CISA.exam.699q

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 type of testing has two major categories: QAT and UAT?

A. Interface testing
B. Unit Testing
C. System Testing
D. Final acceptance testing

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

Explanation/Reference:

QUESTION 2
Which of the following type of testing validate functioning of the application under test with other system, where a set of data is transferred from one system to another?

A. Interface testing
B. Unit Testing
C. System Testing
D. Final acceptance testing

Correct Answer: A

Section: Information System Acquisition, Development and Implementation
Explanation

Explanation/Reference:
Interface or integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

For CISA exam you should know below types of testing:

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.
Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team. The following specific analysis may be carried out during system testing.

Recovery Testing – Checking the systems ability to recover after a software or hardware failure.

Security Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems.

Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour.

Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process.

Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process.

Performance Testing – Comparing the system performance to other equivalent systems using well defined benchmarks.

Final Acceptance Testing -It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.
QAT focuses on documented specifications and the technology employed. It verifies that application works as documented by testing the logical design and the technology itself. It also ensures that the application meet the documented technical specifications and deliverables. QAT is performed primarily by IS department. The participation of end user is minimal and on request. QAT does not focus on functionality testing.

UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods include: Definition of test strategies and procedure. Design of test cases and scenarios Execution of the tests.
Utilization of the result to verify system readiness.
Acceptance criteria are defined criteria that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production possible.
The following were incorrect answers:

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensures internal operation of the programs according to the specification.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team.
Final Acceptance Testing – During this testing phase the defined methods of testing to apply should be incorporated into the organization's QA methodology.

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

CISA review manual 2014 Page number 166

QUESTION 3
Identify the INCORRECT statement from below mentioned testing types

A. Recovery Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems
B. Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour
C. Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process
D. Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process

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

Explanation/Reference:
The word INCORRECT is the keyword used in this question. You need to find out the incorrect option specified above. The term recovery testing is incorrectly defined in the above options. The correct description of recovery testing is: Recovery Testing – Checking the system’s ability to recover after a software or hardware failure

For CISA exam you should know below types of testing:

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.
Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.
System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team. The following specific analysis may be carried out during system testing.

Recovery Testing – Checking the system's ability to recover after a software or hardware failure.

Security Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems.

Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour.

Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process.

Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process.

Performance Testing – Comparing the system performance to other equivalent systems using well defined benchmarks.

Final Acceptance Testing -It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.
QAT focuses on documented specifications and the technology employed. It verifies that application works as documented by testing the logical design and the technology itself. It also ensures that the application meet the documented technical specifications and deliverables. QAT is performed primarily by IS department. The participation of end user is minimal and on request. QAT does not focus on functionality testing.
UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods
include: Definition of test strategies and procedure. Design of test cases and scenarios Execution of the tests.
Utilization of the result to verify system readiness.
Acceptance criteria are defined criteria that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production possible.

The following were incorrect answers:
The other options presented contains valid definitions.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 166

QUESTION 4
Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?

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

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

Explanation/Reference:
Regression testing is 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.

For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

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

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user's desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.

The following were incorrect answers:

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

Black Box Testing - An integrity based form of testing associated with testing components of an information system's "functional" operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 167

QUESTION 5
Which of the following is the process of feeding test data into two systems – the modified system and alternative system and comparing the result?

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

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

Explanation/Reference:

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

For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

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

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user’s desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs) , making operating system registry or configuration file modification, and possibly extra memory utilization.
The following were incorrect answers:

Regression Testing -The process of returning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 167

QUESTION 6
Which of the following statement correctly describes the difference between black box testing and white box testing?

A. Black box testing focuses on functional operative effectiveness where as white box assesses the effectiveness of software program logic
B. White box testing focuses on functional operative effectiveness where as black box assesses the effectiveness of software program logic
C. White box and black box testing focuses on functional operative effectiveness of an information systems without regard to any internal program structure
D. White box and black box testing focuses on the effectiveness of the software program logic

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

Explanation/Reference:
For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

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

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user's desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs) , making operating system registry or configuration file modification, and possibly extra memory utilization.

The following were incorrect answers:
The other options presented does not provides correct difference between black box and white box testing.

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

CISA review manual 2014 Page number 167

QUESTION 7
Which of the following data validation control validates input data against predefined range values?

A. Range Check
B. Table lookups
C. Existence check
D. Reasonableness check

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

Explanation/Reference:
In the Range Check control data should not exceed a predefined range of values

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check -Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check -Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

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

CISA review manual 2014 Page number 215

QUESTION 8
Which of the following control make sure that input data comply with predefined criteria maintained in computerized table of possible values?
A. Range Check B.
Table lookups
C. Existence check
D. Reasonableness check

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

Explanation/Reference:
In table lookups input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check - Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check - Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

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

CISA review manual 2014 Page number 215

QUESTION 9

John had implemented a validation check on the marital status field of a payroll record. A payroll record contains a field for marital status and acceptable status code are M for Married or S for Single. If any other code is entered, record should be rejected. Which of the following data validation control was implemented by John?

A. Range Check
B. Validity Check
C. Existence check
D. Reasonableness check

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

Explanation/Reference:

In a validity check control programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check -Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check -Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

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

CISA review manual 2014 Page number 215

QUESTION 10
While implementing an invoice system, Lily has implemented a database control which checks that new transactions are matched to those previously input to ensure that they have not already been entered. Which of the following control is implemented by Lily?

A. Range Check
B. Duplicate Check
C. Existence check
D. Reasonableness check

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

Explanation/Reference:
In a duplicate check control new transaction are matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check -Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check -Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

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

CISA review manual 2014 Page number 215

QUESTION 11
Hamid needs to shift users from using the application from the existing (Old) system to the replacing (new) system. His manager Lily has suggested he uses an approach in which the newer system is changed over from the older system on a cutoff date and time and the older system is discontinued once the changeover to the new system takes place. Which of the following changeover approach is suggested by Lily?

A. Parallel changeover
B. Phased changeover
C. Abrupt changeover
D. Pilot changeover

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

Explanation/Reference:
In the abrupt changeover approach the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once changeover to the new system takes place.
Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacing (new) system.

Changeover to newer system involves four major steps or activities
Conversion of files and programs; test running on test bed
Installation of new hardware, operating system, application system and the migrated data.
Training employees or user in groups
Scheduling operations and test running for go-live or changeover

Some of the risk areas related to changeover includes:

Asset safeguarding
Data integrity
System effectiveness

Change management challenges
Duplicate or missing records

The following were incorrect answers:

Parallel changeover – This technique includes running the old system, then running both the old and new systems in parallel and finally full changing over to the new system after gaining confidence in the working of new system.

Phased Changeover -In this approach the older system is broken into deliverables modules. Initially, the first module of older system is phased out using the first module of a new system. Then, the second module of the newer system is phased out, using the second module of the newer system and so forth until reaching the last module.

Pilot changeover – Not a valid changeover type.

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

CISA review manual 2014 Page number 172

QUESTION 12
William has been assigned a changeover task. He has to break the older system into deliverable modules. Initially, the first module of the older system is phased out using the first module of a new system. Then, the second module of the old system is phased out, using the second module of the newer system and so forth until reaching the last module. Which of the following changeover system William needs to implement?

A. Parallel changeover
B. Phased changeover
C. Abrupt changeover
D. Pilot changeover

Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation
Explanation/Reference:
In phased changeover approach, the older system is broken into deliverables modules. Initially, the first module of older system is phased out using the first module of a new system. Then, the second module of the newer system is phased out, using the second module of the newer system and so forth until reaching the last module.
Some of the risk areas that may exist in the phased changeover area includes:

Resource challenge
Extension of the project life cycle to cover two systems.

Change management for requirements and customizations to maintain ongoing support of the older systems.

Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacing (new) system.

Changeover to newer system involves four major steps or activities
Conversion of files and programs; test running on test bed
Installation of new hardware, operating system, application system and the migrated data.
Training employees or user in groups
Scheduling operations and test running for go-live or changeover

Some of the risk areas related to changeover includes:

Asset safeguarding
Data integrity
System effectiveness
Change management challenges
Duplicate or missing records

The following were incorrect answers:

Parallel changeover – This technique includes running the old system, then running both the old and new systems in parallel and finally full changing over to the new system after gaining confidence in the working of new system.

Abrupt changeover - In the abrupt changeover approach the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once changeover to the new system takes place.

Pilot changeover – Not a valid changeover type.

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

CISA review manual 2014 Page number 172

QUESTION 13
In which of the following payment mode, the payer creates payment transfer instructions, signs it digitally and sends it to issuer?

A. Electronic Money Model
B. Electronics Checks model
C. Electronic transfer model
D. Electronic withdraw model

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

Explanation/Reference:
Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

For CISA exam you should know below information about payment systems

There are two types of parties involved in all payment systems – the issuer and the user. An issuer is an entity that operates the payment service. An issuer holds the items that the payment represent. The user of the payment service performs two main functions- making payments and receiving payments – and therefore can be described as a payer or payee receptively.

Electronic Money Model -The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Transfer Model -Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

The following were incorrect answers:

Electronic Money Model -The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Withdraw Model – Not a valid type of payment system.

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

CISA review manual 2014 Page number 183

QUESTION 14

Which of the following method of expressing knowledge base consist of a graph in which nodes represent physical or conceptual objects and the arcs describes the relationship between nodes?

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

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

Explanation/Reference:
Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.

For CISA Exam you should know below information about Artificial Intelligence and Expert System
Artificial intelligence is the study and application of the principles by which:

Knowledge is acquired and used
Goals are generated and achieved
Information is communicated
Collaboration is achieved
Concepts are formed
Languages are developed

Two main programming languages that have been developed for artificial intelligence are LISP and PROLOG.
Expert system are compromised primary components, called shells, when they are not populated with particular data, and the shells are designed to host new expert system.

Keys to the system is the knowledge base (KB), which contains specific information or fact patterns associated with a particular subject matter and the rule for interpreting these facts. The KB interface with a database in obtaining data to analyze a particular problem in deriving an expert conclusion. The information in the KB can be expressed in several ways:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule – Expressing declarative knowledge through the use of if-then relationships. For example, if a patient's body temperature is over 39 degree Celsius and their pulse is under 60, then they might be suffering from a certain disease.

Semantic nets – Consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of a data.

Additionally, the inference engine shown is a program that uses the KB and determines the most appropriate outcome based on the information supplied by the user. In addition, an expert system includes the following components

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

Data Interface – Enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

The following were incorrect answers:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule - Expressing declarative knowledge through the use of if-then relationships.

Semantic nets - Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 187

QUESTION 15

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

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

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

Explanation/Reference:

Decision tree uses questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

For CISA Exam you should know below information about Artificial Intelligence and Expert System
Artificial intelligence is the study and application of the principles by which:

Knowledge is acquired and used
Goals are generated and achieved
Information is communicated
Collaboration is achieved
Concepts are formed
Languages are developed

Two main programming languages that have been developed for artificial intelligence are LISP and PROLOG.
Expert system are compromised primary components, called shells, when they are not populated with particular data, and the shells are designed to host new expert system.

Keys to the system is the knowledge base (KB), which contains specific information or fact patterns associated with a particular subject matter and the rule for interpreting these facts. The KB interface with a database in obtaining data to analyze a particular problem in deriving an expert conclusion. The information in the KB can be expressed in several ways:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule – Expressing declarative knowledge through the use of if-then relationships. For example, if a patient's body temperature is over 39 degree Celsius and their pulse is under 60, then they might be suffering from a certain disease.

Semantic nets – Consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of a data.

Additionally, the inference engine shown is a program that uses the KB and determines the most appropriate outcome based on the information supplied by the user. In addition, an expert system includes the following components

Knowledge interface – Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.
Data Interface – Enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

The following were incorrect answers:

Rule - Expressing declarative knowledge through the use of if-then relationships.

Semantic nets - Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.
Knowledge interface - Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

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

CISA review manual 2014 Page number 187

QUESTION 16
An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model depict data entities and how they relate?

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

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

Explanation/Reference:

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.
To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture
Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Context diagram -Outline the major processes of an organization and the external parties with which business interacts.

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Context diagram -Outline the major processes of an organization and the external parties with which business interacts.
Activity or swim-lane diagram – De-construct business processes.

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

CISA review manual 2014 Page number 188

QUESTION 17

An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model outline the major process of an organization and the external parties with which business interacts?

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

Correct Answer: A
Section: Information System Acquisition, Development and Implementation
Explanation
Explanation/Reference:
Context diagram -Outline the major processes of an organization and the external parties with which business interacts.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.
To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.
Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Context diagram -Outline the major processes of an organization and the external parties with which business interacts.
Activity or swim-lane diagram – De-construct business processes.

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

CISA review manual 2014 Page number 188

QUESTION 18
Which of the following layer of an enterprise data flow architecture is concerned with basic data communication?

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

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

Explanation/Reference:
Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.
For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.
To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

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

QUESTION 19
Which of the following layer of an enterprise data flow architecture is concerned with transporting information between the various layers?

A. Data preparation layer

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

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

Explanation/Reference:
Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.
For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.
To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.
Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

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

CISA review manual 2014 Page number 188

QUESTION 20
Which of the following layer of an enterprise data flow architecture does the scheduling of the tasks necessary to build and maintain the Data Warehouse (DW) and also populates Data Marts?

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

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

Explanation/Reference:
Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.
For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.
The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

QUESTION 21
Which of the following layer of an enterprise data flow architecture represents subset of information from the core Data Warehouse selected and organized to meet the needs of a particular business unit or business line?

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

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

Explanation/Reference:
Data Mart layer - Data mart represents subset of information from the core Data Warehouse selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure. For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.
Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

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

CISA review manual 2014 Page number 188

QUESTION 22
Which of the following layer of an enterprise data flow architecture is concerned with the assembly and preparation of data for loading into data marts?

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

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

Explanation/Reference:
Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture
Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.
Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

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

CISA review manual 2014 Page number 188

QUESTION 23
Which of the following layer of an enterprise data flow architecture is responsible for data copying, transformation in Data Warehouse (DW) format and quality control?

A. Data Staging and quality layer
B. Desktop Access Layer

C. Data Mart layer

D. Data access layer

Correct Answer: A

Section: Information System Acquisition, Development and Implementation

Explanation

Explanation/Reference:

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.
Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

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

CISA review manual 2014 Page number 188

QUESTION 24

Which of the following layer of an enterprise data flow architecture represents subsets of information from the core data warehouse?

A. Presentation layer
B. Desktop Access Layer
C. Data Mart layer
D. Data access layer

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

Explanation/Reference:

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure. For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:
Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

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

CISA review manual 2014 Page number 188

QUESTION 25
Which of the following layer from an enterprise data flow architecture captures all data of interest to an organization and organize it to assist in reporting and analysis?

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

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

Explanation/Reference:
Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry. For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.
To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components
The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database. Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

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

CISA review manual 2014 Page number 188

QUESTION 26
Which of the following layer in an enterprise data flow architecture derives enterprise information from operational data, external data and nonoperational data?

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

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

Explanation/Reference:
Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)
A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:
Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.
External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.
Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.
Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.
Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative 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 27
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 28

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 29

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

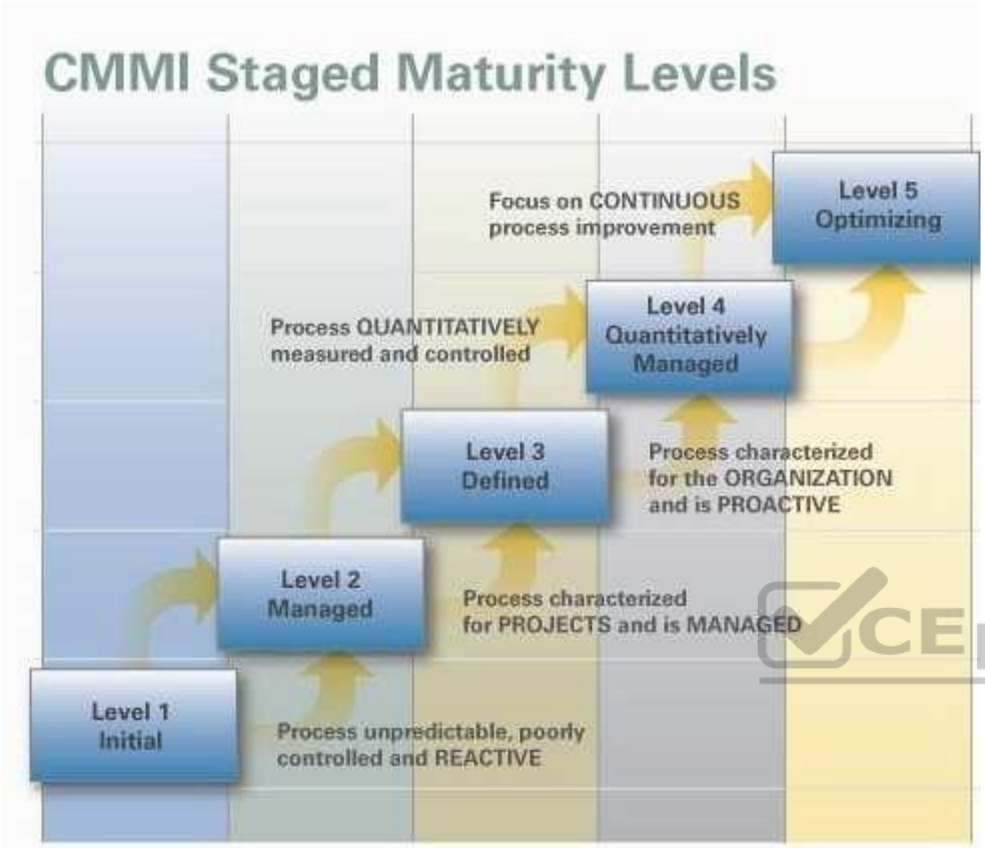
Correct Answer: B
Section: Information System Acquisition, Development and Implementation
Explanation

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


CMMI Staged Maturity Levels
Level 5 Optimizing
Focus on CONTINUOUS process improvement
Level 4 Quantitatively Managed
Process QUANTITATIVELY measured and controlled
Level 3 Defined
Process characterized for the ORGANIZATION and is PROACTIVE
Level 2 Managed
Process characterized for PROJECTS and is MANAGED
Level 1 Initial
Process unpredictable, poorly controlled and REACTIVE

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 30
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:

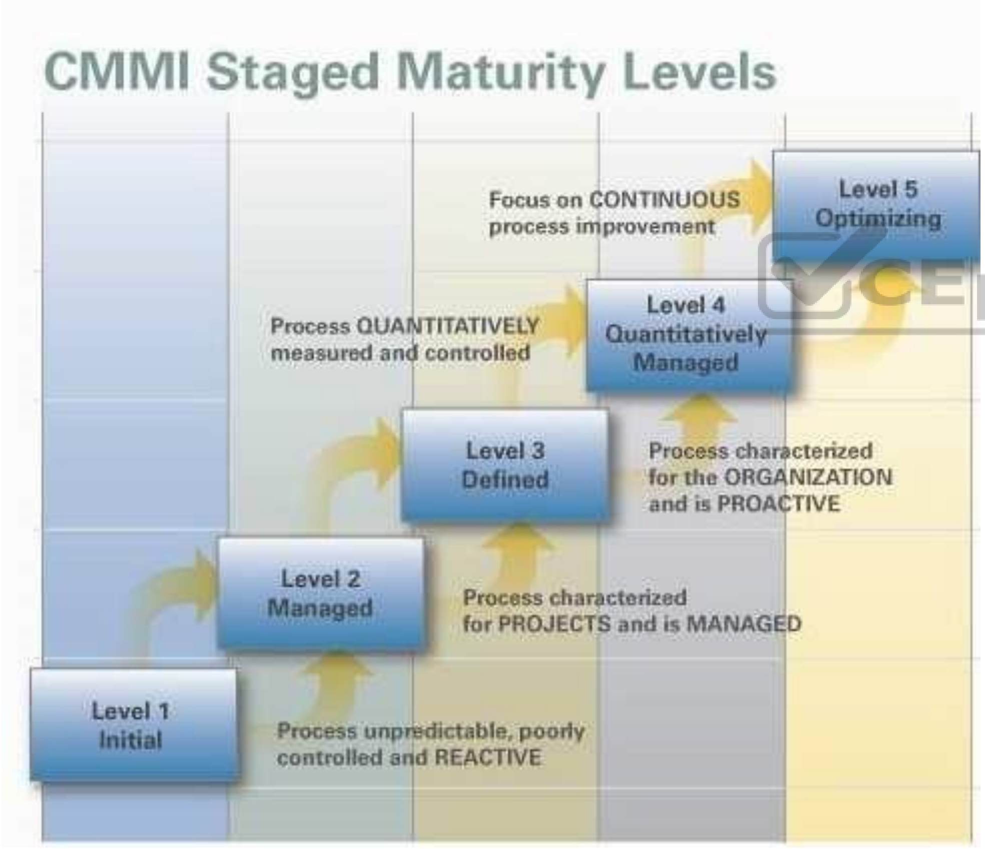
Level 3 is the defined step and focus on process definition and process deployment.

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


CMMI Staged Maturity Levels
Focus on CONTINUOUS process improvement
Level 5 Optimizing
Process QUANTITATIVELY measured and controlled
Level 4 Quantitatively Managed
Level 3 Defined
Process characterized for the ORGANIZATION and is PROACTIVE
Level 2 Managed
Process characterized for PROJECTS and is MANAGED
Level 1 Initial
Process unpredictable, poorly controlled and REACTIVE

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 31
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

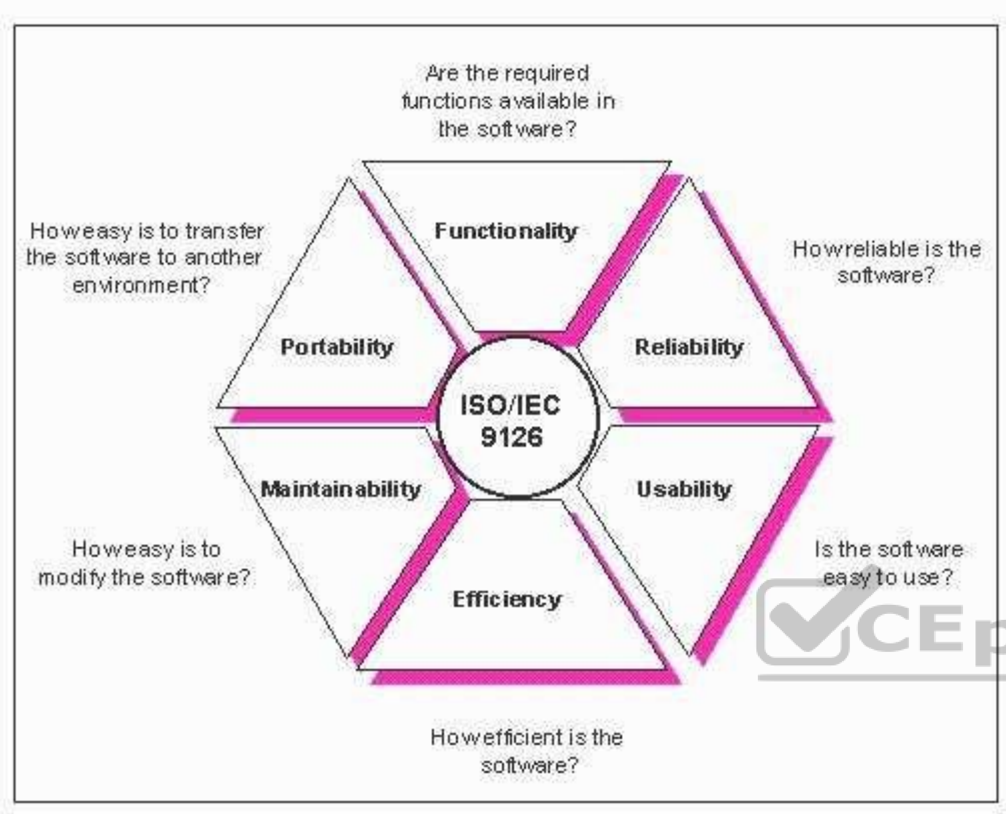

Are the required functions available in the software?
How easy is to transfer the software to another environment?
Functionality
How reliable is the software?
Portability
Reliability
ISO/IEC 9126
Maintainability
Usability
How easy is to modify the software?
Efficiency
Is the software easy to use?
How efficient is the software?

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 32
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 33

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 34
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 35

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 36
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?

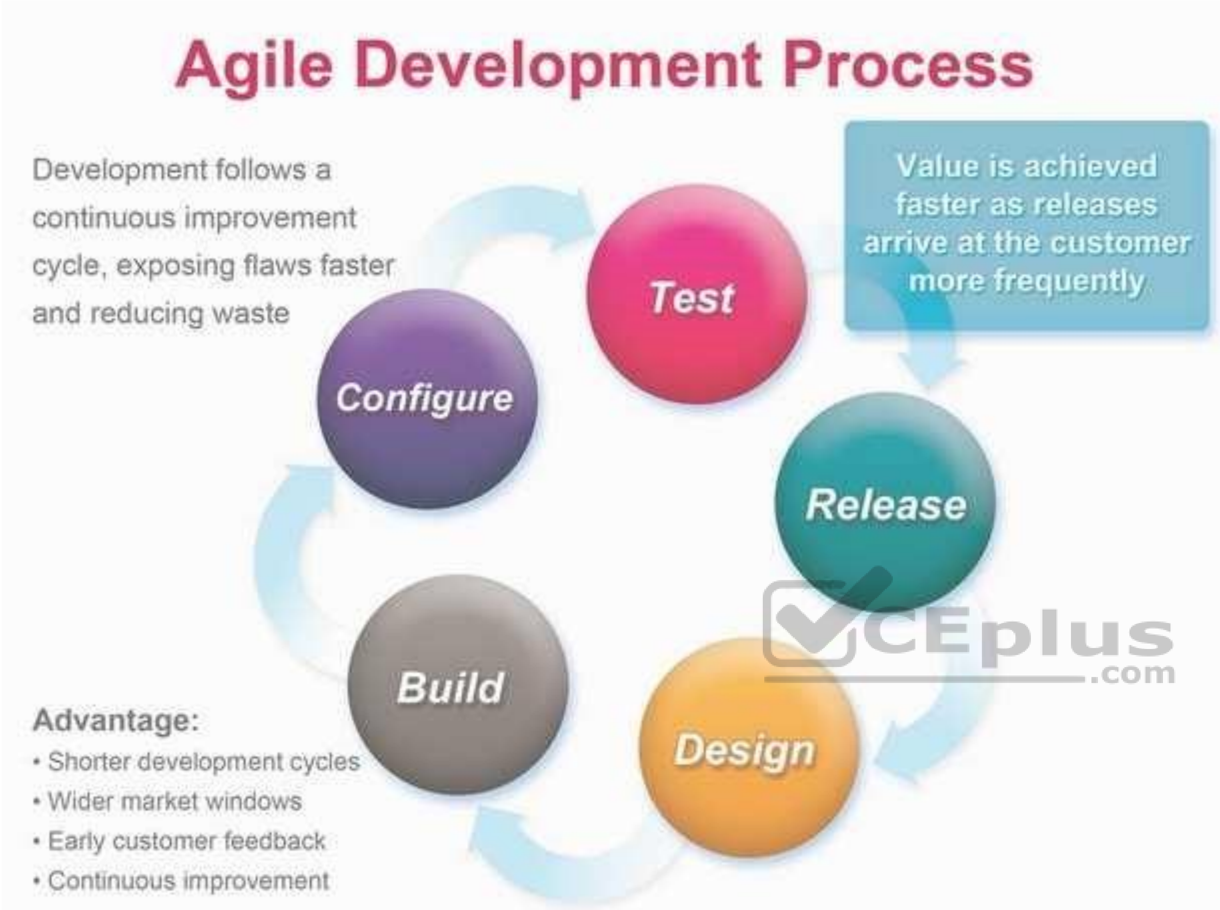
A. Agile Development
B. Software prototyping
C. Rapid application development
D. Component based development

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


Agile Development Process
Development follows a continuous improvement cycle, exposing flaws faster and reducing waste
Value is achieved faster as releases arrive at the customer more frequently
Test
Configure
Release
Build
Design
Advantage:
• Shorter development cycles
• Wider market windows
• Early customer feedback
• Continuous improvement

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 37

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:

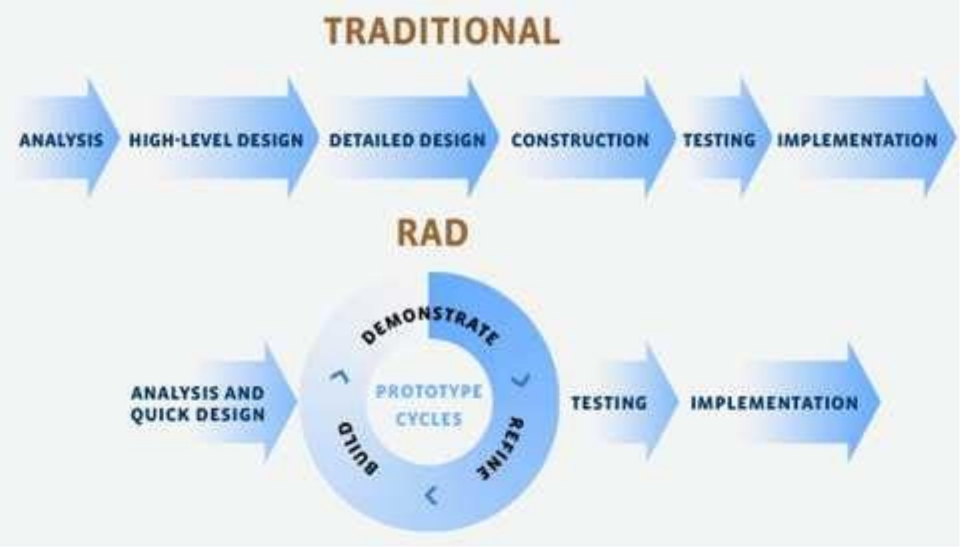
CISA review manual 2014 Page number 194

QUESTION 38
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 39
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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47

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 48
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 49
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.

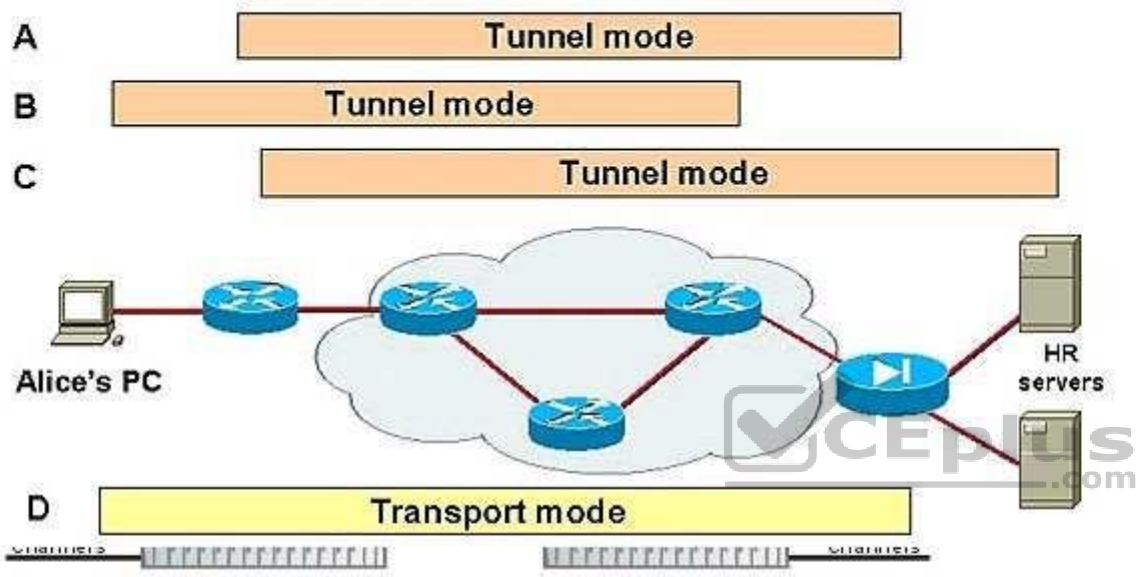
NOTE FROM CLEMENT:
The explanations below are a bit more thorough than what you need to know for the exam. However, they always say a picture is worth one thousand words, I think it is very true when it comes to explaining IPSEC and it's inner working. I have found a great article from CISCO PRESS and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

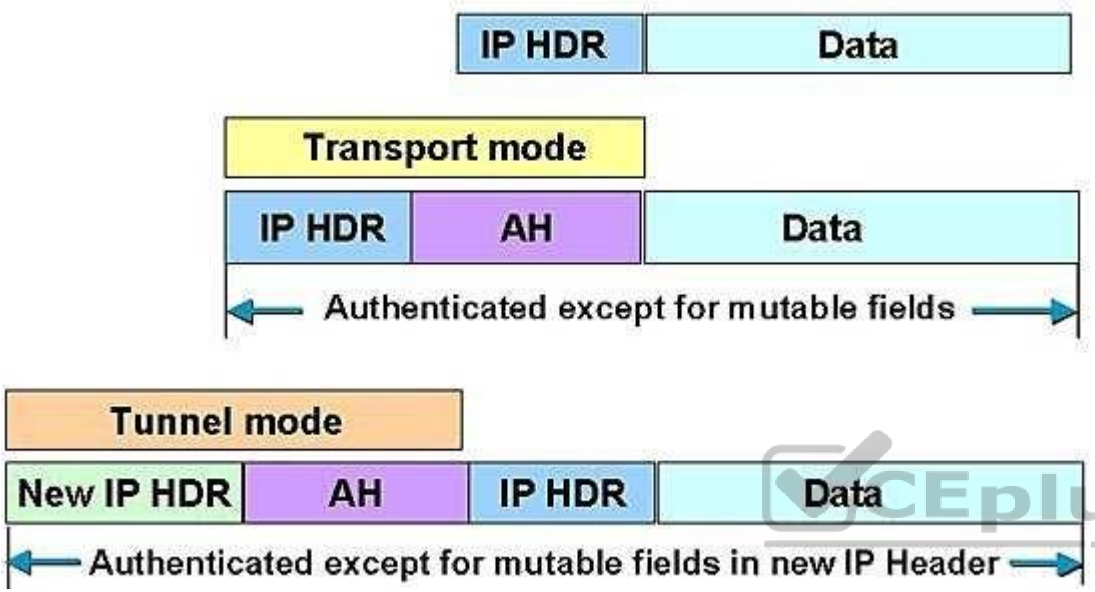
Tunnel and transport modes in IPSec.

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


IP HDR
Data
Transport mode
IP HDR
AH
Data
Authenticated except for mutable fields
Tunnel mode
New IP HDR
AH
IP HDR
Data
Authenticated except for mutable fields in new IP Header

IPSEC AH Tunnel and Transport mode

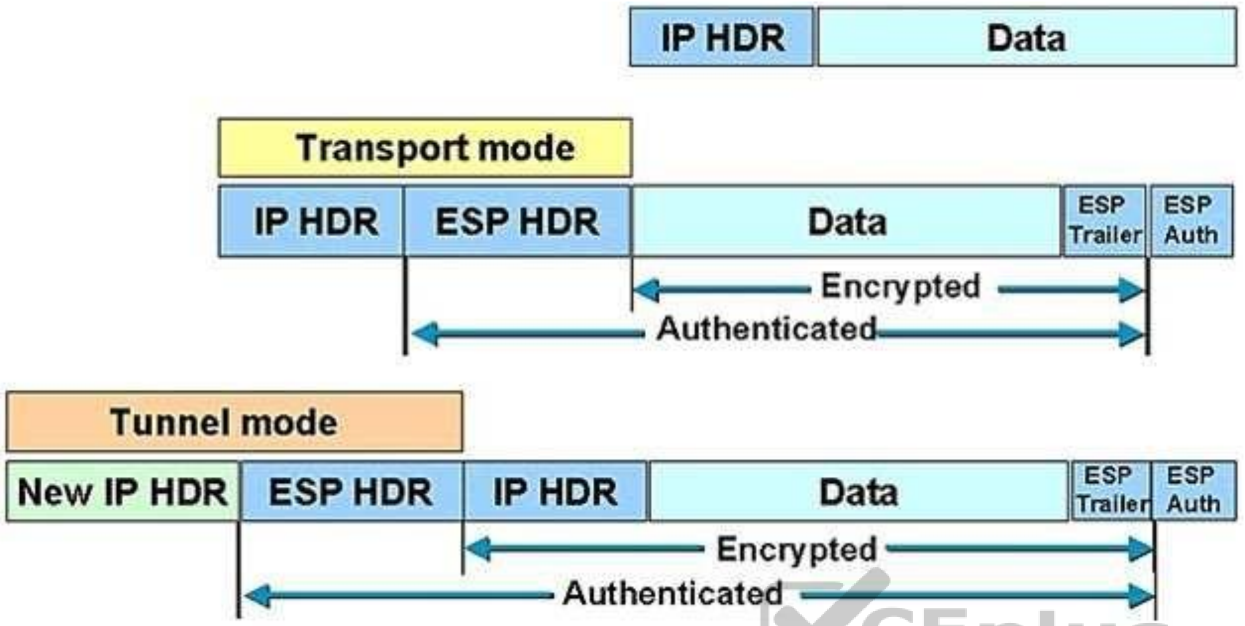
AH Tunnel Versus Transport Mode

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.

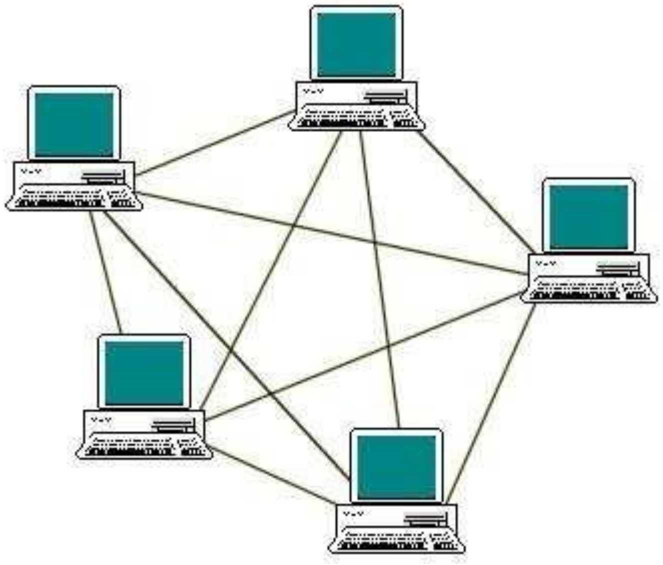
In transport mode, ESP only encrypts the data payload of each packet. ESP can be operated in either tunnel mode (where the original packet is encapsulated into a new one) or transport mode (where only the data payload of each packet is encrypted, leaving the header untouched).

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 50
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:

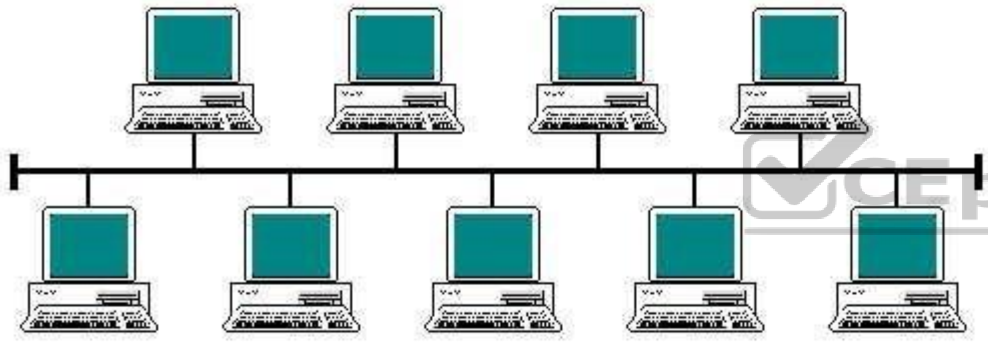
LAN Topologies
Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

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

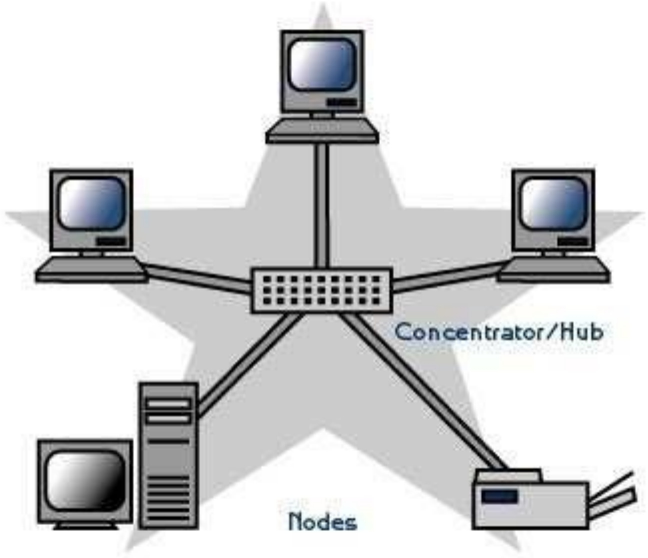


Image from: http://fcit.usf.edu/network/chap5/pics/star.gif

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

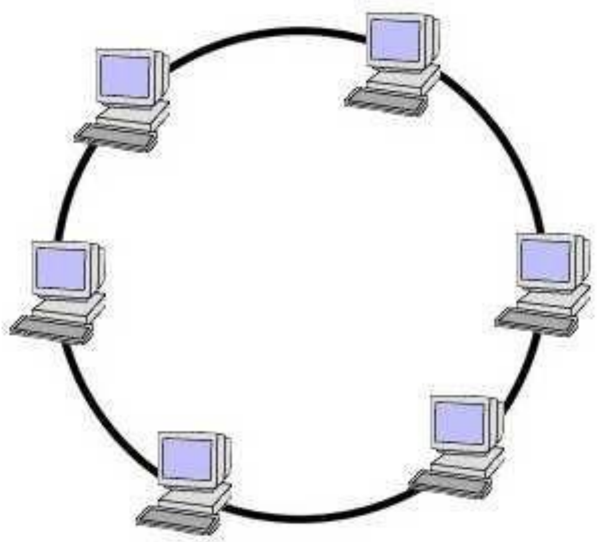


Image from: https://forrester-infosystems.wikispaces.com/

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

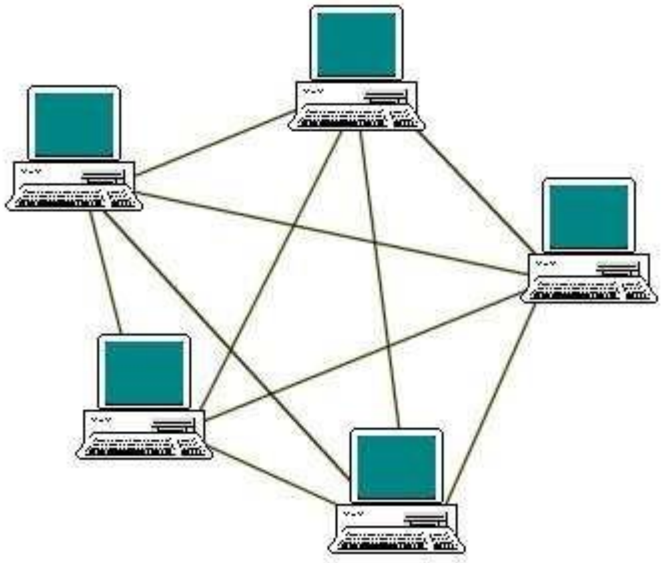


Image from: http://www.technologyuk.net/telecommunications/networks/images/mesh_topology.gif

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 51

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. “

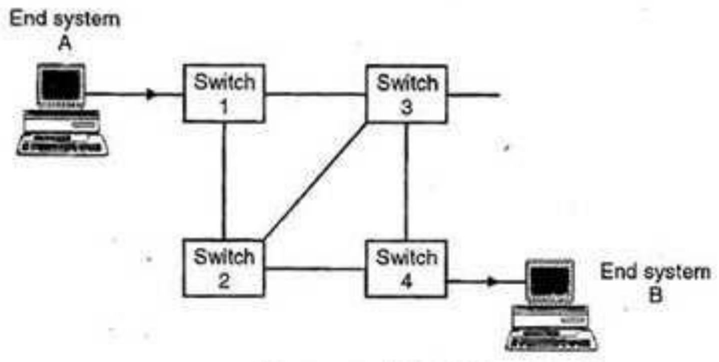
A. Message Switching
B. Packet switching
C. Circuit switching
D. Virtual Circuits

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



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

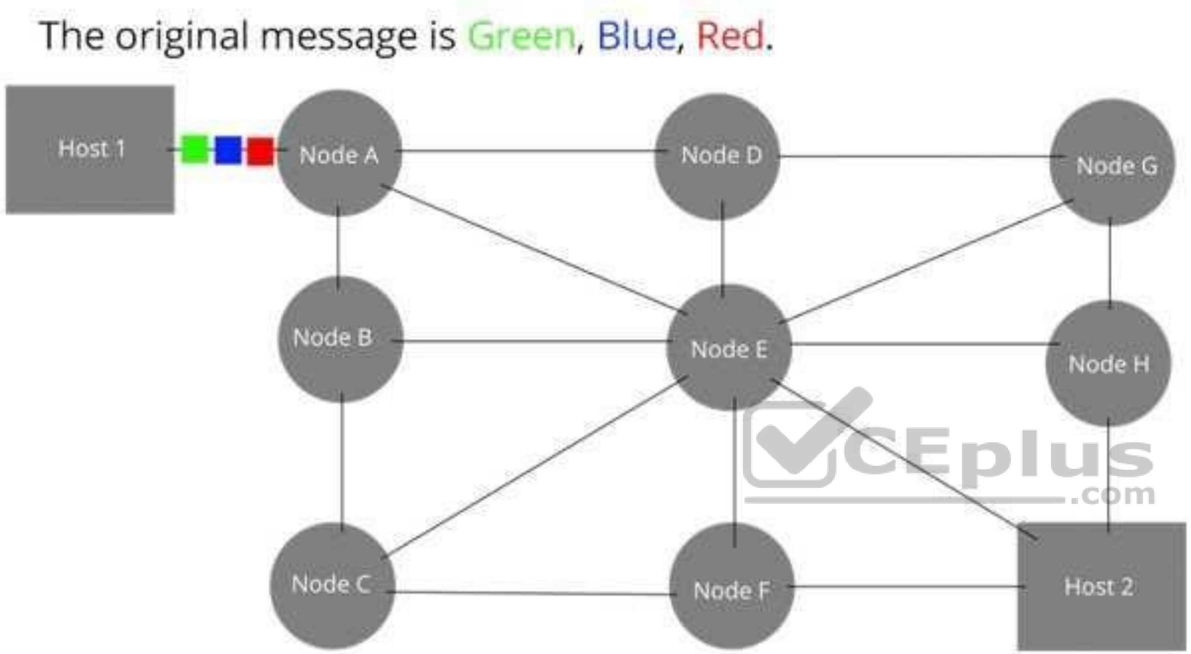


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

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

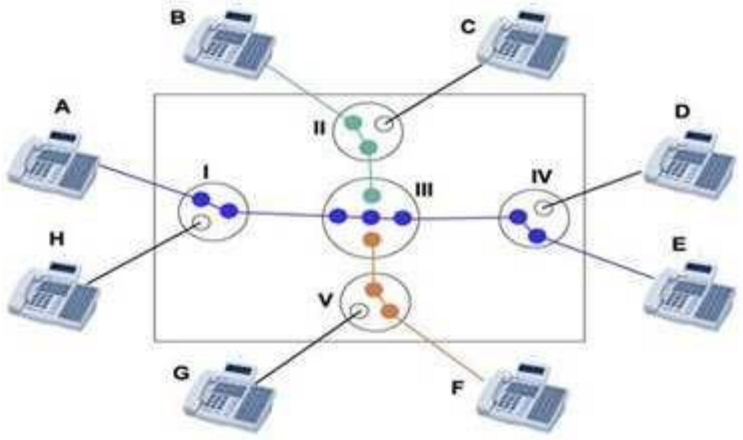
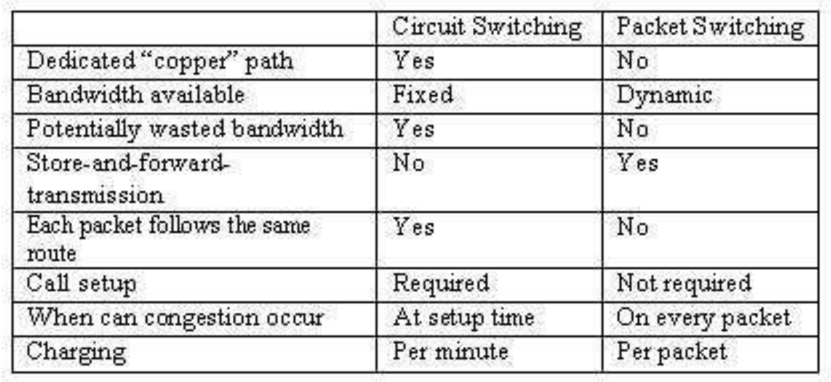


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

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 are not valid choices.

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

QUESTION 52
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?

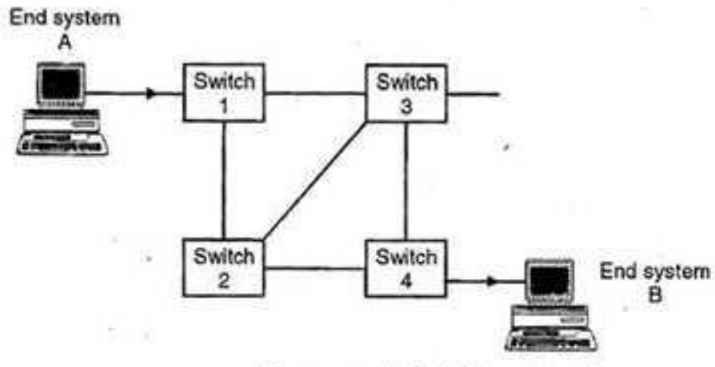
A. Message Switching
B. Packet switching
C. Circuit switching
D. Virtual Circuits

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



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

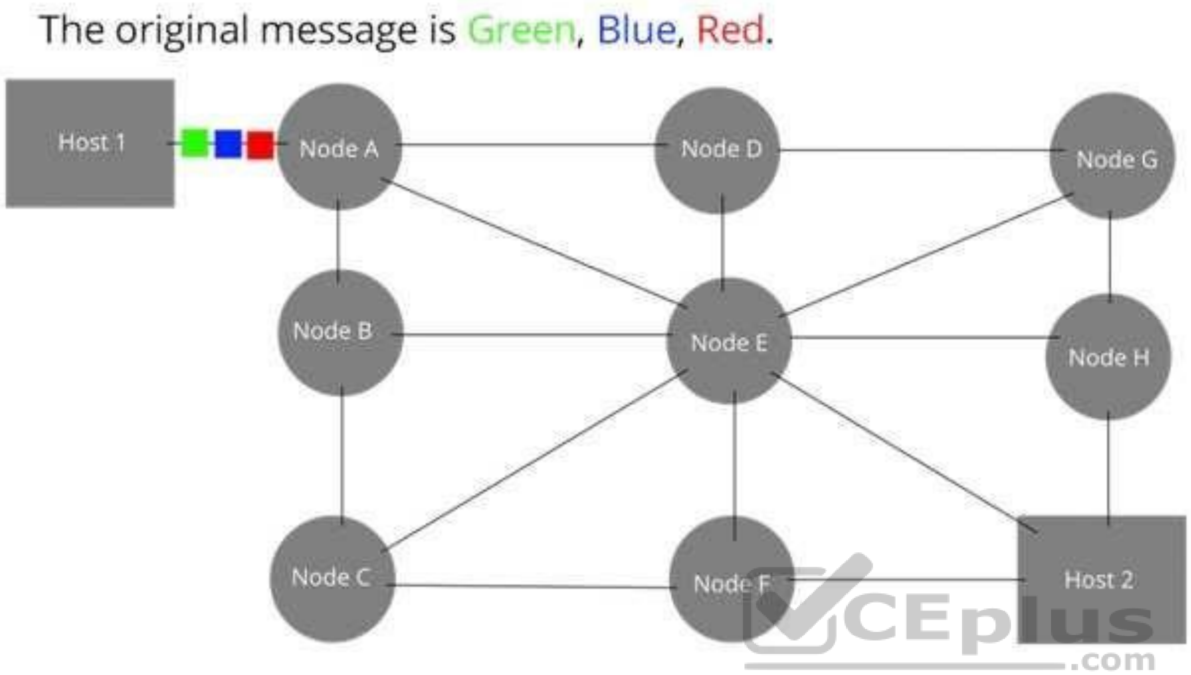


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

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

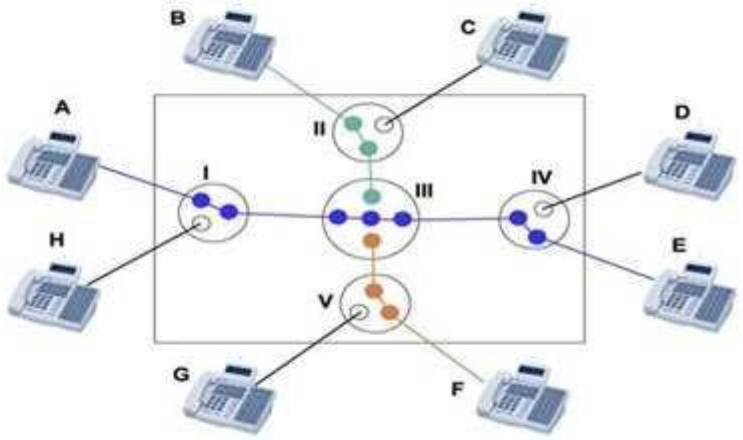
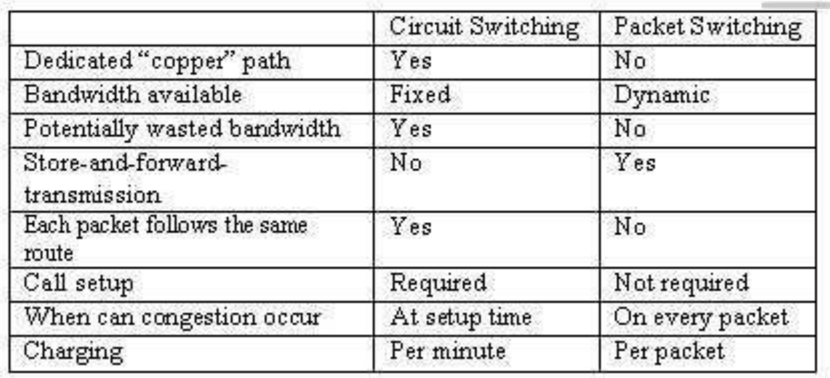


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

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 are not valid choices.

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

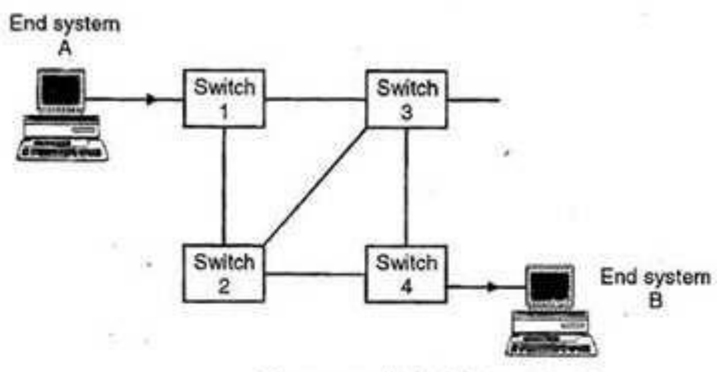
QUESTION 53
In which of the following WAN message transmission technique does two network nodes establish a dedicated communications channel through the network before the nodes may communicate?

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



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

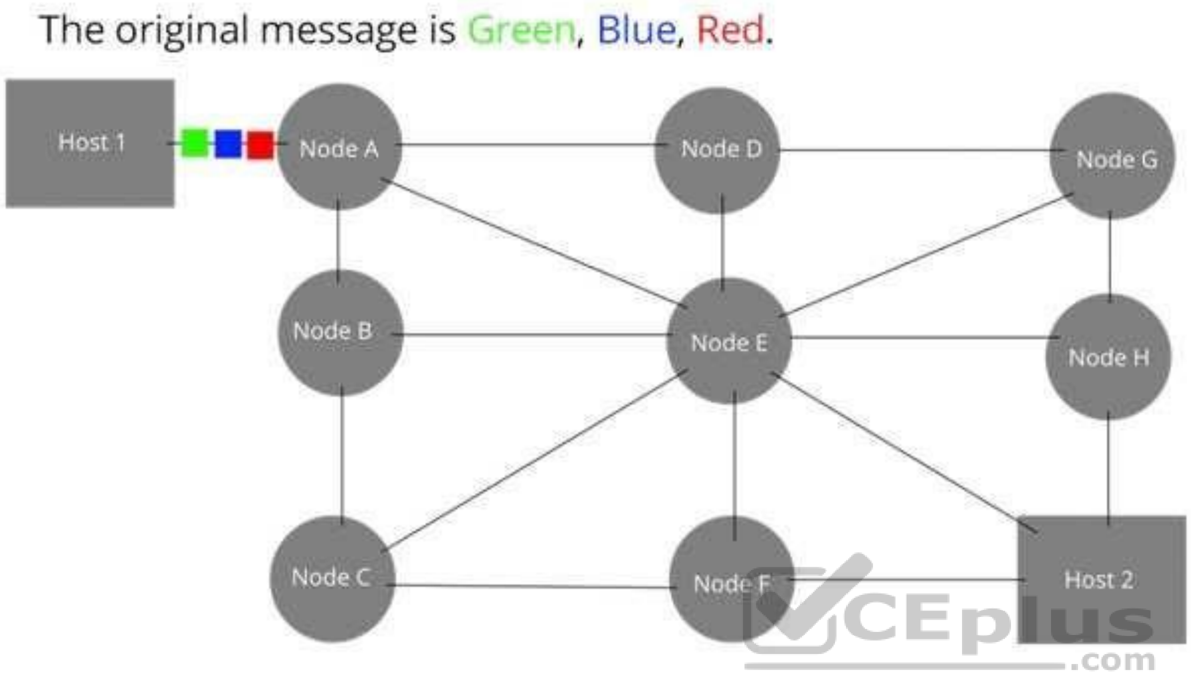


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

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

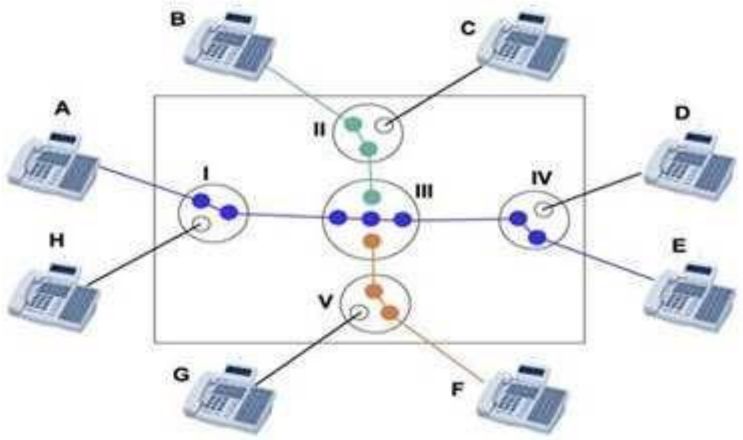
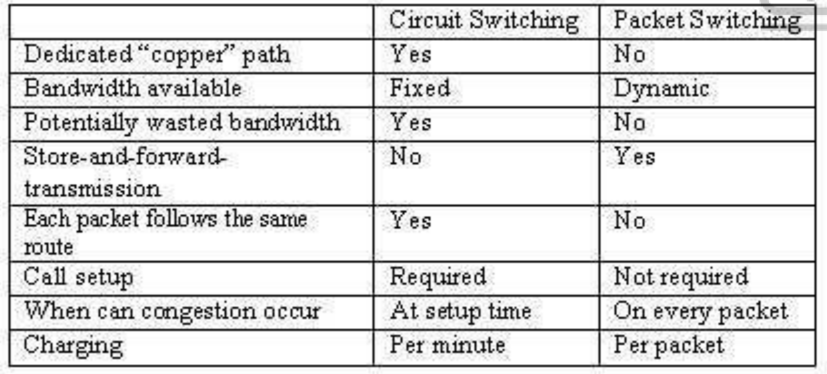


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

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 are not valid choices.

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

QUESTION 54
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

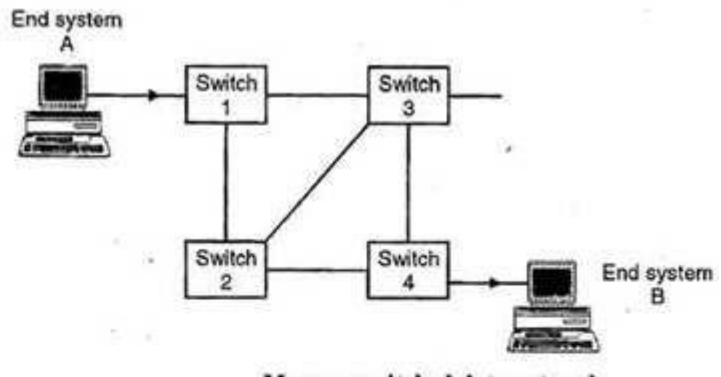
Explanation/Reference:
The word INCORRECTLY is the keyword used in the question. You need to find out a statement which is not valid about circuit switching.

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



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

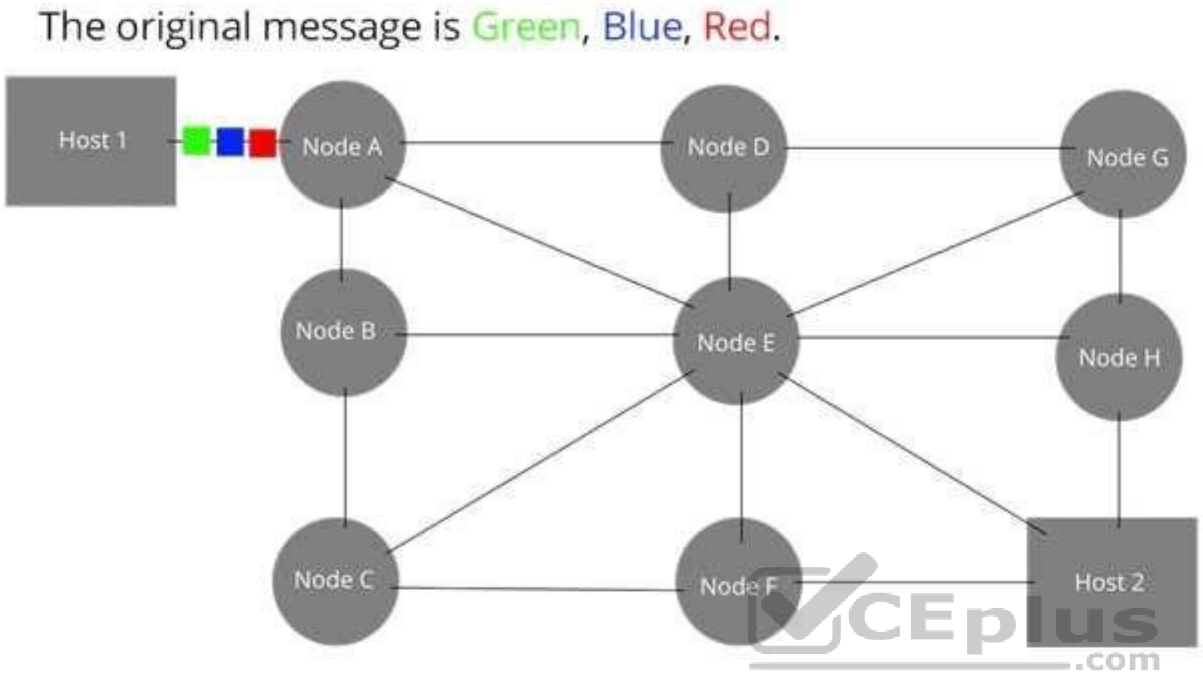


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

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

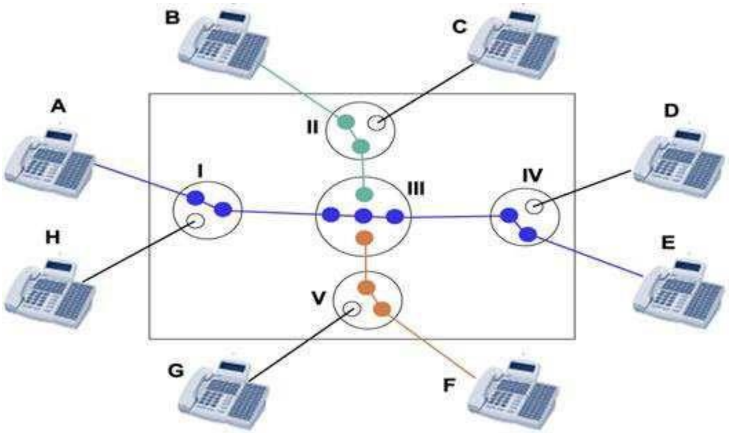
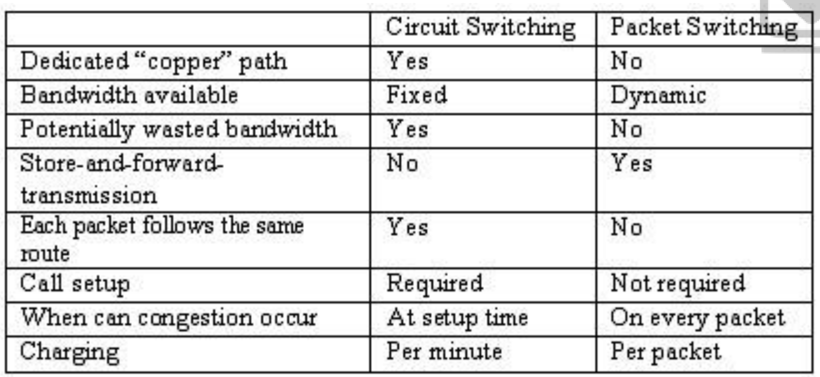


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

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 circuit switching.

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

QUESTION 55
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

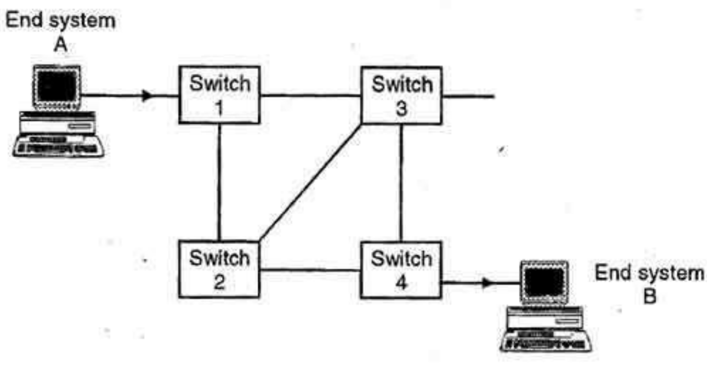
Explanation/Reference:
The word INCORRECTLY is the keyword used in the question. You need to find out a statement which is not valid about packet switching. As in the network switching, packet traverse different path, there will be always variable delay for each packet to reach to destination.

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

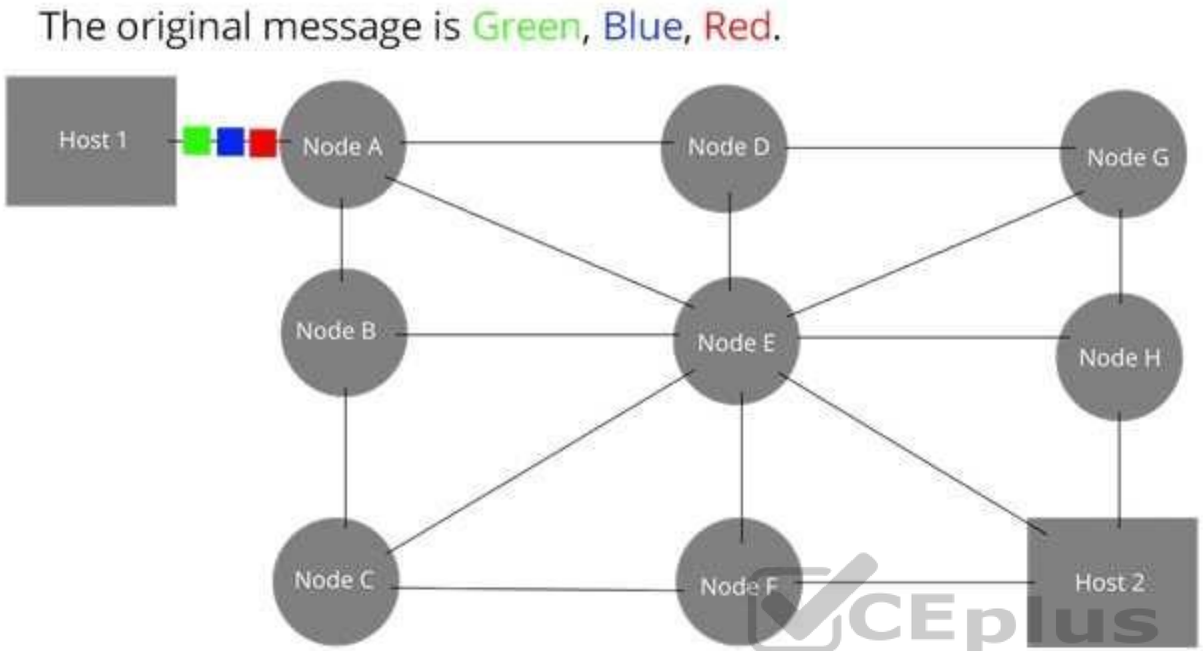


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif

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

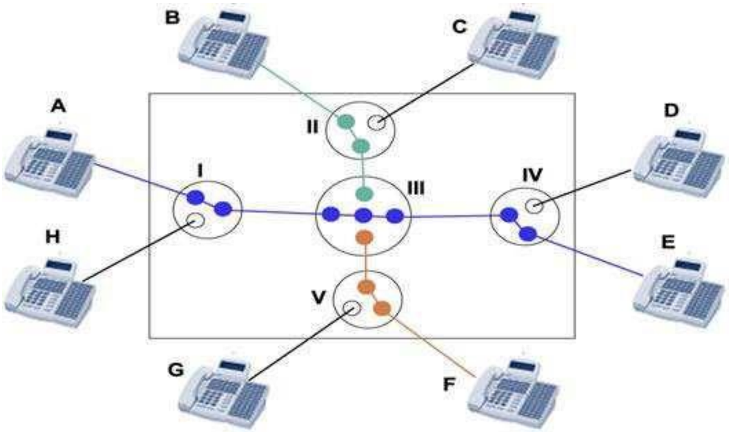
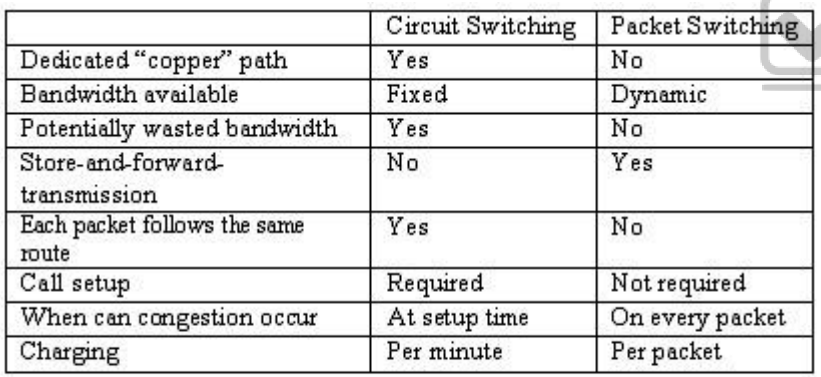


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg

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 56
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:

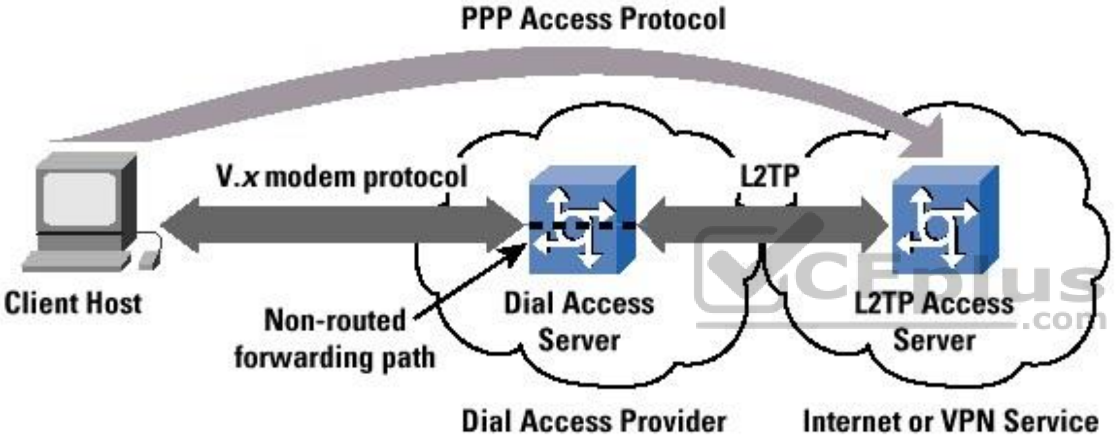
Point-to-point protocol
PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's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

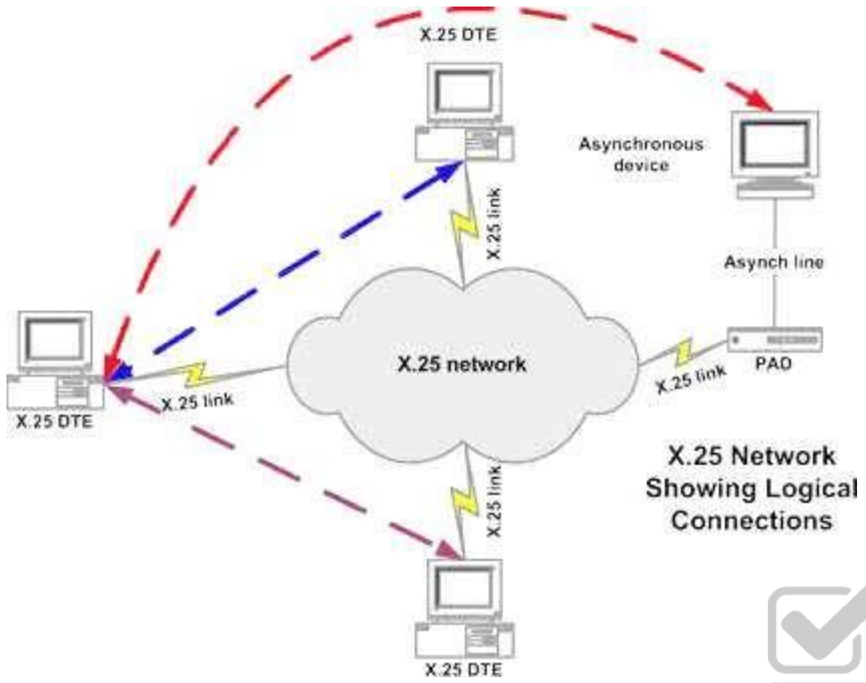
PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

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

Frame Relay

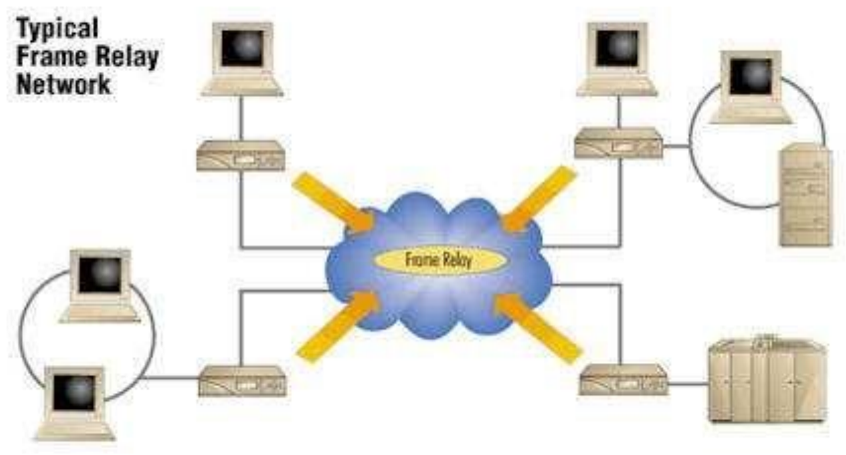
Works on a packet switching
Operates at data link layer of an OSI model
Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

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.

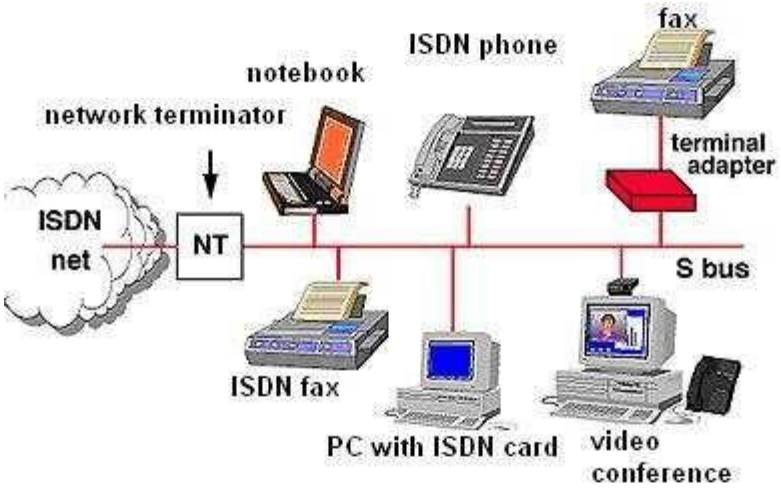


Frame Relay

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



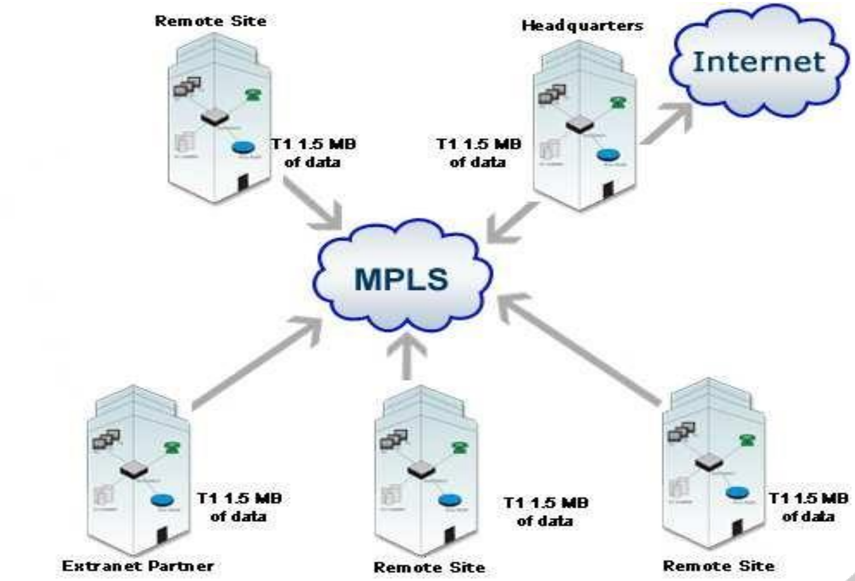
Asynchronous Transfer Mode (ATM)

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 57
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 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 58
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

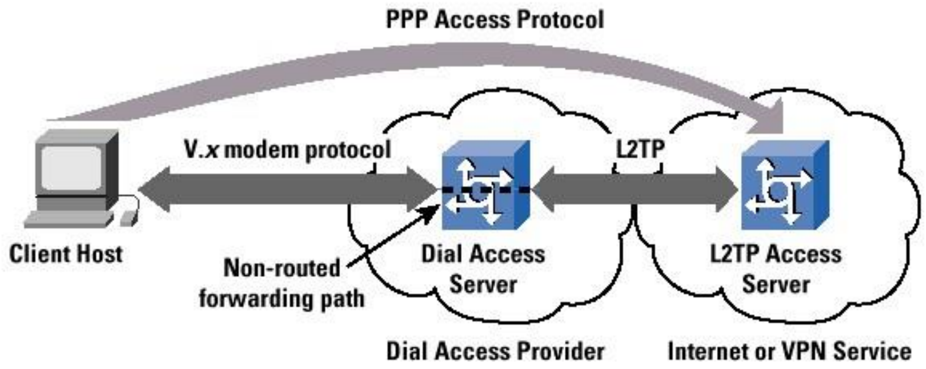


Image from:http://withfriendship.com/images/g/31728/a-pointtopoint-protocol.png

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

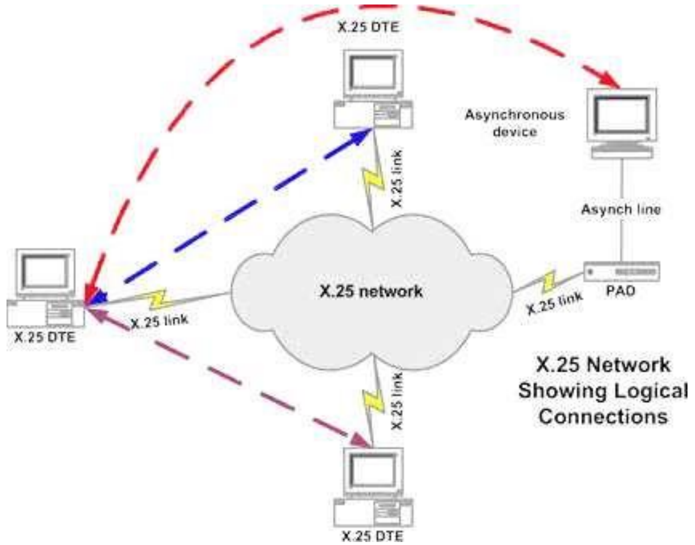


Image from:http://www.sangoma.com/assets/images/content/tutorials_x25_1.gif

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

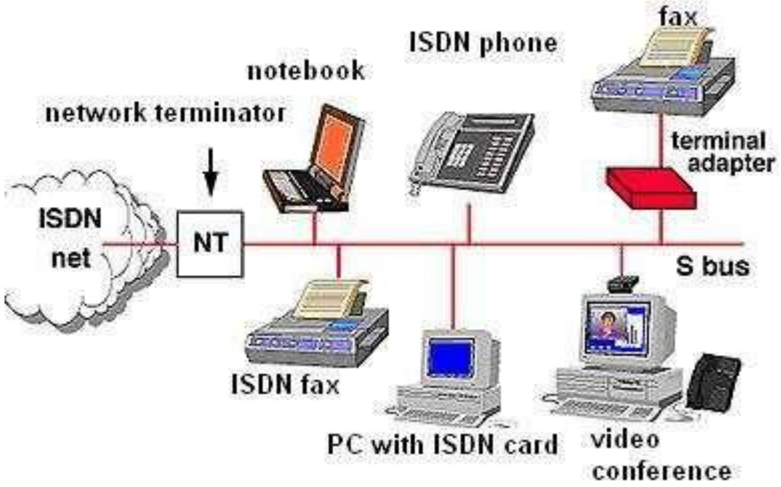


Image from: http://www.cpcstech.com/images/frame-2.jpg

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

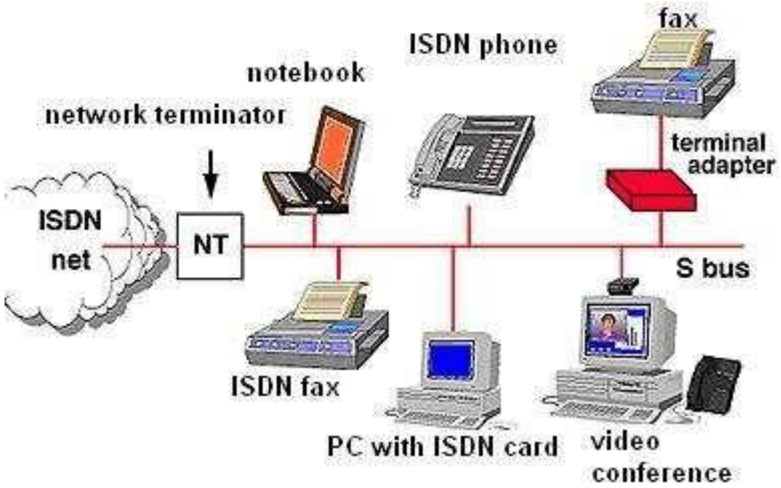


Image from: http://www.hw-server.com/obrazek/network_topology

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

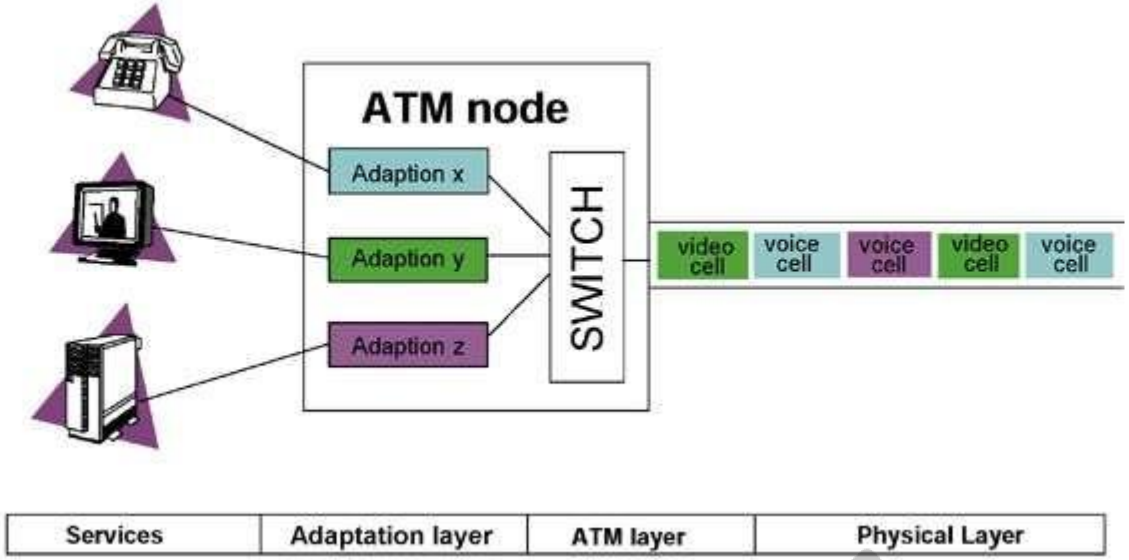


Image from: http://html.rincondelvago.com/000050700.png

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

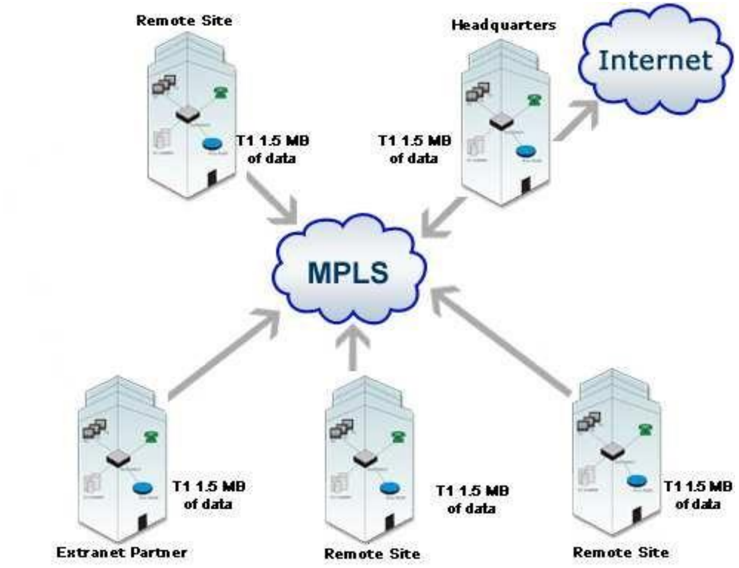


Image from: http://www.carrierbid.com/wp-content/uploads/2011/01/mpls1.gif

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 59
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

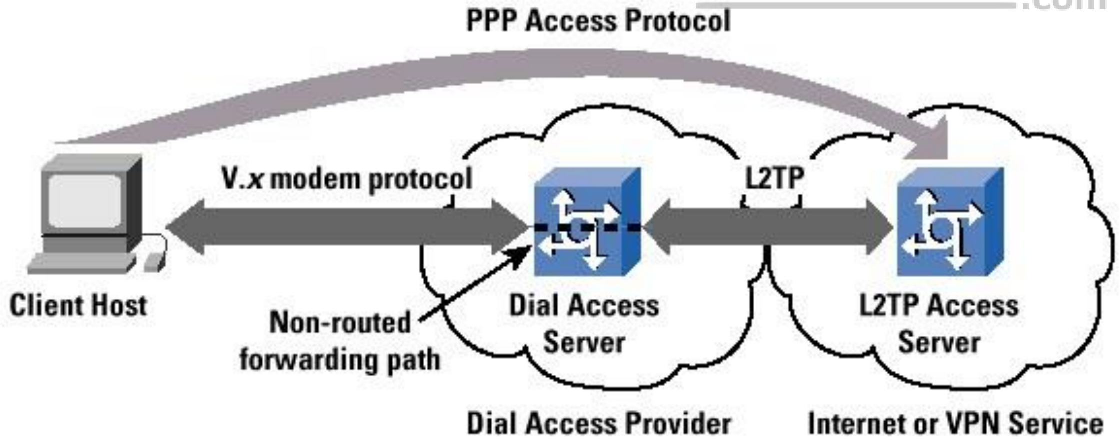
Explanation/Reference:
Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

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.

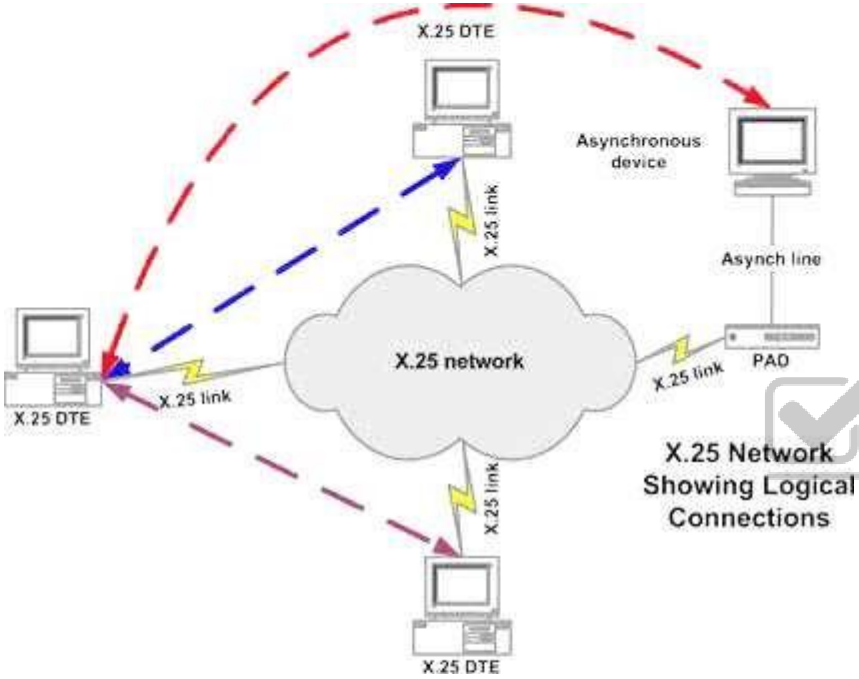


Point-to-point protocol

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



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.

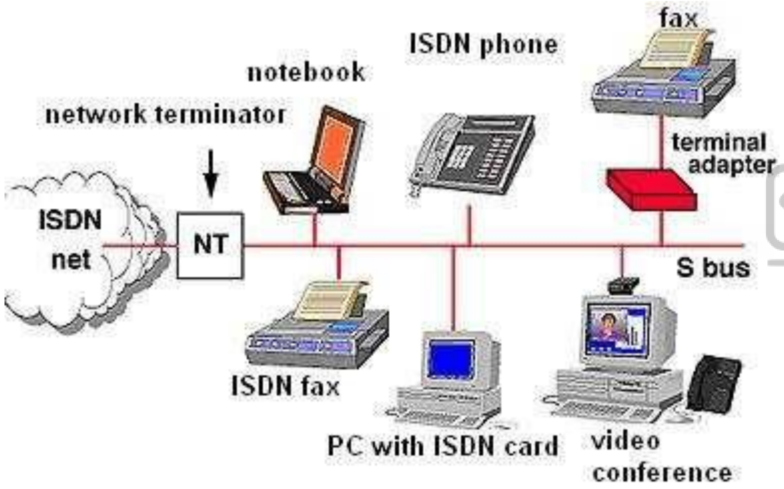
2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

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

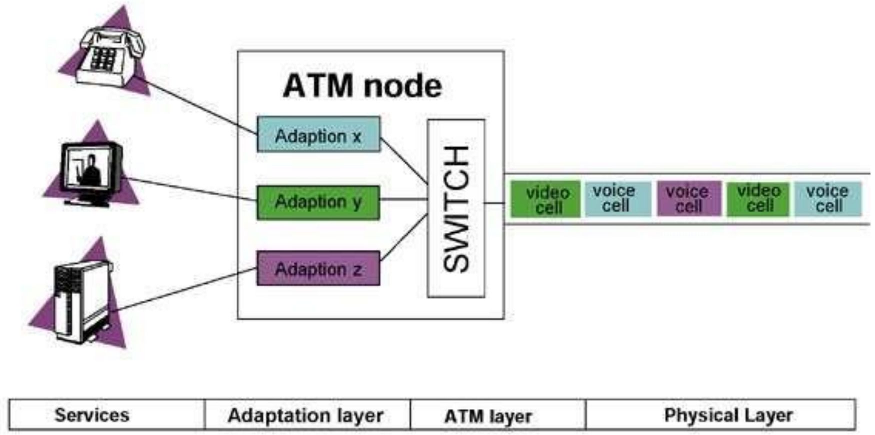
ISDN



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

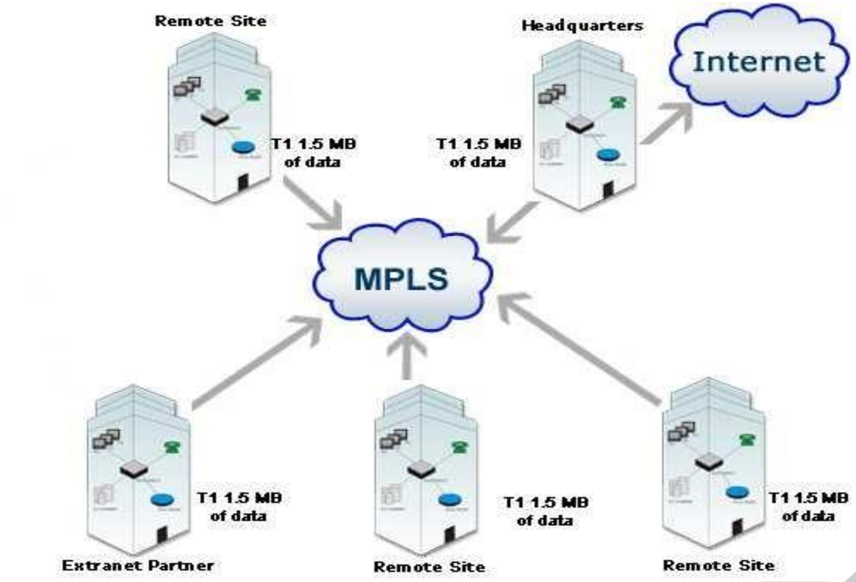
Asynchronous Transfer Mode



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 60
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

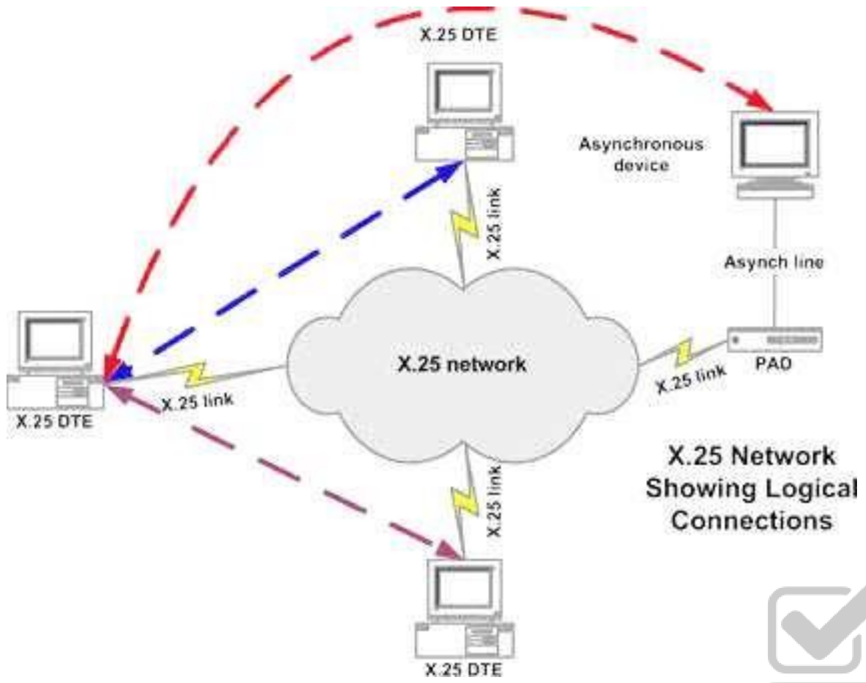
For your exam you should know below information about WAN Technologies:

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

Frame Relay

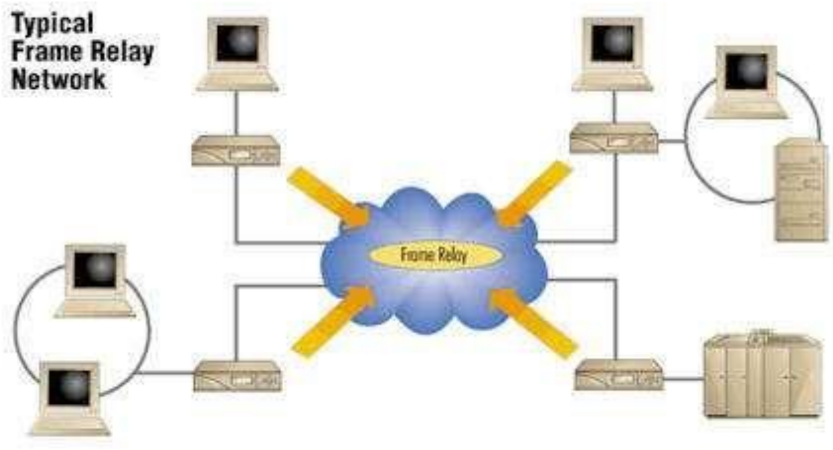
Works on a packet switching
Operates at data link layer of an OSI model
Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

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.

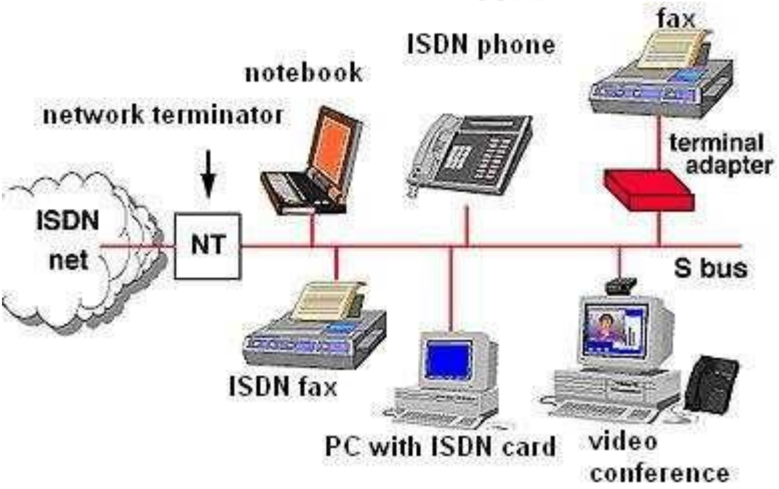
The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.



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.

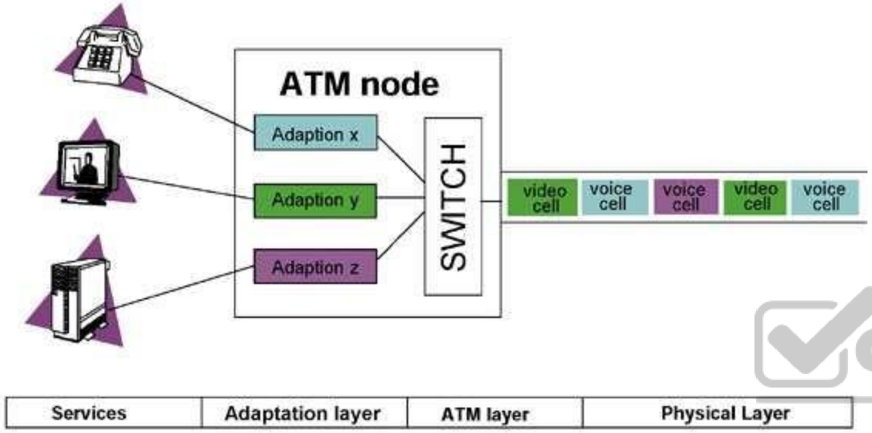


Provide digital point-to-point circuit switching medium.

ISDN

Asynchronous Transfer Mode (ATM)

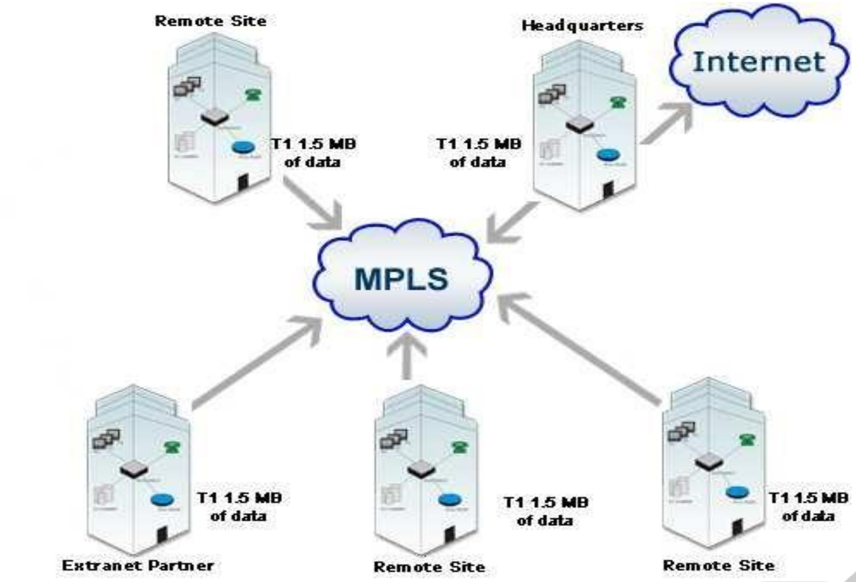
Uses Cell switching method
High speed network technology used for LAN, MAN and WAN
Like a frame relay it is connection oriented technology which creates and uses fixed channel
Data are segmented into fixed size cell of 53 bytes
Some companies have replaces FDDI back-end with ATM



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 61
Which of the following technique is used for speeding up network traffic flow and making it easier to manage?

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

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

Explanation/Reference:

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

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

Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

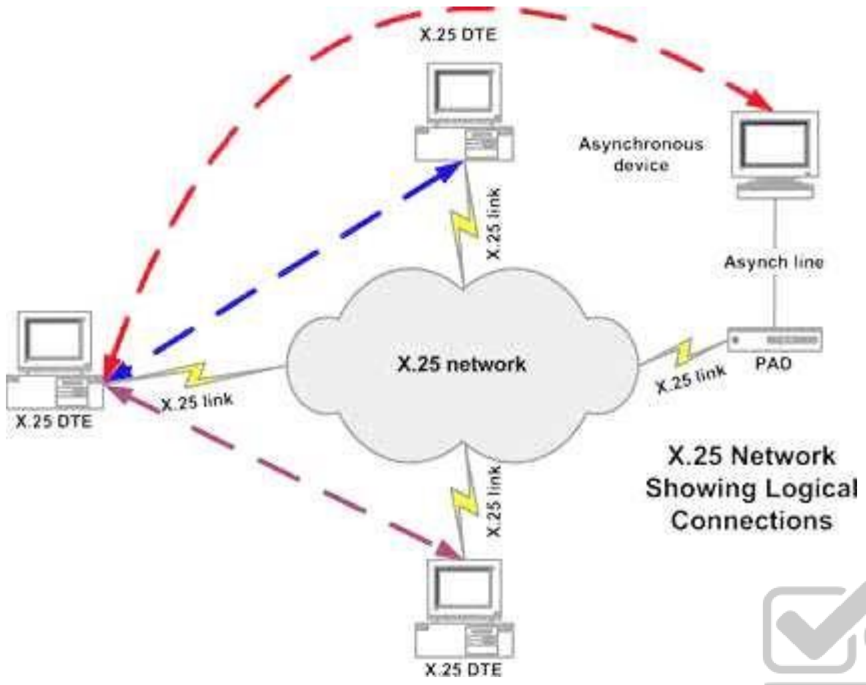
PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

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

Point-to-point protocol

X.25

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.
X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.
Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).
X.25 works at network and data link layer of an OSI model.



X.25

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

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

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

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

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

Frame Relay
Integrated Service Digital Network

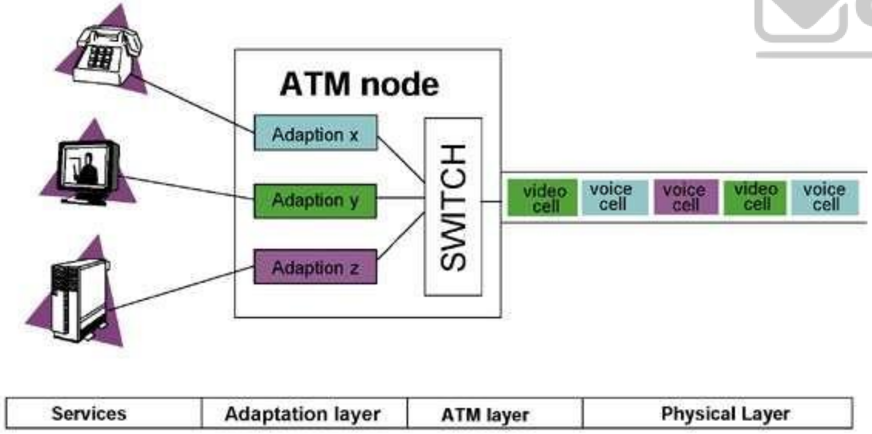
Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.
Same copper telephone wire is used.
Provide digital point-to-point circuit switching medium.

ISDN

Asynchronous Transfer Mode (ATM)

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

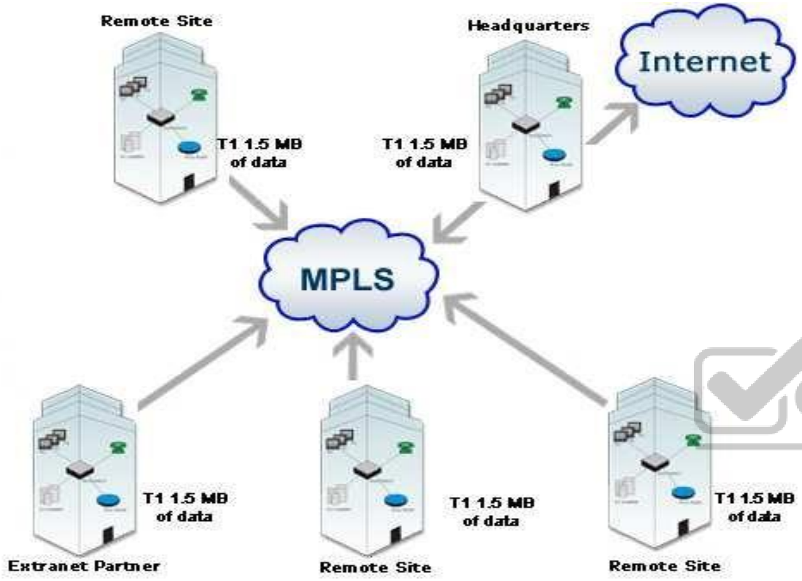
Asynchronous Transfer Mode



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

to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:

X.25 - X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

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

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

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

QUESTION 62

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.

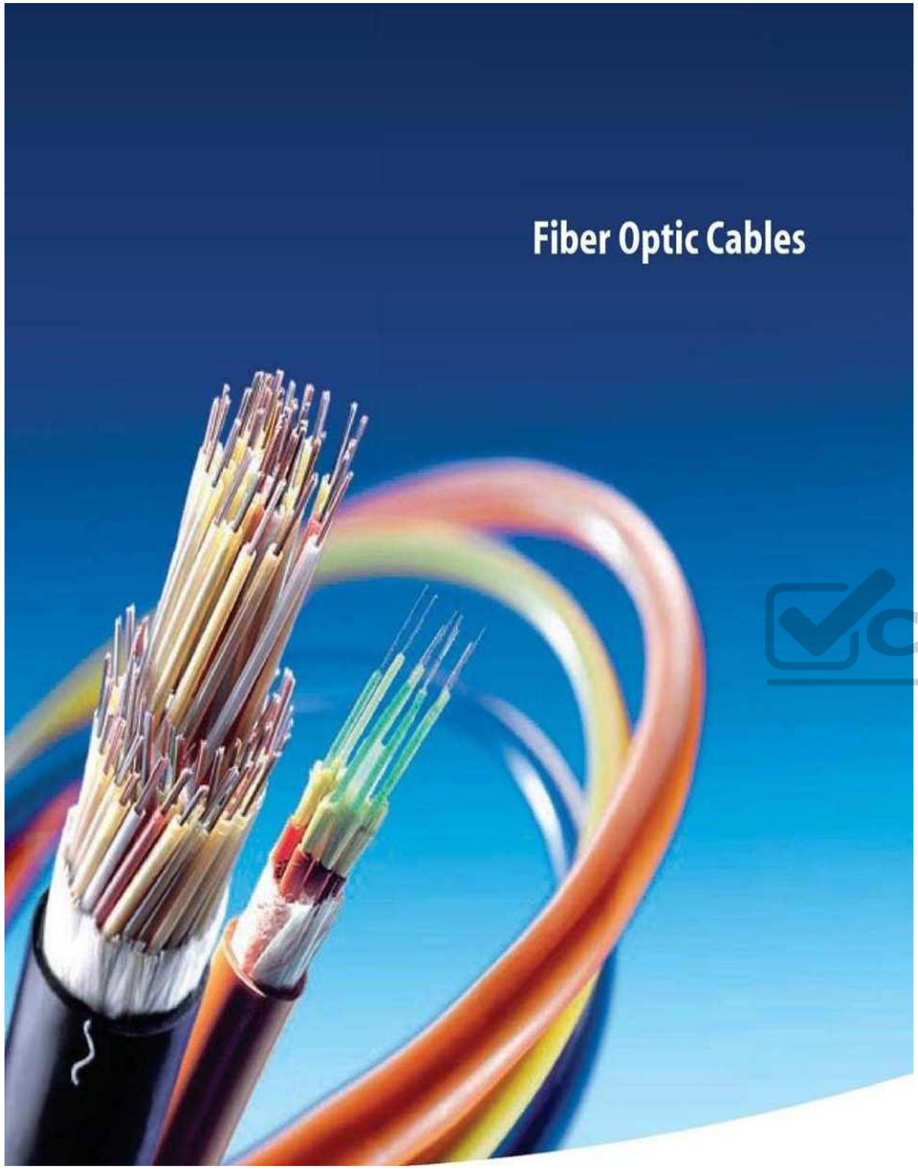
Coaxial Cable

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 63

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 64
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.

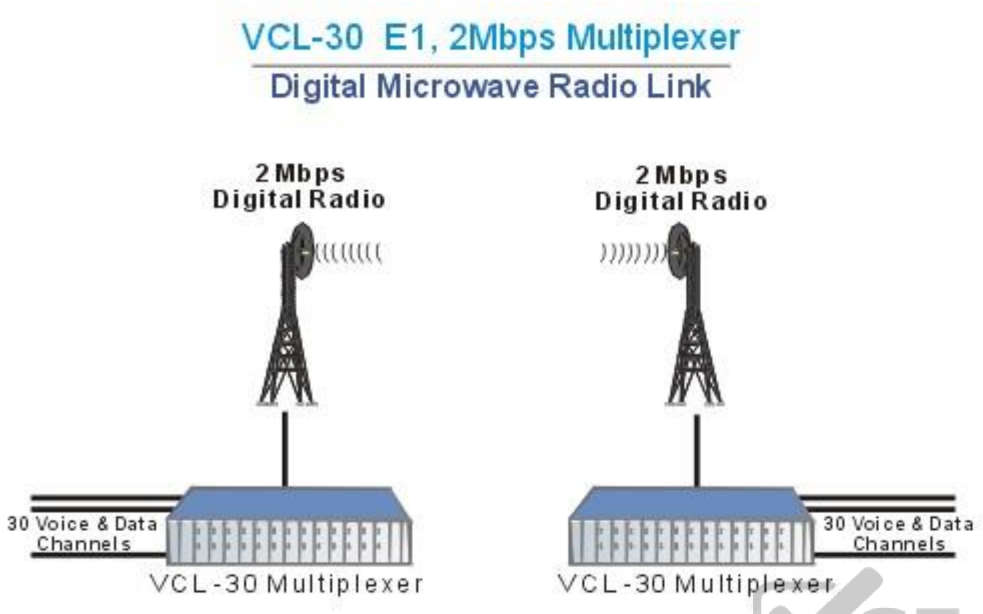
Fiber Optics

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 65
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.

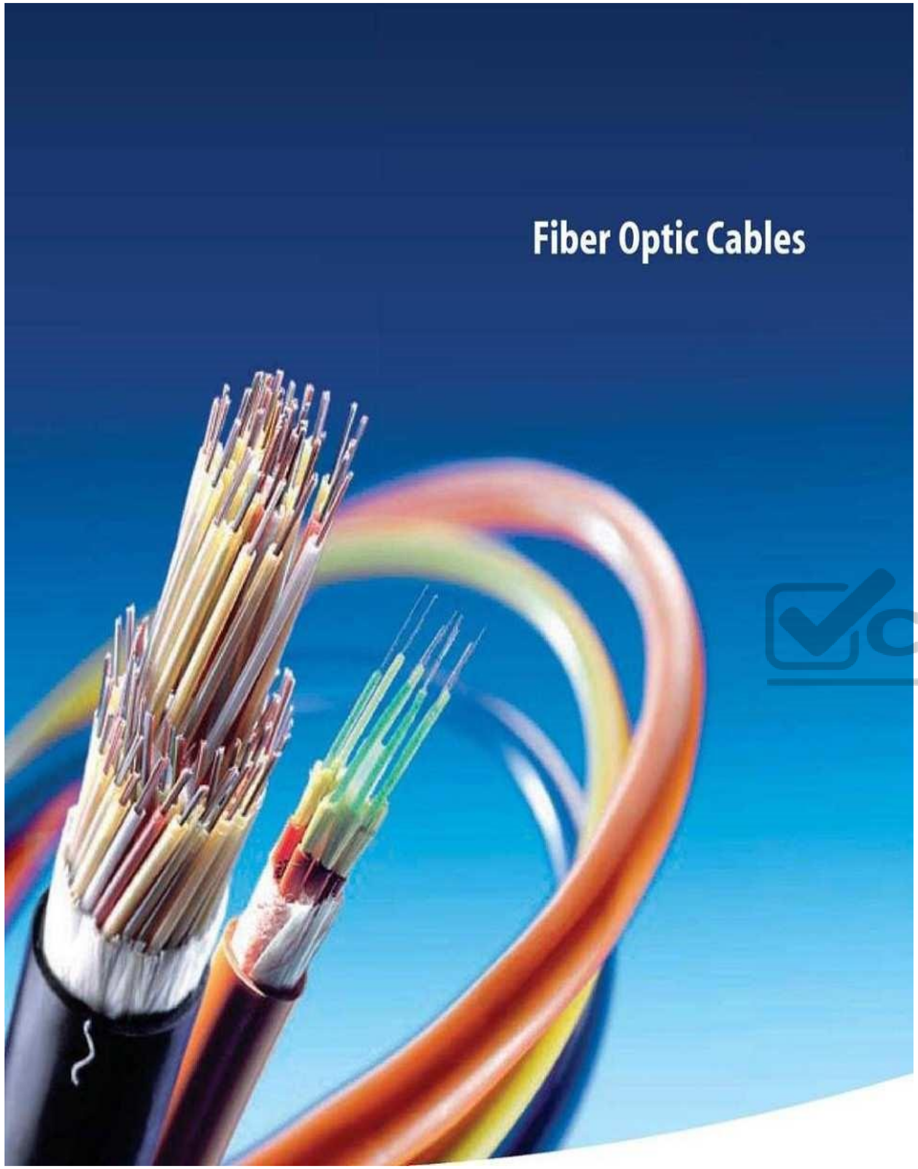
Coaxial cable is expensive and does not support many LAN's. It supports data and video.

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



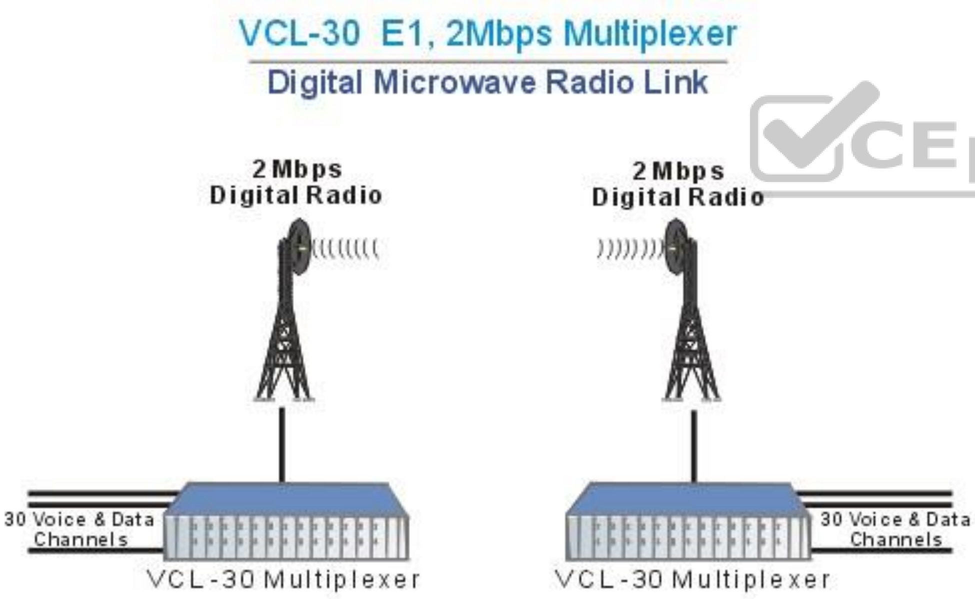
Microwave radio system

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 66
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.

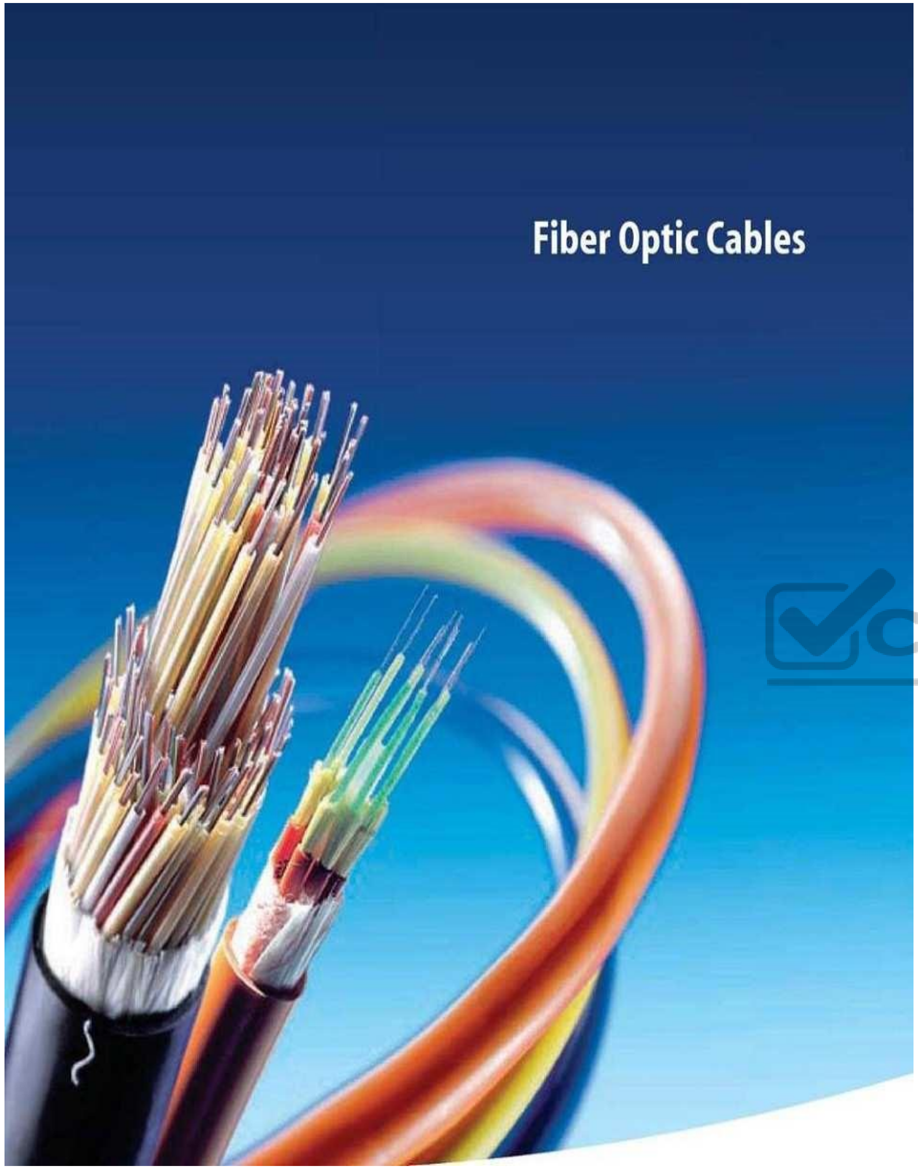
Coaxial Cable

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



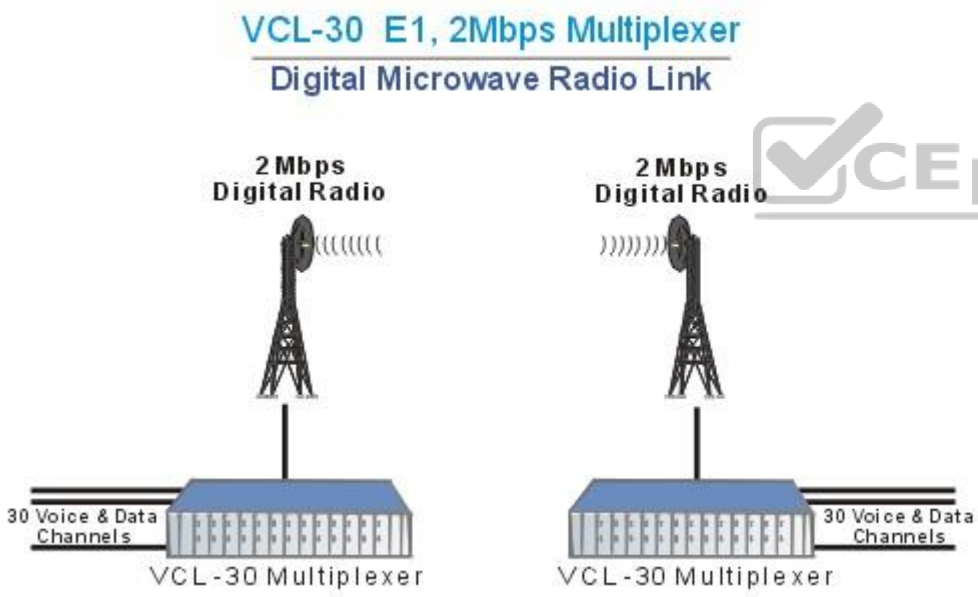
Microwave radio system

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 67
Which of the following is the INCORRECT Layer to Protocol mapping used in the DOD TCP/IP model?

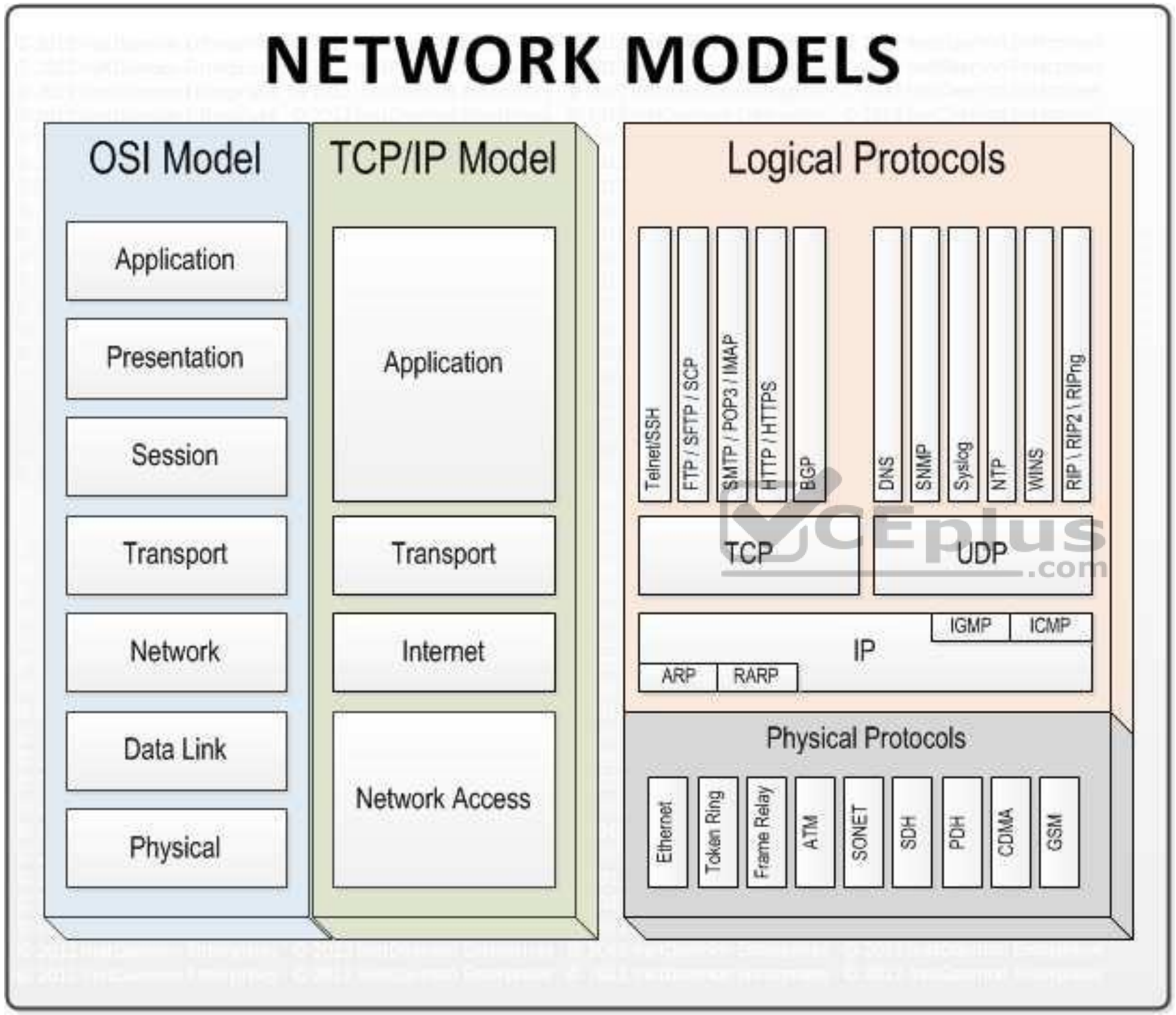
A. Application layer – Telnet
B. Transport layer – ICMP
C. Internet layer – IP
D. Network Access layer – Ethernet

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.

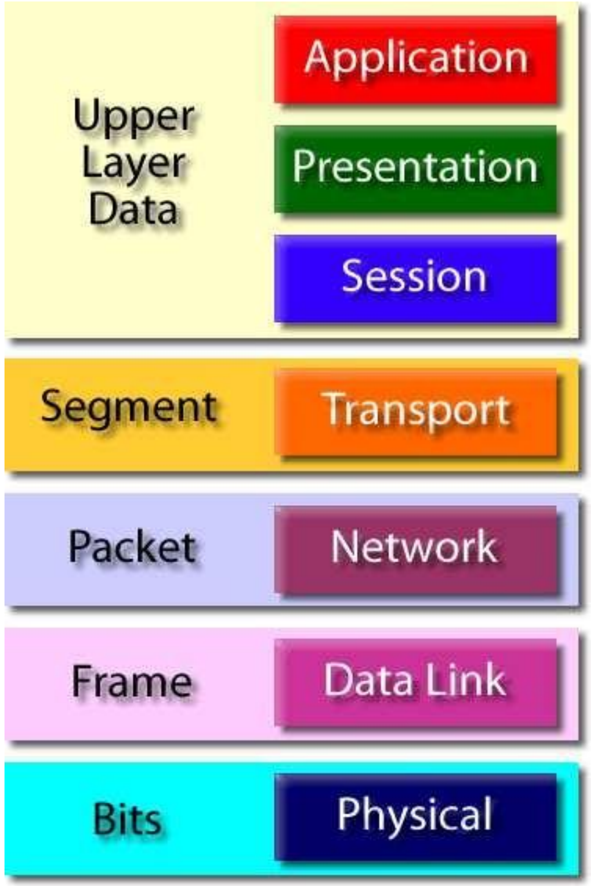
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 68
Which of the following protocol does NOT work at the Application layer of the TCP/IP Models?

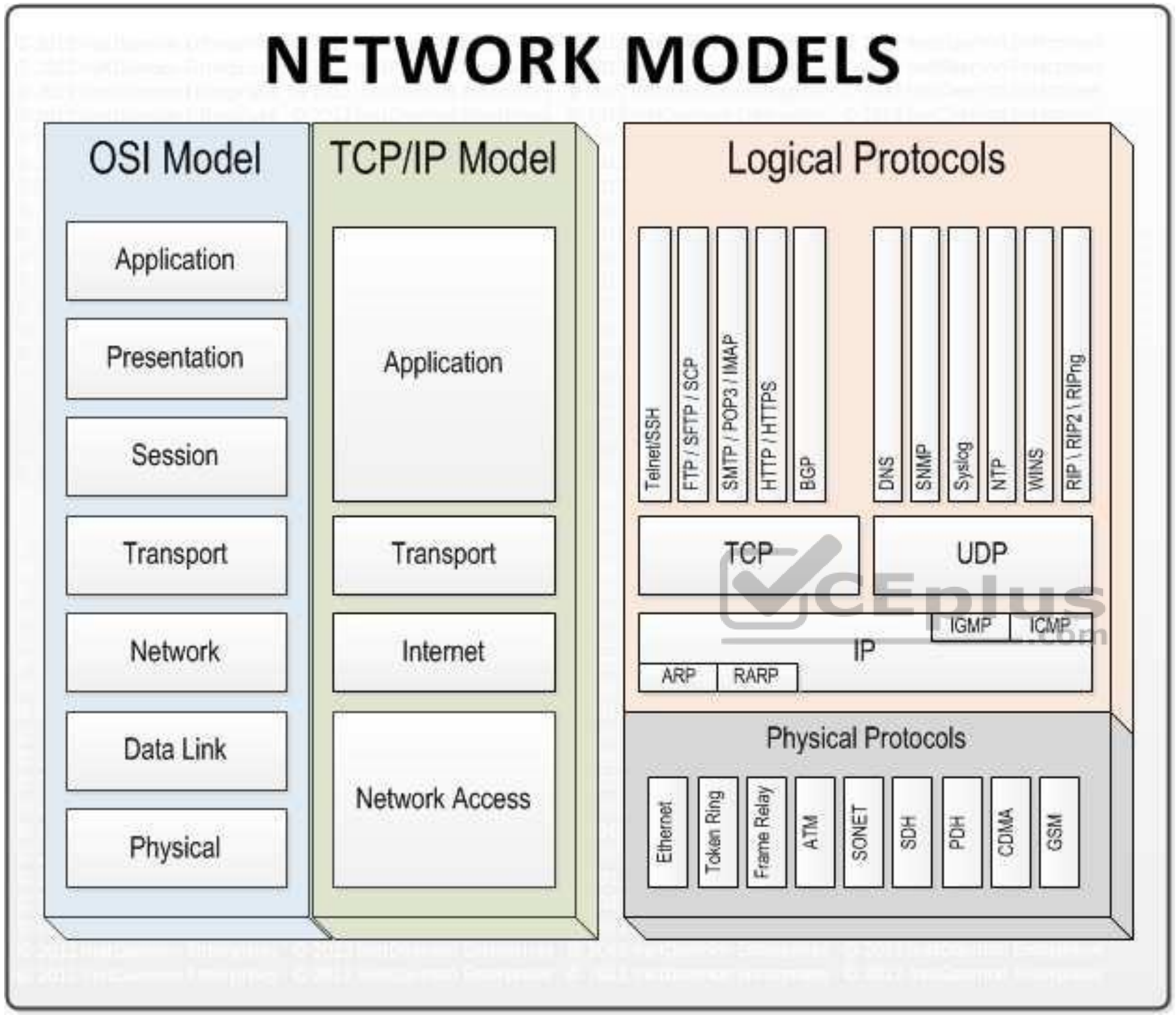
A. HTTP
B. FTP
C. NTP
D. TCP

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

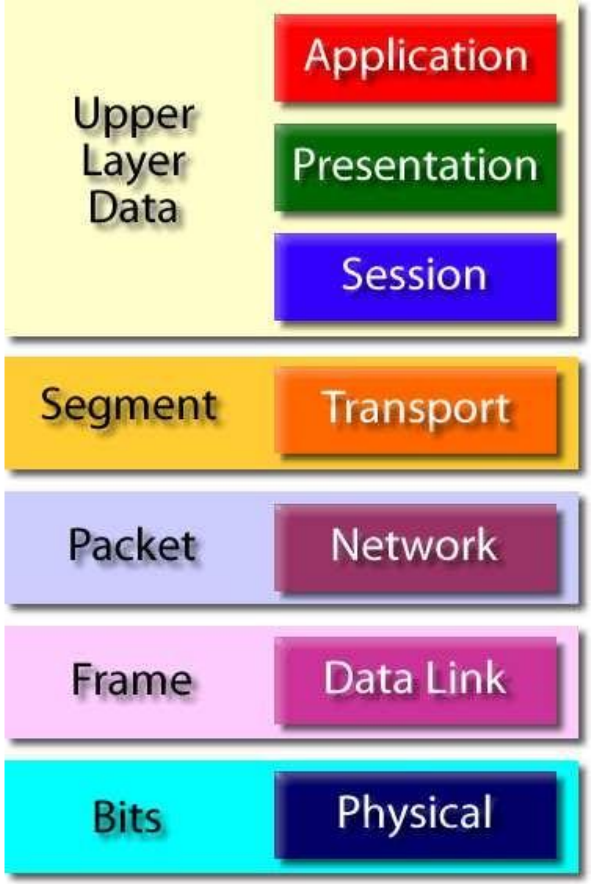
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial 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 69

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

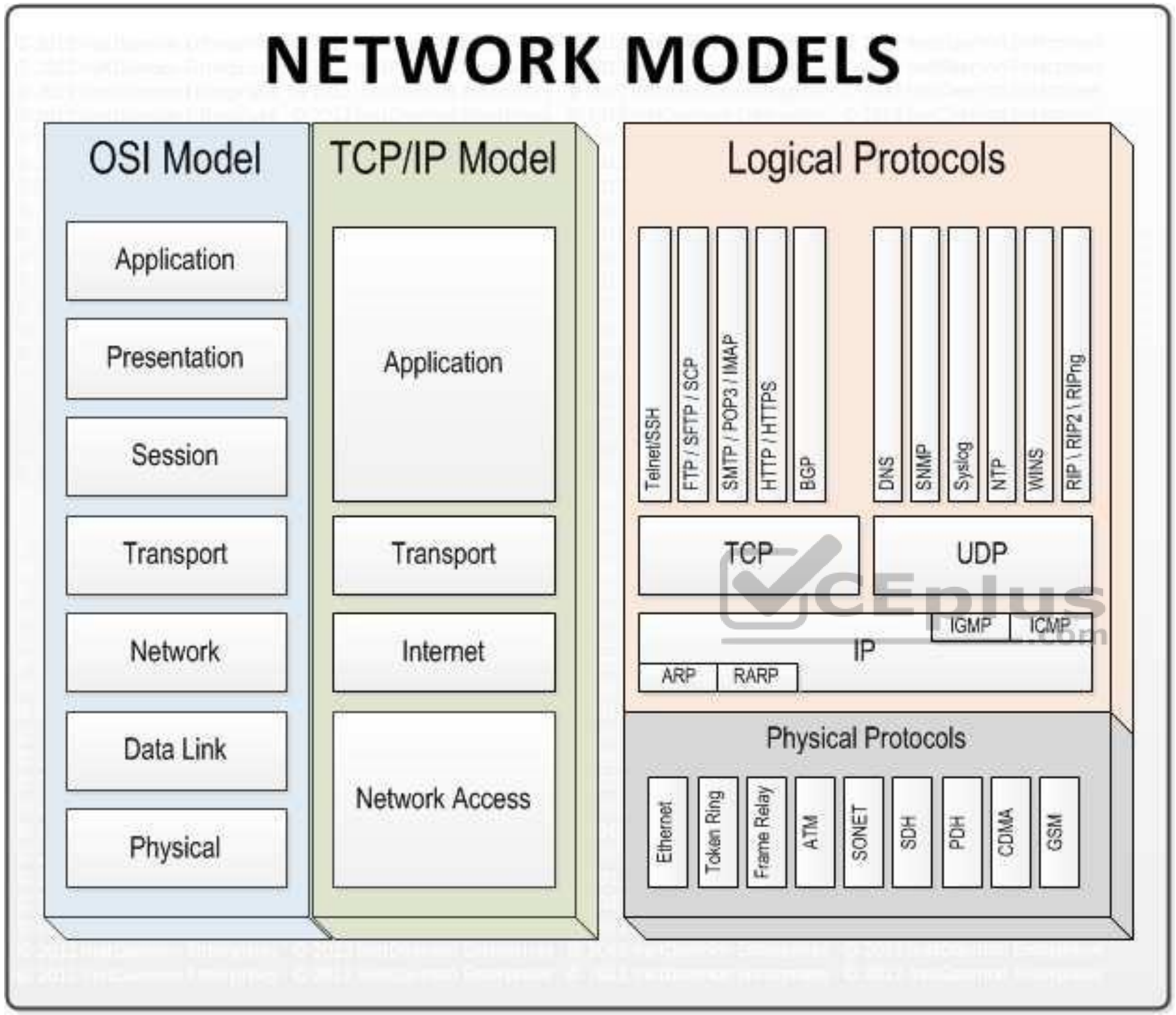
A. Layer 4 switch work at Network interface layer in TCP/IP model
B. Router works at Network interface layer in TCP/IP model
C. Layer 3 switch work at Network interface layer in TCP/IP model
D. Hub works at LAN or WAN interface layer of a TCP/IP model

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

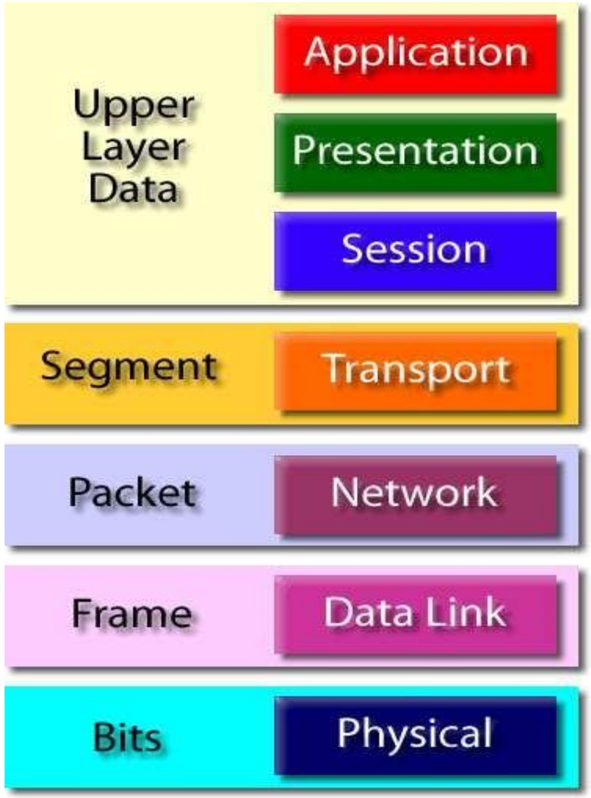
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial 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 70
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

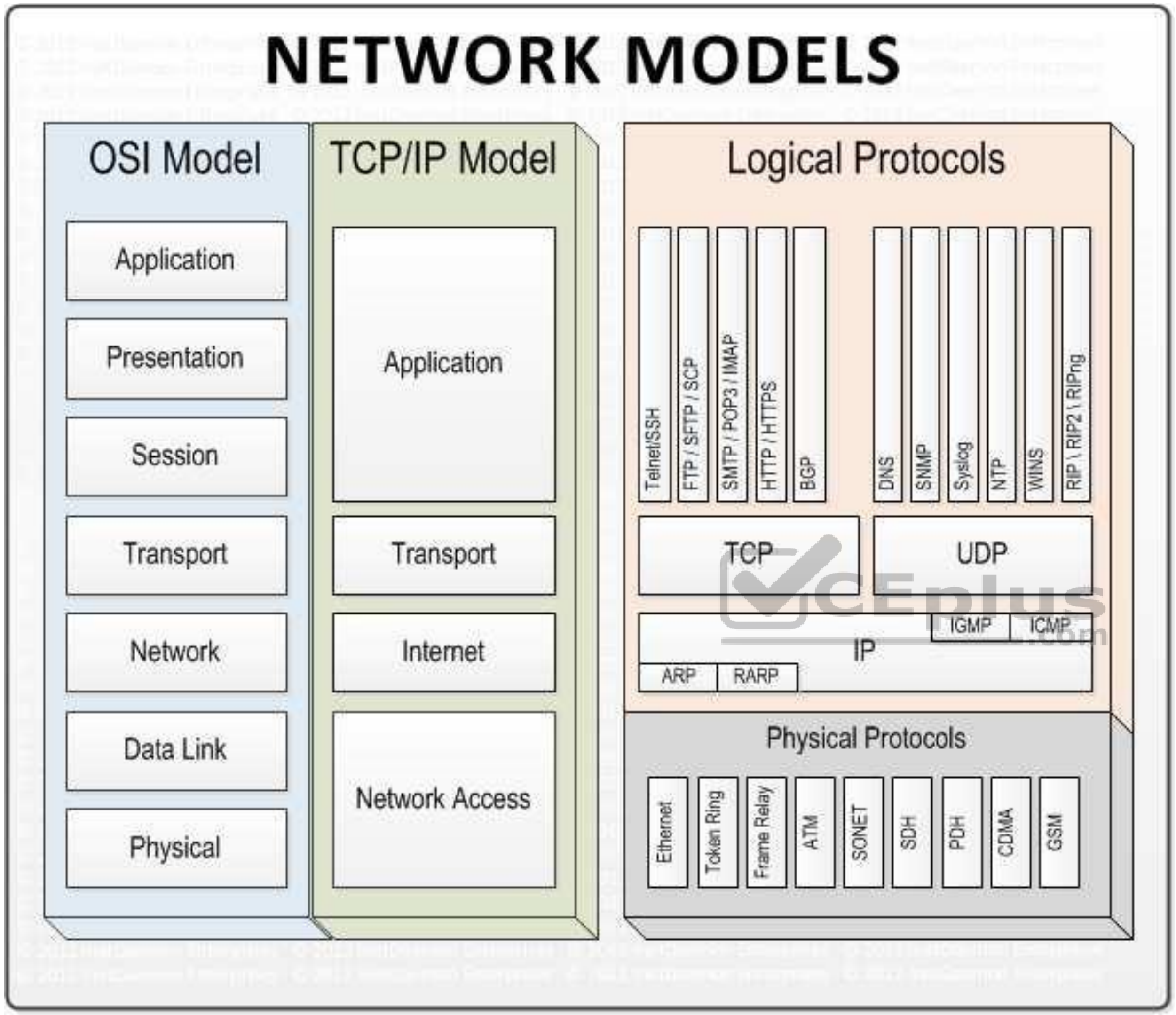
Explanation

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).

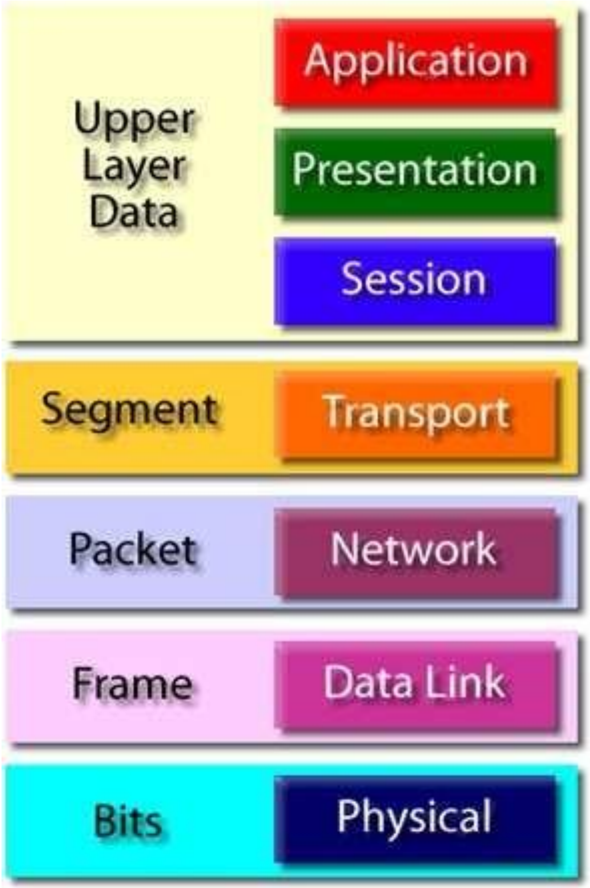
Layer 1. Network Access Layer
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network 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 71

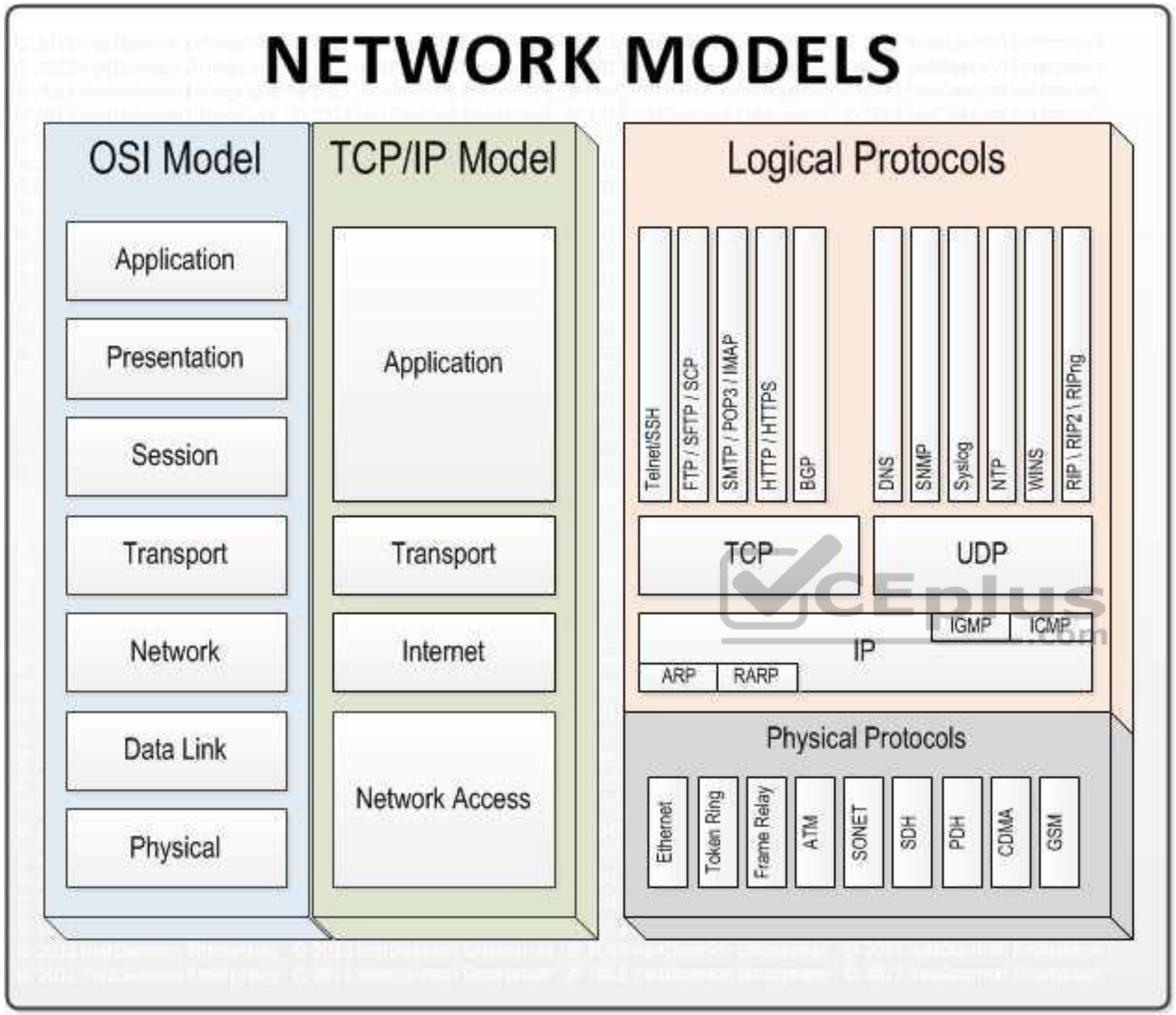
Which of the following is the protocol data unit (PDU) of application layer in TCP/IP model?

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.

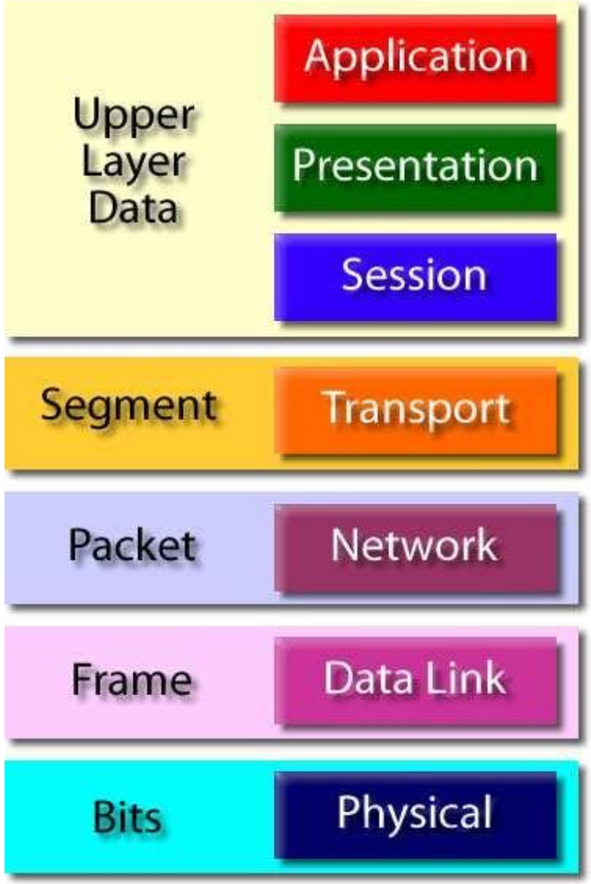
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 72

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

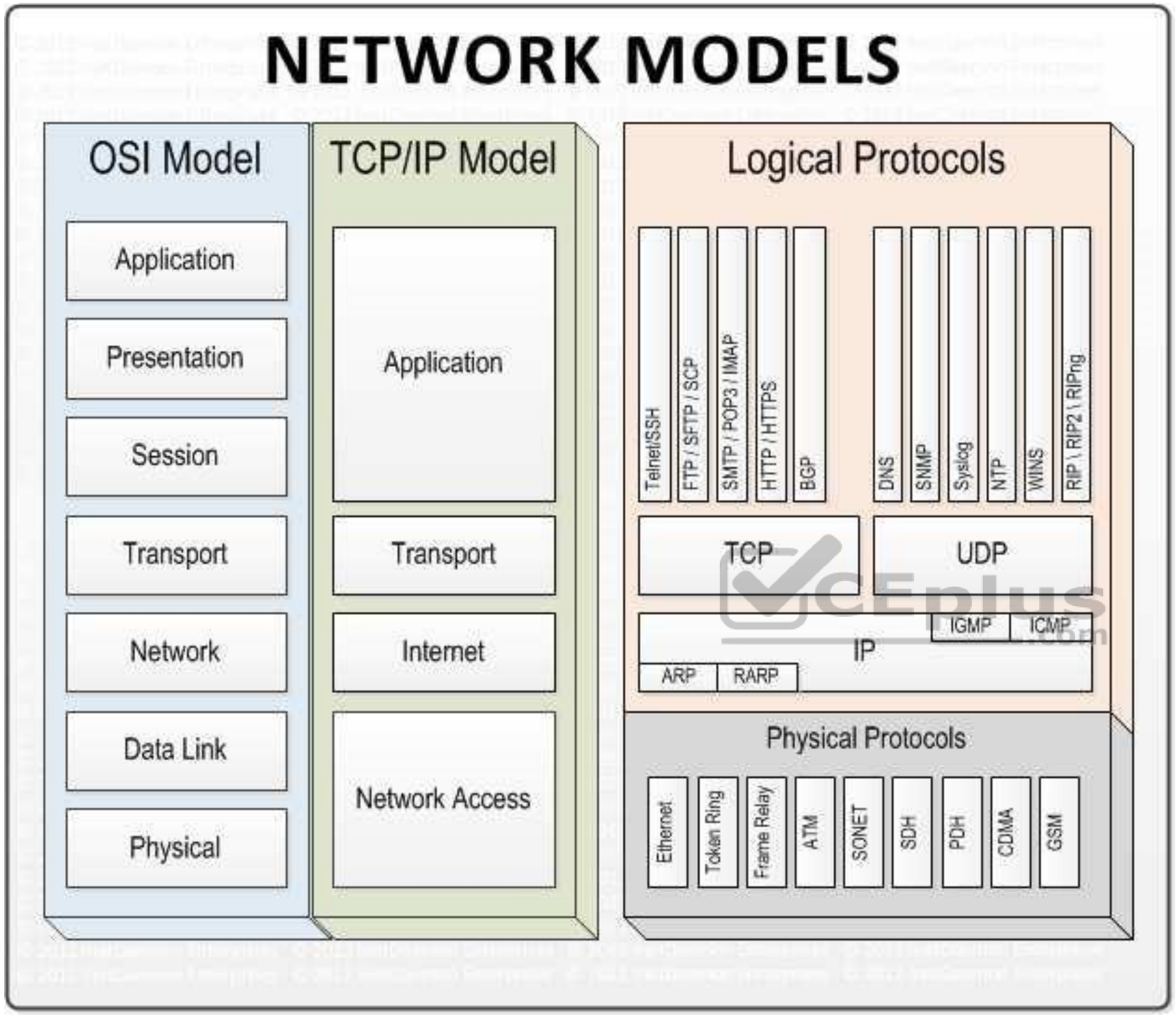
Section: Information System Operations, Maintenance and Support

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.

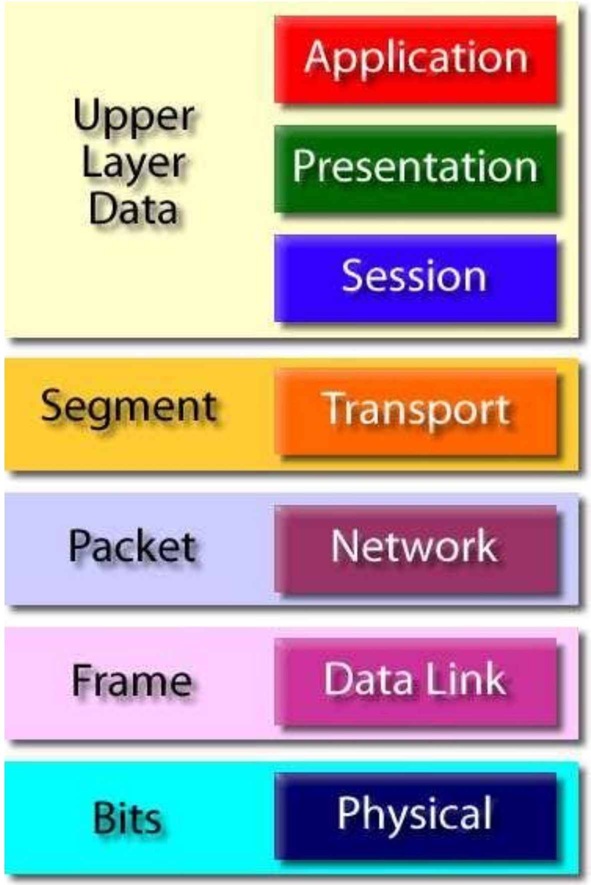
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 73

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

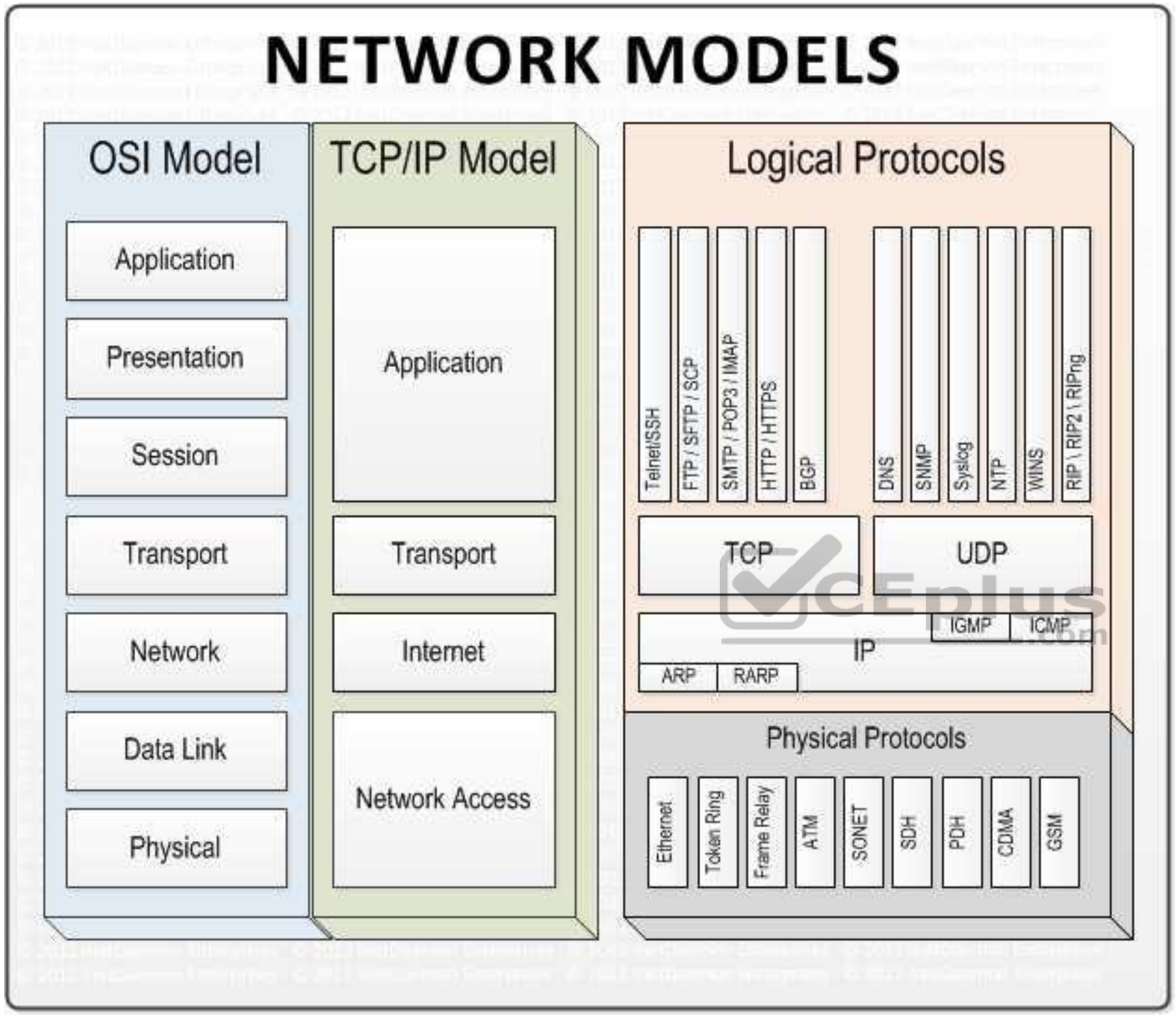
Section: Information System Operations, Maintenance and Support

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.

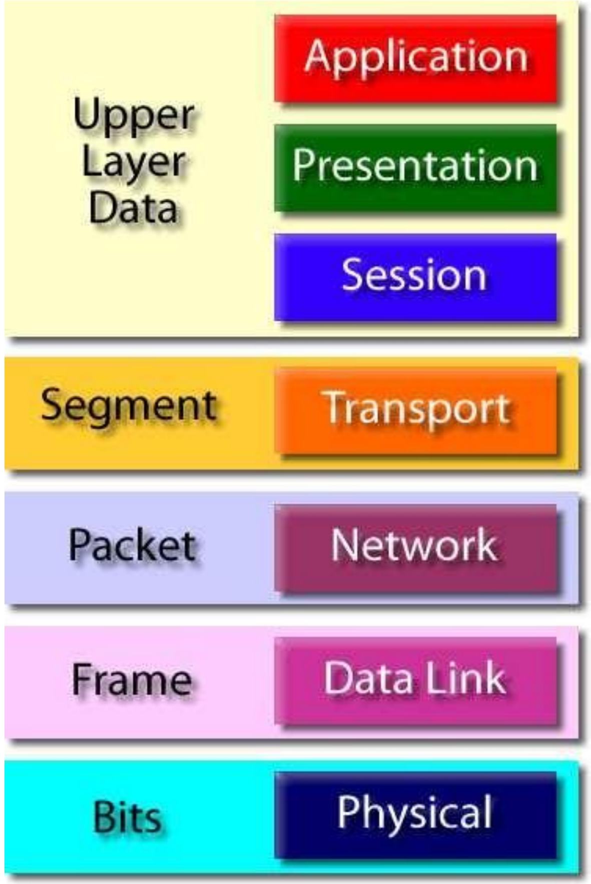
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 74

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

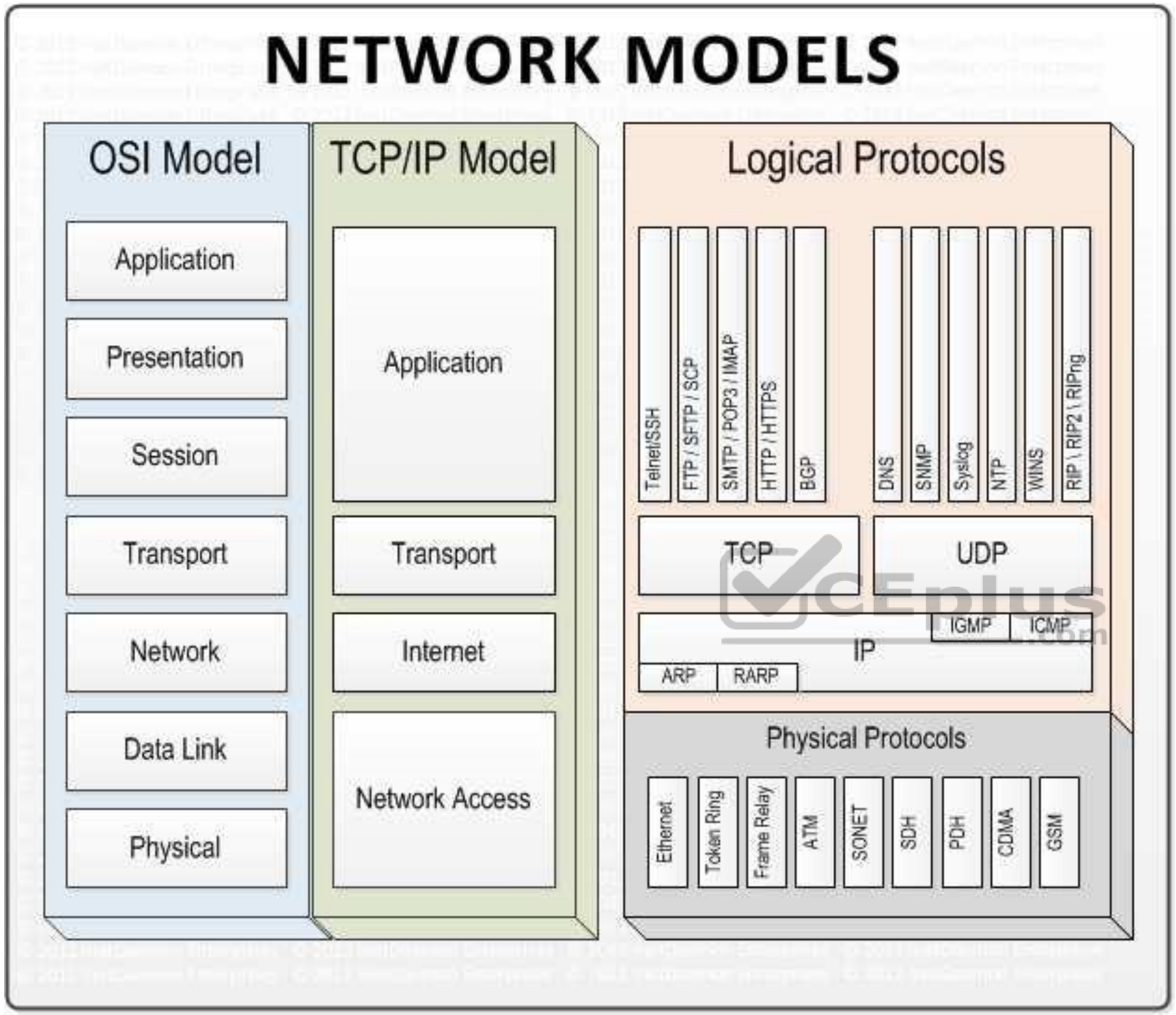
Section: Information System Operations, Maintenance and Support

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.

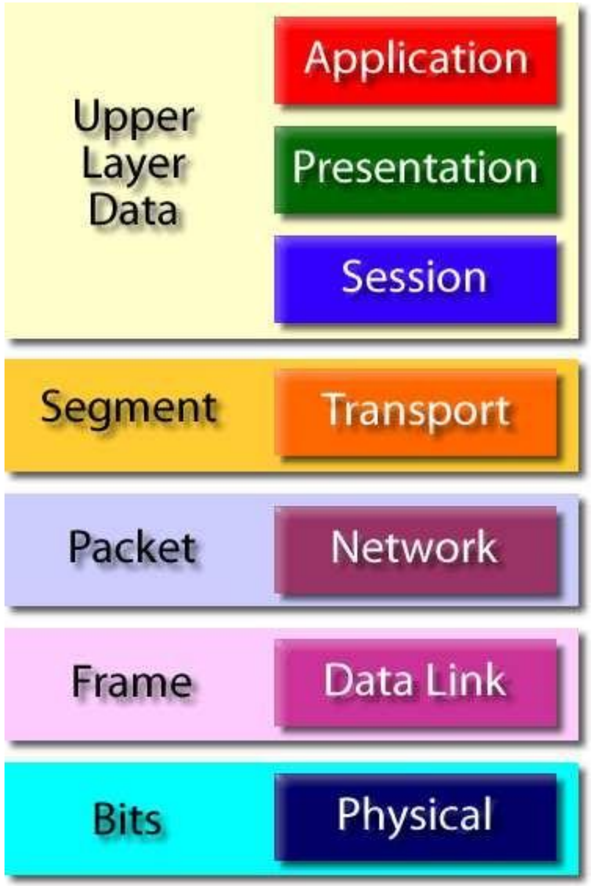
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 75
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

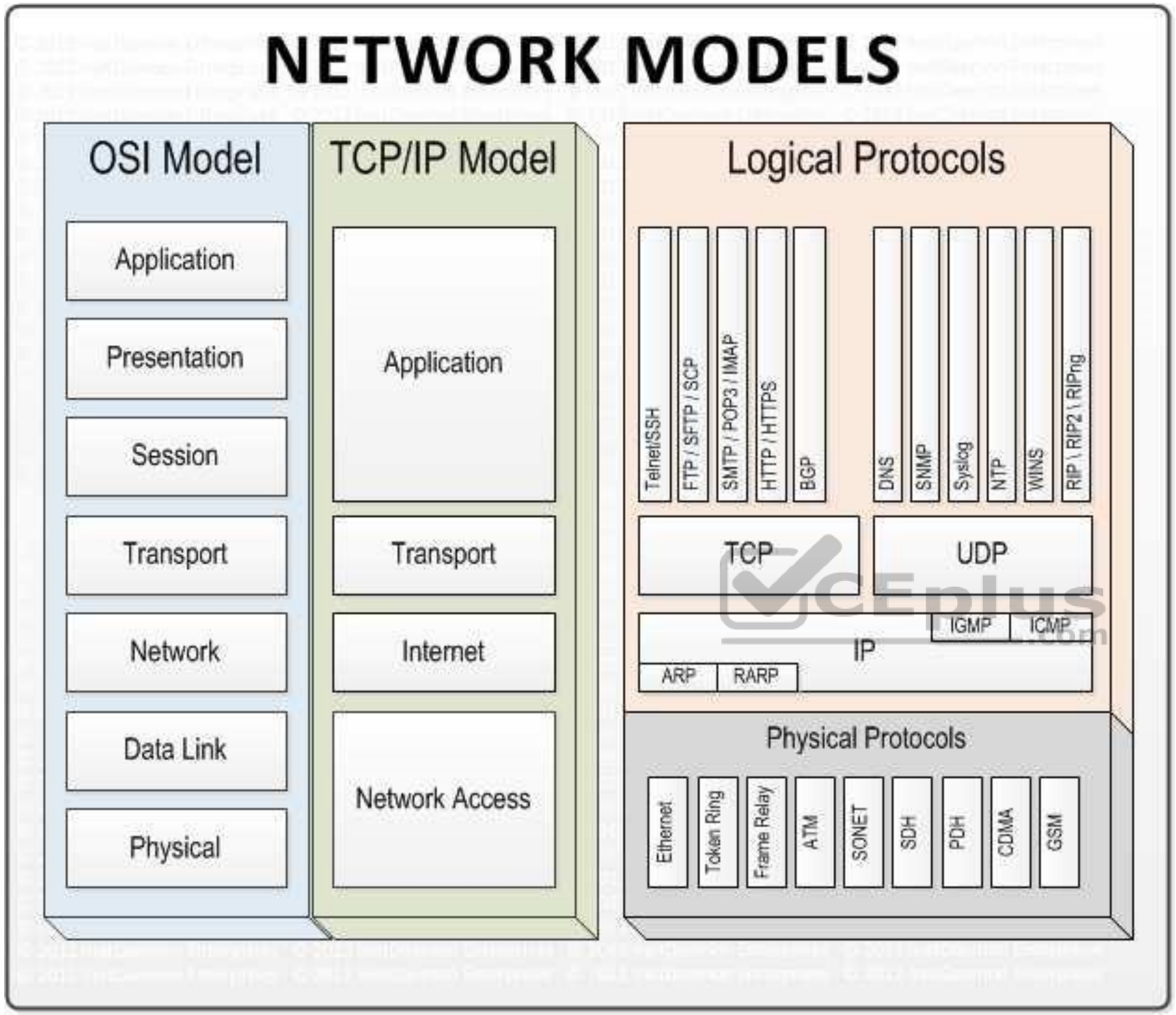
Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

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.

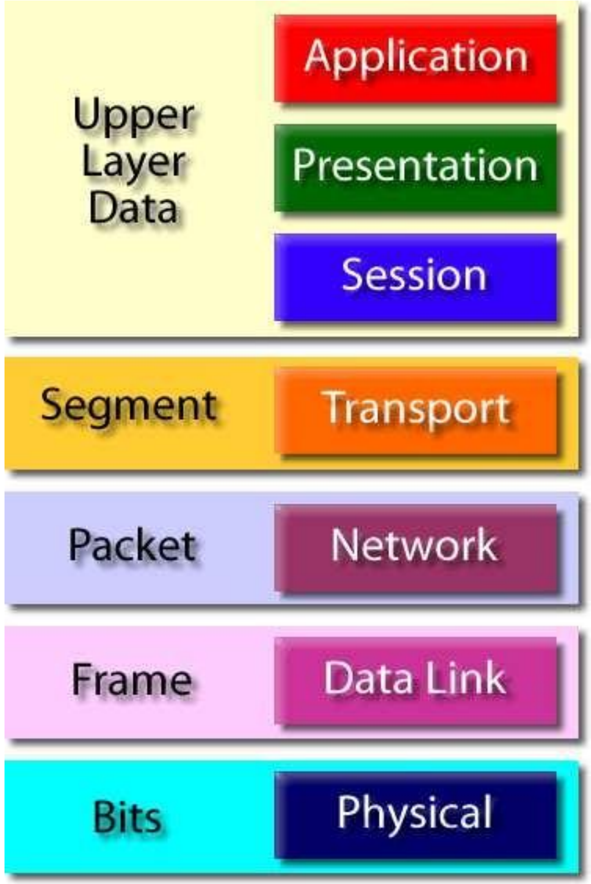
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 76
Which of the following INCORRECTLY describes the layer functions of the LAN or WAN Layer of the TCP/IP model?

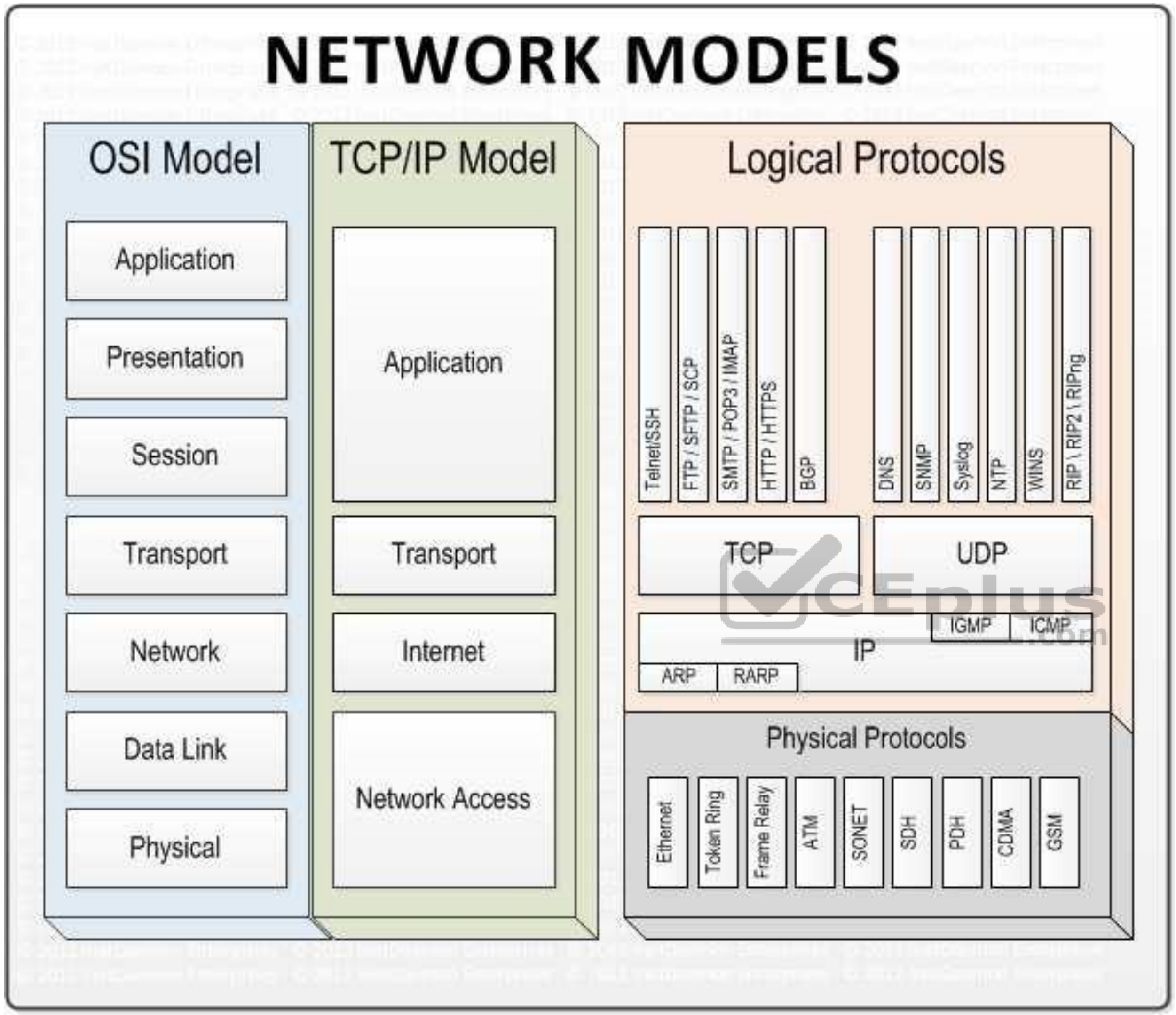
A. Combines packets into bytes and bytes into frame
B. Providers logical addressing which routers use for path determination
C. Provide address to media using MAC address
D. Performs only error detection

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.

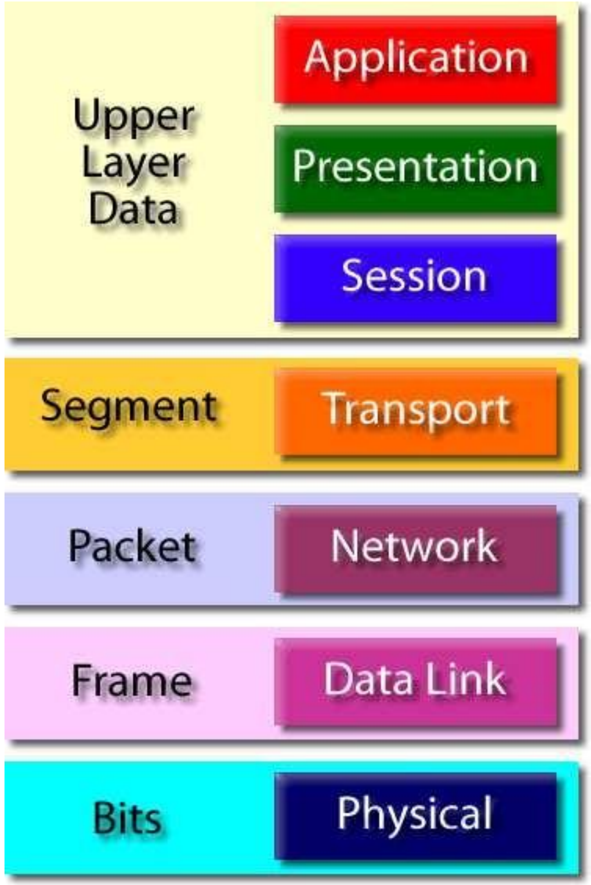
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 77
Which of the following functionality is NOT performed by the application layer of a TCP/IP model?

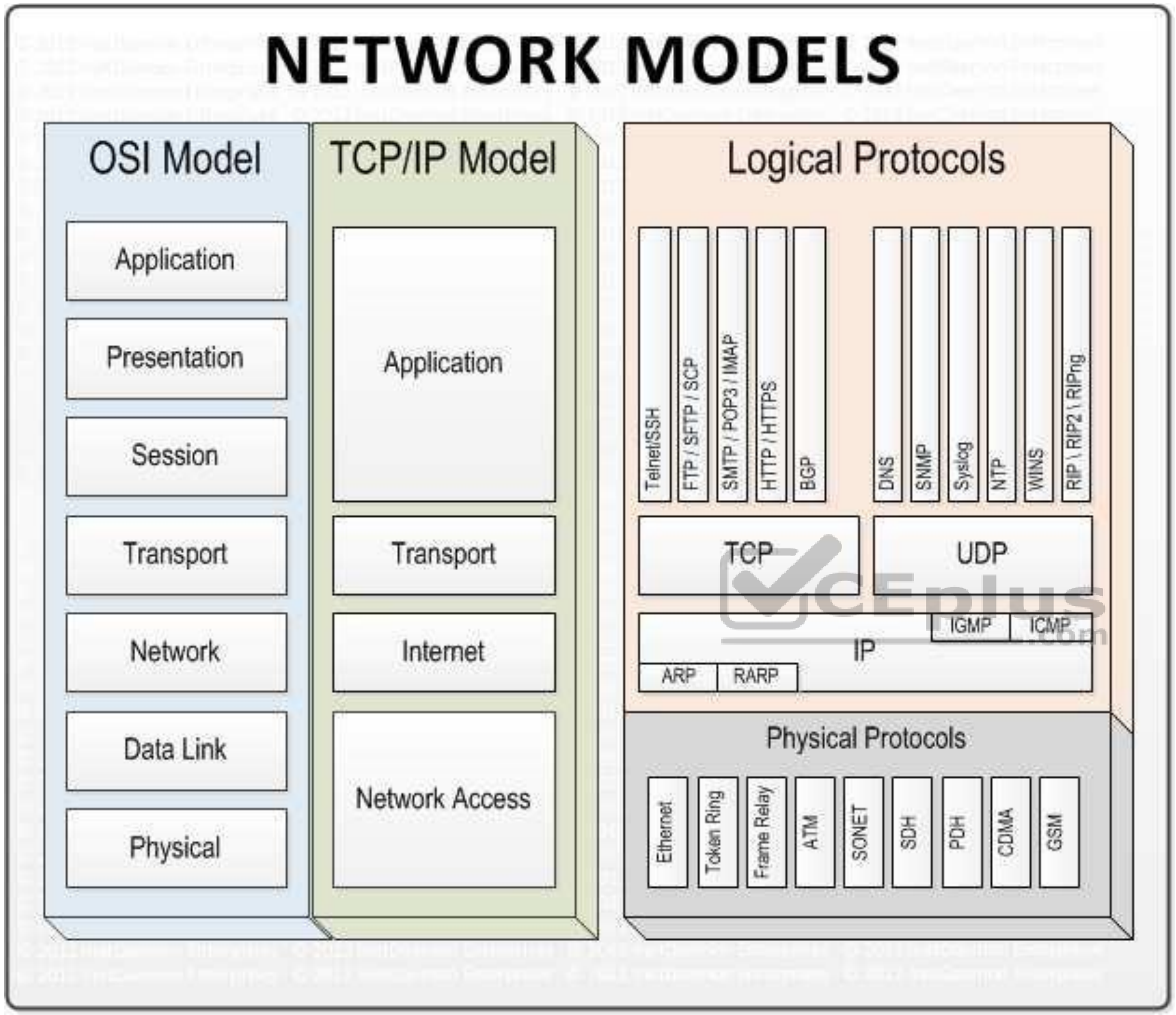
A. Print service, application services
B. Data encryption and compression
C. Dialog management
D. End-to-end connection

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.

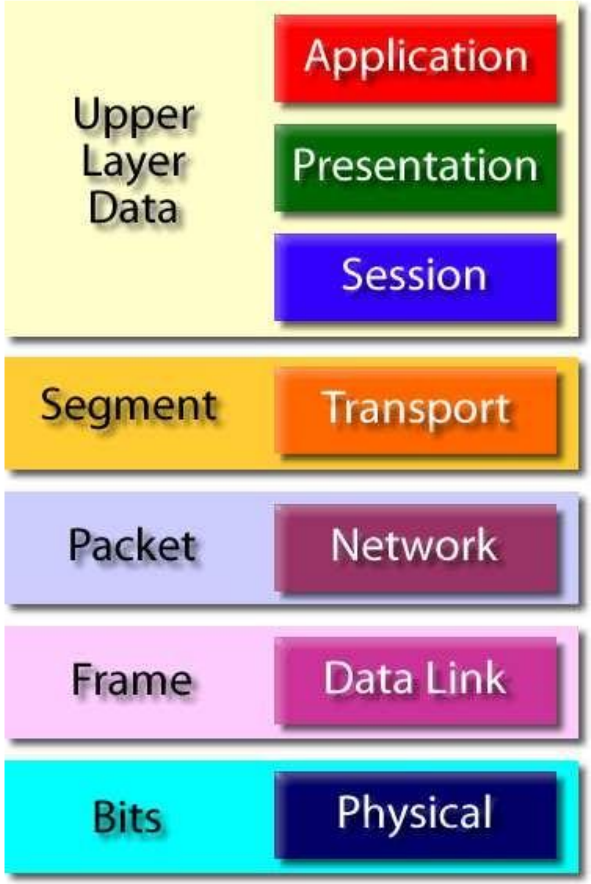
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 78
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

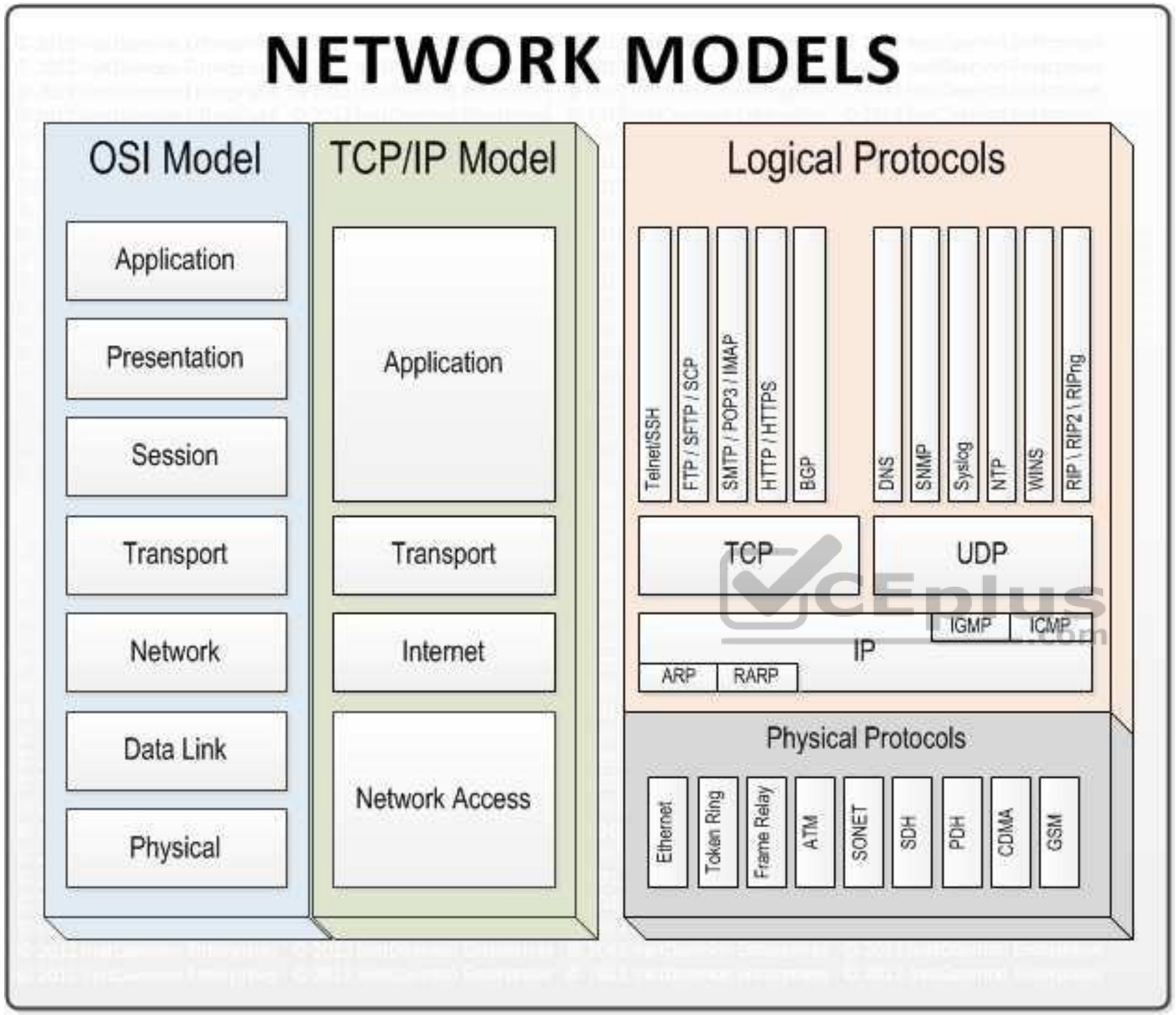
Correct Answer: C
Section: Information System Operations, Maintenance and Support
Explanation

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.

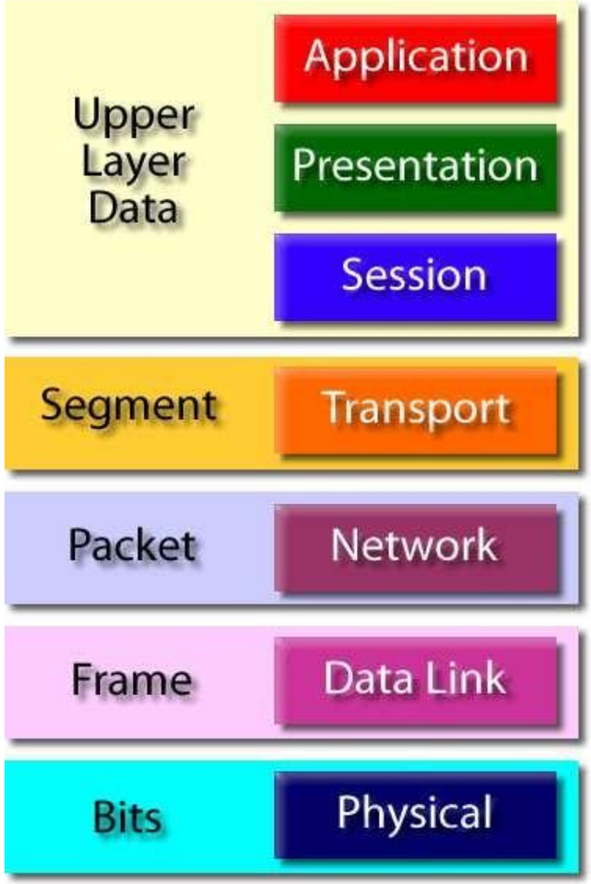
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 79
Which of the following is the INCORRECT “layer - protocol data unit (PDU)" mapping within the TCP/IP model?

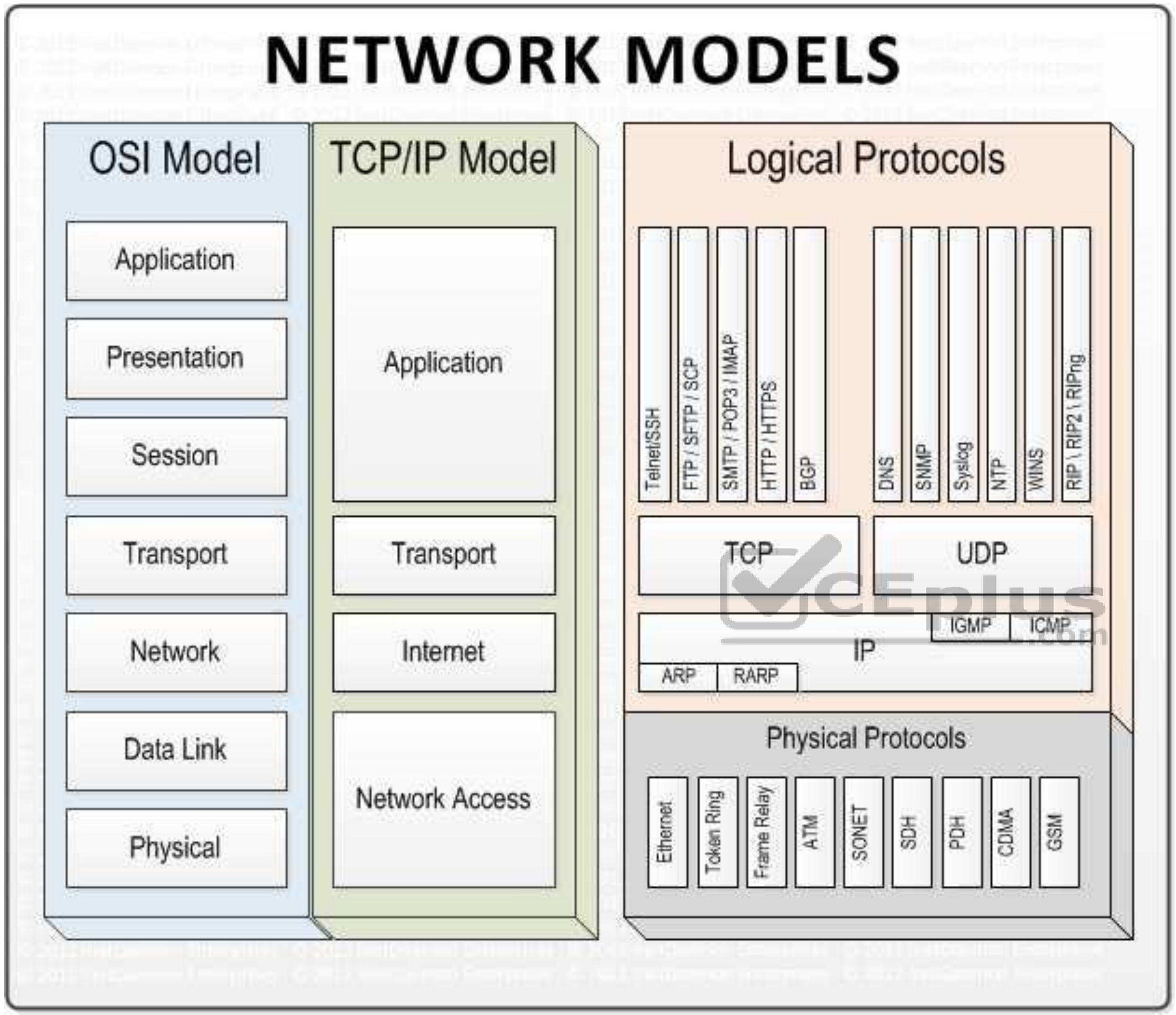
A. Application layer – Data
B. Transport layer – Segment
C. Network layer – Frame
D. Physical layer – bits

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.

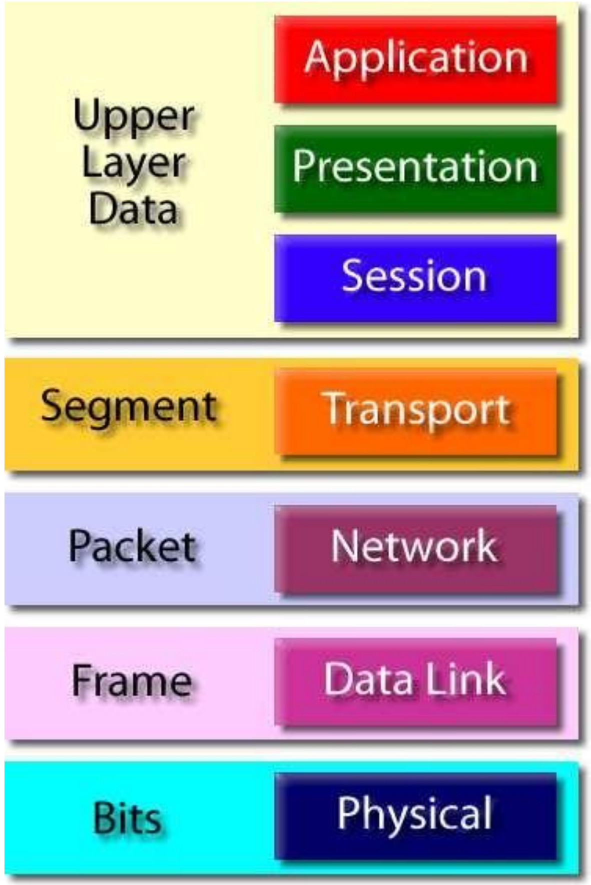
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 80
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 81
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 82
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 83
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 84
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 85
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

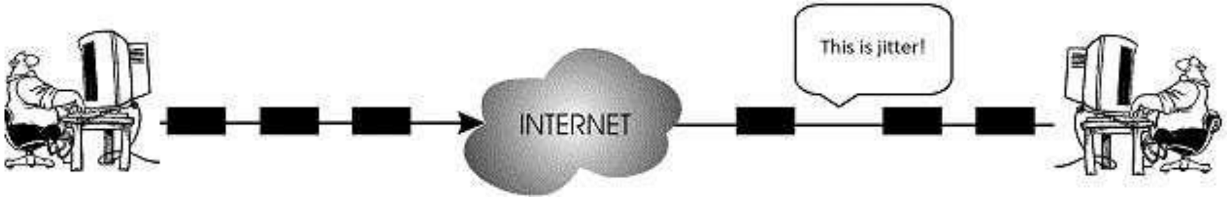


Image from: http://howdoesinternetwork.com/wp-content/uploads/2013/05/jitter.gif

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 86
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 87
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 88
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

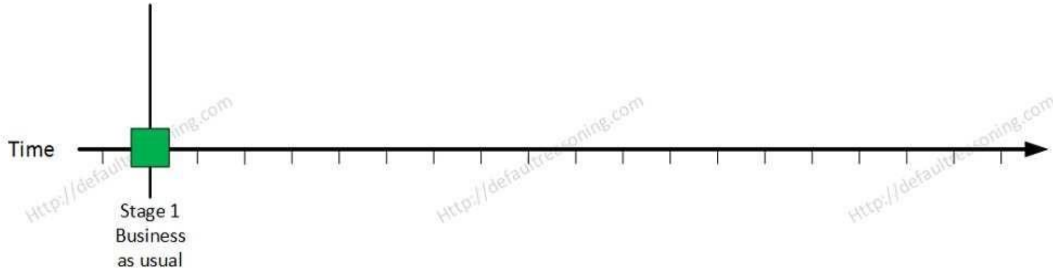


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png

At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs

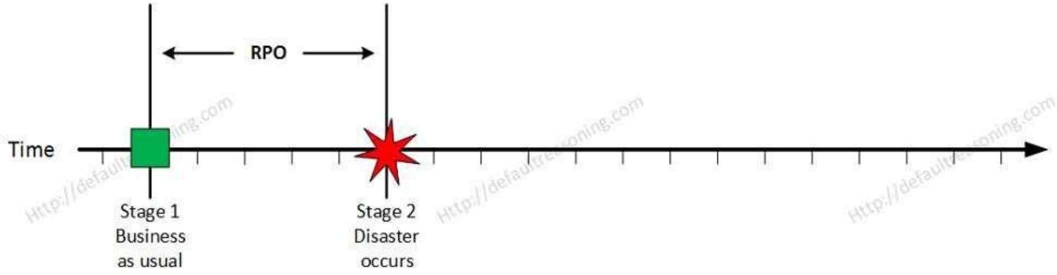


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

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

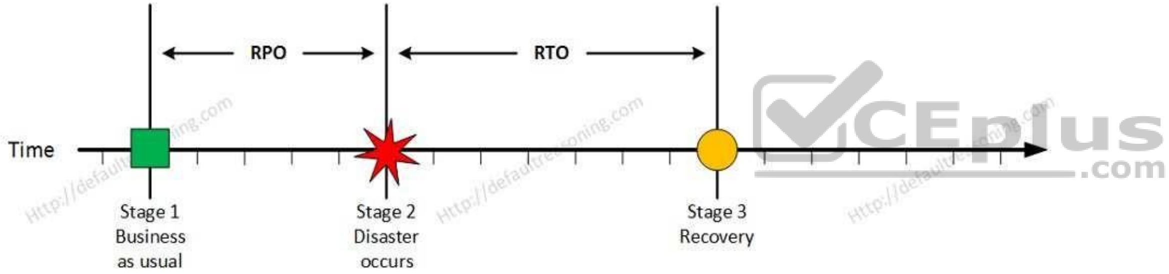


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

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

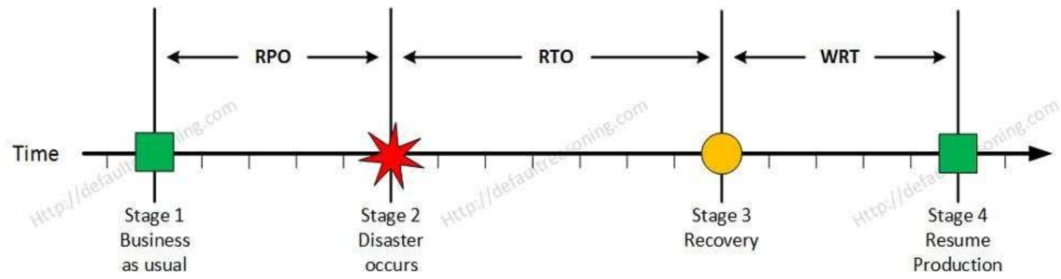


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

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

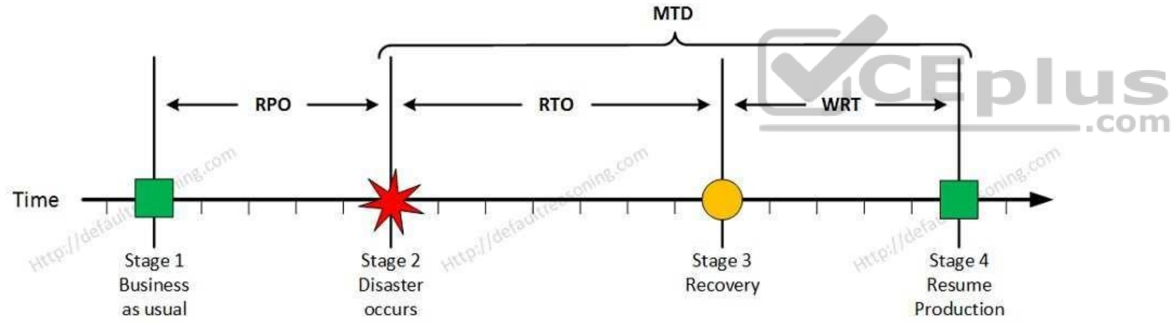


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png

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 89
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.

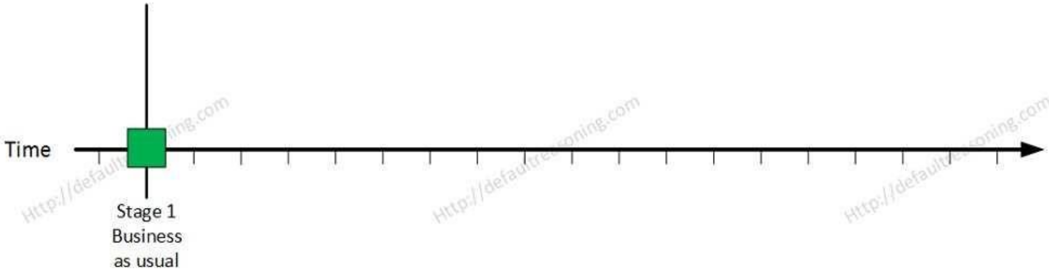
In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance.

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

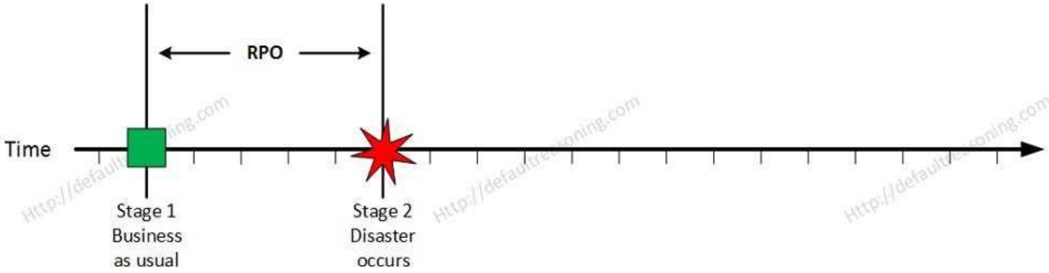


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

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

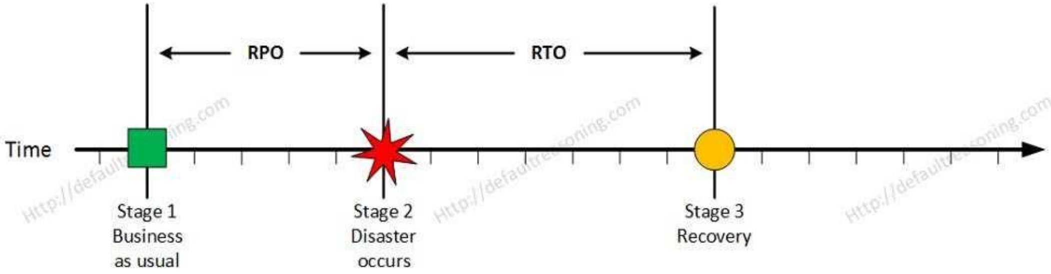


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

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

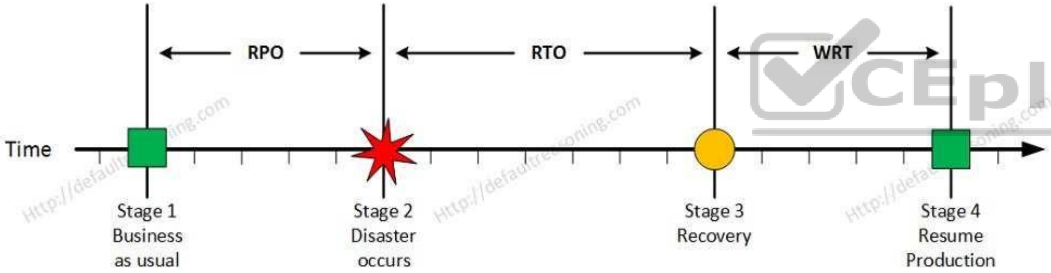


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

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

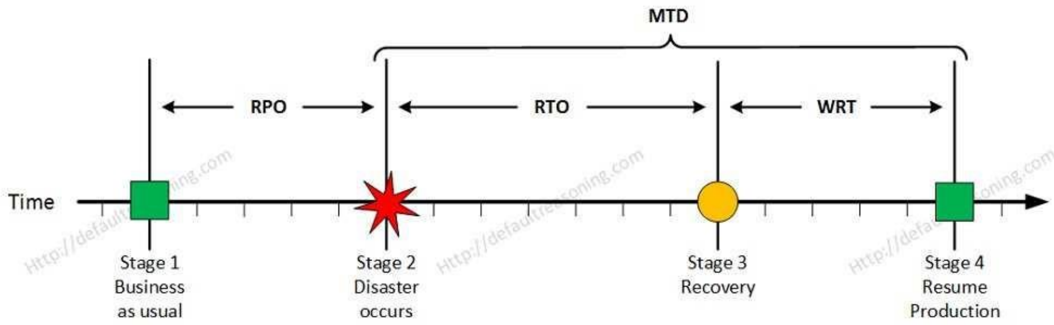


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should 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 90
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?

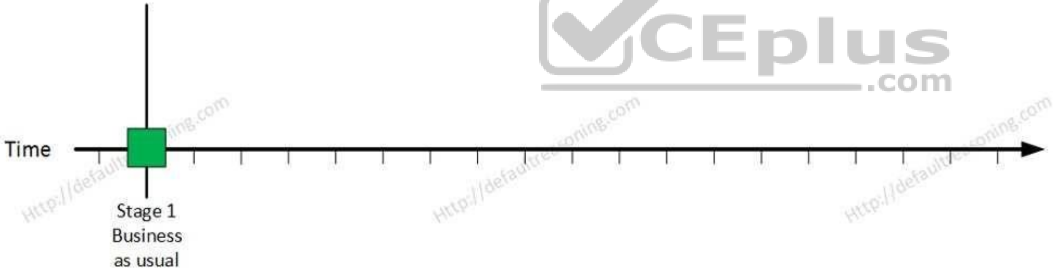
A. RPO
B. RTO
C. WRT
D. MTD

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

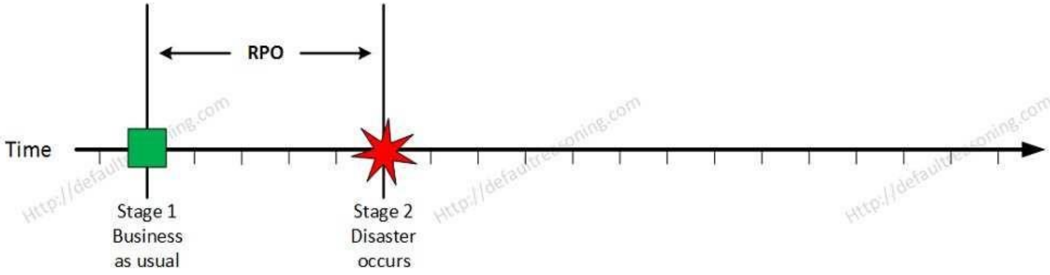


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

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

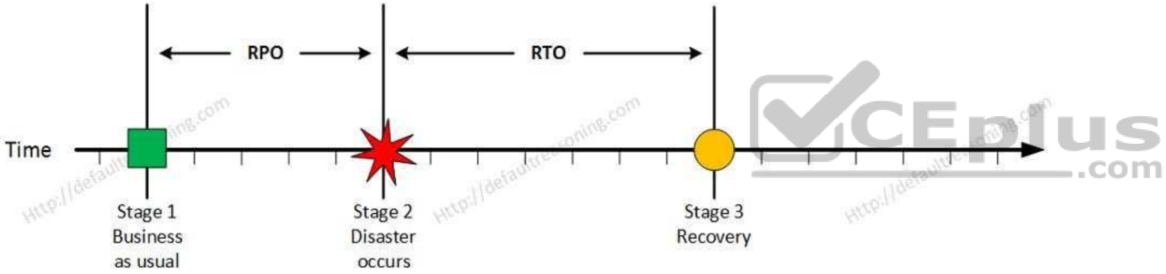


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

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

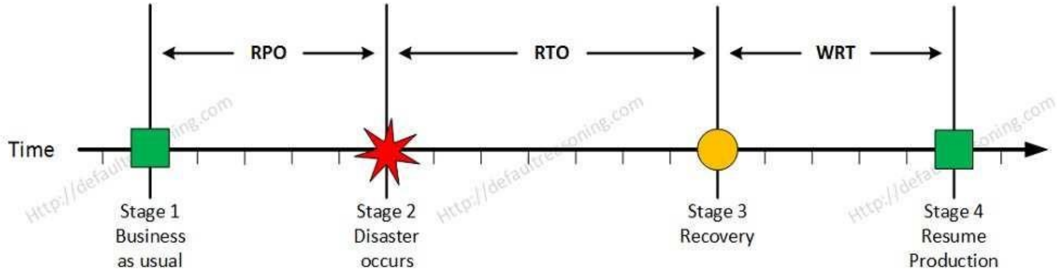


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

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

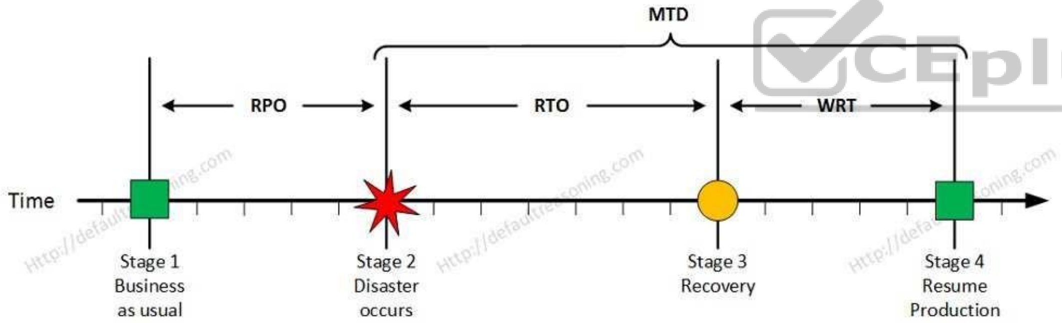


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png

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 91
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

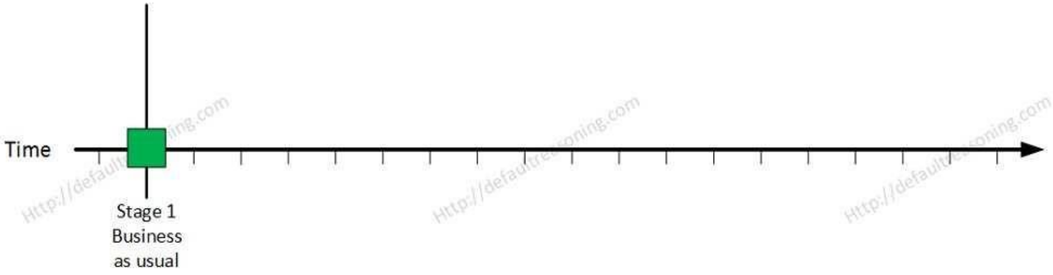


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png

At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs

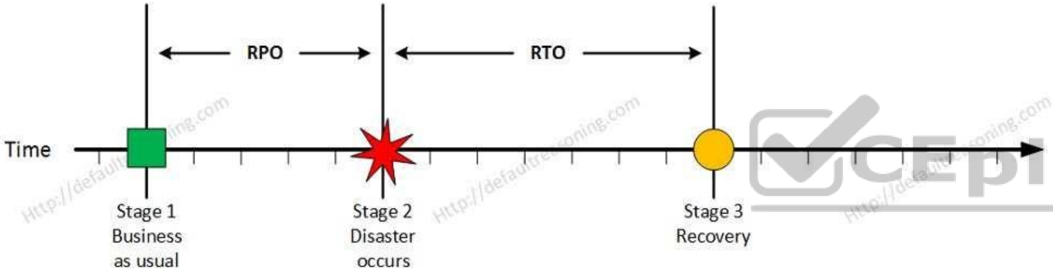


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

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

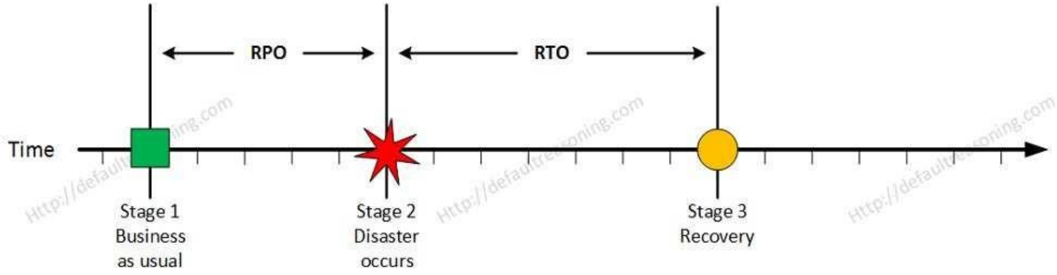


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

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

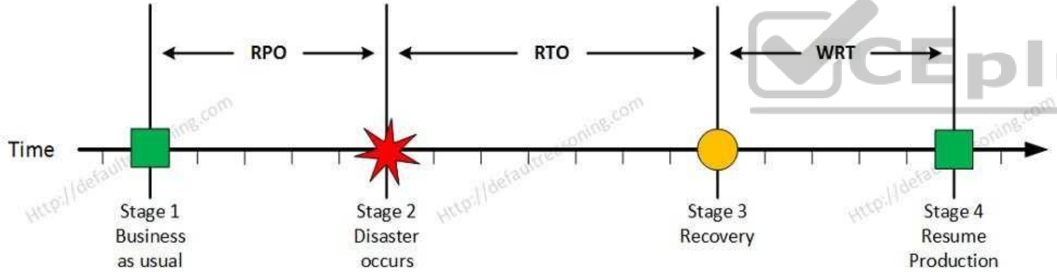


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

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

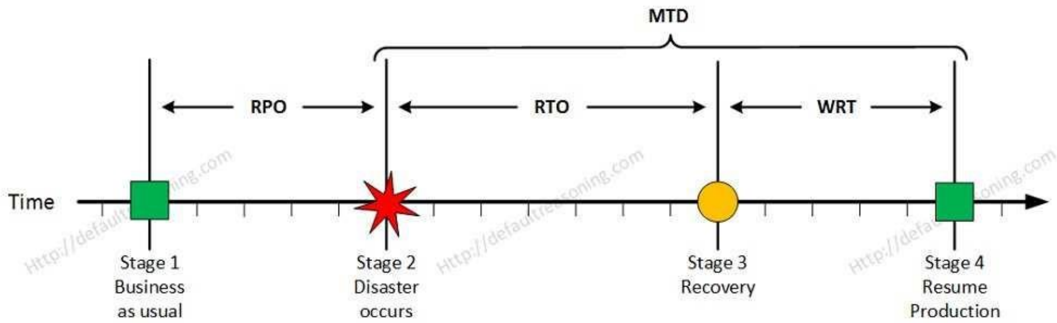


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should 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 92
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

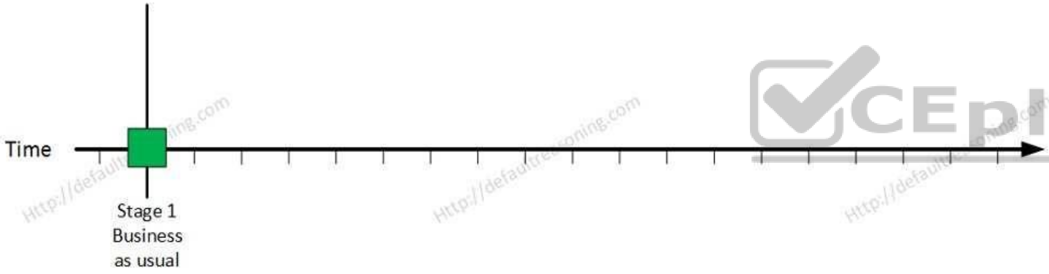


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png

At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs
Disaster Occurs

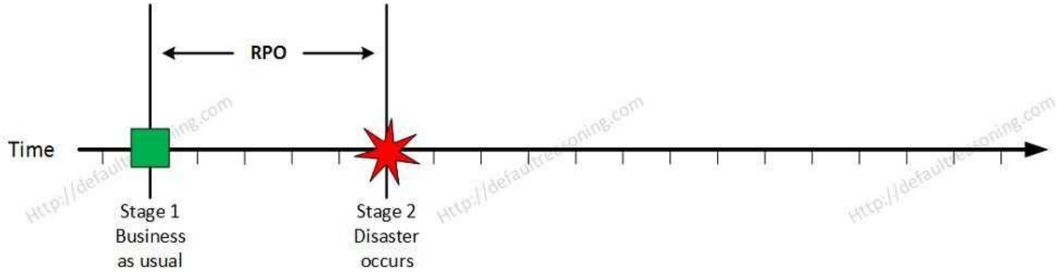


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png

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

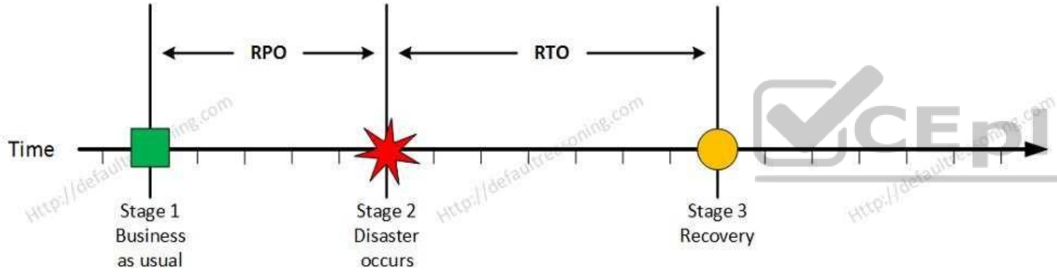


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png

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

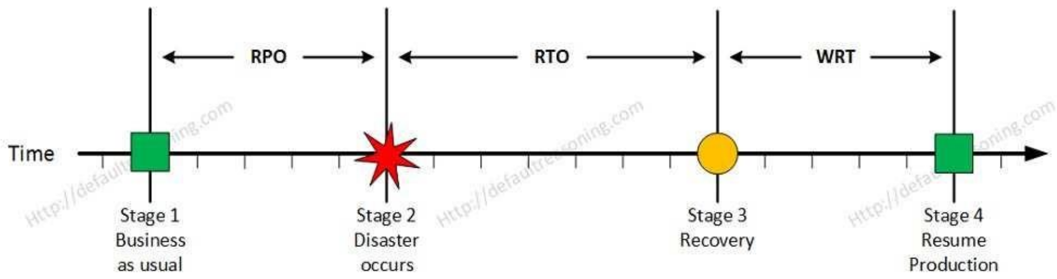


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png

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

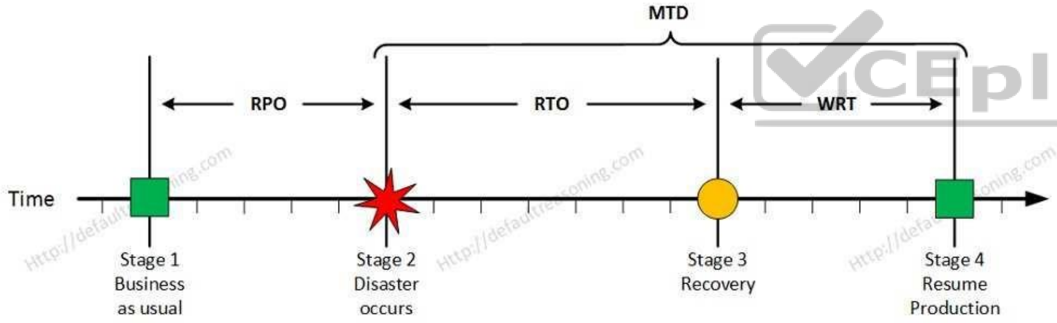


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png

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 93
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 94

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 95

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 96

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 97
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 98
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 99

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 100
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 101

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 102
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 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.

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 103
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 104
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 105

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 106
Which of the following statement INCORRECTLY describes anti-malware?

A 2
B 22
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 107
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 108
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 109
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 110
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 111

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 112
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 113
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 114
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 115
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 116
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 117

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 118
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 119
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 120
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 121
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 122
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 123

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 124
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 125
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 126
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 127

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 128
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 129
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 130
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 131
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 132
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 133
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 134
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 135

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 136

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

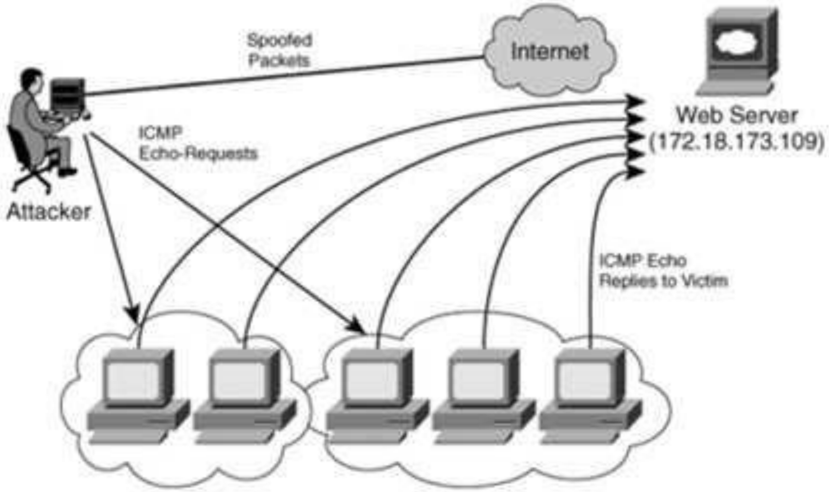


Image reference - http://resources.infosecinstitute.com/wp-content/uploads/012813_1439_HaveYouEver2.png

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 137

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 138
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 139
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 140
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 141
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 142
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 143
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 analysisC. 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 144
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.

Confidentiality
Integrity
Data
Availability

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 145

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 146
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 147
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

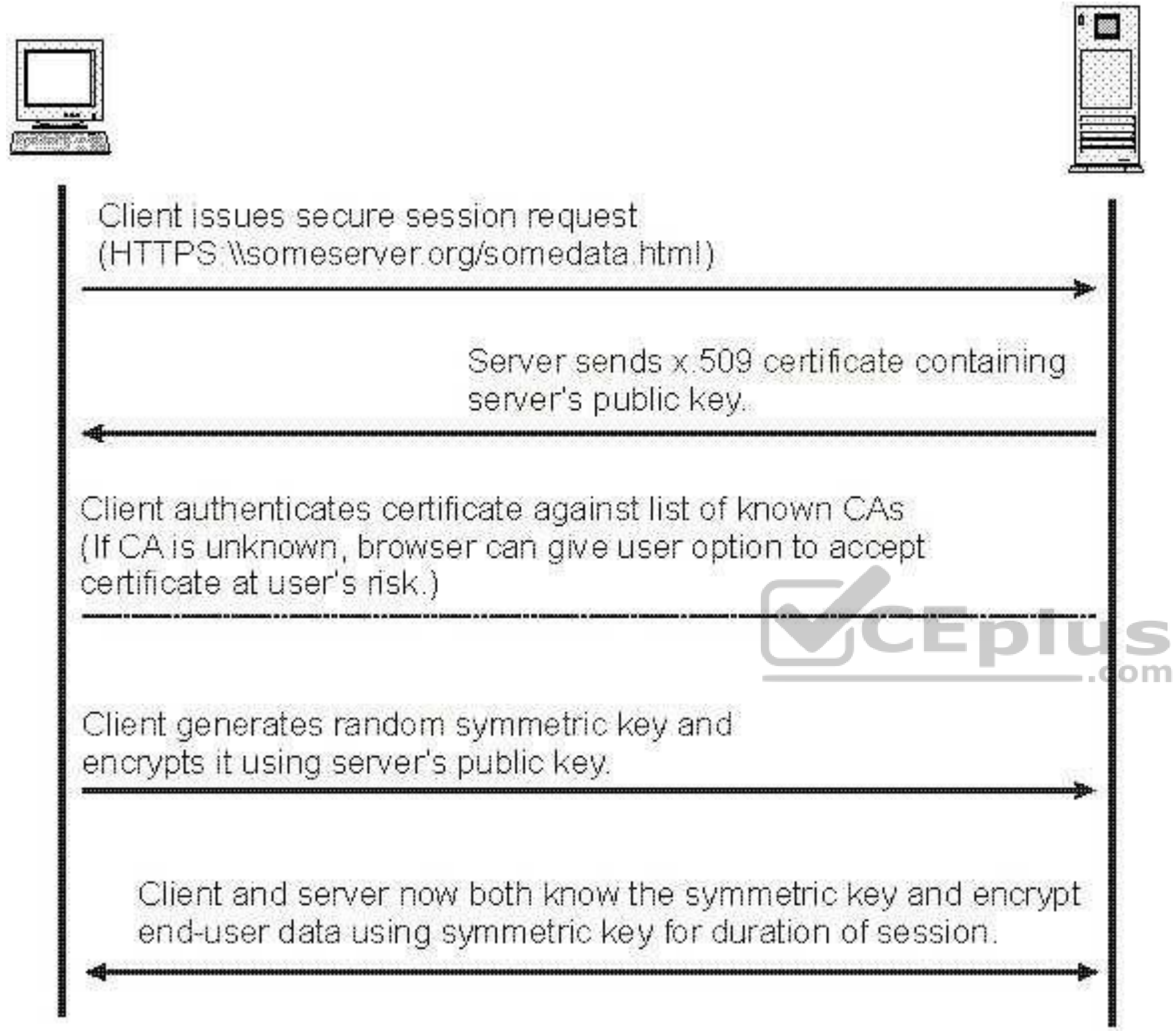

Client issues secure session request
(HTTPS \\someserver.org/somedata.html)
Server sends x.509 certificate containing
server's public key.
Client authenticates certificate against list of known CAs
(If CA is unknown, browser can give user option to accept
certificate at user's risk.)
Client generates random symmetric key and
encrypts it using server's public key.
Client and server now both know the symmetric key and encrypt
end-user data using symmetric key for duration of session.

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 148
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.

QUESTION 149
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 150
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 151
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 152
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 153
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 154
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 155
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 156
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 157
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 158
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 159
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 160
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 161
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 162
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 163

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 164

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 165

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 166

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 167
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 168
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 169

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 170

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 171
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 172
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 173
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 174
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 175
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 176
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 177
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 178
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 179
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 180
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 181
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 182

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 183

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 184

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 185

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 186

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 187

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 188

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 189

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 190

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 191
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 192
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.

QUESTION 193
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 194
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 195
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 196
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 197

Which of the following is a good control for protecting confidential data residing on a PC?

A. Personal firewall
B. File encapsulation
C. File encryption
D. Host-based intrusion detection

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
File encryption is a good control for protecting confidential data residing on a PC.

QUESTION 198

Which of the following is a guiding best practice for implementing logical access controls?

A. Implementing the Biba Integrity Model
B. Access is granted on a least-privilege basis, per the organization's data owners
C. Implementing the Take-Grant access control model
D. Classifying data according to the subject’s requirements

Correct Answer: B

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners.

QUESTION 199
What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

A. A combination of public-key cryptography and digital certificates and two-factor authentication
B. A combination of public-key cryptography and two-factor authentication
C. A combination of public-key cryptography and digital certificates
D. A combination of digital certificates and two-factor authentication

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

QUESTION 200
Which of the following do digital signatures provide?

A. Authentication and integrity of data
B. Authentication and confidentiality of data
C. Confidentiality and integrity of data
D. Authentication and availability of data

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary purpose of digital signatures is to provide authentication and integrity of datA.

QUESTION 201
Regarding digital signature implementation, which of the following answers is correct?

A. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
B. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
C. A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
D. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

QUESTION 202
Which of the following would provide the highest degree of server access control?

A. A mantrap-monitored entryway to the server room
B. Host-based intrusion detection combined with CCTV
C. Network-based intrusion detection
D. A fingerprint scanner facilitating biometric access control

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A fingerprint scanner facilitating biometric access control can provide a very high degree of server access control.

QUESTION 203
What are often the primary safeguards for systems software and data?

A. Administrative access controls
B. Logical access controls
C. Physical access controls
D. Detective access controls

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Logical access controls are often the primary safeguards for systems software and datA.

QUESTION 204
Which of the following is often used as a detection and deterrent control against Internet attacks?

A. Honeypots
B. CCTV
C. VPN
D. VLAN

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Honeypots are often used as a detection and deterrent control against Internet attacks.

QUESTION 205
Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

A. A monitored double-doorway entry system
B. A monitored turnstile entry system
C. A monitored doorway entry system

D. A one-way door that does not allow exit after entry

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A monitored double-doorway entry system, also referred to as a mantrap or deadman door, is used a deterrent control for the vulnerability of piggybacking.

QUESTION 206
Which of the following is an effective method for controlling downloading of files via FTP?

A. An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
B. An application-layer gateway, or proxy firewall
C. A circuit-level gateway
D. A first-generation packet-filtering firewall

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

QUESTION 207
Which of the following provides the strongest authentication for physical access control?

A. Sign-in logs
B. Dynamic passwords
C. Key verification
D. Biometrics

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Biometrics can be used to provide excellent physical access control.

QUESTION 208
What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off?

A. Employee security awareness training
B. Administrator alerts
C. Screensaver passwords
D. Close supervision

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off.

QUESTION 209
What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources?

A. OSI Layer 2 switches with packet filtering enabled
B. Virtual Private Networks
C. Access Control Lists (ACL)
D. Point-to-Point Tunneling Protocol

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
ISPs can use access control lists to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources.

QUESTION 210

What is the key distinction between encryption and hashing algorithms?

A. Hashing algorithms ensure data confidentiality.
B. Hashing algorithms are irreversible.
C. Encryption algorithms ensure data integrity.
D. Encryption algorithms are not irreversible.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A key distinction between encryption and hashing algorithms is that hashing algorithms are irreversible.

QUESTION 211
Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

A. Data diddling
B. Skimming
C. Data corruption
D. Salami attack

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data diddling involves modifying data before or during systems data entry.

QUESTION 212
Which of the following is used to evaluate biometric access controls?

A. FAR
B. EER
C. ERR
D. FRR

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When evaluating biometric access controls, a low equal error rate (EER) is preferred. EER is also called the crossover error rate (CER).

QUESTION 213
Who is ultimately responsible and accountable for reviewing user access to systems?

A. Systems security administrators
B. Data custodians
C. Data owners
D. Information systems auditors

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data owners are ultimately responsible and accountable for reviewing user access to systems.

QUESTION 214
Establishing data ownership is an important first step for which of the following processes?

A. Assigning user access privileges
B. Developing organizational security policies
C. Creating roles and responsibilities
D. Classifying data

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

To properly implement data classification, establishing data ownership is an important first step.

QUESTION 215
Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

A. End-user involvement
B. Senior management involvement
C. Security administration involvement
D. IS auditing involvement

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
End-user involvement is critical during the business impact assessment phase of business continuity planning.

QUESTION 216
What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

A. Paper
B. Preparedness
C. Walk-through
D. Parallel

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Of the three major types of BCP tests (paper, walk-through, and preparedness), only the preparedness test uses actual resources to simulate a system crash and validate the plan's effectiveness.

QUESTION 217
Which of the following typically focuses on making alternative processes and resources available for transaction processing?

A. Cold-site facilities
B. Disaster recovery for networks
C. Diverse processing
D. Disaster recovery for systems

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Disaster recovery for systems typically focuses on making alternative processes and resources available for transaction processing.

QUESTION 218
Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

A. Parallel
B. Preparedness
C. Walk-thorough
D. Paper

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Of the three major types of BCP tests (paper, walk-through, and preparedness), a walk-through test requires only that representatives from each operational area meet to review the plan.

QUESTION 219
What influences decisions regarding criticality of assets?

A. The business criticality of the data to be protected
B. Internal corporate politics
C. The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
D. The business impact analysis

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

QUESTION 220
Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

A. Cold site
B. Alternate site
C. Hot site
D. Warm site

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

QUESTION 221
With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
With the objective of mitigating the risk and impact of a major business interruption, a disaster- recovery plan should endeavor to reduce the length of recovery time necessary and the costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs.

QUESTION 222
Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

A. Cold site
B. Hot site
C. Alternate site
D. Warm site

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data.

QUESTION 223
Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following?

A. IT strategic plan
B. Business continuity plan
C. Business impact analysis
D. Incident response plan

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

QUESTION 224

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _______________________. (fill-in-the-blank)

A. Security administrator
B. Systems auditor
C. Board of directors
D. Financial auditor

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the board of directors.

QUESTION 225
Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Obtaining user approval of program changes is very effective for controlling application changes and maintenance.

QUESTION 226
Library control software restricts source code to:

A. Read-only access
B. Write-only access
C. Full access
D. Read-write access

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Library control software restricts source code to read-only access.

QUESTION 227
When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

A. In program development and change management
B. In program feasibility studies
C. In program development
D. In change management

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Regression testing is used in program development and change management to determine whether new changes have introduced any errors in the remaining unchanged code.

QUESTION 228
What is often the most difficult part of initial efforts in application development?
A. Configuring software
B. Planning security
C. Determining time and resource requirements
D. Configuring hardware

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Determining time and resource requirements for an application-development project is often the most difficult part of initial efforts in application development.

QUESTION 229
What is a primary high-level goal for an auditor who is reviewing a system development project?

A. To ensure that programming and processing environments are segregated
B. To ensure that proper approval for the project has been obtained
C. To ensure that business objectives are achieved
D. To ensure that projects are monitored and administrated effectively

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A primary high-level goal for an auditor who is reviewing a systems- development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

QUESTION 230
Whenever an application is modified, what should be tested to determine the full impact of the change?

A. Interface systems with other applications or systems
B. The entire program, including any interface systems with other applications or systems
C. All programs, including interface systems with other applications or systems
D. Mission-critical functions and any interface systems with other applications or systems

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change.

QUESTION 231
The quality of the metadata produced from a data warehouse is ________________ in the warehouse’s design.

A. Often hard to determine because the data is derived from a heterogeneous data environment
B. The most important consideration
C. Independent of the quality of the warehoused databases
D. Of secondary importance to data warehouse content

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

QUESTION 232
Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Function point analysis (FPA) provides an estimate of the size of an information system based on the number and complexity of a system's inputs, outputs, and files.

QUESTION 233
Who assumes ownership of a systems-development project and the resulting system?

A. User management
B. Project steering committee
C. IT management
D. Systems developers

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
User management assumes ownership of a systems-development project and the resulting system.

QUESTION 234
If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

A. Documentation development
B. Comprehensive integration testing
C. Full unit testing
D. Full regression testing

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If an IS auditor observes individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further comprehensive integration testing.

QUESTION 235
When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When participating in a systems-development project, an IS auditor should also strive to ensure that adequate and complete documentation exists for all projects.

QUESTION 236
What is a reliable technique for estimating the scope and cost of a software-development project?

A. Function point analysis (FPA)
B. Feature point analysis (FPA)
C. GANTT
D. PERT

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A function point analysis (FPA) is a reliable technique for estimating the scope and cost of a software-development project.

QUESTION 237
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

A. Function Point Analysis (FPA)
B. GANTT
C. Rapid Application Development (RAD)
D. PERT

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
PERT is a program-evaluation review technique that considers different scenarios for planning and control projects.

QUESTION 238
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do?

A. Lack of IT documentation is not usually material to the controls tested in an IT audit.
B. The auditor should at least document the informal standards and policies. Furthermore, the IS auditor should create formal documented policies to be implemented.
C. The auditor should at least document the informal standards and policies, and test for a compliance. Furthermore, the IS auditor should recommend management that formal documented policies be developed and implemented.
D. The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should create formal documented policies to be implemented.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, the auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.

QUESTION 239
What often results in project scope creep when functional requirements are not defined as well as they could be?

A. Inadequate software baselining
B. Insufficient strategic planning
C. Inaccurate resource allocation
D. Project delays

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:

Explanation:
Inadequate software baselining often results in project scope creep because functional requirements are not defined as well as they could be.

QUESTION 240
Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data- calculation procedures. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Fourth-generation languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

QUESTION 241
Run-to-run totals can verify data through which stage(s) of application processing?

A. Initial
B. Various
C. Final
D. Output

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Run-to-run totals can verify data through various stages of application processing.

QUESTION 242
________ (fill in the blank) is/are ultimately accountable for the functionality, reliability, and security within IT governance.

A. Data custodians

B. The board of directors and executive officers
C. IT security administration
D. Business unit managers

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The board of directors and executive officers are ultimately accountable for the functionality, reliability, and security within IT governance.

QUESTION 243
What can be used to help identify and investigate unauthorized transactions?

A. Postmortem review
B. Reasonableness checks
C. Data-mining techniques
D. Expert systems

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data-mining techniques can be used to help identify and investigate unauthorized transactions.

QUESTION 244
Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Network environments often add to the complexity of program-to-program communication, making application systems implementation and maintenance more difficult.

QUESTION 245
 isk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a __________________ risk assessment is more appropriate. Fill in the blanks.

A. Quantitative; qualitative
B. Qualitative; quantitativeC. Residual; subjective
D. Quantitative; subjective

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Quantitative risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a qualitative risk assessment is more appropriate.

QUESTION 246
What must an IS auditor understand before performing an application audit?

A. The potential business impact of application risks.
B. Application risks must first be identified.
C. Relative business processes.
D. Relevant application risks.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor must first understand relative business processes before performing an application audit.

QUESTION 247
What is the first step in a business process re-engineering project?

A. Identifying current business processes
B. Forming a BPR steering committee
C. Defining the scope of areas to be reviewedD. Reviewing the organizational strategic plan

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Defining the scope of areas to be reviewed is the first step in a business process re-engineering project.

QUESTION 248
When storing data archives off-site, what must be done with the data to ensure data completeness?

A. The data must be normalized.
B. The data must be validated.
C. The data must be parallel-tested.
D. The data must be synchronized.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When storing data archives off-site, data must be synchronized to ensure data completeness

QUESTION 249
Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

A. Redundancy check
B. Completeness check
C. Accuracy check
D. Parity check

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of data.

QUESTION 250
What is an edit check to determine whether a field contains valid data?

A. Completeness check
B. Accuracy check
C. Redundancy check
D. Reasonableness check

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A completeness check is an edit check to determine whether a field contains valid data.

QUESTION 251
A transaction journal provides the information necessary for detecting unauthorized ___________ (fill in the blank) from a terminal.

A. Deletion
B. Input
C. Access
D. Duplication

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

A transaction journal provides the information necessary for detecting unauthorized input from a terminal.

QUESTION 252

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An intentional or unintentional disclosure of a password is not likely to be evident within control logs.

QUESTION 253

When are benchmarking partners identified within the benchmarking process?

A. In the design stage
B. In the testing stage
C. In the research stage
D. In the development stage

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Benchmarking partners are identified in the research stage of the benchmarking process.

QUESTION 254

A check digit is an effective edit check to:

A. Detect data-transcription errors
B. Detect data-transposition and transcription errors
C. Detect data-transposition, transcription, and substitution errors

D. Detect data-transposition errors

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A check digit is an effective edit check to detect data-transposition and transcription errors.

QUESTION 255
Parity bits are a control used to validate:

A. Data authentication
B. Data completeness
C. Data source
D. Data accuracy

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Parity bits are a control used to validate data completeness.

QUESTION 256
The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

A. Implementor
B. Facilitator
C. Developer
D. Sponsor

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a facilitator.

QUESTION 257
Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

A. Proper authentication
B. Proper identification AND authentication
C. Proper identification
D. Proper identification, authentication, AND authorization

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
If proper identification and authentication are not performed during access control, no accountability can exist for any action performed.

QUESTION 258
Which of the following is the MOST critical step in planning an audit?

A. Implementing a prescribed auditing framework such as COBIT
B. Identifying current controls
C. Identifying high-risk audit targets
D. Testing controls

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In planning an audit, the most critical step is identifying the areas of high risk.

QUESTION 259
To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following?

A. The business objectives of the organization
B. The effect of segregation of duties on internal controls
C. The point at which controls are exercised as data flows through the system
D. Organizational control policies

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of the point at which controls are exercised as data flows through the system.

QUESTION 260
What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

A. Document existing internal controls
B. Perform compliance testing on internal controls
C. Establish a controls-monitoring steering committee
D. Identify high-risk areas within the organization

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When implementing continuous-monitoring systems, an IS auditor's first step is to identify high-risk areas within the organization.

QUESTION 261
What type of risk is associated with authorized program exits (trap doors)?

A. Business risk
B. Audit risk
C. Detective risk
D. Inherent risk

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Inherent risk is associated with authorized program exits (trap doors).

QUESTION 262
Which of the following is best suited for searching for address field duplications?

A. Text search forensic utility software
B. Generalized audit software
C. Productivity audit software
D. Manual review

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Generalized audit software can be used to search for address field duplications.

QUESTION 263
Which of the following is of greatest concern to the IS auditor?

A. Failure to report a successful attack on the network
B. Failure to prevent a successful attack on the network
C. Failure to recover from a successful attack on the network
D. Failure to detect a successful attack on the network

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Lack of reporting of a successful attack on the network is a great concern to an IS auditor.

QUESTION 264

An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

A. True B.
False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

QUESTION 265

An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

QUESTION 266

If an IS auditor finds evidence of risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

A. To advise senior management.
B. To reassign job functions to eliminate potential fraud.
C. To implement compensator controls.
D. Segregation of duties is an administrative control not considered by an IS auditor.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
An IS auditor's primary responsibility is to advise senior management of the risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function.

QUESTION 267
Who is responsible for implementing cost-effective controls in an automated system?

A. Security policy administrators
B. Business unit management
C. Senior management
D. Board of directors

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Business unit management is responsible for implementing cost-effective controls in an automated system.

QUESTION 268
Why does an IS auditor review an organization chart?

A. To optimize the responsibilities and authority of individuals
B. To control the responsibilities and authority of individuals
C. To better understand the responsibilities and authority of individuals
D. To identify project sponsors

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

QUESTION 269

Ensuring that security and control policies support business and IT objectives is a primary objective of:

A. An IT security policies audit

B. A processing audit

C. A software audit

D. A vulnerability assessment

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

Ensuring that security and control policies support business and IT objectives is a primary objective of an IT security policies audit.

QUESTION 270

When auditing third-party service providers, an IS auditor should be concerned with which of the following?

A. Ownership of the programs and files

B. A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

C. A statement of due care

D. Ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

When auditing third-party service providers, an auditor should be concerned with ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster.

QUESTION 271

When performing an IS strategy audit, an IS auditor should review both short-term (one- year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered.

QUESTION 272
What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels?

A. Business impact assessment
B. Risk assessment
C. IS assessment methods
D. Key performance indicators (KPIs)

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
IS assessment methods allow IS management to determine whether the activities of the organization differ from the planned or expected levels.

QUESTION 273
When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

A. Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.

B. Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic plan.
C. Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic plan.
D. Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic plan.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.

QUESTION 274
Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Allowing application programmers to directly patch or change code in production programs increases risk of fraud.

QUESTION 275
Who should be responsible for network security operations?

A. Business unit managers
B. Security administrators
C. Network administrators
D. IS auditors

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Security administrators are usually responsible for network security operations.

QUESTION 276
Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Proper segregation of duties does not prohibit a quality-control administrator from also being responsible for change control and problem management.

QUESTION 277
What can be implemented to provide the highest level of protection from external attack?

A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
B. Configuring the firewall as a screened host behind a router
C. Configuring the firewall as the protecting bastion host
D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

QUESTION 278
The directory system of a database-management system describes:

A. The access method to the data
B. The location of data AND the access method
C. The location of data
D. Neither the location of data NOR the access method

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The directory system of a database-management system describes the location of data and the access method.

QUESTION 279
How is the risk of improper file access affected upon implementing a database system?

A. Risk varies.
B. Risk is reduced.
C. Risk is not affected.
D. Risk is increased.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Improper file access becomes a greater risk when implementing a database system.

QUESTION 280
In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

A. The data should be deleted and overwritten with binary 0s.
B. The data should be demagnetized.
C. The data should be low-level formatted.
D. The data should be deleted.

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
To properly protect against unauthorized disclosure of sensitive data, hard disks should be demagnetized before disposal or release.

QUESTION 281
When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

A. The potential for unauthorized deletion of report copies
B. The potential for unauthorized modification of report copies
C. The potential for unauthorized printing of report copies
D. The potential for unauthorized editing of report copies

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When reviewing print systems spooling, an IS auditor is most concerned with the potential for unauthorized printing of report copies.

QUESTION 282
Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

A. WAP is often configured by default settings and is thus insecure.

B. WAP provides weak encryption for wireless traffic.
C. WAP functions as a protocol-conversion gateway for wireless TLS to Internet SSL.
D. WAP often interfaces critical IT systems.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Functioning as a protocol-conversion gateway for wireless TLS to Internet SSL, the WAP gateway is a component warranting critical concern and review for the IS auditor when auditing and testing controls that enforce message confidentiality

QUESTION 283
Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

A. True
B. False

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

QUESTION 284
How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

A. Modems convert analog transmissions to digital, and digital transmission to analog.
B. Modems encapsulate analog transmissions within digital, and digital transmissions within analog.
C. Modems convert digital transmissions to analog, and analog transmissions to digital.
D. Modems encapsulate digital transmissions within analog, and analog transmissions within digital.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

QUESTION 285
Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem?

A. Expert systems
B. Neural networks
C. Integrated synchronized systems
D. Multitasking applications

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Neural networks are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem.

QUESTION 286
What supports data transmission through split cable facilities or duplicate cable facilities?

A. Diverse routing
B. Dual routing
C. Alternate routing
D. Redundant routing

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Diverse routing supports data transmission through split cable facilities, or duplicate cable facilities.

QUESTION 287
What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

A. A first-generation packet-filtering firewall
B. A circuit-level gateway
C. An application-layer gateway, or proxy firewall, and stateful-inspection firewalls
D. An application-layer gateway, or proxy firewall, but not stateful-inspection firewalls

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An application-layer gateway, or proxy firewall, and stateful-inspection firewalls provide the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic.

QUESTION 288
Which of the following can degrade network performance?

A. Superfluous use of redundant load-sharing gateways
B. Increasing traffic collisions due to host congestion by creating new collision domains
C. Inefficient and superfluous use of network devices such as switches
D. Inefficient and superfluous use of network devices such as hubs

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Inefficient and superfluous use of network devices such as hubs can degrade network performance.

QUESTION 289
Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

A. Automated electronic journaling and parallel processing
B. Data mirroring and parallel processing
C. Data mirroring
D. Parallel processing

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data mirroring and parallel processing are both used to provide near- immediate recoverability for time-sensitive systems and transaction processing.

QUESTION 290
What is an effective control for granting temporary access to vendors and external support personnel?

A. Creating user accounts that automatically expire by a predetermined date
B. Creating permanent guest accounts for temporary use
C. Creating user accounts that restrict logon access to certain hours of the day
D. Creating a single shared vendor administrator account on the basis of least-privileged access

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

QUESTION 291
Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack?

A. Inbound traffic filtering
B. Using access control lists (ACLs) to restrict inbound connection attempts
C. Outbound traffic filtering
D. Recentralizing distributed systems

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Outbound traffic filtering can help prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack.

QUESTION 292
What is a common vulnerability, allowing denial-of-service attacks?

A. Assigning access to users according to the principle of least privilege
B. Lack of employee awareness of organizational security policies
C. Improperly configured routers and router access lists
D. Configuring firewall access rules

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Improperly configured routers and router access lists are a common vulnerability for denial-of- service attacks.

QUESTION 293
What are trojan horse programs?

A. A common form of internal attack
B. Malicious programs that require the aid of a carrier program such as email
C. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
D. A common form of Internet attack

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Trojan horse programs are a common form of Internet attack.

QUESTION 294
What is/are used to measure and ensure proper network capacity management and availability of services?

A. Network performance-monitoring tools

B. Network component redundancy
C. Syslog reporting
D. IT strategic planning

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Network performance-monitoring tools are used to measure and ensure proper network capacity management and availability of services.

QUESTION 295
What can be used to gather evidence of network attacks?

A. Access control lists (ACL)
B. Intrusion-detection systems (IDS)
C. Syslog reporting
D. Antivirus programs

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Intrusion-detection systems (IDS) are used to gather evidence of network attacks.

QUESTION 296
Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

A. Traffic analysis
B. SYN flood
C. Denial of service (DoS)
D. Distributed denial of service (DoS)

Correct Answer: A
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation:
Traffic analysis is a passive attack method used by intruders to determine potential network vulnerabilities. All others are active attacks.

QUESTION 297
Which of the following fire-suppression methods is considered to be the most environmentally friendly?

A. Halon gas
B. Deluge sprinklers
C. Dry-pipe sprinklers
D. Wet-pipe sprinklers

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Although many methods of fire suppression exist, dry-pipe sprinklers are considered to be the most environmentally friendly.

QUESTION 298
What is a callback system?

A. It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fails.
B. It is a remote-access system whereby the user's application automatically redials the remote access server if the initial connection attempt fails.
C. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.
D. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of time.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

A callback system is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

QUESTION 299

What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

A. A dry-pipe sprinkler system
B. A deluge sprinkler system
C. A wet-pipe system
D. A halon sprinkler system

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A dry-pipe sprinkler system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

QUESTION 300

Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key.
True or false?

A. False
B. True

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the sender's public key.

QUESTION 301

Which of the following provides the BEST single-factor authentication?

A. Biometrics
B. Password
C. Token
D. PIN

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Although biometrics provides only single-factor authentication, many consider it to be an excellent method for user authentication.

QUESTION 302
What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

A. An organizational certificate
B. A user certificate
C. A website certificate
D. Authenticode

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A website certificate is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption.

QUESTION 303
Overall business risk for a particular threat can be expressed as:

A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.
B. the magnitude of the impact should a threat source successfully exploit the vulnerability.
C. the likelihood of a given threat source exploiting a given vulnerability.

D. the collective judgment of the risk assessment team.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

QUESTION 304
Which of the following is a substantive test?

A. Checking a list of exception reports
B. Ensuring approval for parameter changes
C. Using a statistical sample to inventory the tape library
D. Reviewing password history reports

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A substantive test confirms the integrity of actual processing. A substantive test would determine if the tape library records are stated correctly. A compliance test determines if controls are being applied in a manner that is consistent with management policies and procedures. Checking the authorization of exception reports, reviewing authorization for changing parameters and reviewing password history reports are all compliance tests.

QUESTION 305
Which of the following is a benefit of a risk-based approach to audit planning? Audit:

A. scheduling may be performed months in advance.
B. budgets are more likely to be met by the IS audit staff.
C. staff will be exposed to a variety of technologies.

D. resources are allocated to the areas of highest concern

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The risk-based approach is designed to ensure audit time is spent on the areas of highest risk. The development of an audit schedule is not addressed by a riskbased approach. Audit schedules may be prepared months in advance using various scheduling methods. A risk approach does not have a direct correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a wider variety of audits will be performed in a given year.

QUESTION 306
An audit charter should:

A. be dynamic and change often to coincide with the changing nature of technology and the audit profession.
B. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
C. document the audit procedures designed to achieve the planned audit objectives.
D. outline the overall authority, scope and responsibilities of the audit function.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An audit charter should state management's objectives for and delegation of authority to IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

QUESTION 307
The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

A. information assets are overprotected.
B. a basic level of protection is applied regardless of asset value.
C. appropriate levels of protection are applied to information assets.
D. an equal proportion of resources are devoted to protecting all information assets.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not overprotecting information. However, an even bigger advantage is making sure that no information assets are over- or under protected. The risk assessment approach will ensure an appropriate level of protection is applied, commensurate with the level of risk and asset value and, therefore, considering asset value. The baseline approach does not allow more resources to be directed toward the assets at greater risk, rather than equally directing resources to all assets.

QUESTION 308
Which of the following sampling methods is MOST useful when testing for compliance?

A. Attribute sampling
B. Variable sampling
C. Stratified mean per unit
D. Difference estimation

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

QUESTION 309

Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

A. Multiple cycles of backup files remain available.
B. Access controls establish accountability for e-mail activity.
C. Data classification regulates what information should be communicated via e-mail.
D. Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

QUESTION 310

An IS auditor is assigned to perform a post implementation review of an application system. Which pf the following situations may have impaired the independence of the IS auditor? The IS auditor:

A. implemented a specific control during the development of the application system.
B. designed an embedded audit module exclusively for auditing the application system.
C. participated as a member of the application system project team, but did not have operational responsibilities.
D. provided consulting advice concerning application system best practices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

Independence may be impaired if an IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system. Choices B and C are situations that do not impair an IS auditor's independence. Choice D is incorrect because an IS auditor's independence is not impaired by providing advice on known best practices.

QUESTION 311
The PRIMARY advantage of a continuous audit approach is that it:

A. does not require an IS auditor to collect evidence on system reliability while processing is taking place.
B. requires the IS auditor to review and follow up immediately on all information collected.
C. can improve system security when used in time-sharing environments that process a large number of transactions.
D. does not depend on the complexity of an organization's computer systems.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The use of continuous auditing techniques can improve system security when used in time- sharing environments that process a large number of transactions, but leave a scarce paper trail. Choice A is incorrect since the continuous audit approach often does require an IS auditor to collect evidence on system reliability while processing is taking place. Choice B is incorrect since an IS auditor normally would review and follow up only on material deficiencies or errors detected. Choice D is incorrect since the use of continuous audit techniques depends on the complexity of an organization's computer systems.

QUESTION 312
When developing a risk-based audit strategy, an IS auditor conduct a risk assessment to ensure that:

A. controls needed to mitigate risks are in place.
B. vulnerabilities and threats are identified.
C. audit risks are considered.
D. a gap analysis is appropriate.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage.
Understanding whether appropriate controls required to mitigate risks are in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be done to compare the actual state to an expected or desirable state.

QUESTION 313

To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

A. schedule the audits and monitor the time spent on each audit.
B. train the IS audit staff on current technology used in the company.
C. develop the audit plan on the basis of a detailed risk assessment.
D. monitor progress of audits and initiate cost control measures.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Monitoring the time (choice A) and audit programs {choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

QUESTION 314

An organization's IS audit charter should specify the:

A. short- and long-term plans for IS audit engagements
B. objectives and scope of IS audit engagements.
C. detailed training plan for the IS audit staff.
D. role of the IS audit function.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

An IS audit charter establishes the role of the information systems audit function. The charter should describe the overall authority, scope, and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee. Short- term and long-term planning is the responsibility of audit management. The objectives and scope of each IS audit should be agreed to in an engagement letter. A training plan, based on the audit plan, should be developed by audit management.

QUESTION 315

An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

A. the controls already in place.
B. the effectiveness of the controls in place.
C. the mechanism for monitoring the risks related to the assets.
D. the threats/vulnerabilities affecting the assets.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
One of the key factors to be considered while assessing the risks related to the use of various information systems is the threats and vulnerabilities affecting the assets. The risks related to the use of information assets should be evaluated in isolation from the installed controls. Similarly, the effectiveness of the controls should be considered during the risk mitigation stage and not during the risk assessment phase A mechanism to continuously monitor the risks related to assets should be put in place during the risk monitoring function that follows the risk assessment phase.

QUESTION 316

In planning an audit, the MOST critical step is the identification of the:

A. areas of high risk.
B. skill sets of the audit staff.
C. test steps in the audit.
D. time allotted for the audit.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

When designing an audit plan, it is important to identify the areas of highest risk to determine the areas to be audited. The skill sets of the audit staff should have been considered before deciding and selecting the audit. Test steps for the audit are not as critical as identifying the areas of risk, and the time allotted for an audit is determined by the areas to be audited, which are primarily selected based on the identification of risks.

QUESTION 317
The extent to which data will be collected during an IS audit should be determined based on the:

A. availability of critical and required information.
B. auditor's familiarity with the circumstances.
C. auditee's ability to find relevant evidence.
D. purpose and scope of the audit being done.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An audit with a narrow purpose and scope would result most likely in less data collection, than an audit with a wider purpose and scope. The scope of an IS audit should not be constrained by the ease of obtaining the information or by the auditor's familiarity with the area being audited. Collecting all the required evidence is a required element of an IS audit, and thescope of the audit should not be limited by the auditee's ability to find relevant evidence.

QUESTION 318
While planning an audit, an assessment of risk should be made to provide:

A. reasonable assurance that the audit will cover material items.
B. definite assurance that material items will be covered during the audit work.
C. reasonable assurance that all items will be covered by the audit.
D. sufficient assurance that all items will be covered during the audit work.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

The ISACA IS Auditing Guideline G15 on planning the IS audit states, 'An assessment of risk should be made to provide reasonable assurance that material items will be adequately covered during the audit work. This assessment should identify areas with a relatively high risk of the existence of material problems.' Definite assurance that material items will be covered during the audit work is an impractical proposition. Reasonable assurance that all items will be covered during the audit work is not the correct answer, as material items need to be covered, not all items.

QUESTION 319

An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

A. the probability of error must be objectively quantified.

B. the auditor wishes to avoid sampling risk.C. generalized audit software is unavailable.

D. the tolerable error rate cannot be determined.

Correct Answer: A

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

Given an expected error rate and confidence level, statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size and quantify the probability of error (confidence coefficient). Choice B is incorrect because sampling risk is the risk of a sample not being representative of the population. This risk exists for both judgment and statistical samples. Choice C is incorrect because statistical sampling does not require the use of generalized audit software. Choice D is incorrect because the tolerable error rate must be predetermined for both judgment and statistical sampling.

QUESTION 320

During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

A. address audit objectives.

B. collect sufficient evidence.

C. specify appropriate tests.

D. minimize audit resources.

Correct Answer: A

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

ISACA auditing standards require that an IS auditor plan the audit work to address the audit objectives. Choice B is incorrect because the auditor does not collect evidence in the planning stage of an audit. Choices C and D are incorrect because they are not the primary goals of audit planning. The activities described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

QUESTION 321

When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

A. sufficient evidence will be collected.
B. all significant deficiencies identified will be corrected within a reasonable period.
C. all material weaknesses will be identified.
D. audit costs will be kept at a minimum level.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Procedures are processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising in the course of an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate and the auditor's past experience plays a key role in making a judgment. ISACA's guidelines provide information on how to meet the standards when performing IS audit work. Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit and not of professional judgment. Professional judgment is not a primary input to the financial aspects of the audit.

QUESTION 322
An IS auditor evaluating logical access controls should FIRST:

A. document the controls applied to the potential access paths to the system.
B. test controls over the access paths to determine if they are functional.
C. evaluate the security environment in relation to written policies and practices
D. obtain an understanding of the security risks to information processing.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation and evaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths-to determine if the controls are functioning. Lastly, the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

QUESTION 323
The PRIMARY purpose of an IT forensic audit is:

A. to participate in investigations related to corporate fraud.

D.

Correct Answer:
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

B. the systematic collection of evidence after a system irregularity.

C. to assess the correctness of an organization's financial statements to determine that there has been criminal activity.

B

Choice B describes a forensic audit. The evidence collected could then be used in judicial proceedings. Forensic audits are not limited to corporate fraud. Assessing the correctness of an organization's financial statements is not the purpose of a forensic audit. Drawing a conclusion to criminal activity would be part of a legal process and not the objective of a forensic audit.

QUESTION 324

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

A. Issue an audit finding
B. Seek an explanation from IS management
C. Review the classifications of data held on the server
D. Expand the sample of logs reviewed

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Audit standards require that an IS auditor gather sufficient and appropriate audit evidence. The auditor has found a potential problem and now needs to determine if this is an isolated incident or a systematic control failure. At this stage it is too preliminary to issue an audit finding and seeking an explanation from management is advisable, but it would be better to gather additional evidence to properly evaluate the seriousness of the situation. A backup failure, which has not been established at this point, will be serious if it involves critical data. However, the issue is not the importance of the data on the server, where a problem has been detected, but whether a systematic control failure that impacts other servers exists.

QUESTION 325

D.

Correct Answer:
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools are MOST suitable for performing that task?

A. CASE tools
B. Embedded data collection toolsC. Heuristic scanning tools Trend/variance detection tools
D

Trend/variance detection tools look for anomalies in user or system behavior, for example, determining whether the numbers for prenumbered documents are sequential or increasing. CASE tools are used to assist software development. Embedded (audit) data collection software is used for sampling and to provide production statistics. Heuristic scanning tools can be used to scan for viruses to indicate possible infected code.

QUESTION 326
An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

A. There are a number of external modems connected to the network.
B. Users can install software on their desktops.
C. Network monitoring is very limited.
D. Many user IDs have identical passwords.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Exploitation of a known user ID and password requires minimal technical knowledge and exposes the network resources to exploitation. The technical barrier is low and the impact can be very high; therefore, the fact that many user IDs have identical passwords represents the greatest threat. External modems represent a security risk, but exploitation still depends on the use of a valid user account. While the impact of users installing software on their desktops can be high {for example, due to the installation of Trojans or key-logging programs), the likelihood is not high due to the level of technical knowledge required to successfully
D.

Correct Answer:
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
penetrate the network. Although network monitoring can be a useful detective control, it will only detect abuse of user accounts in special circumstances and is, therefore, not a first line of defense.

QUESTION 327
Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

A. The preservation of the chain of custody for electronic evidence
B. Time and cost savings
C. Efficiency and effectiveness
Ability to search for violations of intellectual property rights

D.

Correct Answer:
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A

The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Choice B, time and cost savings, and choice C, efficiency and effectiveness, are legitimate concerns that differentiate good from poor forensic software packages. Choice D, the ability to search for intellectual property rights violations, is an example of a use of forensic software.

QUESTION 328
An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

A. matching control totals of the imported data to control totals of the original data.
B. sorting the data to confirm whether the data are in the same order as the original data.
C. reviewing the printout of the first 100 records of original data with the first 100 records of imported data.
D. filtering data for different categories and matching them to the original data.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Matching control totals of the imported data with control totals of the original data is the next logical step, as this confirms the completeness of the imported datA. It is not possible to confirm completeness by sorting the imported data, because the original data may not be in sorted order. Further, sorting does not provide control totals for verifying completeness. Reviewing a printout of 100 records of original data with 100 records of imported data is a process of physical verification and confirms the accuracy of only these records. Filtering data for different categories and matching them to original data would still require that control totals be developed to confirm the completeness of the data.

QUESTION 329
The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

A. Test data

B. Generalized audit software

C. Integrated test facility

D. Embedded audit module

Correct Answer: B

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

Generalized audit software features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recomputations. An IS auditor, using generalized audit software, could design appropriate tests to recompute the payroll, thereby determining if there were overpayments and to whom they were made. Test data would test for the existence of controls that might prevent overpayments, but it would not detect specific, previous miscalculations. Neither an integrated test facility nor an embedded audit module would detect errors for a previous period.

QUESTION 330

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

A. create the procedures document.

B. terminate the audit.

C. conduct compliance testing.

D. identify and evaluate existing practices.

Correct Answer: D

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization. IS auditors should not prepare documentation, as doing so could jeopardize their independence. Terminating the audit may prevent achieving one of the basic audit objectives, i.e., identification of potential risks. Since there are no documented procedures, there is no basis against which to test compliance.

QUESTION 331

In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

A. identify and assess the risk assessment process used by management.
B. identify information assets and the underlying systems.
C. disclose the threats and impacts to management.
D. identify and evaluate the existing controls.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

QUESTION 332
Which of the following should be of MOST concern to an IS auditor?

A. Lack of reporting of a successful attack on the network
B. Failure to notify police of an attempted intrusion
C. Lack of periodic examination of access rights
D. Lack of notification to the public of an intrusion

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Not reporting an intrusion is equivalent to an IS auditor hiding a malicious intrusion, which would be a professional mistake. Although notification to the police may be required and the lack of a periodic examination of access rights might be a concern, they do not represent as big a concern as the failure to report the attack. Reporting to the public is not a requirement and is dependent on the organization's desire, or lack thereof, to make the intrusion known.

QUESTION 333
Which of the following would normally be the MOST reliable evidence for an auditor?

A. A confirmation letter received from a third party verifying an account balance
B. Assurance from line management that an application is working as designed

C. Trend data obtained from World Wide Web (Internet) sources
D. Ratio analysts developed by the IS auditor from reports supplied by line management

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Evidence obtained from independent third parties almost always is considered to be the most reliable. Choices B, C and D would not be considered as reliable.

QUESTION 334
When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

A. The point at which controls are exercised as data flow through the system
B. Only preventive and detective controls are relevant
C. Corrective controls can only be regarded as compensating
D. Classification allows an IS auditor to determine which controls are missing

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect, since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

QUESTION 335
Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

A. Discussion with management
B. Review of the organization chart
C. Observation and interviews
D. Testing of user access rights

Correct Answer: C

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

QUESTION 336
During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

A. test data to validate data input.
B. test data to determine system sort capabilities.
C. generalized audit software to search for address field duplications.
D. generalized audit software to search for account field duplications.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since the name is not the same {due to name variations), one method to detect duplications would be to compare other common fields, such as addresses. A subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

QUESTION 337
Which of the following would be the BEST population to take a sample from when testing program changes?

A. Test library listings
B. Source program listings
C. Program change requests

D. Production library listings

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational data. Source program listings would be timeintensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

QUESTION 338
An integrated test facility is considered a useful audit tool because it:

A. is a cost-efficient approach to auditing application controls.
B. enables the financial and IS auditors to integrate their audit tests.
C. compares processing output with independently calculated data.
D. provides the IS auditor with a tool to analyze a large range of information

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated datA. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

QUESTION 339
Data flow diagrams are used by IS auditors to:

A. order data hierarchically.
B. highlight high-level data definitions.
C. graphically summarize data paths and storage.
D. portray step-by-step details of data generation.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of datA. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

QUESTION 340
Which of the following forms of evidence for the auditor would be considered the MOST reliable?

A. An oral statement from the auditee
B. The results of a test performed by an IS auditor
C. An internally generated computer accounting report
D. A confirmation letter received from an outside source

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Evidence obtained from outside sources is usually more reliable than that obtained from within the organization. Confirmation letters received from outside parties, such as those used to verify accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable, if the auditor did not have a good understanding of the technical area under review.

QUESTION 341
An IS auditor reviews an organizational chart PRIMARILY for:

A. an understanding of workflows.
B. investigating various communication channels.
C. understanding the responsibilities and authority of individuals.
D. investigating the network connected to different employees.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

QUESTION 342
An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

A. Availability of online network documentation
B. Support of terminal access to remote hosts
C. Handling file transfer between hosts and interuser communications
D. Performance management, audit and control

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Network operating system user features include online availability of network documentation. Other features would be user access to various resources of network hosts, user authorization to access particular resources, and the network and host computers used without special user actions or commands. Choices B, C and D are examples of network operating systems functions.

QUESTION 343
An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storage.
B. interview programmers about the procedures currently being followed.

C. compare utilization records to operations schedules.
D. review data file access records to test the librarian function.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

QUESTION 344
Which of the following is an advantage of an integrated test facility (ITF)?

A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.
B. Periodic testing does not require separate test processes.
C. It validates application systems and tests the ongoing operation of the system.
D. The need to prepare test data is eliminated.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: An integrated test facility creates a factitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

QUESTION 345
An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

A. Design further tests of the calculations that are in error.
B. Identify variables that may have caused the test results to be inaccurate.
C. Examine some of the test cases to confirm the results.
D. Document the results and prepare a report of findings, conclusions and recommendations.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would not be made until all results are confirmed.

QUESTION 346
The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs
B. recreating program logic using generalized audit software to calculate monthly totals.
C. preparing simulated transactions for processing and comparing the results to predetermined results.
D. automatic flowcharting and analysis of the source code of the calculation programs.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

QUESTION 347
An IS auditor performing a review of an application's controls would evaluate the:

A. efficiency of the application in meeting the business processes.
B. impact of any exposures discovered.
C. business processes served by the application.
D. application's optimization.

Correct Answer: B

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

QUESTION 348
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 349
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 350
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 351
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 352

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 353

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 354

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 355

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 356
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 357
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 358
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 359
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 360

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 361

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 362
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 363
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 364

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 365

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 366

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 367

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 368
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 369
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 370
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 371
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 372
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 373
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 controlsChoices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

QUESTION 374
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 375
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 376
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 377
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 378

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 379

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 380
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 381
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 382
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 383
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 384
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 385
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 386
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 387
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 388
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 389
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 390
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 391
What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

A. Repeatable but Intuitive
B. Defined
C. Managed and Measurable
D. Optimized

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:

Explanation:
Defined (level 3) is the lowest level at which an IT balanced scorecard is defined.

QUESTION 392
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 393
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 394
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 395
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 396
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 397
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 398

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 399

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 400

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 401

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 402
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 403
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 404
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 405
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 406
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 407
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 408
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 409
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 410

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 411

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 412
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 413
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 414
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 415
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 416

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 417

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 418
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 419
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 420
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 421
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 422
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 423
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 424
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 425
A benefit of open system architecture is that it:

A. facilitates interoperability.
B. facilitates the integration of proprietary components.
C. will be a basis for volume discounts from equipment vendors.
D. allows for the achievement of more economies of scale for equipment.

Correct Answer: A
Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

QUESTION 426

In the context of effective information security governance, the primary objective of value delivery is to:

A. optimize security investments in support of business objectives.
B. implement a standard set of security practices.
C. institute a standards-based solution.
D. implement a continuous improvement culture.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commoditization of standards-based solutions, and implementation of a continuous improvement culture considering security as a process, not an event.

QUESTION 427

Which of the following BEST supports the prioritization of new IT projects?

A. Internal control self-assessment (CSA)
B. Information systems audit
C. Investment portfolio analysis
D. Business risk assessment

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is most desirable to conduct an investment portfolio analysis, which will present not only a clear focus on investment strategy, but will provide the rationale for terminating nonperforming IT projects. Internal control self-assessment (CSA) may highlight noncompliance to the current policy, but may not necessarily be the best source for driving the prioritization of IT projects. Like internal CSA, IS audits may provide only part of the picture for the prioritization of IT projects. Business risk analysis is part of the investment portfolio analysis but, by itself, is not the best method for prioritizing new IT projects.

QUESTION 428
Which of the following is a characteristic of timebox management?

A. Not suitable for prototyping or rapid application development (RAD)
B. Eliminates the need for a quality process
C. Prevents cost overruns and delivery delays
D. Separates system and user acceptance testing

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Timebox management, by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and RAD, and integrates system and user acceptance testing, but does not eliminate the need for a quality process.

QUESTION 429
Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

A. Project database
B. Policy documents
C. Project portfolio database
D. Program organization

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
A project portfolio database is the basis for project portfolio management. It includes project data, such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports. A project database may contain the above for one specific project and updates to various parameters pertaining to the current status of that single project. Policy documents on project management set direction for the design, development, implementation and monitoring of the project. Program organization is the team required (steering committee, quality assurance, systems personnel, analyst, programmer, hardware support, etc.) to meet the delivery objective of the project.

QUESTION 430
To minimize the cost of a software project, quality management techniques should be applied:

A. as close to their writing (i.e., point of origination) as possible.
B. primarily at project start-up to ensure that the project is established in accordance with organizational governance standards.
C. continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate.
D. mainly at project close-down to capture lessons learned that can be applied to future projects.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
While it is important to properly establish a software development project, quality management should be effectively practiced throughout the project. The major source of unexpected costs on most software projects is rework. The general rule is that the earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

QUESTION 431
When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

A. whose sum of activity time is the shortest.
B. that have zero slack time.
C. that give the longest possible completion time.
D. whose sum of slack time is the shortest.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities on the critical path become candidates for crashing, i.e., for reduction in their time by payment of a premium for early completion. Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs vs. time can be obtained.

QUESTION 432
At the completion of a system development project, a post project review should include which of the following?

A. Assessing risks that may lead to downtime after the production release
B. Identifying lessons learned that may be applicable to future projects
C. Verifying the controls in the delivered system are working
D. Ensuring that test data are deleted

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects. An assessment of potential downtime should be made with the operations group and other specialists before implementing a system. Verifying that controls are working should be covered during the acceptance test phase and possibly, again, in the post implementation review. Test data should be retained for future regression testing.

QUESTION 433
An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

A. complexity and risks associated with the project have been analyzed.
B. resources needed throughout the project have been determined.
C. project deliverables have been identified.
D. a contract for external parties involved in the project has been completed.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Understanding complexity and risk, and actively managing these throughout a project are critical to a successful outcome. The other choices, while important during the course of the project, cannot be fully determined at the time the project is initiated, and are often contingent upon the risk and complexity of the project.

QUESTION 434
An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

A. stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.
B. accept the project manager's position as the project manager is accountable for the outcome of the project.
C. offer to work with the risk manager when one is appointed.
D. inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: the majority of project risks can typically be identified before a project begins, allowing mitigation/avoidance plans to be put in place to deal with the risks. A project should have a clear link back to corporate strategy and tactical plans to support this strategy. The process of setting corporate strategy, setting objectives and developing tactical plans should include the consideration of risks. Appointing a risk manager is a good practice but waiting until the project has been impacted by risks is misguided. Risk management needs to be forward looking; allowing risks to evolve into issues that adversely impact the project represents a failure of risk management. With or without a risk manager, persons within and outside of the project team need to be consulted and encouraged to comment when they believe new risks have emerged or risk priorities have changed. The IS auditor has an obligation to the project sponsor and the organization to advise on appropriate project manage me practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

QUESTION 435
While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

A. effectiveness of the QA function because it should interact between project management and user management

B. efficiency of the QA function because it should interact with the project implementation team.
C. effectiveness of the project manager because the project manager should interact with the QA function.
D. efficiency of the project manager because the QA function will need to communicate with the project implementation team.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To be effective the quality assurance (QA) function should be independent of project management. The QA function should never interact with the project implementation team since this can impact effectiveness. The project manager does not interact with the QA function, which should not impact the effectiveness of the project manager. The QA function does not interact with the project implementation team, which should not impact the efficiency of the project manager.

QUESTION 436
When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

A. increases in quality can be achieved, even if resource allocation is decreased.
B. increases in quality are only achieved if resource allocation is increased.
C. decreases in delivery time can be achieved, even if resource allocation is decreased.
D. decreases in delivery time can only be achieved if quality is decreased.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased an increase in quality can be achieved, if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.

QUESTION 437
An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

A. Report that the organization does not have effective project management.

B. Recommend the project manager be changed.
C. Review the IT governance structure.
D. Review the conduct of the project and the business case.

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to making the project over budget and over schedule. The organization may have effective project management practices and sound IT governance and still be behind schedule or over budget. There is no indication that the project manager should be changed without looking into the reasons for the overrun.

QUESTION 438
Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

A. Function point analysis
B. Earned value analysis
C. Cost budget
D. Program Evaluation and Review Technique

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Earned value analysis (EVA) is an industry standard method for measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the schedule and budget as the project proceeds. It compares the planned amount of work with what has actually been completed, to determine if the cost, schedule and work accomplished are progressing in accordance with the plan. EVA works most effectively if a well-formed work breakdown structure exists. Function point analysis (FPA) is an indirect measure of software size and complexity and, therefore, does not address the elements of time and budget. Cost budgets do not address time. PERT aids in time and deliverables management, but lacks projections for estimates at completion (EACs) and overall financial management.

QUESTION 439

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

A. project be discontinued.
B. business case be updated and possible corrective actions be identified.
C. project be returned to the project sponsor for reapproval.
D. project be completed and the business case be updated later.

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation: An IS auditor should not recommend discontinuing or completing the project before reviewing an updated business case. The IS auditor should recommend that the business case be kept current throughout the project since it is a key input to decisions made throughout the life of any project.

QUESTION 440
An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

A. Project sponsor
B. System development project team (SPDT)
C. Project steering committee
D. User project team (UPT)

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support. The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics for the project. The project sponsor is not responsible for reviewing the progress of the project. A system development project team (SDPT) completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for reviewing the progress of the project. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

QUESTION 441

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor
B. Database administrator
C. Project manager
D. Data owner

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
During the data conversion stage of a project, the data owner is primarily responsible for reviewing and signing-off that the data are migrated completely, accurately and are valid. An IS auditor is not responsible for reviewing and signing-off on the accuracy of the converted data. However, an IS auditor should ensure that there is a review and sign-off by the data owner during the data conversion stage of the project. A database administrator's primary responsibility is to maintain the integrity of the database and make the database available to users. A database administrator is not responsible for reviewing migrated data. A project manager provides day-to- day management and leadership of the project, but is not responsible for the accuracy and integrity of the data.

QUESTION 442

An advantage of using sanitized live transactions in test data is that:

A. all transaction types will be included.
B. every error condition is likely to be tested.
C. no special routines are required to assess the results.
D. test transactions are representative of live processing.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Test data will be representative of live processing; however, it is unlikely that all transaction types or error conditions will be tested in this way.

QUESTION 443

An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

A. users may prefer to use contrived data for testing.
B. unauthorized access to sensitive data may result.
C. error handling and credibility checks may not be fully proven.
D. the full functionality of the new process may not necessarily be tested.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Unless the data are sanitized, there is a risk of disclosing sensitive data.
QUESTION 444
Which of the following is the PRIMARY purpose for conducting parallel testing?

A. To determine if the system is cost-effective
B. To enable comprehensive unit and system testing
C. To highlight errors in the program interfaces with files
D. To ensure the new system meets user requirements

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
The purpose of parallel testing is to ensure that the implementation of a new system will meet user requirements. Parallel testing may show that the old system is, in fact, better than the new system, but this is not the primary reason. Unit and system are completed before parallel testing. Program interfaces with files are tested for errors during system testing.

QUESTION 445
The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

A. rules.
B. decision trees.C. semantic nets.
D. dataflow diagrams.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a dataflow diagram and make use of an inheritance mechanism to prevent duplication of data.

QUESTION 446
An advantage in using a bottom-up vs. a top-down approach to software testing is that:

A. interface errors are detected earlier.
B. confidence in the system is achieved earlier.
C. errors in critical modules are detected earlier.
D. major functions and processing are tested earlier.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upward until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices in this question all refer to advantages of a top-down approach, which follows the opposite path, either in depth-first or breadth-first search order.

QUESTION 447

During which of the following phases in system development would user acceptance test plans normally be prepared?

A. Feasibility study
B. Requirements definition
C. implementation planning
D. Postimplementation review

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
During requirements definition, the project team will be working with the users to define their precise objectives and functional needs. At this time, the users should be working with the team to consider and document hot the system functionality can be tested ensure it meets their stated needs. The feasibility study is too early for such detailed user involvement, and the implementation planning and postimplementation review phases are too late. An IS auditor should know at what point user testing should be planned to ensure it is most effective and efficient.

QUESTION 448

The use of object-oriented design and development techniques would MOST likely:

A. facilitate the ability to reuse modules.
B. improve system performance.
C. enhance control effectiveness.
D. speed up the system development life cycle.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

One of the major benefits of object-oriented design and development is the ability to reuse modules. The other options do not normally benefit from the objectoriented technique.

QUESTION 449
Which of the following should be included in a feasibility study for a project to implement an EDI process?

A. The encryption algorithm format
B. The detailed internal control procedures
C. The necessary communication protocols
D. The proposed trusted third-party agreement

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Encryption algorithms, third-party agreements and internal control procedures are too detailed for this phase. They would only be outlined and any cost or performance implications shown. The communications protocols must be included, as there may be significant cost implications if new hardware and software are involved, and risk implications if the technology is new to the organization.

QUESTION 450
When a new system is to be implemented within a short time frame, it is MOST important to:
A. finish writing user manuals.
B. perform user acceptance testing.
C. add last-minute enhancements to functionalities.
D. ensure that the code has been documented and reviewed.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly. The completion of the user manuals is similar to the performance of code reviews. If time is tight, the last thing one would want to do is add another enhancement, as it would be necessary to

freeze the code and complete the testing, then make any other changes as future enhancements. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirement.

QUESTION 451

An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

A. a backup server be available to run ETCS operations with up-to-date data.
B. a backup server be loaded with all the relevant software and data.
C. the systems staff of the organization be trained to handle any event.
D. source code of the ETCS application be placed in escrow.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Whenever proprietary application software is purchased, the contract should provide for a source code agreement. This will ensure that the purchasing company will have the opportunity to modify the software should the vendor cease to be in business. Having a backup server with current data and staff training is critical but not as critical as ensuring the availability of the source code.

QUESTION 452

The MOST likely explanation for the use of applets in an Internet application is that:

A. it is sent over the network from the server.

B. the server does not run the program and the output is not sent over the network.
C. they improve the performance of the web server and network.
D. it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

An applet is a JAVA program that is sent over the network from the web server, through a web browser and to the client machine; the code is then run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on the web server and network-over which the server and client are connected-drastically improves through the use of applets. Performance improvement is more important than the reasons offered in choices A and B. Since JAVA virtual machine (JVM) is embedded in most web browsers, the applet download through the web browser runs on the client machine from the web browser, not from the web server, making choice D incorrect.

QUESTION 453
Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

A. Intrusion detection systems
B. Data mining techniques
C. Firewalls
D. Packet filtering routers

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Data mining is a technique used to detect trends or patterns of transactions or datA. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.

QUESTION 454
Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

A. existence of a set of functions and their specified properties.
B. ability of the software to be transferred from one environment to another.
C. capability of software to maintain its level of performance under stated conditions.
D. relationship between the performance of the software and the amount of resources used.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. Choice B refers to portability; choice C refers to reliability and choice D refers to efficiency.

QUESTION 455
During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:

A. increased maintenance.
B. improper documentation of testing.
C. inadequate functional testing.
D. delays in problem resolution.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The major risk of combining quality assurance testing and user acceptance testing is that functional testing may be inadequate. Choices A, B and D are not as important.

QUESTION 456
The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

A. facilitates user involvement.
B. allows early testing of technical features.
C. facilitates conversion to the new system.
D. shortens the development time frame.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

The greatest advantage of RAD is the shorter time frame for the development of a system. Choices A and B are true, but they are also true for the traditional systems development life cycle. Choice C is not necessarily always true.

QUESTION 457
An IS auditor reviewing a proposed application software acquisition should ensure that the:

A. operating system (OS) being used is compatible with the existing hardware platform.
B. planned OS updates have been scheduled to minimize negative impacts on company needs.
C. OS has the latest versions and updates.
D. products are compatible with the current or planned OS.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choices A, B and C are incorrect because none of them are related to the area being audited. In reviewing the proposed application, the auditor should ensure that the products to be purchased are compatible with the current or planned OS. Regarding choice, A, if the OS is currently being used, it is compatible with the existing hardware platform, because if it is not it would not operate properly. In choice B, the planned OS updates should be scheduled to minimize negative impacts on the organization. For choice C, the installed OS should be equipped with the most recent versions and updates (with sufficient history and stability).

QUESTION 458
The GREATEST benefit in implementing an expert system is the:

A. capturing of the knowledge and experience of individuals in an organization.
B. sharing of knowledge in a central repository.
C. enhancement of personnel productivity and performance.
D. reduction of employee turnover in key departments.

Correct Answer: A
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:

The basis for an expert system is the capture and recording of the knowledge and experience of individuals in an organization. Coding and entering the knowledge in a central repository, shareable within the enterprise, is a means of facilitating the expert system. Enhancing personnel productivity and performance is a benefit; however, it is not as important as capturing the knowledge and experience. Employee turnover is not necessarily affected by an expert system.

QUESTION 459
By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

A. reliable products are guaranteed.
B. programmers' efficiency is improved.
C. security requirements are designed.
D. predictable software processes are followed.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
By evaluating the organization's development projects against the CMM, an IS auditor determines whether the development organization follows a stable, predictable software process. Although the likelihood of success should increase as the software processes mature toward the optimizing level, mature processes do not guarantee a reliable product. CMM does not evaluate technical processes such as programming nor does it evaluate security requirements or other application controls.

QUESTION 460
The waterfall life cycle model of software development is most appropriately used when:

A. requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.
B. requirements are well understood and the project is subject to time pressures.
C. the project intends to apply an object-oriented design and programming approach.
D. the project will involve the use of new technology.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Historically, the waterfall model has been best suited to the stable conditions described in choice

A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative development life cycle gives the advantage of breaking down the scope of the overall system to be delivered, making the requirements gathering and design activities more manageable. The ability to deliver working software earlier also acts to alleviate uncertainty and may allow an earlier realization of benefits. The choice of a design and programming approach is not itself a determining factor of the type of software development life cycle that is appropriate. The use of new technology in a project introduces a significant element of risk. An iterative form of development, particularly one of the agile methods that focuses on early development of actual working software, is likely to be the better option to manage this uncertainty.

QUESTION 461
Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

A. A sufficient quantity of data for each test case
B. Data representing conditions that are expected in actual processing
C. Completing the test on schedule
D. A random sample of actual data

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: Selecting the right kind of data is key in testing a computer system. The data should not only include valid and invalid data but should be representative of actual processing; quality is more important than quantity. It is more important to have adequate test data than to complete the testing on schedule. It is unlikely that a random sample of actual data would cover all test conditions and provide a reasonable representation of actual data.

QUESTION 462
During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:

A. buffer overflow.
B. brute force attack.
C. distributed denial-of-service attack.
D. war dialing attack.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Poorly written code, especially in web-based applications, is often exploited by hackers using buffer overflow techniques. A brute force attack is used to crack passwords. A distributed denial- of-service attack floods its target with numerous packets, to prevent it from responding to legitimate requests. War dialing uses modem-scanning tools to hack PBXs.

QUESTION 463
Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

A. Bottom up
B. Sociability testing
C. Top-down
D. System test

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The top-down approach to testing ensures that interface errors are detected early and that testing of major functions is conducted early. A bottom-up approach to testing begins with atomic units, such as programs and modules, and works upward until a complete system test has taken place. Sociability testing and system tests take place at a later stage in the development process.

QUESTION 464
During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

A. test data covering critical applications.
B. detailed test plans.
C. quality assurance test specifications.
D. user acceptance testing specifications

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation: A key objective in any software development project is to ensure that the developed software will meet the business objectives and the requirements of the user. The users should be involved in the requirements definition phase of a development project and user acceptance test specification should be developed during this phase. The other choices are generally performed during the system testing phase.

QUESTION 465

Which of the following is an advantage of the top-down approach to software testing?

A. Interface errors are identified early

B. Testing can be started before all programs are complete

C. it is more effective than other testing approaches

D. Errors in critical modules are detected sooner

Correct Answer: A

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

The advantage of the top-down approach is that tests of major functions are conducted early, thus enabling the detection of interface errors sooner. The most effective testing approach is dependent on the environment being tested. Choices B and D are advantages of the bottom-up approach to system testing.

QUESTION 466

During the system testing phase of an application development project the IS auditor should review the:

A. conceptual design specifications.

B. vendor contract.

C. error reports.

D. program change requests.

Correct Answer: C

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

Testing is crucial in determining that user requirements have been validated. The IS auditor should be involved in this phase and review error reports for their precision in recognizing erroneous data and review the procedures for resolving errors. A conceptual design specification is a document prepared during the requirements definition phase. A vendor contract is prepared during a software acquisition process. Program change requests would normally be reviewed as a part of the postimplementation phase.

QUESTION 467
Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

A. increase the time allocated for system testing
B. implement formal software inspections
C. increase the development staff
D. Require the sign-off of all project deliverables

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: inspections of code and design are a proven software quality technique. An advantage of this approach is that defects are identified before they propagate through the development life cycle. This reduces the cost of correction as less rework is involved. Allowing more time for testing may discover more defects; however, little is revealed as to why the quality problems are occurring and the cost of the extra testing, and the cost of rectifying the defects found will be greater than if they had been discovered earlier in the development process. The ability of the development staff can have a bearing on the quality of what is produced; however, replacing staff can be expensive and disruptive, and the presence of a competent staff cannot guarantee quality in the absence of effective quality management processes. Sign-off of deliverables may help detect defects if signatories are diligent about reviewing deliverable content; however, this is difficult to enforce.
Deliverable reviews normally do not go down to the same level of detail as software inspections.

QUESTION 468
Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

A. Applications may not be subject to testing and IT general controls
B. increased development and maintenance costs
C. increased application development time
D. Decision-making may be impaired due to diminished responsiveness to requests for information

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

End-user developed applications may not be subjected to an independent outside review by systems analysts and frequently are not created in the context of a formal development methodology. These applications may lack appropriate standards, controls, quality assurance procedures, and documentation. A risk of enduser applications is that management may rely on them as much as traditional applications. End-user computing (EUC) systems typically result in reduced application development and maintenance costs, and a reduced development cycle time. EUC systems normally increase flexibility and responsiveness to management's information requests.

QUESTION 469

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

A. System owners

B. System users

C. System designers

D. System builders

Correct Answer: A

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system.

Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

QUESTION 470

The MAJOR advantage of a component-based development approach is the:

A. ability to manage an unrestricted variety of data types.

B. provision for modeling complex relationships.

C. capacity to meet the demands of a changing environment.

D. support of multiple development environments.

Correct Answer: D

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic. The other choices are not the most significant advantages of a component-based development approach.

QUESTION 471

The specific advantage of white box testing is that it:

A. verifies a program can operate successfully with other parts of the system.
B. ensures a program's functional operating effectiveness without regard to the internal program structure.
C. determines procedural accuracy or conditions of a program's specific logic paths.
D. examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system.

Correct Answer: C

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths. Verifying the program can operate successfully with other parts of the system is sociability testing. Testing the program's functionality without knowledge of internal structures is black box testing. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

QUESTION 472

Following best practices, formal plans for implementation of new information systems are developed during the:

A. development phase.
B. design phase.C. testing phase.
D. deployment phase.

Correct Answer: B

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

Planning for implementation should begin well in advance of the actual implementation date. A formal implementation plan should be constructed in the design phase and revised as the development progresses.

QUESTION 473

An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?

A. Use a process-based maturity model such as the capability maturity model (CMM)
B. Regular monitoring of task-level progress against schedule
C. Extensive use of software development tools to maximize team productivity
D. Postiteration reviews that identify lessons learned for future use in the project

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
A key tenet of the Agile approach to software project management is team learning and the use of team learning to refine project management and software development processes as the project progresses. One of the best ways to achieve this is that, at the end of each iteration, the team considers and documents what worked well and what could have worked better, and identifies improvements to be implemented in subsequent iterations. CMM and Agile really sit at opposite poles. CMM places heavy emphasis on predefined formal processes and formal project management and software development deliverables. Agile projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics.
Additionally, less importance is placed on formal paper- based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile projects produce releasable software in short iterations, typically ranging from 4 to 8 weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant. Agile projects do make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of greater importance.

QUESTION 474

An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

A. Consider feasibility of a separate user acceptance environment
B. Schedule user testing to occur at a given time each day
C. implement a source code version control tool
D. Only retest high priority defects

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A separate environment or environments is normally necessary for testing to be efficient and effective, and to ensure the integrity of production code, it is important that the development and testing code base be separate. When defects are identified they can be fixed in the development environment, without interrupting testing, before being migrated in a controlled manner to the test environment. A separate test environment can also be used as the final staging area from which code is migrated to production. This enforces a separation between development and production code. The logistics of setting up and refreshing customized test data is easier if a separate environment is maintained. If developers and testers are sharing the same environment, they have to work effectively at separate times of the day. It is unlikely that this would provide optimum productivity. Use of a source code control tool is a good practice, but it does not properly mitigate the lack of an appropriate testing environment. Even low priority fixes run the risk of introducing unintended results when combined with the rest of the system code. To prevent this, regular regression testing covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

QUESTION 475

Which of the following types of testing would determine whether a new or modifies system can operate in its target environment without adversely impacting other existing systems?

A. Parallel testing
B. Pilot testing
C. Interface/integration testing
D. Sociability testing

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a clientserver or web development. Parallel testing is the process of feeding data into two systems-the modified system and an alternate system- and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. Pilot testing takes place first at one location and is then extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure.

QUESTION 476

At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

A. report the error as a finding and leave further exploration to the auditee's discretion.
B. attempt to resolve the error.
C. recommend that problem resolution be escalated.
D. ignore the error, as it is not possible to get objective evidence for the software error.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

QUESTION 477

Which of the following is an implementation risk within the process of decision support systems?

A. Management control
B. Semistructured dimensions
C. inability to specify purpose and usage patterns
D. Changes in decision processes

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DDS.

QUESTION 478

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 479
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 480
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 481
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 482
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 483
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 484
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 485
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 486
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 487
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 488
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 489
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 490
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 491
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 492
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 493
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 494
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 495
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 496

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 497

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 498
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 499
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 500
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 501
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.

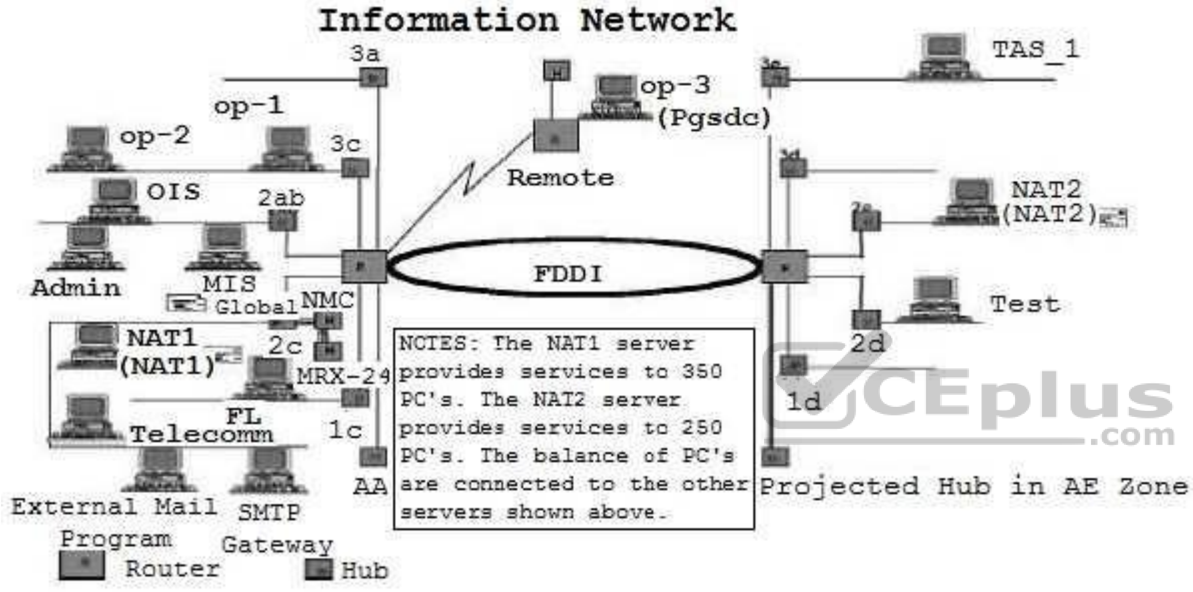
Correct Answer: C
Section: Protection of Information Assets
Explanation

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 502

Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?



NCTES: The NAT1 server provides services to 350 PC's. The NAT2 server provides services to 250 PC's. The balance of PC's are connected to the other servers shown above.

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

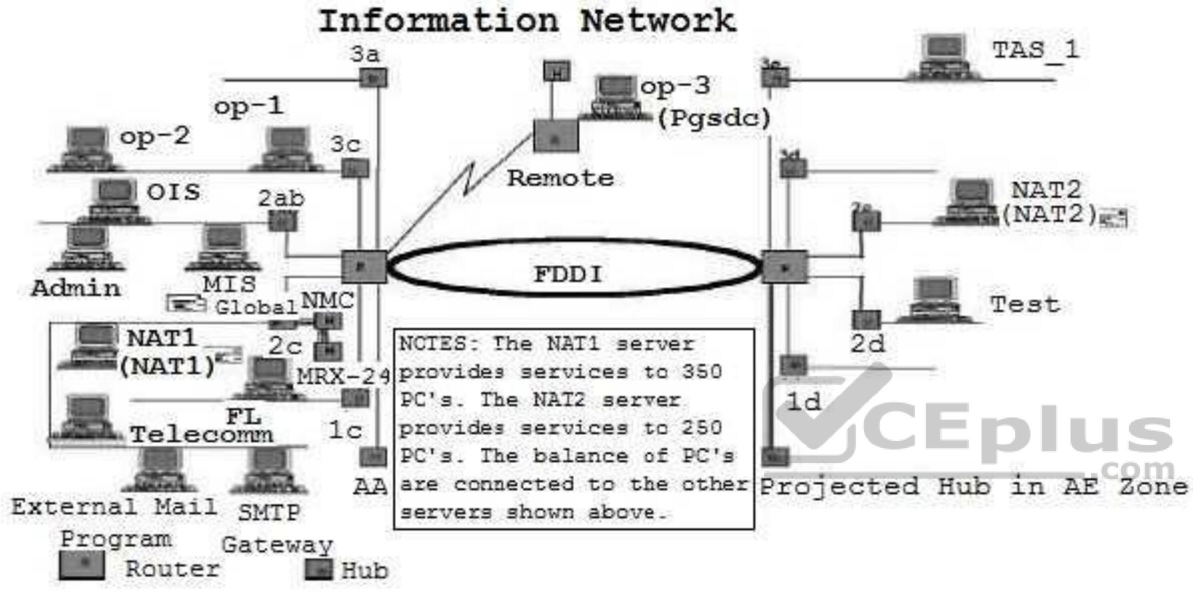
Explanation/Reference:

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 503

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?



NOTES: The NAT1 server provides services to 350 PC's. The NAT2 server provides services to 250 PC's. The balance of PC's are connected to the other servers shown above.

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

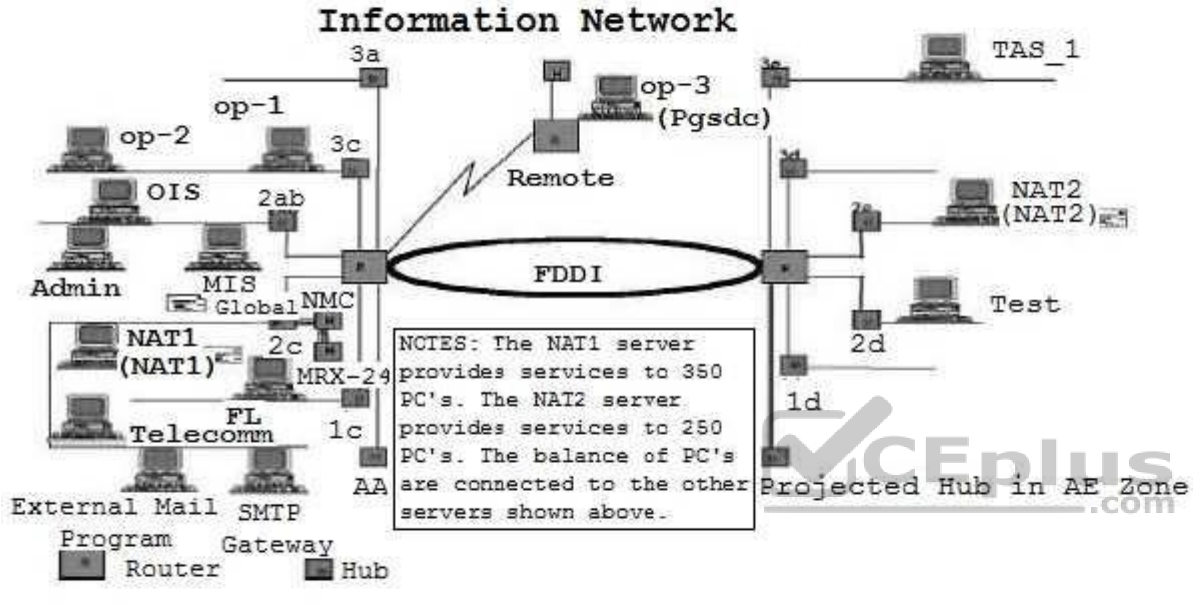
Correct Answer: C
Section: Protection of Information Assets
Explanation

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 504

In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?



NCTES: The NAT1 server provides services to 350 PC's. The NAT2 server provides services to 250 PC's. The balance of PC's are connected to the other servers shown above.

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 505

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 506
In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

A. address of the domain server.
B. resolution service for the name/address.
C. IP addresses for the internet.
D. domain name system.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
DNS is utilized primarily on the Internet for resolution of the name/address of the web site. It is an Internet service that translates domain names into IP addresses. As names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time a domain name is used, a DNS service must translate the name into the corresponding IP address. The DNS system has its own network, if one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

A.

QUESTION 507

In what way is a common gateway interface (CGI) MOST often used on a webserver?

Consistent way for transferring data to the application program and back to the user

B. Computer graphics imaging method for movies and TV

C. Graphic user interface for web design

D. interface to access the private gateway domain

Correct Answer: A

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word orienteering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

QUESTION 508

Receiving an EDI transaction and passing it through the communication's interface stage usually requires:

A. translating and unbundling transactions.

B. routing verification procedures.

C. passing data to the appropriate application system.

D. creating a point of receipt audit log.

Correct Answer: B

Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

A.
The communication’s interface stage requires routing verification procedures. Edi or ANSI X12 is a standard that must be interpreted by an application for transactions to be processed and then to be invoiced, paid and sent, whether they are for merchandise or services. There is no point sending and receiving EDI transactions if they cannot be processed by an internal system.
Unpacking transactions and recording audit logs are important elements that help follow business rules and establish controls, but are not part of the communication's interface stage.

QUESTION 509
Which of the following would be considered an essential feature of a network management system?

A graphical interface to map the network topology
B. Capacity to interact with the Internet to solve the problems
C. Connectivity to a help desk for advice on difficult issues
D. An export facility for piping data to spreadsheets

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To trace the topology of the network, a graphical interface would be essential. It is not necessary that each network be on the internet and connected to a help desk, while the ability to export to a spreadsheet is not an essential element.

QUESTION 510
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:

A.

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 511

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 512
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 513
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 514
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 515
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 516
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 517

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 518
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 519
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 520
To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

A. business software.
B. infrastructure platform tools.
C. application services.
D. system development tools.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
Projects should identify the complexities of the IT Infrastructure that can be simplified or isolated by the development of application services. Application services isolate system developers from the complexities of the IT infrastructure and offer common functionalities that are shared by many applications. Application services take the form of interfaces, middleware, etc. Business software focuses on business processes, whereas application services bridge the gap between applications and the IT Infrastructure components. Infrastructure platform tools are related to core hardware and software components required for development of the IT infrastructure. Systems development tools represent development components of the IT infrastructure development.

QUESTION 521
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 522
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 523
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 524
An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

A. Simple Object Access Protocol (SOAP)
B. Address Resolution Protocol (ARP)
C. Routing Information Protocol (RIP)
D. Transmission Control Protocol (TCP)

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Address Resolution Protocol (ARP) provides dynamic address mapping between an IP address and hardware address. Simple Object Access Protocol (SOAP) is a platform- independent XML- based protocol, enabling applications to communicate with each other over the Internet, and does not deal with media access control (MAC) addresses. Routing Information Protocol (RIP) specifies how routers exchange routing table information. Transmission Control Protocol (TCP) enables two hosts to establish a connection and exchange streams of data.

QUESTION 525
An IS auditor examining the configuration of an operating system to verify the controls should review the:

D.

A. transaction logs.

B. authorization tables.

C. parameter settings.

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 526
When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:

A. an integrated services digital network (ISDN) data link.

B. traffic engineering.

C. wired equivalent privacy (WEP) encryption of data.

D. analog phone terminals.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To ensure that quality of service requirements are achieved, the Voice-over IP (VoIP) service over the wide area network (WAN) should be protected from packet losses, latency or jitter. To reach this objective, the network performance can be managed using statistical techniques such as traffic engineering. The standard bandwidth of an integrated services digital network (ISDN) data link would not provide the quality of services required for corporate VoIP services. WEP is an encryption scheme related to wireless networking. The VoIP phones are usually connected to a corporate local area network (LAN) and are not analog.

D.

QUESTION 527

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

A. Session keys are dynamic
B. Private symmetric keys are used
C. Keys are static and shared
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 528

During the audit of a database server, which of the following would be considered the GREATEST exposure?

A. The password does not expire on the administrator account
B. Default global security settings for the database remain unchanged
C. Old data have not been purged
D. Database activity is not fully logged

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

Default security settings for the database could allow issues like blank user passwords or passwords that were the same as the username. Logging all database activity is not practical. Failure to purge old data may present a performance issue but is not an immediate security concern. Choice A is an exposure but not as serious as B.

QUESTION 529

D.

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 530
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 531
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 532
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 533
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 534
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 535
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 536
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 537
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 538
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 539
The role of the certificate authority (CA) as a third party is to:

A. provide secured communication and networking services based on certificates.
B. host a repository of certificates with the corresponding public and secret keys issued by that CA.
C. act as a trusted intermediary between two communication partners.
D. confirm the identity of the entity owning a certificate issued by that CA.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The primary activity of a CA is to issue certificates. The primary role of the CA is to check the identity of the entity owning a certificate and to confirm the integrity of any certificate it issued. Providing a communication infrastructure is not a CA activity. The secret keys belonging to the certificates would not be archived at the CA. The CA can contribute to authenticating the communicating partners to each other, but the CA is not involved in the communication stream itself.

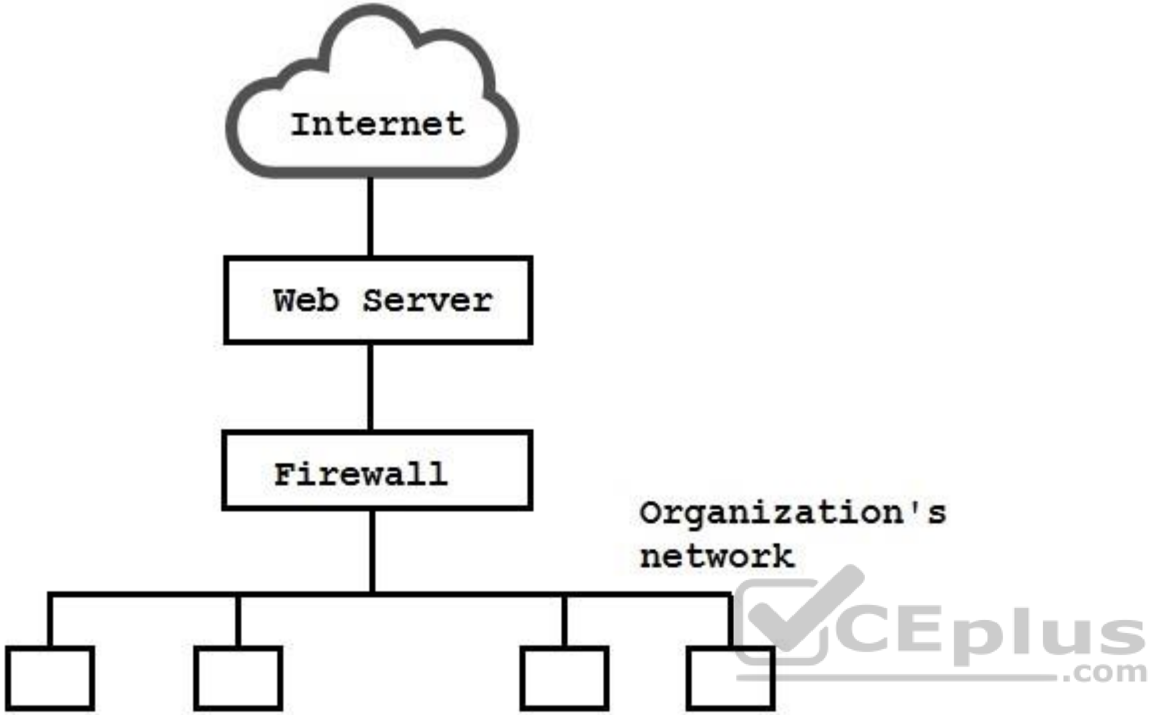
QUESTION 540
Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

A. The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
B. All personal SET certificates are stored securely in the buyer's computer.
C. The buyer is liable for any transaction involving his/her personal SET certificates.
D. The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The usual agreement between the credit card issuer and the cardholder stipulates that the cardholder assumes responsibility for any use of their personal SET certificates for e- commerce transactions. Depending upon the agreement between the merchant and the buyer's credit card issuer, the merchant will have access to the credit card number and expiration date. Secure data storage in the buyer's computer (local computer security) is not part of the SET standard. Although the buyer is not required to enter their credit card data, they will have to handle the wallet software.

QUESTION 541
E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

A. alert the appropriate staff.
B. create an entry in the log.
C. close firewall-2.
D. close firewall-1.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Traffic for the internal network that did not originate from the mail gateway is a sign that firewall-1 is not functioning properly. This may have been caused by an attack from a hacker. Closing firewall-2 is the first thing that should be done, thus preventing damage to the internal network.
After closing firewall-2, the malfunctioning of firewall-1 can be investigated. The IDS should trigger the closing of firewall-2 either automatically or by manual intervention. Between the detection by the IDS and a response from the system administrator valuable time can be lost, in which a hacker could also compromise firewall-2. An entry in the log is valuable for later analysis, but before that, the IDS should close firewall-2. If firewall-1 has already been compromised by a hacker, it might not be possible for the IDS to close it.

QUESTION 542
An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

A. The data collected on attack methods
B. The information offered to outsiders on the honeypot
C. The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
D. The risk that the honeypot would be subject to a distributed denial-of-service attack

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Choice C represents the organizational risk that the honeypot could be used as a point of access to launch further attacks on the enterprise's systems. Choices A and B are purposes for deploying a honeypot, not a concern. Choice D, the risk that the honeypot would be subject to a distributed denial-of-service (DDoS) attack, is not relevant, as the honeypot is not a critical device for providing service.
QUESTION 543
Which of the following should be a concern to an IS auditor reviewing a wireless network?

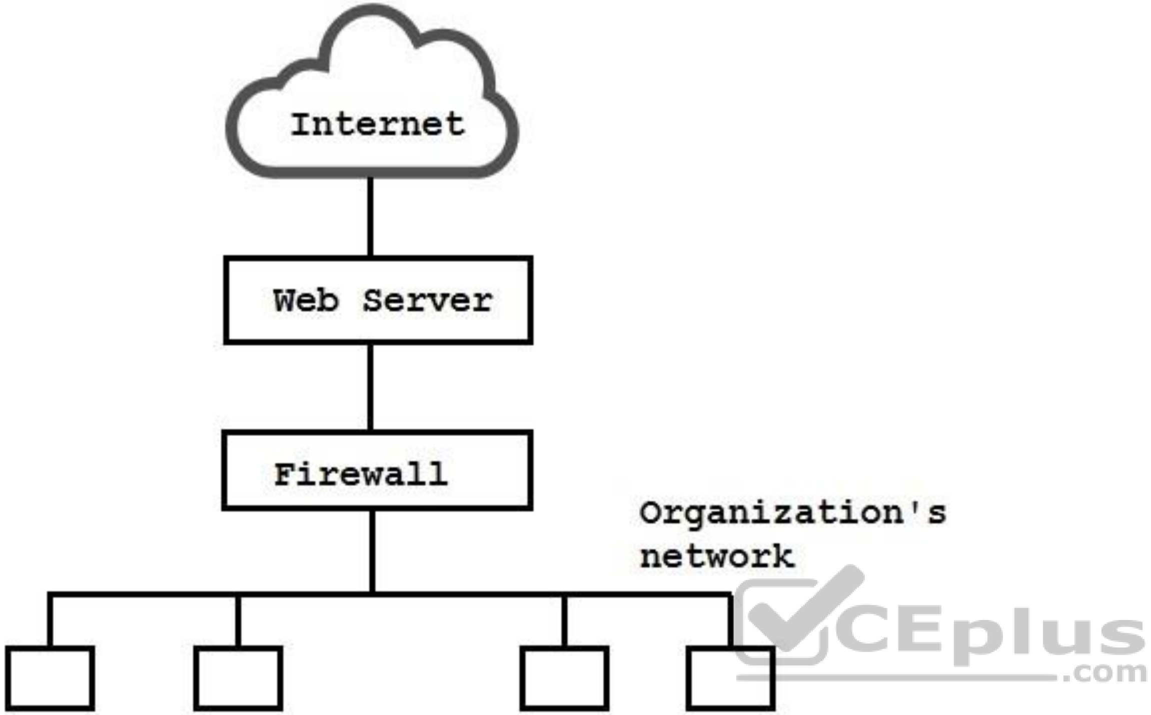
A. 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
B. SSID (Service Set IDentifier) broadcasting has been enabled.
C. Antivirus software has been installed in all wireless clients.
D. MAC (Media Access Control) access control filtering has been deployed.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
SSID broadcasting allows a user to browse for available wireless networks and to access them without authorization. Choices A, C and D are used to strengthen a wireless network.

QUESTION 544
To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



A. Firewall and the organization's network.
B. Internet and the firewall.
C. Internet and the web server.
D. Web server and the firewall.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Attack attempts that could not be recognized by the firewall will be detected if a network- based intrusion detection system is placed between the firewall and the organization's network. A network-based intrusion detection system placed between the internet and the firewall will detect attack attempts, whether they do or do not enter the firewall.

QUESTION 545

Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

A. Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
B. The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
C. Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
D. Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To ensure authenticity and confidentiality, a message must be encrypted twice: first with the sender's private key, and then with the receiver's public key. The receiver can decrypt the message, thus ensuring confidentiality of the message. Thereafter, the decrypted message can be decrypted with the public key of the sender, ensuring authenticity of the message. Encrypting the message with the sender's private key enables anyone to decrypt it.

QUESTION 546

An efficient use of public key infrastructure (PKI) should encrypt the:

A. entire message.
B. private key.
C. public key.
D. symmetric session key.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Public key (asymmetric) cryptographic systems require larger keys (1,024 bits) and involve intensive and time-consuming computations. In comparison, symmetric encryption is considerably faster, yet relies on the security of the process for exchanging the secret key. To enjoy the benefits of both systems, a symmetric session key is exchanged using public key methods, after which it serves as the secret key for encrypting/decrypting messages sent between two parties.

QUESTION 547

Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

A. DES
B. AES
C. Triple DES
D. RSA

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

Advanced Encryption Standard (AES), a public algorithm that supports keys from 128 to 256 bits in size, not only provides good security, but provides speed and versatility across a variety of computer platforms. AES runs securely and efficiently on large computers, desktop computers and even small devices such as smart cards. DES is not considered a strong cryptographic solution since its entire key space can be brute forced by large computer systems within a relatively short period of time. Triple DES can take up to three times longer than DES to perform encryption and decryption. RSA keys are large numbers that are suitable only for short messages, such as the creation of a digital signature.

QUESTION 548

Disabling which of the following would make wireless local area networks more secure against unauthorized access?

A. MAC (Media Access Control) address filtering
B. WPA (Wi-Fi Protected Access Protocol)
C. LEAP (Lightweight Extensible Authentication Protocol)
D. SSID (service set identifier) broadcasting

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

Disabling SSID broadcasting adds security by making it more difficult for unauthorized users to find the name of the access point. Disabling MAC address filtering would reduce security. Using MAC filtering makes it more difficult to access a WLAN, because it would be necessary to catch traffic and forge the MAC address. Disabling WPA reduces security. Using WPA adds security by encrypting the traffic. Disabling LEAP reduces security. Using LEAP adds security by encrypting the wireless traffic.

QUESTION 549
Which of the following is BEST suited for secure communications within a small group?

A. Key distribution center
B. Certification authority
C. Web of trust
D. Kerberos Authentication System

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Web of trust is a key distribution method suitable for communication in a small group. It ensures pretty good privacy (PGP) and distributes the public keys of users within a group. Key distribution center is a distribution method suitable for internal communication for a large group within an institution, and it will distribute symmetric keys for each session. Certification authority is a trusted third party that ensures the authenticity of the owner of the certificate. This is necessary for large groups and formal communication. A Kerberos Authentication System extends the function of a key distribution center, by generating 'tickets' to define the facilities on networked machines which are accessible to each user.

QUESTION 550
Which of the following is the MOST important action in recovering from a cyberattack?

A. Creation of an incident response team
B. Use of cybenforensic investigators
C. Execution of a business continuity plan
D. Filling an insurance claim

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation: The most important key step in recovering from cyberattacks is the execution of a business continuity plan to quickly and cost-effectively recover critical systems, processes and data. The incident response team should exist prior to a cyberattack. When a cyberattack is suspected, cybenforensic investigators should be used to set up alarms, catch intruders within the network, and track and trace them over the Internet. After taking the above steps, an organization may have a residual risk that needs to be insured and claimed for traditional and electronic exposures.

QUESTION 551
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 552
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 553
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 554
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 555
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 556
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 557

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 558

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 559
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 560
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 561
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 562
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 563
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 564
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 565
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 566
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 567
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 568
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 569

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 570

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 571
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 572

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 573
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 574
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 575
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 576

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 577

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 578

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 579

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 580
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 581
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 582
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 583
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 584
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 585
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 586
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 587
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 588
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 589
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 590
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 591
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 592
When using a digital signature, the message digest is computed:

A. only by the sender.
B. only by the receiver.
C. by both the sender and the receiver.
D. by the certificate authority (CA).

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A digital signature is an electronic identification of a person or entity. It is created by using asymmetric encryption. To verify integrity of data, the sender uses a cryptographic hashing algorithm against the entire message to create a message digest to be sent along with the message. Upon receipt of the message, the receiver will recompute the hash using the same algorithm and compare results with what was sent to ensure the integrity of the message.

QUESTION 593
Which of the following would effectively verify the originator of a transaction?
A. Using a secret password between the originator and the receiver
B. Encrypting the transaction with the receiver's public key
C. Using a portable document format (PDF) to encapsulate transaction content
D. Digitally signing the transaction with the source's private key

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

A digital signature is an electronic identification of a person, created by using a public key algorithm, to verify to a recipient the identity of the source of a transaction and the integrity of its content. Since they are a 'shared secret' between the user and the system itself, passwords are considered a weaker means of authentication. Encrypting the transaction with the recipient's public key will provide confidentiality for the information, while using a portable document format(PDF) will probe the integrity of the content but not necessarily authorship.

QUESTION 594

A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network would use:

A. eavesdropping

B. spoofing.

C. traffic analysis.D. masquerading.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

In traffic analysis, which is a passive attack, an intruder determines the nature of the traffic flow between defined hosts and through an analysis of session length, frequency and message length, and the intruder is able to guess the type of communication taking place. This typically is used when messages are encrypted and eavesdropping would not yield any meaningful results, in eavesdropping, which also is a passive attack, the intruder gathers the information flowing through the network with the intent of acquiring and releasing message contents for personal analysis or for third parties. Spoofing and masquerading are active attacks, in spoofing, a user receives an e-mail that appears to have originated from one source when it actually was sent from another source. In masquerading, the intruder presents an identity other than the original identity.

QUESTION 595

Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the:

A. registration authority (RA).

B. certificate authority (CA).

C. certificate repository.

D. receiver.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:
A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. As a part of the public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate. The CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will decrypt the certificate with the CA's public key.

QUESTION 596
IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

A. Review and, where necessary, upgrade firewall capabilities
B. Install modems to allow remote maintenance support access
C. Create a physically distinct network to handle VoIP traffic
D. Redirect all VoIP traffic to allow clear text logging of authentication credentials

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Firewalls used as entry points to a Voice-over Internet Protocol (VoIP) network should be VoIP- capable. VoIP network services such as H.323 introduce complexities that are likely to strain the capabilities of older firewalls. Allowing for remote support access is an important consideration. However, a virtual private network (VPN) would offer a more secure means of enabling this access than reliance on modems. Logically separating the VoIP and data network is a good idea. Options such as virtual LANS (VLA.NS), traffic shaping, firewalls and network address translation (NAT) combined with private IP addressing can be used; however, physically separating the networks will increase both cost and administrative complexity. Transmitting or storing clear text information, particularly sensitive information such as authentication credentials, will increase network vulnerability. When designing a VoIP network, it is important to avoid introducing any processing that will unnecessarily increase latency since this will adversely impact VoIP quality.

QUESTION 597
Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

A. Statistical-based
B. Signature-based
C. Neural network
D. Host-based

Correct Answer: A

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal network activity may at times include unexpected behavior (e.g., a sudden massive download by multiple users), these activities will be flagged as suspicious. A signature-based IDS is limited to its predefined set of detection rules, just like a virus scanner. A neural network combines the previous two IDSs to create a hybrid and better system. Host-based is another classification of IDS. Any of the three IDSs above may be host- or network-based.

QUESTION 598
When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

A. hardware is protected against power surges.
B. integrity is maintained if the main power is interrupted.
C. immediate power will be available if the main power is lost.
D. hardware is protected against long-term power fluctuations.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A voltage regulator protects against short-term power fluctuations. It normally does not protect against long-term surges, nor does it maintain the integrity if power is interrupted or lost.

QUESTION 599
Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?
A. Halon gas
B. Wet-pipe sprinklersC. Dry-pipe sprinklers
D. Carbon dioxide gas

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation: Water sprinklers, with an automatic power shutoff system, are accepted as efficient because they can be set to automatic release without threat to life, and water is environmentally friendly.
Sprinklers must be dry-pipe to prevent the risk of leakage. Halon is efficient and effective as it does not threaten human life and, therefore, can be set to automatic release, but it is environmentally damaging and very expensive. Water is an acceptable medium but the pipes should be empty to avoid leakage, so a full system is not a viable option. Carbon dioxide is accepted as an environmentally acceptable gas, but it is less efficient because it cannot be set to automatic release in a staffed site since it threatens life.

QUESTION 600
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 601
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 602
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 603
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 604
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 605
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 606
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 607
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 608

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 609

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 610
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 611
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 612

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 613

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 614
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 615
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 616
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 617

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 618
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 619
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 620
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 621
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 622
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 623
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.

A.

QUESTION 624

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:

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 625

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:

A.
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 626
Which of the following is the MOST important objective of data protection?

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 627
An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to- disk solution. This is appropriate because:

A. fast synthetic backups for offsite storage are supported.
B. backup to disk is always significantly faster than backup to tape.
C. tape libraries are no longer needed.
D. data storage on disks is more reliable than on tapes.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

A.

Disk-to-disk (D2D) backup should not be seen as a direct replacement for backup to tape; rather, it should be viewed as part of a multitier backup architecture that takes advantage of the best features of both tape and disk technologies. Backups to disks are not dramatically faster than backups to tapes in a balanced environment. Most often than not there is hardly a difference, since the limiting components are not tape or disk drives but the overall sustained bandwidth of the backup server's backplane. The advantage in terms of speed is in restoring performance, since all data are on hand and can be accessed randomly, resulting in a dramatic enhancement in throughput. This makes fast synthetic backups (making a full back up without touching the host's data only by using the existing incremental backups) efficient and easy. Although the cost of disks has been reduced, tape-based backup can offer an overall cost advantage over disk-only solutions. Even if RAID arrays are used for D2Dstorage, a failed drive must be swapped out and the RAID set rebuilt before another disk drive fails, thus making this kind of backup more risky and not suitable as a solution of last resort. In contrast, a single tape drive failure does not produce any data loss since the data resides on the tape media. In a multidrive library, the loss of the use of a single tape drive has no impact on the overall level of data protection. Conversely, the loss of a disk drive in an array can put all data at risk. This in itself reinforces the benefits of a disk-to-disk-to-any storage hierarchy, as data could be protected by a tertiary stage of disk storage and ultimately tape. Beyond the drive failure issue, tape has an inherent reliability advantage over any disk drive as it has no boot sector or file allocation table that can be infected or manipulated by a virus.

QUESTION 628
During a disaster recovery test, an IS auditor observes that the performance of the disaster recovery site's server is slow. To find the root cause of this, the IS auditor should FIRST review the:

A. event error log generated at the disaster recovery site.
B. disaster recovery test plan.
C. disaster recovery plan (DRP).
D. configurations and alignment of the primary and disaster recovery sites.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since the configuration of the system is the most probable cause, the IS auditor should review that first. If the issue cannot be clarified, the IS auditor should then review the event error log. The disaster recovery test plan and the disaster recovery plan (DRP) would not contain information about the system configuration.

QUESTION 629
An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:

A. a data loss of up to 1 minute, but the processing must be continuous.
B. a 1-minute processing interruption but cannot tolerate any data loss.
C. a processing interruption of 1 minute or more.
D. both a data less and processing interruption longer than 1 minute.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery point objective (RPO) measures how much data loss can be accepted. Choices B, C and D are incorrect since they exceed the RTO limits set by the scenario.

QUESTION 630

Which of the following issues should be the GREATEST concern to the IS auditor when reviewing an IT disaster recovery test?

A. Due to the limited test time window, only the most essential systems were tested. The other systems were tested separately during the rest of the year.
B. During the test it was noticed that some of the backup systems were defective or not working, causing the test of these systems to fail.
C. The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
D. Every year, the same employees perform the test. The recovery plan documents are not used since every step is well known by all participants.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A disaster recovery test should test the plan, processes, people and IT systems. Therefore, if the plan is not used, its accuracy and adequacy cannot be verified. Disaster recovery should not rely on key staff since a disaster can occur when they are not available. It is common that not all systems can be tested in a limited test time frame. It is important, however, that those systems which are essential to the business are tested, and that the other systems are eventually tested throughout the year. One aim of the test is to identify and replace defective devices so that all systems can be replaced in the case of a disaster. Choice B would only be a concern if the number of discovered problems is systematically very high, in a real disaster, there is no need for a clean shutdown of the original production environment since the first priority is to bring the backup site up.

QUESTION 631

The frequent updating of which of the following is key to the continued effectiveness of a disaster recovery plan (DRP)?

A. Contact information of key personnel
B. Server inventory documentation
C. individual roles and responsibilities
D. Procedures for declaring a disaster

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In the event of a disaster, it is important to have a current updated list of personnel who are key to the operation of the plan. Choices B, C and D would be more likely to remain stable overtime.

QUESTION 632
A live test of a mutual agreement for IT system recovery has been carried out, including a four- hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:

A. system and the IT operations team can sustain operations in the emergency environment.
B. resources and the environment could sustain the transaction load.
C. connectivity to the applications at the remote site meets response time requirements.
D. workflow of actual business operations can use the emergency system in case of a disaster.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The applications have been intensively operated, therefore choices B, C and D have been actually tested, but the capability of the system and the IT operations team to sustain and support this environment (ancillary operations, batch closing, error corrections, output distribution, etc.) is only partially tested.

QUESTION 633
To address an organization's disaster recovery requirements, backup intervals should not exceed the:

A. service level objective (SLO).
B. recovery time objective (RTO).
C. recovery point objective (RPO).
D. maximum acceptable outage (MAO).

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The recovery point objective (RPO) defines the point in time to which data must be restored after a disaster so as to resume processing transactions. Backups should be performed in a way that the latest backup is no older than this maximum time frame. If service levels are not met, the usual consequences are penalty payments, not cessation of business. Organizations will try to set service level objectives (SLOs) so as to meet established targets. The resulting time for the service level agreement (SLA) will usually be longer than the RPO. The recovery time objective (RTO) defines the time period after the disaster in which normal business functionality needs to be restored. The maximum acceptable outage (MAO) is the maximum amount of system downtime that is tolerable. It can be used as a synonym for RTO. However, the RTO denotes an objective/target, while the MAO constitutes a vital necessity for an organization's survival.

QUESTION 634
After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?

A. Test and maintain the plan.

B. Develop a specific plan.
C. Develop recovery strategies.
D. implement the plan.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster. After selecting a strategy, a specific plan can be developed, tested and implemented.

QUESTION 635
Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?

A. Pilot
B. Paper
C. Unit
D. System

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A paper test is appropriate for testing a BCP. it is a walkthrough of the entire plan, or part of the plan, involving major players in the plan's execution, who reason out what may happen in a particular disaster. Choices A, C and D are not appropriate for a BCP.

QUESTION 636
An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?

A. Nonavailability of an alternate private branch exchange (PBX) system
B. Absence of a backup for the network backbone
C. Lack of backup systems for the users' PCs
D. Failure of the access card system

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Failure of a network backbone will result in the failure of the complete network and impact the ability of all users to access information on the network. The nonavailability of an alternate PBX system will result in users not being able to make or receive telephone calls or faxes; however, users may have alternate means of communication, such as a mobile phone or e-mail. Lack of backup systems for user PCs will impact only the specific users, not all users. Failure of the access card system impacts the ability to maintain records of the users who are entering the specified work areas; however, this could be mitigated by manual monitoring controls.

QUESTION 637
As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

A. Organizational risks, such as single point-of-failure and infrastructure risk
B. Threats to critical business processes
C. Critical business processes for ascertaining the priority for recovery
D. Resources required for resumption of business

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The identification of the priority for recovering critical business processes should be addressed first. Organizational risks should be identified next, followed by the identification of threats to critical business processes. Identification of resources for business resumption will occur after the tasks mentioned.

QUESTION 638
Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?

A. verify compatibility with the hot site.
B. Review the implementation report.
C. Perform a walk-through of the disaster recovery plan.
D. Update the IS assets inventory.

Correct Answer: D
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
An IS assets inventory is the basic input for the business continuity/disaster recovery plan, and the plan must be updated to reflect changes in the IS infrastructure. The other choices are procedures required to update the disaster recovery plan after having updated the required assets inventory.

QUESTION 639
Which of the following would contribute MOST to an effective business continuity plan (BCP)?

A. Document is circulated to all interested parties
B. Planning involves all user departments
C. Approval by senior management
D. Audit by an external IS auditor

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The involvement of user departments in the BCP is crucial for the identification of the business processing priorities. The BCP circulation will ensure that the BCP document is received by all users. Though essential, this does not contribute significantly to the success of the BCP. A BCP approved by senior management would not ensure the quality of the BCP, nor would an audit necessarily improve the quality of the BCP.

QUESTION 640
To develop a successful business continuity plan, end user involvement is critical during which of the following phases?

A. Business recovery strategy
B. Detailed plan development
C. Business impact analysis (BIA)

D. Testing and maintenance

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
End user involvement is critical in the BIA phase. During this phase the current operations of the business needs to be understood and the impact on the business of various disasters must be evaluated. End users are the appropriate persons to provide relevant information for these tasks, inadequate end user involvement in this stage could result in an inadequate understanding of business priorities and the plan not meeting the requirements of the organization.

QUESTION 641
Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?

A. A hot site contracted and available as needed.
B. A business continuity manual is available and current.
C. insurance coverage is adequate and premiums are current.
D. Media backups are performed on a timely basis and stored offsite.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.

QUESTION 642
The PRIMARY objective of business continuity and disaster recovery plans should be to:

A. safeguard critical IS assets.
B. provide for continuity of operations.
C. minimize the loss to an organization.
D. protect human life.

Correct Answer: D

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people. All other priorities are important but are secondary objectives of a business continuity and disaster recovery plan.

QUESTION 643
After a full operational contingency test, an IS auditor performs a review of the recovery steps. The auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the auditor recommend?

A. Perform an integral review of the recovery tasks.
B. Broaden the processing capacity to gain recovery time.
C. Make improvements in the facility's circulation structure.
D. increase the amount of human resources involved in the recovery.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Performing an exhaustive review of the recovery tasks would be appropriate to identify the way these tasks were performed, identify the time allocated to each of the steps required to accomplish recovery, and determine where adjustments can be made. Choices B, C and D could be actions after the described review has been completed.

QUESTION 644
While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/backup at an offsite location would be:

A. shadow file processing.
B. electronic vaulting.
C. hard-disk mirroring.
D. hot-site provisioning.

Correct Answer: A
Section: Protection of Information Assets

Explanation

Explanation/Reference:

Explanation:

In shadow file processing, exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently. This is used for critical data files, such as airline booking systems. Electronic vaulting electronically transmits data either to direct access storage, an optical disc or another storage medium; this is a method used by banks. Hard-disk mirroring provides redundancy in case the primary hard disk fails. All transactions and operations occur on two hard disks in the same server. A hot site is an alternate site ready to take over business operations within a few hours of any business interruption and is not a method for backing up data.

QUESTION 645

Depending on the complexity of an organization's business continuity plan (BCP), the plan may be developed as a set of more than one plan to address various aspects of business continuity and disaster recovery, in such an environment, it is essential that:

A. each plan is consistent with one another.

B. all plans are integrated into a single plan.

C. each plan is dependent on one another.

D. the sequence for implementation of all plans is defined.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation:

Depending on the complexity of an organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan. However, each plan has to be consistent with other plans to have a viable business continuity planning strategy. It may not be possible to define a sequence in which plans have to be implemented, as it may be dependent on the nature of disaster, criticality, recovery time, etc.

QUESTION 646

During a business continuity audit an IS auditor found that the business continuity plan (BCP) covered only critical processes. The IS auditor should:

A. recommend that the BCP cover all business processes.

B. assess the impact of the processes not covered.

C. report the findings to the IT manager.

D. redefine critical processes.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The business impact analysis needs to be either updated or revisited to assess the risk of not covering all processes in the plan. It is possible that the cost of including all processes might exceed the value of those processes; therefore, they should not be covered. An IS auditor should substantiate this by analyzing the risk.

QUESTION 647
An IS auditor noted that an organization had adequate business continuity plans (BCPs) for each individual process, but no comprehensive BCP. Which would be the BEST course of action for the IS auditor?

A. Recommend that an additional comprehensive BCP be developed.
B. Determine whether the BCPs are consistent.
C. Accept the BCPs as written.
D. Recommend the creation of a single BCP.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Depending on the complexity of the organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan; however, each plan should be consistent with other plans to have a viable business continuity planning strategy.

QUESTION 648
When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?

A. Business continuity self-audit
B. Resource recovery analysis
C. Risk assessment
D. Gap analysis

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Risk assessment and business impact assessment are tools for understanding business- for- business continuity planning. Business continuity self-audit is a tool for evaluating the adequacy of the BCP, resource recovery analysis is a tool for identifying a business resumption strategy, while the role gap analysis can play in business continuity planning is to identify deficiencies in a plan. Neither of these is used for gaining an understanding of the business.

QUESTION 649
During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?

A. Evacuation plan
B. Recovery priorities
C. Backup storages
D. Call tree

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Protecting human resources during a disaster-related event should be addressed first. Having separate BCPs could result in conflicting evacuation plans, thus jeopardizing the safety of staff and clients. Choices B, C and D may be unique to each department and could be addressed separately, but still should be reviewed for possible conflicts and/or the possibility of cost reduction, but only after the issue of human safety has been analyzed.

QUESTION 650
Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:

A. downtime costs.
B. resumption costs.
C. recovery costs.
D. walkthrough costs.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Since the recovery time is longer in plan B, resumption and recovery costs can be expected to be lower. Walkthrough costs are not a part of disaster recovery. Since the management considered a higher window for recovery in plan B, downtime costs included in the plan are likely to be higher.

QUESTION 651
The optimum business continuity strategy for an entity is determined by the:

A. lowest downtime cost and highest recovery cost.
B. lowest sum of downtime cost and recovery cost.
C. lowest recovery cost and highest downtime cost.
D. average of the combined downtime and recovery cost.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Both costs have to be minimized, and the strategy for which the costs are lowest is the optimum strategy. The strategy with the highest recovery cost cannot be the optimum strategy. The strategy with the highest downtime cost cannot be the optimum strategy. The average of the combined downtime and recovery cost will be higher than the lowest combined cost of downtime and recovery.

QUESTION 652
The PRIMARY objective of testing a business continuity plan is to:

A. familiarize employees with the business continuity plan.
B. ensure that all residual risks are addressed.
C. exercise all possible disaster scenarios.
D. identify limitations of the business continuity plan.

Correct Answer: D
Section: Protection of Information Assets

Explanation

Explanation/Reference:
Explanation:
Testing the business continuity plan provides the best evidence of any limitations that may exist. Familiarizing employees with the business continuity plan is a secondary benefit of a test. It is not cost effective to address residual risks in a business continuity plan, and it is not practical to test all possible disaster scenarios.

QUESTION 653
In determining the acceptable time period for the resumption of critical business processes:

A. only downtime costs need to be considered.
B. recovery operations should be analyzed.
C. both downtime costs and recovery costs need to be evaluated.
D. indirect downtime costs should be ignored.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Both downtime costs and recovery costs need to be evaluated in determining the acceptable time period before the resumption of critical business processes. The outcome of the business impact analysis (BIA) should be a recovery strategy that represents the optimal balance. Downtime costs cannot be looked at in isolation. The quicker information assets can be restored and business processing resumed, the smaller the downtime costs. However, the expenditure needed to have the redundant capability required to recover information resources might be prohibitive for nonessential business processes. Recovery operations do not determine the acceptable time period for the resumption of critical business processes, and indirect downtime costs should be considered in addition to the direct cash outflows incurred due to business disruption. The indirect costs of a serious disruption to normal business activity, e.g., loss of customer and supplier goodwill and loss of market share, may actually be more significant than direct costs over time, thus reaching the point where business viability is threatened.

QUESTION 654
An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the PRIMARY task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?

A. Review whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations.
B. Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster.
C. Review the methodology adopted by the organization in choosing the service provider.

D. Review the accreditation of the third-party service provider's staff.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Reviewing whether the service provider's business continuity plan (BCP) process is aligned with the organization's BCP and contractual obligations is the correct answer since an adverse effect or disruption to the business of the service provider has a direct bearing on the organization and its customers. Reviewing whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster is not the correct answer since the presence of penalty clauses, although an essential element of a SLA, is not a primary concern. Choices C and D are possible concerns, but of lesser importance.

QUESTION 655
An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

A. alignment of the BCP with industry best practices.
B. results of business continuity tests performed by IS and end-user personnel.
C. off-site facility, its contents, security and environmental controls.
D. annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:

The effectiveness of the business continuity plan (BCP) can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives. All other choices do not provide the assurance of the effectiveness of the BCP.

QUESTION 656
To optimize an organization's business contingency plan (BCP), an IS auditor should recommend conducting a business impact analysis (BIA) in order to determine:

A. the business processes that generate the most financial value for the organization and therefore must be recovered first.
B. the priorities and order for recovery to ensure alignment with the organization's business strategy.

C. the business processes that must be recovered following a disaster to ensure the organization's survival.
D. he priorities and order of recovery which will recover the greatest number of systems in the shortest time frame.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
To ensure the organization's survival following a disaster, it is important to recover the most critical business processes first, it is a common mistake to overemphasize value (A) rather than urgency. For example, while the processing of incoming mortgage loan payments is important from a financial perspective, it could be delayed for a few days in the event of a disaster. On the other hand, wiring funds to close on a loan, while not generating direct revenue, is far more critical because of the possibility of regulatory problems, customer complaints and reputation issues. Choices B and D are not correct because neither the long-term business strategy nor the mere number of recovered systems has a direct impact at this point in time.

QUESTION 657
A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor MOST likely raise an issue?

A. The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
B. The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
C. The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.
D. The organization plans to rent a shared alternate site with emergency workplaces which has only enough room for half of the normal staff. **Correct**

Answer: B

Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It is a common mistake to use scenario planning for business continuity. The problem is that it is impossible to plan and document actions for every possible scenario. Planning for just selected scenarios denies the fact that even improbable events can cause an organization to break down. Best practice planning addresses the four possible areas of impact in a disaster: premises, people, systems, and suppliers and other dependencies. All scenarios can be reduced to these four categories and can be handled simultaneously. There are very few special scenarios which justify an additional separate analysis, it is a good idea to use best practices and external advice for such an important topic, especially since knowledge of the right level of preparedness and the judgment about

adequacy of the measures taken is not available in every organization. The recovery time objectives (RTOs) are based on the essential business processes required to ensure the organization's survival, therefore it would be inappropriate for them to be based on IT capabilities. Best practice guidelines recommend having 20%-40% of normal capacity available at an emergency site; therefore, a value of 50% would not be a problem if there are no additional factors.

QUESTION 658
A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?

A. Full-scale test with relocation of all departments, including IT, to the contingency site
B. Walk-through test of a series of predefined scenarios with all critical personnel involved
C. IT disaster recovery test with business departments involved in testing the critical applications
D. Functional test of a scenario with limited IT involvement

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
After a tabletop exercise has been performed, the next step would be a functional test, which includes the mobilization of staff to exercise the administrative and organizational functions of a recovery. Since the IT part of the recovery has been tested for years, it would be more efficient to verify and optimize the business continuity plan (BCP) before actually involving IT in a full-scale test. The full-scale test would be the last step of the verification process before entering into a regular annual testing schedule. A full-scale test in the situation described might fail because it would be the first time that the plan is actually exercised, and a number of resources (including IT) and time would be wasted. The walk- through test is the most basic type of testing. Its intention is to make key staff familiar with the plan and discuss critical plan elements, rather than verifying its adequacy. The recovery of applications should always be verified and approved by the business instead of being purely IT-driven. A disaster recovery test would not help in verifying the administrative and organizational parts of the BCP which are not IT-related.

QUESTION 659
Everything not explicitly permitted is forbidden has which of the following kinds of tradeoff?

A.
it improves security at a cost in functionality.
B. it improves functionality at a cost in security.
C. it improves security at a cost in system performance.
D. it improves performance at a cost in functionality.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"Everything not explicitly permitted is forbidden (default deny) improves security at a cost in functionality. This is a good approach if you have lots of security threats. On the other hand, ""Everything not explicitly forbidden is permitted"" (default permit) allows greater functionality by sacrificing security. This is only a good approach in an environment where security threats are non- existent or negligible."

QUESTION 660
Default permit is only a good approach in an environment where:

A. security threats are non-existent or negligible.
B. security threats are non-negligible.
C. security threats are serious and severe.
D. users are trained.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"Everything not explicitly permitted is forbidden (default deny) improves security at a cost in functionality. This is a good approach if you have lots of security threats. On the other hand, ""Everything not explicitly forbidden is permitted"" (default permit) allows greater functionality by sacrificing security. This is only a good approach in an environment where security threats are non- existent or negligible."

QUESTION 661

B.
Talking about the different approaches to security in computing, the principle of regarding the computer system itself as largely an untrusted system emphasizes:

A. most privilege

full privilege

C. least privilege
D. null privilege
E. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
There are two different approaches to security in computing. One focuses mainly on external threats, and generally treats the computer system itself as a trusted system. The other regards the computer system itself as largely an untrusted system, and redesigns it to make it more secure in a number of ways. This technique enforces the principle of least privilege to great extent, where an entity has only the privileges that are needed for its function.

QUESTION 662
Which of the following refers to the proving of mathematical theorems by a computer program?

A. Analytical theorem proving
B. Automated technology proving
C. Automated theorem processingD. Automated theorem proving
E. None of the choices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Automated theorem proving (ATP) is the proving of mathematical theorems by a computer program. Depending on the underlying logic, the problem of deciding the validity of a theorem varies from trivial to impossible. Commercial use of automated theorem proving is mostly concentrated in integrated circuit design and verification.

C.

QUESTION 663

Which of the following BEST describes the concept of ""defense in depth""?

A. more than one subsystem needs to be compromised to compromise the security of the system and the information it holds.
B. multiple firewalls are implemented.
multiple firewalls and multiple network OS are implemented.
D. intrusion detection and firewall filtering are required.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"With 0""defense in depth"", more than one subsystem needs to be compromised to compromise the security of the system and the information it holds. Subsystems should default to secure settings, and wherever possible should be designed to ""fail secure"" rather than ""fail insecure""."

QUESTION 664

"Under the concept of ""defense in depth"", subsystems should be designed to:"

A. ""fail insecure"""
B. ""fail secure"""
C. ""react to attack"""
D. ""react to failure"""
E. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"With 0""defense in depth"", more than one subsystem needs to be compromised to compromise the security of the system and the information it holds. Subsystems should default to secure settings, and wherever possible should be designed to ""fail secure"" rather than ""fail insecure"".

D.

QUESTION 665

Security should ALWAYS be an all or nothing issue.

A. True
B. True for trusted systems only
C. True for untrusted systems only
D. False

E. None of the choices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Security should not be an all or nothing issue. The designers and operators of systems should assume that security breaches are inevitable in the long term. Full audit trails should be kept of system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined.

QUESTION 666
The 'trusted systems' approach has been predominant in the design of:

A. many earlier Microsoft OS products
B. the IBM AS/400 series
C. the SUN Solaris series
D. most OS products in the market
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The 'trusted systems' approach has been predominant in the design of many Microsoft OS products, due to the long-standing Microsoft policy of emphasizing functionality and 'ease of use'.

QUESTION 667
Which of the following terms generally refers to small programs designed to take advantage of a software flaw that has been discovered?

A. exploit
B. patch
C. quick fix
D. service pack
E. malware

F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"The term ""exploit"" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in a certain programs processing of a specific file type, such as a non-executable media file."

QUESTION 668
Codes from exploit programs are frequently reused in:

A. trojan horses only.
B. computer viruses only.
C. OS patchers.
D. eavedroppers.
E. trojan horses and computer viruses.
F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"The term ""exploit"" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in a certain programs processing of a specific file type, such as a non-executable media file."

QUESTION 669
Machines that operate as a closed system can NEVER be eavesdropped.

A. True B.
False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware such as TEMPEST.

QUESTION 670
TEMPEST is a hardware for which of the following purposes?

A. Eavedropping
B. Social engineering
C. Virus scanning
D. Firewalling
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware such as TEMPEST.

QUESTION 671
Human error is being HEAVILY relied upon on by which of the following types of attack?

A. Eavedropping
B. DoS
C. DDoS
D. ATP
E. Social Engineering
F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:

QUESTION 672
A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them. zombie computers are being HEAVILY relied upon on by which of the following types of attack?

A. Eavedropping
B. DoS
C. DDoS
D. ATP
E. Social EngineeringF. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:

Explanation: "Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (""zombie computers"") are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion."

QUESTION 673
Attack amplifier is often being HEAVILY relied upon on by which of the following types of attack?

A. Packet dropping
B. ToS
C. DDoS
D. ATP
E. Wiretapping
F. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts are used to flood a target system with network requests. One technique to exhaust victim resources is through the use of an attack amplifier - where the attacker takes advantage of poorly designed protocols on 3rd party machines in order to instruct these hosts to launch the flood.

QUESTION 674
Back Orifice is an example of:

A. a virus.
B. a legitimate remote control software.
C. a backdoor that takes the form of an installed program.
D. an eavesdropper.
E. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:

"A backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing ""legitimate"" program, or executable file. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports."

QUESTION 675
Which of the following will replace system binaries and/or hook into the function calls of the operating system to hide the presence of other programs (choose the most precise answer)?

A. rootkits
B. virus
C. trojan
D. tripwire
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"A backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing ""legitimate"" program, or executable file. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports."

QUESTION 676
Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?

A. Direct access attacks
B. Indirect access attacks
C. Port attack
D. Window attack
E. Social attack
F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Direct access attacks make use of common consumer devices that can be used to transfer data surreptitiously. Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media or portable devices.

QUESTION 677
Which of the following types of attack almost always requires physical access to the targets?

A. Direct access attack
B. Wireless attack
C. Port attack
D. Window attack
E. System attack
F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Direct access attacks make use of common consumer devices that can be used to transfer data surreptitiously. Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media or portable devices.

QUESTION 678
Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?

A. key pair
B. Oakley
C. certificate
D. 3-DES
E. one-time pad
F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation: It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad --has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

QUESTION 679
Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

A. Blowfish
B. Tripwire
C. certificate
D. DES
E. one-time pad F. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad - has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

QUESTION 680
Why is one-time pad not always preferable for encryption (choose all that apply):

A. it is difficult to use securely.
B. it is highly inconvenient to use.
C. it requires licensing fee.
D. it requires internet connectivity.
E. it is Microsoft only.

F. None of the choices.

Correct Answer: AB
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad - has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

QUESTION 681
You may reduce a cracker's chances of success by (choose all that apply):

A. keeping your systems up to date using a security scanner.
B. hiring competent people responsible for security to scan and update your systems.
C. using multiple firewalls.
D. using multiple firewalls and IDS.
E. None of the choices.

Correct Answer: AB
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Only a small fraction of computer program code is mathematically proven, or even goes through comprehensive information technology audits or inexpensive but extremely valuable computer security audits, so it is quite possible for a determined cracker to read, copy, alter or destroy data in well secured computers, albeit at the cost of great time and resources. You may reduce a cracker's chances by keeping your systems up to date, using a security scanner or/and hiring competent people responsible for security.

QUESTION 682
Which of the following measures can protect systems files and data, respectively?

A. User account access controls and cryptography
B. User account access controls and firewall

C. User account access controls and IPS
D. IDS and cryptography
E. Firewall and cryptography
F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
User account access controls and cryptography can protect systems files and data, respectively. On the other hand, firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering.

QUESTION 683
Which of the following is by far the most common prevention system from a network security perspective?

A. Firewall
B. IDS
C. IPS
D. Hardened OS
E. Tripwire
F. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
User account access controls and cryptography can protect systems files and data, respectively. On the other hand, firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering.

QUESTION 684
Which of the following are designed to detect network attacks in progress and assist in post- attack forensics?

A. Intrusion Detection Systems
B. Audit trails
C. System logs
D. Tripwire
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Intrusion Detection Systems are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

QUESTION 685
"Nowadays, computer security comprises mainly "preventive"" measures."

A. True
B. True only for trusted networks
C. True only for untrusted networks
D. False
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
"Nowadays, computer security comprises mainly ""preventive"" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network and is normally implemented as software running on the machine or as physical integrated hardware."

QUESTION 686
The majority of software vulnerabilities result from a few known kinds of coding defects, such as (choose all that apply):

A. buffer overflows

B. format string vulnerabilities
C. integer overflow
D. code injection
E. command injectionF. None of the choices.

Correct Answer: ABCDE
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The majority of software vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. Some common languages such as C and C++ are vulnerable to all of these defects. Languages such as Java are immune to some of these defects but are still prone to code/ command injection and other software defects which lead to software vulnerabilities.

QUESTION 687
ALL computer programming languages are vulnerable to command injection attack.

A. True
B. False

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
The majority of software vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. Some common languages such as C and C++ are vulnerable to all of these defects. Languages such as Java are immune to some of these defects but are still prone to code/ command injection and other software defects which lead to software vulnerabilities.

QUESTION 688
Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer?

A. buffer overflow
B. format string vulnerabilities
C. integer misappropriation

D. code injection
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

QUESTION 689
Buffer overflow aims primarily at corrupting:

A. system processor
B. network firewall
C. system memory
D. disk storage
E. None of the choices.

Correct Answer: C
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

QUESTION 690
Which of the following measures can effectively minimize the possibility of buffer overflows?

A. Sufficient bounds checking
B. Sufficient memory
C. Sufficient processing capability
D. Sufficient code injection
E. None of the choices

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Buffer overflows may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits. Sufficient bounds checking by either the programmer or the compiler can prevent buffer overflows.

QUESTION 691
Which of the following types of attack makes use of unfiltered user input as the format string parameter in the print () function of the C language?

A. buffer overflows
B. format string vulnerabilities
C. integer overflow
D. code injection
E. command injectionF. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation
Explanation/Reference:
Explanation:
Format string attacks are a new class of vulnerabilities recently discovered. It can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as print (). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token.

QUESTION 692
Which of the following terms is used more generally for describing concealment routines in a malicious program?

A. virus
B. worm
C. trojan horse
D. spyware
E. rootkits

F. backdoor
G. None of the choices.

Correct Answer: E
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
Rootkits can prevent a malicious process from being reported in the process table, or keep its files from being read. Originally, a rootkit was a set of tools installed by a human attacker on a Unix system where the attacker had gained administrator access. Today, the term is used more generally for concealment routines in a malicious program.

QUESTION 693
Which of the following refers to a method of bypassing normal system authentication procedures?

A. virus
B. worm
C. trojan horse
D. spyware
E. rootkits
F. backdoor
G. None of the choices.

Correct Answer: F
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A backdoor is a method of bypassing normal authentication procedures.
Many computer manufacturers used to preinstall backdoors on their systems to provide technical support for customers. Hackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors, hackers prefer to use either Trojan horse or computer worm.

QUESTION 694
To install backdoors, hackers generally prefer to use:

A. either Trojan horse or computer worm.
B. either Tripwire or computer virus.
C. either eavedropper or computer worm.
D. either Trojan horse or eavedropper.
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
A backdoor is a method of bypassing normal authentication procedures.
Many computer manufacturers used to preinstall backdoors on their systems to provide technical support for customers. Hackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors, hackers prefer to use either Trojan horse or computer worm.

QUESTION 695
In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as:

A. wormnets
B. trojannets
C. spynets
D. botnets
E. rootnets F. backdoor

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In order to coordinate the activity of many infected computers, attackers are used coordinating systems known as botnets. In a botnet, the malware or mailbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously.

QUESTION 696
In a botnet, mailbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?

A. Chat system
B. SMS system
C. Email system
D. Log system
E. Kernel systemF. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as botnets. In a botnet, the malware or mailbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously.

QUESTION 697
Which of the following software tools is often used for stealing money from infected PC owner through taking control of the modem?

A. System patcher
B. Porn dialer
C. War dialer
D. T1 dialer
E. T3 dialer
F. None of the choices.

Correct Answer: B
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
One way of stealing money from infected PC owner is to take control of the modem and dial an expensive toll call. Dialer such as porn dialer software dials up a premium-rate telephone number and leave the line open, charging the toll to the infected user.

QUESTION 698
Which of the following is an oft-cited cause of vulnerability of networks?

A. software monoculture
B. software diversification
C. single line of defense
D. multiple DMZ
E. None of the choices.

Correct Answer: A
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An oft-cited cause of vulnerability of networks is homogeneity or software monoculture. In particular, Microsoft Windows has such a large share of the market that concentrating on it will enable a cracker to subvert a large number of systems. Introducing inhomogeneity purely for the sake of robustness would however bring high costs in terms of training and maintenance.

QUESTION 699
Introducing inhomogeneity to your network for the sake of robustness would have which of the following drawbacks?

A. poorer performance.
B. poor scalability.
C. weak infrastructure.
D. high costs in terms of training and maintenance.
E. None of the choices.

Correct Answer: D
Section: Protection of Information Assets
Explanation

Explanation/Reference:
Explanation:
An oft-cited cause of vulnerability of networks is homogeneity or software monoculture. In particular, Microsoft Windows has such a large share of the market that concentrating on it will enable a cracker to subvert a large number of systems. Introducing inhomogeneity purely for the sake of robustness would however bring high costs in terms of training and maintenance.