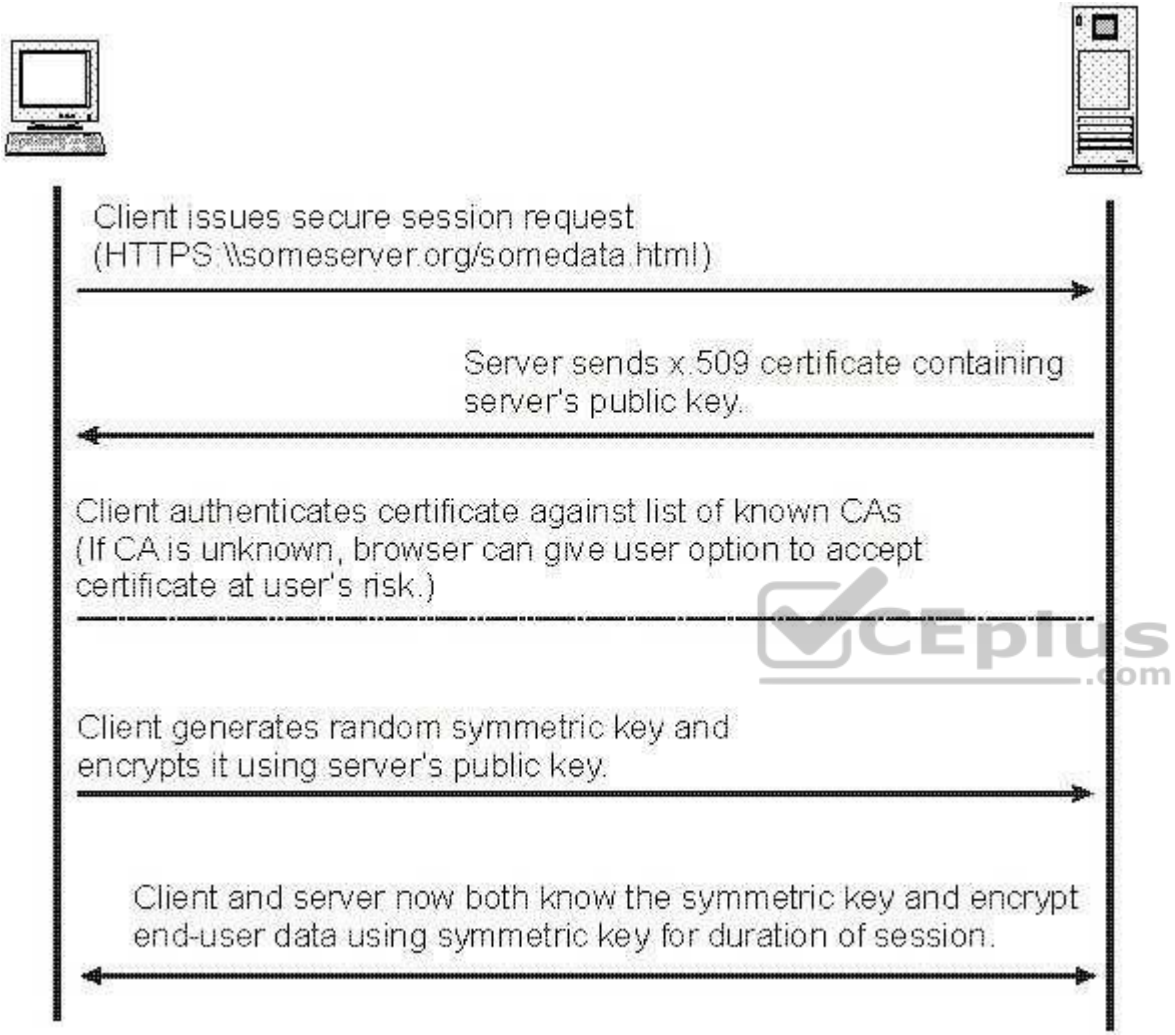


Image Reference - http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/handshak.gif

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 161
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 require 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 require 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.

NEW QUESTIONS

QUESTION 162
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 163
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 164
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 165
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 166
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 167
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 168
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 169
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 170
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 171
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 172
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 173
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 174
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 175
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 176
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 177
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 178
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 179
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 180
An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

A. defining the conceptual schema.
B. defining security and integrity checks.
C. liaising with users in developing data model.
D. mapping data model with the internal schema.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A DBA only in rare instances should be mapping data elements from the data model to the internal schema (physical data storage definitions). To do so would eliminate data independence for application systems. Mapping of the data model occurs with the conceptual schema since the conceptual schema represents the enterprise wide view of data within an organization and is the basis for deriving and end-user department data model.

QUESTION 181
To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

A. the entire message and thereafter enciphering the message digest using the sender's private key.
B. any arbitrary part of the message and thereafter enciphering the message digest using the sender's private key.
C. the entire message and thereafter enciphering the message using the sender's private key.
D. the entire message and thereafter enciphering the message along with the message digest using the sender's private key.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
A digital signature is a cryptographic method that ensures data integrity, authentication of the message, and non-repudiation. To ensure these, the sender first creates a message digest by applying a cryptographic hashing algorithm against the entire message and thereafter enciphers the message digest using the sender's private key. A message digest is created by applying a cryptographic hashing algorithm against the entire message not on any arbitrary part of the message. After creating the message digest, only the message digest is enciphered using the sender's private key, not the message.

QUESTION 182
A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

A. digest signature.
B. electronic signature.
C. digital signature.
D. hash signature.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

QUESTION 183
A critical function of a firewall is to act as a:

A. special router that connects the Internet to a LAN.
B. device for preventing authorized users from accessing the LAN.
C. server used to connect authorized users to private trusted network resources.
D. proxy server to increase the speed of access to authorized users.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users of other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling the outside resources to which its own users have access. Basically, a firewall, working closely with a router program, filters all network packets to determine whether or not to forward them toward their destination. A firewall includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so no incoming request can get directed to private network resources.

QUESTION 184
Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

A. Spool
B. Cluster controller
C. Protocol converter
D. Front end processor

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A front-end processor is a hardware device that connects all communication lines to a central computer to relieve the central computer.

QUESTION 185
The use of a GANTT chart can:

A. aid in scheduling project tasks. B.
determine project checkpoints.
C. ensure documentation standards.
D. direct the post-implementation review.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

QUESTION 186
Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

A. Gateway
B. Protocol converter
C. Front-end communication processor
D. Concentrator/multiplexor

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A gateway performs the job of translating e-mail formats from one network to another so messages can make their way through all the networks.

QUESTION 187
Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

A. Specific developments only
B. Business requirements only
C. All phases of the installation must be documented
D. No need to develop a customer specific documentation

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

QUESTION 188
A hub is a device that connects:

A. two LANs using different protocols.
B. a LAN with a WAN.
C. a LAN with a metropolitan area network (MAN).
D. two segments of a single LAN.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A hub is a device that connects two segments of a single LAN. A hub is a repeater. It provides transparent connectivity to users on all segments of the same LAN. It is a level 1 device.

QUESTION 189
A LAN administrator normally would be restricted from:

A. having end-user responsibilities.
B. reporting to the end-user manager.
C. having programming responsibilities.
D. being responsible for LAN security administration.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A LAN administrator should not have programming responsibilities but may have end- user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator also may be responsible for security administration over the LAN.

QUESTION 190
Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

A. A neural network
B. Database management software
C. Management information systems
D. Computer assisted audit techniques

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A neural network will monitor and learn patterns, reporting exceptions for investigation.

QUESTION 191
A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

A. duplicate check.
B. table lookup.
C. validity check.
D. parity check.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated.

QUESTION 192
For which of the following applications would rapid recovery be MOST crucial?
A. Point-of-sale system B.
Corporate planning
C. Regulatory reporting
D. Departmental chargeback

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly.

QUESTION 193
The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manual.
B. performance of a comprehensive security control review by the IS auditor.
C. adoption of a corporate information security policy statement.
D. purchase of security access control software.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

QUESTION 194
A malicious code that changes itself with each file it infects is called a:

A. logic bomb.
B. stealth virus.
C. trojan horse.
D. polymorphic virus.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

QUESTION 195
Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

A. Paper test
B. Post test
C. Preparedness test
D. Walk-through

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments. A paper test is a walkthrough of the plan, involving major players, who attempt to determine what might happen in a particular type of service disruption in the plan's execution. A paper test usually precedes the preparedness test. A post-test is actually a test phase and is comprised of a group of activities, such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third- party systems. A walkthrough is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

QUESTION 196

An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the DRP?

A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for the disaster recovery. A paper test is a structured walk- through of the disaster recovery plan and should be conducted before a preparedness test. A full operational test is conducted after the paper and preparedness test. A regression test is not a disaster recovery planning (DRP) test and is used in software maintenance.

QUESTION 197
The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

A. Relocate the shut off switch.
B. Install protective covers.
C. Escort visitors.
D. Log environmental failures.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation.

QUESTION 198
Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

A. Acceptance testing is to be managed by users.
B. A quality plan is not part of the contracted deliverables.
C. Not all business functions will be available on initial implementation.
D. Prototyping is being used to confirm that the system meets business requirements.

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

QUESTION 199
In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

A. registration authority (RA).
B. issuing certification authority (CA).
C. subject CA.
D. policy management authority.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA. In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate.

QUESTION 200
Which of the following is a data validation edit and control?

A. Hash totals
B. Reasonableness checks
C. Online access controls
D. Before and after image reporting

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A reasonableness check is a data validation edit and control, used to ensure that data conforms to predetermined criteria.

QUESTION 201
A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

A. reasonableness check.
B. parity check.
C. redundancy check.
D. check digits.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data.

QUESTION 202
What is the primary objective of a control self-assessment (CSA) program?

A. Enhancement of the audit responsibility
B. Elimination of the audit responsibility
C. Replacement of the audit responsibility
D. Integrity of the audit responsibility

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

QUESTION 203
IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?
A. True B.
False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

QUESTION 204
As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

A. The same value.
B. Greater value.
C. Lesser value.
D. Prior audit reports are not relevant.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

QUESTION 205
The PRIMARY purpose of audit trails is to:

A. improve response time for users.
B. establish accountability and responsibility for processed transactions.
C. improve the operational efficiency of the system.
D. provide useful information to auditors who may wish to track transactions

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space. Choice D is also a valid reason; however, it is not the primary reason.

Answer: C

Explanation:
The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

QUESTION 206
How does the process of systems auditing benefit from using a risk-based approach to audit planning?

A. Controls testing starts earlier.
B. Auditing resources are allocated to the areas of highest concern.
C. Auditing risk is reduced.
D. Controls testing is more thorough.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning.

QUESTION 207
After an IS auditor has identified threats and potential impacts, the auditor should:

A. Identify and evaluate the existing controls
B. Conduct a business impact analysis (BIA)
C. Report on existing controls
D. Propose new controls

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
After an IS auditor has identified threats and potential impacts, the auditor should then identify and evaluate the existing controls.

QUESTION 208
The use of statistical sampling procedures helps minimize:

A. Detection risk
B. Business risk
C. Controls risk
D. Compliance risk

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of statistical sampling procedures helps minimize detection risk.

QUESTION 209
What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

A. Business risk
B. Detection risk
C. Residual risk
D. Inherent risk

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

QUESTION 210
A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

A. can identify high-risk areas that might need a detailed review later.
B. allows IS auditors to independently assess risk.
C. can be used as a replacement for traditional audits.
D. allows management to relinquish responsibility for control.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Choice B is incorrect, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Choice C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Choice D is incorrect, because CSA does not allow management to relinquish its responsibility for control.

QUESTION 211
What type of approach to the development of organizational policies is often driven by risk assessment?

A. Bottom-up
B. Top-down
C. Comprehensive

D. Integrated

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A bottom-up approach to the development of organizational policies is often driven by risk assessment.

QUESTION 212
Who is accountable for maintaining appropriate security measures over information assets?

A. Data and systems owners
B. Data and systems users
C. Data and systems custodians
D. Data and systems auditors

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data and systems owners are accountable for maintaining appropriate security measures over information assets.

QUESTION 213
Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions.

QUESTION 214
What should an IS auditor do if he or she observes that project-approval procedures do not exist?

A. Advise senior management to invest in project-management training for the staff
B. Create project-approval procedures for future project implementations
C. Assign project leaders
D. Recommend to management that formal approval procedures be adopted and documented

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If an IS auditor observes that project-approval procedures do not exist, the IS auditor should recommend to management that formal approval procedures be adopted and documented.

QUESTION 215
Who is ultimately accountable for the development of an IS security policy?

A. The board of directors
B. Middle management
C. Security administrators
D. Network administrators

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The board of directors is ultimately accountable for the development of an IS security policy.

QUESTION 216
Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Proper segregation of duties normally prohibits a LAN administrator from also having programming responsibilities.

QUESTION 217
A core tenant of an IS strategy is that it must:

A. Be inexpensive
B. Be protected as sensitive confidential information
C. Protect information confidentiality, integrity, and availability
D. Support the business objectives of the organization

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Above all else, an IS strategy must support the business objectives of the organization.

QUESTION 218
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 219
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 220
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 221
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 222
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 223
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 224
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 225
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 226
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 227
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 228
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 229
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 230
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 231
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 232
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 233
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 234
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 235
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 236
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 237
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 238
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 239
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 240
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 241
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 242
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 243
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 244
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 245
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 246
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 247
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 248

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 249
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 250

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 251
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 252
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 253
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 254

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 255
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 256
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 257
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 258
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 259
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 260
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 261
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 262
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 263
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 264
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 265
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 266
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 267
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 268
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 269
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 270
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 271
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 272
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 273
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 274
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 275
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 276
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 277
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 278
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 279
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 280

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 281
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 282

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 283
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 284
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 285
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 286
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 287
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 288
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:

QUESTION 289
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 290
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 291
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 292
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 293
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 294
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 295
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 296
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 297
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 298
When segregation of duties concerns exists between IT support staff and end users, what would be suitable compensating control?

C.

A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs
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 299
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.

C.

QUESTION 300

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
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 301

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

C.
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 302
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 303
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 304

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 305
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 306
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 307
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 308
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 309
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 310
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 311
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 312
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 313
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 314
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 315
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 316
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 317
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 318
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 319
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 320
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 321
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 322
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 323
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 324
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 325
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 326
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 327

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 328
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 329
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 330
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 331

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 332
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 333
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 334
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 335
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 336
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 337
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 338
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 339
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 340
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 341
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 342
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 343
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 344
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 345
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 346
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 347
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 348
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 349
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 350
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 351
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 352
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 353

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 354
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 355
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 356
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 357
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 358
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 359
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 360
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 361
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 362
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 363
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 364
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 365
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 366
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 367
Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?

A. Accuracy of the source data
B. Credibility of the data source
C. Accuracy of the extraction process
D. Accuracy of the data transformation

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Accuracy of source data is a prerequisite for the quality of the data in a data warehouse. Credibility of the data source, accurate extraction processes and accurate transformation routines are all important, but would not change inaccurate data into quality (accurate) data.

QUESTION 368
When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

A. Use of a cryptographic hashing algorithm
B. Enciphering the message digest
C. Deciphering the message digest
D. A sequence number and time stamp

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When transmitting data, a sequence number and/or time stamp built into the message to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed. This is known as replay protection, and could be used to verify that a payment instruction was not duplicated. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the transaction. When the message is deciphered by the receiver using the sender's public key, it ensures that the message could only have come from the sender. This process of sender authentication achieves nonrepudiation.

QUESTION 369
When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

A. not be concerned since there may be other compensating controls to mitigate the risks.
B. ensure that overrides are automatically logged and subject to review.
C. verify whether all such overrides are referred to senior management for approval.
D. recommend that overrides not be permitted.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log. An IS auditor should not assume that compensating controls exist. As long as the overrides are policy- compliant, there is no need for senior management approval or a blanket prohibition.

QUESTION 370
When using an integrated test facility (ITF), an IS auditor should ensure that:

A. production data are used for testing.
B. test data are isolated from production data.
C. a test data generator is used.
D. master files are updated with the test data.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An integrated test facility (ITF) creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live data. While this ensures that periodic testing does not require a separate test process, there is a need to isolate test data from production data. An IS auditor is not required to use production data or a test data generator. Production master files should not be updated with test data.

QUESTION 371
A clerk changed the interest rate for a loan on a master file. The rate entered is outside the normal range for such a loan. Which of the following controls is MOST effective in providing reasonable assurance that the change was authorized?

A. The system will not process the change until the clerk's manager confirms the change by entering an approval code.
B. The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager.
C. The system requires the clerk to enter an approval code.
D. The system displays a warning message to the clerk.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choice A would prevent or detect the use of an unauthorized interest rate. Choice B informs the manager after the fact that a change was made, thereby making it possible for transactions to use an unauthorized rate prior to management review. Choices C and D do not prevent the clerk from entering an unauthorized rate change.

QUESTION 372
The GREATEST advantage of using web services for the exchange of information between two systems is:

A. secure communications.
B. improved performance.
C. efficient interfacing.
D. enhanced documentation.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

QUESTION 373
An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are in place. The BEST response the auditor can make is to:

A. review the integrity of system access controls.
B. accept management's statement that effective access controls are in place.
C. stress the importance of having a system control framework in place.
D. review the background checks of the accounts payable staff.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Experience has demonstrated that reliance purely on preventative controls is dangerous. Preventative controls may not prove to be as strong as anticipated or their effectiveness can deteriorate over time. Evaluating the cost of controls versus the quantum of risk is a valid management concern. However, in a high-risk system a comprehensive control framework is needed, intelligent design should permit additional detective and corrective controls to be established that don't have high ongoing costs, e.g., automated interrogation of logs to highlight suspicious individual transactions or data patterns. Effective access controls are, in themselves, a positive but, for reasons outlined above, may not sufficiently compensate for other control weaknesses. In this situation the IS auditor needs to be proactive. The IS auditor has a fundamental obligation to point out control weaknesses that give rise to unacceptable risks to the organization and work with management to have these corrected. Reviewing background checks on accounts payable staff does not provide evidence that fraud will not occur.

QUESTION 374
When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

A. excessive transaction turnaround time.
B. application interface failure.
C. improper transaction authorization.
D. no validated batch totals.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Foremost among the risks associated with electronic data interchange (EDI) is improper transaction authorization. Since the interaction with the parties is electronic, there is no inherent authentication. The other choices, although risks, are not as significant.

QUESTION 375
When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

A. The risks associated with the use of the products are periodically assessed
B. The latest version of software is listed for each product
C. Due to licensing issues the list does not contain open source software
D. After hours' support is offered

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since the business conditions surrounding vendors may change, it is important for an organization to conduct periodic risk assessments of the vendor software list. This might be best incorporated into the IT risk management process. Choices B, C and D are possible considerations but would not be the most important.

QUESTION 376
An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

A. reverse engineering.
B. prototyping.
C. software reuse.
D. reengineering.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

QUESTION 377
An IS auditor performing an application maintenance audit would review the log of program changes for the:

A. authorization of program changes.
B. creation date of a current object module.
C. number of program changes actually made.
D. creation date of a current source program.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a changelog would most likely contain date information for the source and executable modules.

QUESTION 378
After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?

A. Stress
B. Black box
C. Interface
D. System

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.

QUESTION 379
When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?

A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.
B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
C. A single implementation is planned, immediately decommissioning the legacy system.
D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risks. Decommissioning or disposing of the old hardware would complicate any fallback strategy, should the new system not operate correctly. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

QUESTION 380
Which of the following reports should an IS auditor use to check compliance with a service level agreements (SLA) requirement for uptime?

A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.
QUESTION 381
A benefit of quality of service (QoS) is that the:

A. entire network's availability and performance will be significantly improved.
B. telecom carrier will provide the company with accurate service-level compliance reports.
C. participating applications will have guaranteed service levels.
D. communications link will be supported by security controls to perform secure online transactions.

Correct Answer: C
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation:
The main function of QoS is to optimize network performance by assigning priority to business applications and end users, through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

QUESTION 382
An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

A. Overall number of users supported
B. Percentage of incidents solved in the first call
C. Number of incidents reported to the help desk
D. Number of agents answering the phones

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since it is about service level (performance) indicators, the percentage of incidents solved on the first call is the only option that is relevant. Choices A, C and D are not quality measures of the help desk service.

QUESTION 383
The PRIMARY objective of service-level management (SLM) is to:
A. define, agree, record and manage the required levels of service.
B. ensure that services are managed to deliver the highest achievable level of availability.
C. keep the costs associated with any service at a minimum.
D. monitor and report any legal noncompliance to business management.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The objective of service-level management (SLM) is to negotiate, document and manage (i.e., provide and monitor) the services in the manner in which the customer requires those services. This does not necessarily ensure that services are delivered at the highest achievable level of availability (e.g., redundancy and clustering). Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb. SLM cannot ensure that costs for all services will be kept at a low or minimum level, since costs associated with a service will directly reflect the customer's requirements. Monitoring and reporting legal noncompliance is not a part of SLM.

QUESTION 384
Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

A. Minimizing costs for the services provided
B. Prohibiting the provider from subcontracting services
C. Evaluating the process for transferring knowledge to the IT department
D. Determining if the services were provided as contracted

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is acceptable, seamless and in line with contractual agreements. Minimizing costs, if applicable and achievable (depending on the customer's need) is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department. Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements. Subcontracting providers could be a concern, but it would not be the primary concern. Transferring knowledge to the internal IT department might be desirable under certain circumstances, but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.

QUESTION 385
IT best practices for the availability and continuity of IT services should:
A. minimize costs associated with disaster-resilient components.
B. provide for sufficient capacity to meet the agreed upon demands of the business.
C. provide reasonable assurance that agreed upon obligations to customers can be met.
D. produce timely performance metric reports.

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is important that negotiated and agreed commitments (i.e., service level agreements [SLAs]) can be fulfilled all the time. If this were not achievable, IT should not have agreed to these requirements, as entering into such a commitment would be misleading to the business. 'All the time' in this context directly relates to the 'agreed obligations' and does not imply that a service has to be available 100 percent of the time. Costs are a result of availability and service continuity management and may only be partially controllable. These costs directly reflect the agreed upon obligations. Capacity management is a necessary, but not sufficient, condition of availability.
Despite the possibility that a lack of capacity may result in an availability issue, providing the capacity necessary for seamless operations of services would be done within capacity management, and not within availability management. Generating reports might be a task of availability and service continuity management, but that is true for many other areas of interest as well (e.g., incident, problem, capacity and change management).

QUESTION 386
During a human resources (HR) audit, an IS auditor is informed that there is a verbal agreement between the IT and HR departments as to the level of IT services expected. In this situation, what should the IS auditor do FIRST?

A. Postpone the audit until the agreement is documented
B. Report the existence of the undocumented agreement to senior management
C. Confirm the content of the agreement with both departments
D. Draft a service level agreement (SLA) for the two departments

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor should first confirm and understand the current practice before making any recommendations. The agreement can be documented after it has been established that there is an agreement in place. The fact that there is not a written agreement does not justify postponing the audit, and reporting to senior management is not necessary at this stage of the audit. Drafting a service level agreement (SLA) is not the IS auditor's responsibility.
QUESTION 387
Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

A. The use of diskless workstations
B. Periodic checking of hard drives

C. The use of current antivirus software
D. policies that result in instant dismissal if violated

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software, unless the software contains a virus. Diskless workstations act as a preventive control and are not effective, since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

QUESTION 388
To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

A. System access log files
B. Enabled access control software parameters
C. Logs of access control violations
D. System configuration files for control options used

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

QUESTION 389
Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?
A. A system downtime log
B. Vendors' reliability figures
C. Regularly scheduled maintenance log
D. A written preventive maintenance schedule

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

QUESTION 390
Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

A. Sensitive data can be read by operators.
B. Data can be amended without authorization.
C. Unauthorized report copies can be printed.
D. Output can be lost in the event of system failure.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operations. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

QUESTION 391
Applying a retention date on a file will ensure that:

A. data cannot be read until the date is set. B.
data will not be deleted before that date.
C. backup copies are not retained after that date.
D. datasets having the same name are differentiated.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

QUESTION 392
Which of the following is a network diagnostic tool that monitors and records network information?

A. Online monitor
B. Downtime report
C. Help desk report
D. Protocol analyzer

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

QUESTION 393
Which of the following will help detect changes made by an intruder to the system log of a server?

A. Mirroring the system log on another server

B. Simultaneously duplicating the system log on a write-once disk
C. Write-protecting the directory containing the system log
D. Storing the backup of the system log offsite

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write-protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

QUESTION 394
IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
B. The service provider does not have incident handling procedures.
C. Recently a corrupted database could not be recovered because of library management problems.
D. incident logs are not being reviewed.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

QUESTION 395
Which of the following BEST ensures the integrity of a server's operating system?

A. Protecting the server in a secure location
B. Setting a boot password

C. Hardening the server configuration
D. Implementing activity logging

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Hardening a system means to configure it in the most secure manner (install latest security patches, properly define the access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenario-it is a detective control (not a preventive one), and the attacker who already gained privileged access can modify logs or disable them.

QUESTION 396
The MOST significant security concerns when using flash memory (e.g., USB removable disk) is that the:

A. contents are highly volatile.
B. data cannot be backed up.
C. data can be copied.
D. device may not be compatible with other peripherals.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Unless properly controlled, flash memory provides an avenue for anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other peripheral; therefore, compatibility is not an issue.

QUESTION 397
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 398
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 399
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 400
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 401
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 402
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 403
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 404
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 405
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 406
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 407
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 408
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 409

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 410
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 411
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 412
During maintenance of a relational database, several values of the foreign key in a transaction table of a relational database have been corrupted. The consequence is that:

A. the detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processed.
B. there is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transactions.
C. the database will immediately stop execution and lose more information.
D. the database will no longer accept input data.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When the external key of a transaction is corrupted or lost, the application system will normally be incapable of directly attaching the master data to the transaction data. This will normally cause the system to undertake a sequential search and slow down the processing. If the concerned files are big, this slowdown will be

unacceptable. Choice B is incorrect, since a system can recover the corrupted external key by reindexing the table. Choices C and D would not result from a corrupted foreign key.

QUESTION 413
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 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 414
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.
B. 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 415
A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

A. concurrent access.
B. deadlocks.
C. unauthorized access to data.
D. a loss of data integrity.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity. Deadlocks are not caused by denormalization. Access to data is controlled by defining user rights to information, and is not affected by denormalization.

QUESTION 416
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.
B. Centralize all request processing in one department to avoid parallel processing of the same request.
C. Change the application architecture so that common data are 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 417
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 418
An IS auditor finds that, at certain times of the day, the data warehouse query performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?
A. Permanent table-space allocation B.
Commitment and rollback controls
C. User spool and database limit controls
D. Read/write access log controls

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 419
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.

QUESTION 420
Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?
A. Parity check
B. Echo check
C. 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 421
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:
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 422
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 423
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 424
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 425
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 426
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 427
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 428
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 429
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 430
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 431
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 432
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 433
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 434
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 435
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 436
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 437
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 438
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 439
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 440
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 441
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 442
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 443
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 444
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 445
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 446
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 447
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 448
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 449
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 450
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 451
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 452
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 453
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 454
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 455
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 456
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 457
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 458
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 459
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 460
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 461
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 462
Neural networks are effective in detecting fraud because they can:

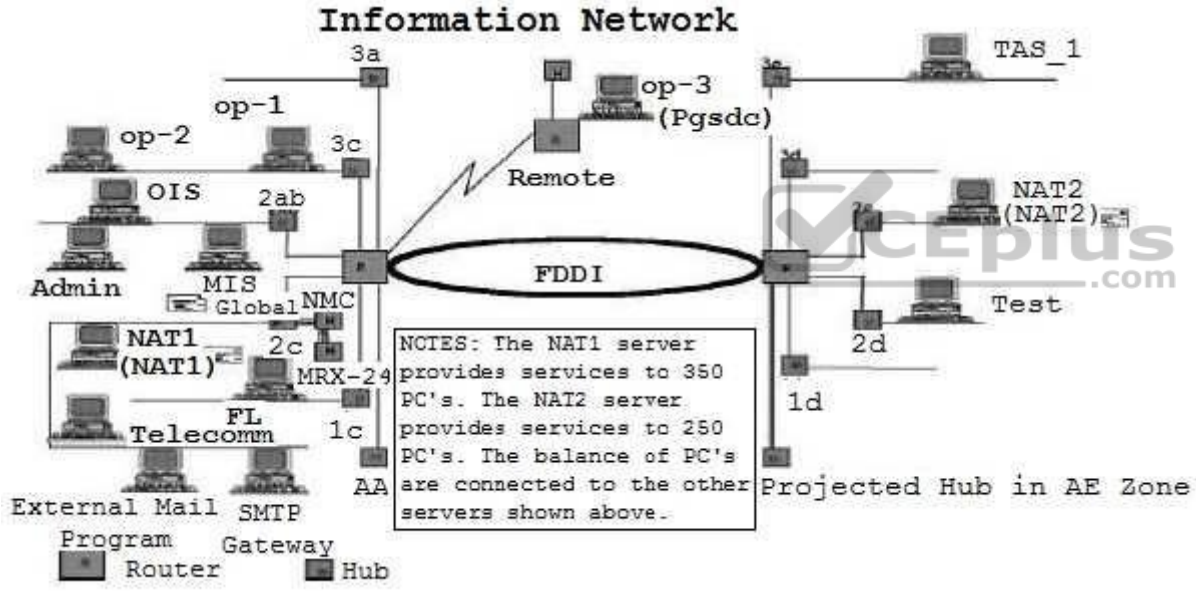
A. discover new trends since they are inherently linear.
B. solve problems where large and general sets of training data are not obtainable.
C. attack problems that require consideration of a large number of input variables.
D. make assumptions about the shape of any curve relating variables to the output.

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 463
Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?



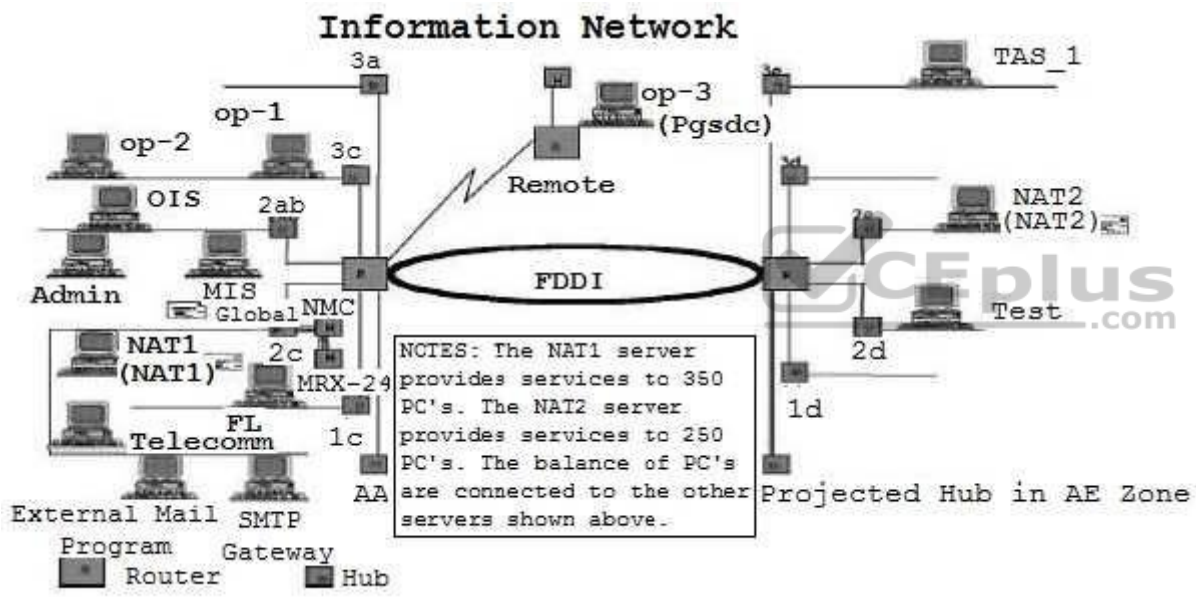
A. No firewalls are needed
B. Op-3 location only
C. MIS (Global) and NAT2
D. SMTP Gateway and op-3

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 464
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?



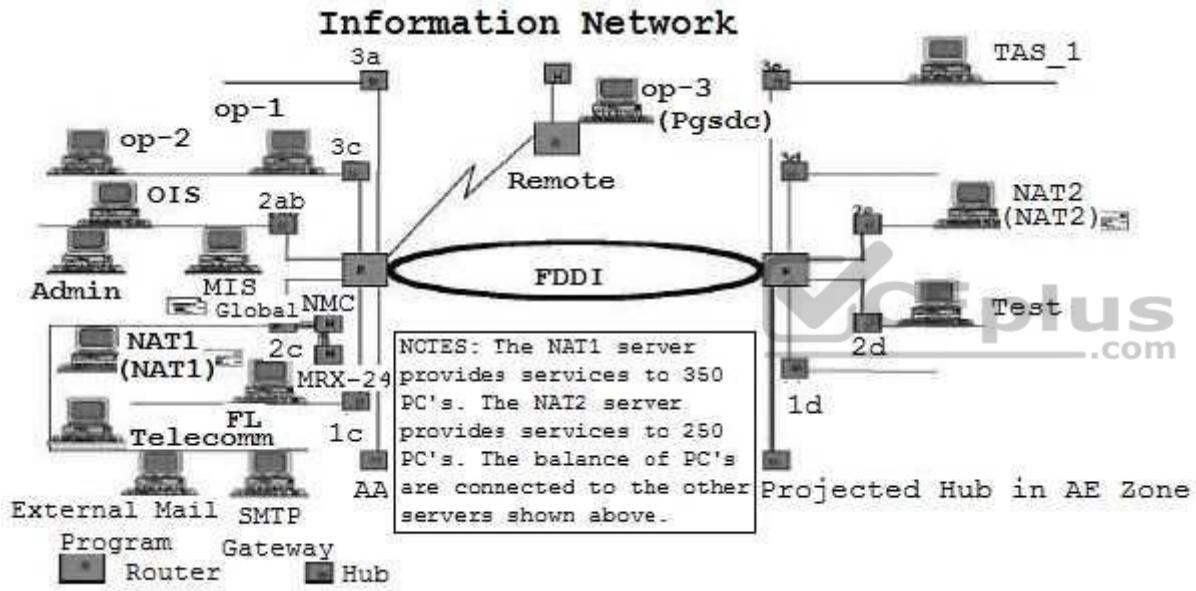
A. Intelligent hub
B. Physical security over the hubs
C. Physical security and an intelligent hub
D. No controls are necessary since this is not a weakness

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 465
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 466
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 467

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.

QUESTION 468
In what way is a common gateway interface (CGI) MOST often used on a webserver?

A. Consistent way for transferring data to the application program and back to the user
B. Computer graphics imaging method for movies and TV
C. Graphic user interface for web design
D. interface to access the private gateway domain

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word orienteering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

QUESTION 469
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:
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 470
Which of the following would be considered an essential feature of a network management system?

A. 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 471

The most likely error to occur when implementing a firewall is:

A. incorrectly configuring the access lists.
B. compromising the passwords due to social engineering.
C. connecting a modem to the computers in the network.
D. inadequately protecting the network and server from virus attacks.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An updated and flawless access list is a significant challenge and, therefore, has the greatest chance for errors at the time of the initial installation. Passwords do not apply to firewalls, a modem bypasses a firewall and a virus attack is not an element in implementing a firewall.

QUESTION 472
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 473
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 474
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 475
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 476
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 477

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 478
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 479
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 480
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 481
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 lT 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 482
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 483
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 484
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 485
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.

A.

QUESTION 486

An IS auditor examining the configuration of an operating system to verify the controls should review the:

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 487

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

A.
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 488
Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?
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 489
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.

A.

QUESTION 490

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 491
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 492
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 493
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 494
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 495
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 496
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 497
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 498
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 499
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 500
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 501
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 502
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 503

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 504
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 505
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 506
An IS auditor conducting an access control review in a client-server environment discovers that all printing options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:

A. exposure is greater, since information is available to unauthorized users.
B. operating efficiency is enhanced, since anyone can print any report at any time.
C. operating procedures are more effective, since information is easily available.
D. user friendliness and flexibility is facilitated, since there is a smooth flow of information among users.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside as electronic files, because print options allow for printing in an electronic form as well.

QUESTION 507
Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:

A. change the company's security policy.
B. educate users about the risk of weak passwords.

C. build in validations to prevent this during user creation and password change.
D. require a periodic review of matching user ID and passwords for detection and correction.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risks of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

QUESTION 508
The PRIMARY objective of a logical access control review is to:

A. review access controls provided through software.
B. ensure access is granted per the organization's authorities.
C. walk through and assess the access provided in the IT environment.
D. provide assurance that computer hardware is adequately protected against abuse.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The scope of a logical access control review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical access control review, rather than objectives. Choice D is relevant to a physical access control review.

QUESTION 509
Naming conventions for system resources are important for access control because they:

A. ensure that resource names are not ambiguous.
B. reduce the number of rules required to adequately protect resources.
C. ensure that user access to resources is clearly and uniquely identified.
D. ensure that internationally recognized names are used to protect resources.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Naming conventions for system resources are important for the efficient administration of security controls. The conventions can be structured, so resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous cannot be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

QUESTION 510
Which of the following exposures could be caused by a line grabbing technique?

A. Unauthorized data access
B. Excessive CPU cycle usage
C. Lockout of terminal polling
D. Multiplexor control dysfunction

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Line grabbing will enable eavesdropping, thus allowing unauthorized data access, it will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

QUESTION 511
Electromagnetic emissions from a terminal represent an exposure because they:

A. affect noise pollution.
B. disrupt processor functions.
C. produce dangerous levels of electric current.
D. can be detected and displayed.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Emissions can be detected by sophisticated equipment and displayed, thus giving unauthorized persons access to data. They should not cause disruption of CPUs or effect noise pollution.

QUESTION 512
Security administration procedures require read-only access to:

A. access control tables.
B. security log files.
C. logging options.
D. user profiles.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update the way the transactions and user activities are monitored, captured, stored, processed and reported.

QUESTION 513
With the help of a security officer, granting access to data is the responsibility of:

A. data owners.
B. programmers.
C. system analysts.
D. librarians.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners' approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (e.g., read or update).

QUESTION 514
The FIRST step in data classification is to:
A. establish ownership.
B. perform a criticality analysis.
C. define access rules.
D. create a data dictionary.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Data classification is necessary to define access rules based on a need-to-do and need-to- know basis. The data owner is responsible for defining the access rules; therefore, establishing ownership is the first step in data classification. The other choices are incorrect. A criticality analysis is required for protection of data, which takes input from data classification. Access definition is complete after data classification and input for a data dictionary is prepared from the data classification process.

QUESTION 515
Which of the following provides the framework for designing and developing logical access controls?

A. Information systems security policy
B. Access control lists
C. Password management
D. System configuration files

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The information systems security policy developed and approved by an organization's top management is the basis upon which logical access control is designed and developed. Access control lists, password management and systems configuration files are tools for implementing the access controls.

QUESTION 516
A hacker could obtain passwords without the use of computer tools or programs through the technique of:

A. social engineering.
B. sniffers.
C. back doors.
D. Trojan horses.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Social engineering is based on the divulgence of private information through dialogues, interviews, inquiries, etc., in which a user may be indiscreet regarding their or someone else's personal datA. A sniffer is a computer tool to monitor the traffic in networks. Back doors are computer programs left by hackers to exploit

vulnerabilities. Trojan horses are computer programs that pretend to supplant a real program; thus, the functionality of the program is not authorized and is usually malicious in nature.

QUESTION 517
The reliability of an application system's audit trail may be questionable if:

A. user IDs are recorded in the audit trail.
B. the security administrator has read-only rights to the audit file.
C. date and time stamps are recorded when an action occurs.
D. users can amend audit trail records when correcting system errors.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An audit trail is not effective if the details in it can be amended.

QUESTION 518
Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an EFT system?

A. Three users with the ability to capture and verify their own messages
B. Five users with the ability to capture and send their own messages
C. Five users with the ability to verify other users and to send their own messages
D. Three users with the ability to capture and verify the messages of other users and to send their own messages

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The ability of one individual to capture and verify messages represents an inadequate segregation, since messages can be taken as correct and as if they had already been verified.

QUESTION 519

An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

A. critical
B. vital.
C. sensitive.
D. noncritical.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Sensitive functions are best described as those that can be performed manually at a tolerable cost for an extended period of time. Critical functions are those that cannot be performed unless they are replaced by identical capabilities and cannot be replaced by manual methods. Vital functions refer to those that can be performed manually but only for a brief period of time; this is associated with lower costs of disruption than critical functions. Noncritical functions may be interrupted for an extended period of time at little or no cost to the company, and require little time or cost to restore.

QUESTION 520
The implementation of access controls FIRST requires:

A. a classification of IS resources.
B. the labeling of IS resources.
C. the creation of an access control list.
D. an inventory of IS resources.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
QUESTION 521
Which of the following is an example of the defense in-depth security principle?

A. Using two firewalls of different vendors to consecutively check the incoming network traffic
B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic

C. Having no physical signs on the outside of a computer center building
D. Using two firewalls in parallel to check different types of incoming traffic

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Defense in-depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

QUESTION 522
Which of the following would be the BEST access control procedure?

A. The data owner formally authorizes access and an administrator implements the user authorization tables.
B. Authorized staff implements the user authorization tables and the data owner sanctions them.
C. The data owner and an IS manager jointly create and update the user authorization tables.
D. The data owner creates and updates the user authorization tables.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedure for authorizing access.

QUESTION 523
Which of the following would MOST effectively reduce social engineering incidents?

A. Security awareness training
B. increased physical security measures
C. E-mail monitoring policy

D. intrusion detection systems

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the intrusion. An e-mail monitoring policy informs users that all e- mail in the organization is subject to monitoring; it does not protect the users from potential security incidents and intruders. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

QUESTION 524
An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

A. Piggybacking
B. Dumpster diving
C. Shoulder surfing
D. Impersonation

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If a password is displayed on a monitor, any person nearby could look over the shoulder of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to 'the display of passwords.' If the policy referred to 'the display and printing of passwords' then it would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information), impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

QUESTION 525
To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

A. the company policy be changed.

B. passwords are periodically changed.
C. an automated password management tool be used.
D. security awareness training is delivered.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing their old password for a designated period of time. Choices A, B and D do not enforce compliance.

QUESTION 526
An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

A. more than one individual can claim to be a specific user.
B. there is no way to limit the functions assigned to users.
C. user accounts can be shared.
D. users have a need-to-know privilege.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Without an appropriate authorization process, it will be impossible to establish functional limits and accountability. The risk that more than one individual can claim to be a specific user is associated with the authentication processes, rather than with authorization. The risk that user accounts can be shared is associated with identification processes, rather than with authorization. The need-to-know basis is the best approach to assigning privileges during the authorization process.

QUESTION 527
An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

A. Digitalized signatures
B. Hashing
C. Parsing

D. Steganography

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Steganography is a technique for concealing the existence of messages or information. An increasingly important stenographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes, and is widely applied in the design of programming languages or in data entry editing.

QUESTION 528
The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

A. Piggybacking
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have their badge read at every controlled door no unauthorized person could enter the sensitive areA. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

QUESTION 529
Which of the following presents an inherent risk with no distinct identifiable preventive controls?

A. Piggybacking
B. Viruses
C. Data diddling
D. Unauthorized application shutdown

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses, because it requires limited technical knowledge and occurs before computer security can protect the data. There are only compensating controls for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-re plicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdown of an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which is effective if there are proper access controls.

QUESTION 530
Which of the following is a general operating system access control function?

A. Creating database profiles
B. Verifying user authorization at a field level
C. Creating individual accountability
D. Logging database access activities for monitoring access violation

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Creating individual accountability is the function of the general operating system. Creating database profiles, verifying user authorization at a field level and logging database access activities for monitoring access violations are all database-level access control functions.

QUESTION 531
Which of the following BEST restricts users to those functions needed to perform their duties?

A. Application level access control
B. Data encryption
C. Disabling floppy disk drives
D. Network monitoring device

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of application-level access control programs is a management control that restricts access by limiting users to only those functions needed to perform their duties. Data encryption and disabling floppy disk drives can restrict users to specific functions, but are not the best choices. A network monitoring device is a detective control, not a preventive control.

QUESTION 532
For a discretionary access control to be effective, it must:

A. operate within the context of mandatory access controls.
B. operate independently of mandatory access controls.
C. enable users to override mandatory access controls when necessary.
D. be specifically permitted by the security policy.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Mandatory access controls are prohibitive; anything that is not expressly permitted is forbidden. Only within this context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. When systems enforce mandatory access control policies, they must distinguish between these and the mandatory access policies that offer more flexibility.
Discretionary controls do not override access controls and they do not have to be permitted in the security policy to be effective.

QUESTION 533

An IS auditor examining a biometric user authentication system establishes the existence of a control weakness that would allow an unauthorized individual to update the centralized database on the server that is used to store biometric templates. Of the following, which is the BEST control against this risk?

A. Kerberos
B. Vitality detection
C. Multimodal biometrics
D. Before-image/after-image logging

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Kerberos is a network authentication protocol for client-server applications that can be used to restrict access to the database to authorized users. Choices B and C are incorrect because vitality detection and multimodal biometrics are controls against spoofing and mimicry attacks. Before-image/after-image logging of database transactions is a detective control, as opposed to Kerberos, which is a preventative control.

QUESTION 534
From a control perspective, the PRIMARY objective of classifying information assets is to:

A. establish guidelines for the level of access controls that should be assigned.
B. ensure access controls are assigned to all information assets.
C. assist management and auditors in risk assessment.
D. identify which assets need to be insured against losses.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Information has varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources, management can establish guidelines for the level of access controls that should be assigned. End user management and the security administrator will use these classifications in their risk assessment process to assign a given class to each asset.

QUESTION 535

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 536
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 537
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 538
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 539
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 540
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 541
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 542
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 543

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 544
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 545

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 546
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 547
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 548
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 549
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 550
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 551
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 552
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 553
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 554
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 555
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 556
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 557
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 558
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 559
What method might an IS auditor utilize to test wireless security at branch office locations?

A. War dialing
B. Social engineering
C. War driving
D. Password cracking
Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

War driving is a technique for locating and gaining access to wireless networks by driving or walking with a wireless equipped computer around a building. War dialing is a technique for gaining access to a computer or a network through the dialing of defined blocks of telephone numbers, with the hope of getting an answer from a modem. Social engineering is a technique used to gather information that can assist an attacker in gaining logical or physical access to data or resources. Social engineering exploits human weaknesses. Password crackers are tools used to guess users' passwords by trying combinations and dictionary words.

QUESTION 560
In a public key infrastructure, a registration authority:

A. verifies information supplied by the subject requesting a certificate.
B. issues the certificate after the required attributes are verified and the keys are generated.
C. digitally signs a message to achieve nonrepudiation of the signed message.
D. registers signed messages to protect them from future repudiation.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A registration authority is responsible for verifying information supplied by the subject requesting a certificate, and verifies the requestor's right to request certificate attributes and that the requestor actually possesses the private key corresponding to the public key being sent.
Certification authorities, not registration authorities, actually issue certificates once verification of the information has been completed; because of this, choice B is incorrect. On the other hand, the sender who has control of their private key signs the message, not the registration authority. Registering signed messages is not a task performed by registration authorities.

QUESTION 561
Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is:

A. restricted to predefined MAC addresses.
B. encrypted using static keys.
C. encrypted using dynamic keys.
D. initiated from devices that have encrypted storage.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
When using dynamic keys, the encryption key is changed frequently, thus reducing the risk of the key being compromised and the message being decrypted. Limiting the number of devices that can access the network does not address the issue of encrypting the session. Encryption with static keys-using the same key for a long period of time-risks that the key would be compromised. Encryption of the data on the connected device (laptop, PDA, etc.) addresses the confidentiality of the data on the device, not the wireless session.

QUESTION 562
Which of the following provides the MOST relevant information for proactively strengthening security settings?

A. Bastion host
B. Intrusion detection system
C. Honeypot
D. Intrusion prevention system

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The design of a honeypot is such that it lures the hacker and provides clues as to the hacker's methods and strategies and the resources required to address such attacks. A bastion host does not provide information about an attack. Intrusion detection systems and intrusion prevention systems are designed to detect and address an attack in progress and stop it as soon as possible. A honeypot allows the attack to continue, so as to obtain information about the hacker's strategy and methods.

QUESTION 563
Over the long term, which of the following has the greatest potential to improve the security incident response process?

A. A walkthrough review of incident response procedures
B. Postevent reviews by the incident response team
C. Ongoing security training for users
D. Documenting responses to an incident

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:

Explanation:
Postevent reviews to find the gaps and shortcomings in the actual incident response processes will help to improve the process over time. Choices A, C and D are desirable actions, but postevent reviews are the most reliable mechanism for improving security incident response processes.

QUESTION 564
When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

A. Number of nonthreatening events identified as threatening
B. Attacks not being identified by the system
C. Reports/logs being produced by an automated tool
D. Legitimate traffic being blocked by the system

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Attacks not being identified by the system present a higher risk, because they are unknown and no action will be taken to address the attack. Although the number of false-positives is a serious issue, the problem will be known and can be corrected. Often, IDS reports are first analyzed by an automated tool to eliminate known false-positives, which generally are not a problem. An IDS does not block any traffic.

QUESTION 565
Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

A. Logic bombs
B. Phishing
C. Spyware
D. Trojan horses

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Trojan horses are malicious or damaging code hidden within an authorized computer program. Hackers use Trojans to mastermind DDOS attacks that affect computers that access the same Internet site at the same moment, resulting in overloaded site servers that may no longer be able to process legitimate requests.

Logic bombs are programs designed to destroy or modify data at a specific time in the future. Phishing is an attack, normally via e-mail, pretending to be an authorized person or organization requesting information. Spyware is a program that picks up information from PC drives by making copies of their contents.

QUESTION 566
Validated digital signatures in an e-mail software application will:

A. help detect spam.
B. provide confidentiality.
C. add to the workload of gateway servers.
D. significantly reduce available bandwidth.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Validated electronic signatures are based on qualified certificates that are created by a certification authority (CA), with the technical standards required to ensure the key can neither be forced nor reproduced in a reasonable time. Such certificates are only delivered through a registration authority (RA) after a proof of identity has been passed. Using strong signatures in e- mail traffic, nonrepudiation can be assured and a sender can be tracked. The recipient can configure their e-mail server or client to automatically delete e-mails from specific senders. For confidentiality issues, one must use encryption, not a signature, although both methods can be based on qualified certificates. Without any filters directly applied on mail gateway servers to block traffic without strong signatures, the workload will not increase. Using filters directly on a gateway server will result in an overhead less than antivirus software imposes. Digital signatures are only a few bytes in size and will not slash bandwidth. Even if gateway servers were to check CRLs, there is little overhead.

QUESTION 567
In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

A. connectionless integrity.
B. data origin authentication.
C. antireplay service.
D. confidentiality.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Both protocols support choices A, B and C, but only the ESP protocol provides confidentiality via encryption.

QUESTION 568
An IS auditor notes that IDS log entries related to port scanning are not being analyzed. This lack of analysis will MOST likely increase the risk of success of which of the following attacks?

A. Denial-of-service
B. Replay
C. Social engineering
D. Buffer overflow

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Prior to launching a denial-of-service attack, hackers often use automatic port scanning software to acquire information about the subject of their attack. A replay attack is simply sending the same packet again. Social engineering exploits end-user vulnerabilities, and buffer overflow attacks exploit poorly written code.

QUESTION 569
IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

A. Port scanning
B. Back door
C. Man-in-the-middle

D. War driving

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A war driving attack uses a wireless Ethernet card, set in promiscuous mode, and a powerful antenna to penetrate wireless systems from outside. Port scanning will often target the external firewall of the organization. A back door is an opening left in software that enables an unknown entry into a system. Man-in-the-middle attacks intercept a message and either replace or modify it.

QUESTION 570
Which of the following encryption techniques will BEST protect a wireless network from a man-in-the-middle attack?

A. 128-bit wired equivalent privacy (WEP)
B. MAC-based pre-shared key(PSK)
C. Randomly generated pre-shared key (PSKJ
D. Alphanumeric service set identifier (SSID)

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A randomly generated PSK is stronger than a MAC-based PSK, because the MAC address of a computer is fixed and often accessible. WEP has been shown to be a very weak encryption technique and can be cracked within minutes. The SSID is broadcast on the wireless network in plaintext.

QUESTION 571
The IS management of a multinational company is considering upgrading its existing virtual private network (VPN) to support voice-over IP (VoIP) communications via tunneling. Which of the following considerations should be PRIMARILY addressed?

A. Reliability and quality of service (QoS)
B. Means of authentication
C. Privacy of voice transmissions
D. Confidentiality of data transmissions

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The company currently has a VPN; issues such as authentication and confidentiality have been implemented by the VPN using tunneling. Privacy of voice transmissions is provided by the VPN protocol. Reliability and QoS are, therefore, the primary considerations to be addressed.

QUESTION 572
Which of the following antispam filtering techniques would BEST prevent a valid, variable- length e-mail message containing a heavily weighted spam keyword from being labeled as spam?

A. Heuristic (rule-based)
B. Signature-based
C. Pattern matching
D. Bayesian (statistical)

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Bayesian filtering applies statistical modeling to messages, by performing a frequency analysis on each word within the message and then evaluating the message as a whole. Therefore, it can ignore a suspicious keyword if the entire message is within normal bounds. Heuristic filtering is less effective, since new exception rules may need to be defined when a valid message is labeled as spam. Signature-based filtering is useless against variable- length messages, because the calculated MD5 hash changes all the time. Finally, pattern matching is actually a degraded rule- based technique, where the rules operate at the word level using wildcards, and not at higher levels.

QUESTION 573
Which of the following public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key?

A. Certificate revocation list (CRL)
B. Certification practice statement (CPS)
C. Certificate policy (CP)
D. PKI disclosure statement (PDS)

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The CPS is the how-to part in policy-based PKI. The CRL is a list of certificates that have been revoked before their scheduled expiration date. The CP sets the requirements that are subsequently implemented by the CPS. The PDS covers critical items such as the warranties, limitations and obligations that legally bind each party.

QUESTION 574
Active radio frequency ID (RFID) tags are subject to which of the following exposures?

A. Session hijacking
B. Eavesdropping
C. Malicious code
D. Phishing

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Like wireless devices, active RFID tags are subject to eavesdropping. They are by nature not subject to session hijacking, malicious code or phishing.

QUESTION 575
When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

A. Use the IP address of an existing file server or domain controller.
B. Pause the scanning every few minutes to allow thresholds to reset. C. Conduct the scans during evening hours when no one is logged-in.
D. Use multiple scanning tools since each tool has different characteristics.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Pausing the scanning every few minutes avoids overtaxing the network as well as exceeding thresholds that may trigger alert messages to the network administrator. Using the IP address of a server would result in an address contention that would attract attention. Conducting scans after hours would increase the chance of detection, since there would be less traffic to conceal ones activities. Using different tools could increase the likelihood that one of them would be detected by an intrusion detection system.

QUESTION 576
Two-factor authentication can be circumvented through which of the following attacks?

A. Denial-of-service
B. Man-in-the-middle
C. Key logging
D. Brute force

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A man-in-the-middle attack is similar to piggybacking, in that the attacker pretends to be the legitimate destination, and then merely retransmits whatever is sent by the authorized user along with additional transactions after authentication has been accepted. A denial-of- service attack does not have a relationship to authentication. Key logging and brute force could circumvent a normal authentication but not a two-factor authentication.

QUESTION 577
An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

A. digitally signing all e-mail messages.
B. encrypting all e-mail messages.
C. compressing all e-mail messages.
D. password protecting all e-mail messages.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity. Password protecting all e-mail messages would ensure that only those who have the password would be able to open the message; however, it would not ensure the authenticity of the sender.

QUESTION 578
Sending a message and a message hash encrypted by the sender's private key will ensure:

A. authenticity and integrity.
B. authenticity and privacy.
C. integrity and privacy.
D. privacy and nonrepudiation.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If the sender sends both a message and a message hash encrypted by its private key, then the receiver can apply the sender's public key to the hash and get the message hash. The receiver can apply the hashing algorithm to the message received and generate a hash. By matching the generated hash with the one received, the receiver is ensured that the message has been sent by the specific sender, i.e., authenticity, and that the message has not been changed enroute. Authenticity and privacy will be ensured by first using the sender's private key and then the receiver's public key to encrypt the message. Privacy and integrity can be ensured by using the receiver's public key to encrypt the message and sending a message hash/digest. Only nonrepudiation can be ensured by using the sender's private key to encrypt the message. The sender's public key, available to anyone, can decrypt a message; thus, it does not ensure privacy.

QUESTION 579
Which of the following is a passive attack to a network?

A. Message modification
B. Masquerading
C. Denial of service
D. Traffic analysis

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The intruder determines the nature of the flow of traffic (traffic analysis) between defined hosts and is able to guess the type of communication taking place. Message modification involves the capturing of a message and making unauthorized changes or deletions, changing the sequence or delaying transmission of captured messages. Masquerading is an active attack in which the intruder presents an identity other than the original identity. Denial of service occurs when a computer connected to the internet is flooded with data and/or requests that must be processed.

QUESTION 580
An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. An IS auditor recommends replacing the non-upgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

A. The new access points with stronger security are affordable.
B. The old access points are poorer in terms of performance.
C. The organization's security would be as strong as its weakest points.
D. The new access points are easier to manage.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The old access points should be discarded and replaced with products having strong security; otherwise, they will leave security holes open for attackers and thus make the entire network as weak as they are. Affordability is not the auditor's major concern. Performance is not as important as security in this situation. Product manageability is not the IS auditor's concern.

QUESTION 581
An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

A. encrypting the hash of the newsletter using the advisor's private key.
B. encrypting the hash of the newsletter using the advisor's public key.
C. digitally signing the document using the advisor's private key.
D. encrypting the newsletter using the advisor's private key.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
There is no attempt on the part of the investment advisor to prove their identity or to keep the newsletter confidential. The objective is to assure the receivers that it came to them without any modification, i.e., it has message integrity. Choice A is correct because the hash is encrypted using the advisor's private key. The recipients can open the newsletter, recompute the hash and decrypt the received hash using the advisor's public key. If the two hashes are equal, the newsletter was not modified in transit. Choice B is not feasible, for no one other than the investment advisor can open it. Choice C addresses sender authentication but not message integrity. Choice D addresses confidentiality, but not message integrity, because anyone can obtain the investment advisor's public key, decrypt the newsletter, modify it and send it to others. The interceptor will not be able to use the advisor's private key, because they do not have it. Anything encrypted using the interceptor's private key can be decrypted by the receiver only by using their public key.

QUESTION 582
An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol is disabled at all wireless access points. This practice:

A. reduces the risk of unauthorized access to the network.

B. is not suitable for small networks.
C. automatically provides an IP address to anyone.
D. increases the risks associated with Wireless Encryption Protocol (WEP).

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to anyone connected to the network. With DHCP disabled, static IP addresses must be used and represent less risk due to the potential for address contention between an unauthorized device and existing devices on the network. Choice B is incorrect because DHCP is suitable for small networks.
Choice C is incorrect because DHCP does not provide IP addresses when disabled. Choice D is incorrect because disabling of the DHCP makes it more difficult to exploit the well-known weaknesses in WEP.

QUESTION 583
A virtual private network (VPN) provides data confidentiality by using:

A. Secure Sockets Layer (SSL)
B. Tunneling
C. Digital signatures
D. Phishing

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
VPNs secure data in transit by encapsulating traffic, a process known as tunneling. SSL is a symmetric method of encryption between a server and a browser. Digital signatures are not used in the VPN process, while phishing is a form of a social engineering attack.

QUESTION 584
In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

A. common gateway interface (CGI) scripts.
B. enterprise Java beans (EJBs).
C. applets.
D. web services.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Common gateway interface (CGI) scripts are executable machine independent software programs on the server that can be called and executed by a web server page. CGI performs specific tasks such as processing inputs received from clients. The use of CGI scripts needs to be evaluated, because as they run in the server, a bug in them may allow a user to gain unauthorized access to the server and from there gain access to the organization's network.
Applets are programs downloaded from a web server and executed on web browsers on client machines to run any web-based applications. Enterprise java beans (EJBs) and web services have to be deployed by the web server administrator and are controlled by the application server. Their execution requires knowledge of the parameters and expected return values.

QUESTION 585
An IS auditor reviewing access controls for a client-server environment should FIRST:

A. evaluate the encryption technique.

B. identify the network access points.
C. review the identity management system.
D. review the application level access controls.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A client-server environment typically contains several access points and utilizes distributed techniques, increasing the risk of unauthorized access to data and processing. To evaluate the security of the client server environment, all network access points should be identified. Evaluating encryption techniques, reviewing the identity management system and reviewing the application level access controls would be performed at a later stage of the review.

QUESTION 586
To prevent IP spoofing attacks, a firewall should be configured to drop a packet if:

A. the source routing field is enabled.
B. it has a broadcast address in the destination field.
C. a reset flag (RST) is turned on for the TCP connection.
D. dynamic routing is used instead of static routing.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
IP spoofing takes advantage of the source-routing option in the IP protocol. With this option enabled, an attacker can insert a spoofed source IP address. The packet will travel the network according to the information within the source-routing field, bypassing the logic in each router, including dynamic and static routing (choice D). Choices B and C do not have any relation to IP spoofing attacks. If a packet has a broadcast destination address (choice B), it will be sent to all addresses in the subnet. Turning on the reset flag (RST) (choice C) is part of the normal procedure to end a TCP connection.

QUESTION 587
An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

A. IDS sensors are placed outside of the firewall.
B. a behavior-based IDS is causing many false alarms.

C. a signature-based IDS is weak against new types of attacks.
D. the IDS is used to detect encrypted traffic.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An intrusion detection system (IDS) cannot detect attacks within encrypted traffic, and it would be a concern if someone was misinformed and thought that the IDS could detect attacks in encrypted traffic. An organization can place sensors outside of the firewall to detect attacks.
These sensors are placed in highly sensitive areas and on extranets. Causing many false alarms is normal for a behavior-based IDS, and should not be a matter of concern. Being weak against new types of attacks is also expected from a signature- based IDS, because it can only recognize attacks that have been previously identified.

QUESTION 588
Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

A. Encrypts the information transmitted over the network
B. Makes other users' certificates available to applications
C. Facilitates the implementation of a password policy
D. Stores certificate revocation lists (CRLs)
Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A directory server makes other users' certificates available to applications. Encrypting the information transmitted over the network and storing certificate revocation lists (CRLs) are roles performed by a security server. Facilitating the implementation of a password policy is not relevant to public key infrastructure (PKI).

QUESTION 589
An organization is using symmetric encryption. Which of the following would be a valid reason for moving to asymmetric encryption? Symmetric encryption:

A. provides authenticity.
B. is faster than asymmetric encryption.
C. can cause key management to be difficult.

D. requires a relatively simple algorithm.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In a symmetric algorithm, each pair of users' needs a unique pair of keys, so the number of keys grows and key management can become overwhelming. Symmetric algorithms do not provide authenticity, and symmetric encryption is faster than asymmetric encryption. Symmetric algorithms require mathematical calculations, but they are not as complex as asymmetric algorithms.

QUESTION 590
Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

A. A remote access server
B. A proxy server
C. A personal firewall
D. A password-generating token

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A personal firewall is the best way to protect against hacking, because it can be defined with rules that describe the type of user or connection that is or is not permitted. A remote access server can be mapped or scanned from the Internet, creating security exposures. Proxy servers can provide protection based on the IP address and ports; however, an individual would need to have in-depth knowledge to do this, and applications can use different ports for the different sections of their program. A password-generating token may help to encrypt the session but does not protect a computer against hacking.

QUESTION 591
When installing an intrusion detection system (IDS), which of the following is MOST important?

A. Properly locating it in the network architecture
B. Preventing denial-of-service (DoS) attacks
C. Identifying messages that need to be quarantined
D. Minimizing the rejection errors

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Proper location of an intrusion detection system (IDS) in the network is the most important decision during installation. A poorly located IDS could leave key areas of the network unprotected. Choices B, C and D are concerns during the configuration of an IDS, but if the IDS is not placed correctly, none of them would be adequately addressed.

QUESTION 592
In a public key infrastructure (PKI), which of the following may be relied upon to prove that an online transaction was authorized by a specific customer?

A. Nonrepudiation
B. Encryption
C. Authentication
D. Integrity

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Nonrepudiation, achieved through the use of digital signatures, prevents the claimed sender from later denying that they generated and sent the message. Encryption may protect the data transmitted over the Internet, but may not prove that the transactions were made. Authentication is necessary to establish the identification of all parties to a communication. Integrity ensures that transactions are accurate but does not provide the identification of the customer.

QUESTION 593
Which of the following ensures confidentiality of information sent over the internet?

A. Digital signature
B. Digital certificate
C. Online Certificate Status Protocol
D. Private key cryptosystem

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Confidentiality is assured by a private key cryptosystem. Digital signatures assure data integrity, authentication and nonrepudiation, but not confidentially. A digital certificate is a certificate that uses a digital signature to bind together a public key with an identity; therefore, it does not address confidentiality. Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of a digital certificate.

QUESTION 594
To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:

A. access control servers.
B. session border controllers.
C. backbone gateways.
D. intrusion detection system (IDS).

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Session border controllers enhance the security in the access network and in the core. In the access network, they hide a user's real address and provide a managed public address. This public address can be monitored, minimizing the opportunities for scanning and denial-of-service (DoS) attacks. Session border controllers permit access to clients behind firewalls while maintaining the firewall's effectiveness. In the core, session border controllers protect the users and the network. They hide network topology and users' real addresses. They can also monitor bandwidth and quality of service. Securing the access control server, backbone gateways and intrusion detection systems (IDSs) does not effectively protect against DoS attacks.

QUESTION 595
Which of the following attacks targets the Secure Sockets Layer (SSL)?

A. Man-in-the middle
B. Dictionary
C. Password sniffing
D. Phishing

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Attackers can establish a fake Secure Sockets Layer (SSL) server to accept user's SSL traffic and then route to the real SSL server, so that sensitive information can be discovered. A dictionary attack that has been launched to discover passwords would not attack SSL since SSL does not rely on passwords. SSL traffic is encrypted; thus it is not possible to sniff the password. A phishing attack targets a user and not SSL Phishing attacks attempt to have the user surrender private information by falsely claiming to be a trusted person or enterprise.

QUESTION 596
Which of the following potentially blocks hacking attempts?

A. intrusion detection system
B. Honeypot system
C. Intrusion prevention system
D. Network security scanner

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An intrusion prevention system (IPS) is deployed as an in-line device that can detect and block hacking attempts. An intrusion detection system (IDS) normally is deployed in sniffing mode and can detect intrusion attempts, but cannot effectively stop them. A honeypot solution traps the intruders to explore a simulated target. A network security scanner scans for the vulnerabilities, but it will not stop the intrusion.

QUESTION 597
A web server is attacked and compromised. Which of the following should be performed FIRST to handle the incident?
A. Dump the volatile storage data to a disk.
B. Run the server in a fail-safe mode.
C. Disconnect the web server from the network.
D. Shut down the web server.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The first action is to disconnect the web server from the network to contain the damage and prevent more actions by the attacker. Dumping the volatile storage data to a disk may be used at the investigation stage but does not contain an attack in progress. To run the server in a fail-safe mode, the server needs to be shut down. Shutting down the server could potentially erase information that might be needed for a forensic investigation or to develop a strategy to prevent future similar attacks.

QUESTION 598
To address a maintenance problem, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a:

A. Secure Shell (SSH-2) tunnel for the duration of the problem.
B. two-factor authentication mechanism for network access.
C. dial-in access.
D. virtual private network (VPN) account for the duration of the vendor support contract.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
For granting temporary access to the network, a Secure Shell (SSH-2) tunnel is the best approach. It has auditing features and allows restriction to specific access points. Choices B, C and D all give full access to the internal network. Two-factor authentication and virtual private network (VPN) provide access to the entire network and are suitable for dedicated users. Dial-in access would need to be closely monitored or reinforced with another mechanism to ensure authentication to achieve the same level of security as SSH-2.

QUESTION 599
What is the BEST approach to mitigate the risk of a phishing attack?
A. implement an intrusion detection system (IDS)
B. Assess web site security
C. Strong authentication
D. User education

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Phishing attacks can be mounted in various ways; intrusion detection systems (IDSs) and strong authentication cannot mitigate most types of phishing attacks. Assessing web site security does not mitigate the risk. Phishing uses a server masquerading as a legitimate server. The best way to mitigate the risk of phishing is to educate users to take caution with suspicious internet communications and not to trust them until verified. Users require adequate training to recognize suspicious web pages and e-mail.

QUESTION 600
A sender of an e-mail message applies a digital signature to the digest of the message. This action provides assurance of the:

A. date and time stamp of the message.
B. identity of the originating computer.
C. confidentiality of the message's content.
D. authenticity of the sender.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The signature on the digest can be used to authenticate the sender. It does not provide assurance of the date and time stamp or the identity of the originating computer. Digitally signing an e-mail message does not prevent access to its content and, therefore, does not assure confidentiality.

QUESTION 601
The BEST filter rule for protecting a network from being used as an amplifier in a denial of service (DoS) attack is to deny all:

A. outgoing traffic with IP source addresses externa! to the network.
B. incoming traffic with discernible spoofed IP source addresses.
C. incoming traffic with IP options set.
D. incoming traffic to critical hosts.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Outgoing traffic with an IP source address different than the IP range in the network is invalid, in most of the cases, it signals a DoS attack originated by an internal user or by a previously compromised internal machine; in both cases, applying this filter will stop the attack.

QUESTION 602
The network of an organization has been the victim of several intruders' attacks. Which of the following measures would allow for the early detection of such incidents?

A. Antivirus software
B. Hardening the servers
C. Screening routers
D. Honeypots

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Honeypots can collect data on precursors of attacks. Since they serve no business function, honeypots are hosts that have no authorized users other than the honeypot administrators. All activity directed at them is considered suspicious. Attackers will scan and attack honeypots, giving administrators data on new trends and attack tools, particularly malicious code. However, honeypots are a supplement to, not a replacement for, properly securing networks, systems and applications. If honeypots are to be used by an organization, qualified incident handlers and intrusion detection analysts should manage them. The other choices do not provide indications of potential attacks.

QUESTION 603
A company has decided to implement an electronic signature scheme based on public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The MOST significant risk of this approach is:

A. use of the user's electronic signature by another person if the password is compromised.
B. forgery by using another user's private key to sign a message with an electronic signature.
C. impersonation of a user by substitution of the user's public key with another person's public key.
D. forgery by substitution of another person's private key on the computer.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The user's digital signature is only protected by a password. Compromise of the password would enable access to the signature. This is the most significant risk.
Choice B would require subversion of the public key infrastructure mechanism, which is very difficult and least likely.
Choice C would require that the message appear to have come from a different person and therefore the true user's credentials would not be forged. Choice D has the same consequence as choice C.

QUESTION 604
An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is MOST important?

A. The tools used to conduct the test
B. Certifications held by the IS auditor
C. Permission from the data owner of the server
D. An intrusion detection system (IDS) is enabled

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The data owner should be informed of the risks associated with a penetration test, what types of tests are to be conducted and other relevant details. All other choices are not as important as the data owner's responsibility for the security of the data assets.

QUESTION 605
After observing suspicious activities in a server, a manager requests a forensic analysis.
Which of the following findings should be of MOST concern to the investigator?
A. Server is a member of a workgroup and not part of the server domain

B. Guest account is enabled on the server
C. Recently, 100 users were created in the server
D. Audit logs are not enabled for the server

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Audit logs can provide evidence which is required to proceed with an investigation and should not be disabled. For business needs, a server can be a member of a workgroup and, therefore, not a concern. Having a guest account enabled on a system is a poor security practice but not a forensic investigation concern. Recently creating 100 users in the server may have been required to meet business needs and should not be a concern.

QUESTION 606
Which of the following would be the GREATEST cause for concern when data are sent over the Internet using HTTPS protocol?

A. Presence of spyware in one of the ends
B. The use of a traffic sniffing tool
C. The implementation of an RSA-compliant solution
D. A symmetric cryptography is used for transmitting data

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Encryption using secure sockets layer/transport layer security (SSL/TLS) tunnels makes it difficult to intercept data in transit, but when spyware is running on an end user's computer, data are collected before encryption takes place. The other choices are related to encrypting the traffic, but the presence of spyware in one of the ends captures the data before encryption takes place.

QUESTION 607
A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?

A. Reviewing logs frequently
B. Testing and validating the rules

C. Training a local administrator at the new location
D. Sharing firewall administrative duties

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A mistake in the rule set can render a firewall insecure. Therefore, testing and validating the rules is the most important factor in ensuring a successful deployment. A regular review of log files would not start until the deployment has been completed. Training a local administrator may not be necessary if the firewalls are managed from a central location. Having multiple administrators is a good idea, but not the most important.

QUESTION 608
The human resources (HR) department has developed a system to allow employees to enroll in benefits via a web site on the corporate Intranet. Which of the following would protect the confidentiality of the data?

A. SSL encryption
B. Two-factor authentication
C. Encrypted session cookies
D. IP address verification

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The main risk in this scenario is confidentiality, therefore the only option which would provide confidentiality is Secure Socket Layer (SSL) encryption. The remaining options deal with authentication issues.

QUESTION 609
What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

A. Malicious code could be spread across the network
B. VPN logon could be spoofed
C. Traffic could be sniffed and decrypted

D. VPN gateway could be compromised

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
VPN is a mature technology; VPN devices are hard to break. However, when remote access is enabled, malicious code in a remote client could spread to the organization's network. Though choices B, C and D are security risks, VPN technology largely mitigates these risks.

QUESTION 610
The use of digital signatures:

A. requires the use of a one-time password generator.
B. provides encryption to a message.
C. validates the source of a message.
D. ensures message confidentiality.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of a digital signature verifies the identity of the sender, but does not encrypt the whole message, and hence is not enough to ensure confidentiality. A onetime password generator is an option, but is not a requirement for using digital signatures.

QUESTION 611
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 612
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 613
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 electricityC. 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 614
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 615
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 616
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 617
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 618
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 619
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 620
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 621
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 622
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 623
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 624
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 625
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 626
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 627
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 628
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 629
Which of the following is the MOST reliable form of single factor personal identification?

A. Smart card
B. Password
C. Photo identification
D. iris scan

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Since no two irises are alike, identification and verification can be done with confidence. There is no guarantee that a smart card is being used by the correct person since it can be shared, stolen or lost and found. Passwords can be shared and, if written down, carry the risk of discovery. Photo IDs can be forged or falsified.

QUESTION 630
A data center has a badge-entry system. Which of the following is MOST important to protect the computing assets in the center?

A. Badge readers are installed in locations where tampering would be noticed
B. The computer that controls the badge system is backed up frequently
C. A process for promptly deactivating lost or stolen badges exists
D. All badge entry attempts are logged

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Tampering with a badge reader cannot open the door, so this is irrelevant. Logging the entry attempts may be of limited value. The biggest risk is from unauthorized individuals who can enter the data center, whether they are employees or not. Thus, a process of deactivating lost or stolen badges is important. The configuration of the system does not change frequently, therefore frequent backup is not necessary.

QUESTION 631
Which of the following physical access controls effectively reduces the risk of piggybacking?

A. Biometric door locks
B. Combination door locks
C. Deadman doors
D. Bolting door locks

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Deadman doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding areA. This effectively reduces the risk of piggybacking. An individual's unique body features such as voice, retina, fingerprint or signature activate biometric door locks;

however, they do not prevent or reduce the risk of piggybacking. Combination door locks, also known as cipher locks, use a numeric key pad or dial to gain entry. They do not prevent or reduce the risk of piggybacking since unauthorized individuals may still gain access to the processing center. Bolting door locks require the traditional metal key to gain entry. Unauthorized individuals could still gain access to the processing center along with an authorized individual.

QUESTION 632
The MOST effective biometric control system is the one:

A. which has the highest equal-error rate (EER).
B. which has the lowest EER.
C. for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
D. for which the FRR is equal to the failure-to-enroll rate (FER).

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The equal-error rate (EER) of a biometric system denotes the percent at which the false- acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of FRR.

QUESTION 633
Which of the following is the BEST way to satisfy a two-factor user authentication?
A. A smart card requiring the user's PIN
B. User ID along with password
C. Iris scanning plus fingerprint scanning
D. A magnetic card requiring the user's PIN

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). An ID and password, what the user knows, is a single-factor user authentication. Choice C is not a two- factor user authentication

because it is only biometric. Choice D is similar to choice A, but the magnetic card may be copied; therefore, choice A is the best way to satisfy a two-factor user authentication.

QUESTION 634
What should an organization do before providing an external agency physical access to its information processing facilities (IPFs)?

A. The processes of the external agency should be subjected to an IS audit by an independent agency.
B. Employees of the external agency should be trained on the security procedures of the organization.
C. Any access by an external agency should be limited to the demilitarized zone (DMZ).
D. The organization should conduct a risk assessment and design and implement appropriate controls.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Physical access of information processing facilities (IPFs) by an external agency introduces additional threats into an organization. Therefore, a risk assessment should be conducted and controls designed accordingly. The processes of the external agency are not of concern here. It is the agency's interaction with the organization that needs to be protected. Auditing their processes would not be relevant in this scenario. Training the employees of the external agency may be one control procedure, but could be performed after access has been granted. Sometimes an external agency may require access to the processing facilities beyond the demilitarized zone (DMZ). For example, an agency which undertakes maintenance of servers may require access to the main server room. Restricting access within the DMZ will not serve the purpose.

QUESTION 635
An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:
A. nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
B. access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
C. card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
D. the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Physical security is meant to control who is entering a secured area, so identification of all individuals is of utmost importance. It is not adequate to trust unknown external people by allowing them to write down their alleged name without proof, e.g., identity card, driver's license. Choice B is not a concern because if the name and address of the organization was written on the card, a malicious finder could use the card to enter the organization's premises. Separating card issuance from technical rights management is a method to ensure a proper segregation of duties so that no single person can produce a functioning card for a restricted area within the organization's premises. Choices B and C are good practices, not concerns. Choice D may be a concern, but not as important since a system failure of the card programming device would normally not mean that the readers do not function anymore. It simply means that no new cards can be issued, so this option is minor compared to the threat of improper identification.

QUESTION 636
Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

A. Overwriting the tapes
B. initializing the tape labels
C. Degaussing the tapes
D. Erasing the tapes

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

QUESTION 637
Which of the following is the MOST important objective of data protection?
A. identifying persons who need access to information
B. Ensuring the integrity of information
C. Denying or authorizing access to the IS system
D. Monitoring logical accesses

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

QUESTION 638
Which of the following aspects of symmetric key encryption influenced the development of asymmetric encryption?

A. Processing power
B. Volume of data
C. Key distribution
D. Complexity of the algorithm

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Symmetric key encryption requires that the keys be distributed. The larger the user group, the more challenging the key distribution. Symmetric key cryptosystems are generally less complicated and, therefore, use less processing power than asymmetric techniques, thus making it ideal for encrypting a large volume of data. The major disadvantage is the need to get the keys into the hands of those with whom you want to exchange data, particularly in e-commerce environments, where customers are unknown, untrusted entities

QUESTION 639
A hard disk containing confidential data was damaged beyond repair. What should be done to the hard disk to prevent access to the data residing on it?

A. Rewrite the hard disk with random Os and Is.

B. Low-level format the hard disk.
C. Demagnetize the hard disk.
D. Physically destroy the hard disk.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Physically destroying the hard disk is the most economical and practical way to ensure that the data cannot be recovered. Rewriting data and low-level formatting are impractical, because the hard disk is damaged. Demagnetizing is an inefficient procedure, because it requires specialized and expensive equipment to be fully effective.

QUESTION 640
Which of the following is the MOST robust method for disposing of magnetic media that contains confidential information?

A. Degaussing
B. Defragmenting
C. Erasing
D. Destroying

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Destroying magnetic media is the only way to assure that confidential information cannot be recovered. Degaussing or demagnetizing is not sufficient to fully erase information from magnetic media. The purpose of defragmentation is to eliminate fragmentation in file systems and does not remove information. Erasing or deleting magnetic media does not remove the information; this method simply changes a file's indexing information.

QUESTION 641
Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

A. Policies that require instant dismissal if such devices are found
B. Software for tracking and managing USB storage devices
C. Administratively disabling the USB port

D. Searching personnel for USB storage devices at the facility's entrance

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Software for centralized tracking and monitoring would allow a USB usage policy to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management. A policy requiring dismissal may result in increased employee attrition and business requirements would not be properly addressed. Disabling ports would be complex to manage and might not allow for new business needs. Searching of personnel for USB storage devices at the entrance to a facility is not a practical solution since these devices are small and could be easily hidden.

QUESTION 642
An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

A. Run a low-level data wipe utility on all hard drives
B. Erase all data file directories
C. Format all hard drives
D. Physical destruction of the hard drive

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The most effective method is physical destruction. Running a low-level data wipe utility may leave some residual data that could be recovered; erasing data directories and formatting hard drives are easily reversed, exposing all data on the drive to unauthorized individuals.

QUESTION 643
To ensure authentication, confidentiality and integrity of a message, the sender should encrypt the hash of the message with the sender's:
A. public key and then encrypt the message with the receiver's private key.
B. private key and then encrypt the message with the receiver's public key.
C. public key and then encrypt the message with the receiver's public key.
D. private key and then encrypt the message with the receiver's private key.

Correct Answer: B

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Obtaining the hash of the message ensures integrity; signing the hash of the message with the sender's private key ensures the authenticity of the origin, and encrypting the resulting message with the receiver's public key ensures confidentiality. The other choices are incorrect.

QUESTION 644
Which of the following would be the MOST significant audit finding when reviewing a point-of-sale (POS) system?

A. invoices recorded on the POS system are manually entered into an accounting application
B. An optical scanner is not used to read bar codes for the generation of sales invoices
C. Frequent power outages occur, resulting in the manual preparation of invoices
D. Customer credit card information is stored unencrypted on the local POS system

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is important for the IS auditor to determine if any credit card information is stored on the local point-of-sale (POS) system. Any such information, if stored, should be encrypted or protected by other means to avoid the possibility of unauthorized disclosure. Manually inputting sale invoices into the accounting application is an operational issue, if the POS system were to be interfaced with the financial accounting application, the overall efficiency could be improved. The nonavailability of optical scanners to read bar codes of the products and power outages are operational issues.

QUESTION 645
When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?

A. Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization.
B. All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
C. Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
D. The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Deleting and formatting does not completely erase the data but only marks the sectors that contained files as being free. There are tools available over the Internet which allow one to reconstruct most of a hard disk's contents. Overwriting a hard disk at the sector level would completely erase data, directories, indices and master file tables. Reformatting is not necessary since all contents are destroyed. Overwriting several times makes useless some forensic measures which are able to reconstruct former contents of newly overwritten sectors by analyzing special magnetic features of the platter's surface. While hole-punching does not delete file contents, the hard disk cannot be used anymore, especially when head parking zones and track zero information are impacted. Reconstructing data would be extremely expensive since all analysis must be performed under a clean room atmosphere and is only possible within a short time frame or until the surface is corroded. Data reconstruction from shredded hard disks is virtually impossible, especially when the scrap is mixed with other metal parts. If the transport can be secured and the destruction be proved as described in the option, this is a valid method of disposal.

QUESTION 646
At a hospital, medical personal carry handheld computers which contain patient health data. These handheld computers are synchronized with PCs which transfer data from a hospital database. Which of the following would be of the most importance?

A. The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss.
B. The employee who deletes temporary files from the local PC, after usage, is authorized to maintain PCs.
C. Timely synchronization is ensured by policies and procedures.
D. The usage of the handheld computers is allowed by the hospital policy.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data confidentiality is a major requirement of privacy regulations. Choices B, C and D relate to internal security requirements, and are secondary when compared to compliance with data privacy laws.

QUESTION 647
Which of the following would BEST support 24/7 availability?

A. Daily backup
B. offsite storage
C. Mirroring
D. Periodic testing

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Mirroring of critical elements is a too! that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not of themselves support continuous availability.

QUESTION 648
The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:

A. achieve performance improvement.
B. provide user authentication.
C. ensure availability of data.
D. ensure the confidentiality of data.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk; if disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication and does nothing to provide for data confidentiality.

QUESTION 649
Which of the following is the MOST important criterion when selecting a location for an offsite storage facility for IS backup files? The offsite facility must be:

A. physically separated from the data center and not subject to the same risks.
B. given the same level of protection as that of the computer data center.
C. outsourced to a reliable third party.
D. equipped with surveillance capabilities.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

QUESTION 650
If a database is restored using before-image dumps, where should the process begin following an interruption?

A. Before the last transaction
B. After the last transaction
C. As the first transaction after the latest checkpoint
D. At the last transaction before the latest checkpoint

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.