PRACTICE CISA EXAM

Chapter 1 – 6

1. 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

The correct answer is:
B. Generalized audit software

Explanation:
Generalized audit software features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recomputations. The IS auditor, using generalized audit software, could design appropriate tests to recompute the payroll and, thereby, determine 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.

Area: 1

2. Reviewing management's long-term strategic plans helps the IS auditor:

A. gain an understanding of an organization's goals and objectives.
B. test the enterprise's internal controls.
C. assess the organization's reliance on information systems.
D. determine the number of audit resources needed.

The correct answer is:
A. gain an understanding of an organization's goals and objectives.

Explanation:
Strategic planning sets corporate or departmental objectives into motion. Strategic planning is time- and project-oriented, but must also address and help determine priorities to meet business needs. Reviewing long-term strategic plans would not achieve the objectives expressed by the other choices.

Area: 1

3. 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.

The correct answer is:
D. identify and evaluate existing practices.

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. An IS auditor should not prepare documentation, and if they did, their independence could be jeopardized. 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.

Area: 1

4. The traditional role of an IS auditor in a control self-assessment (CSA) should be that of:

A. facilitator.
B. manager.
C. partner.
D. stakeholder.

The correct answer is:
A. facilitator.

Explanation:
When CSA programs are established, IS auditors become internal control professionals and assessment facilitators. IS auditors are the facilitators and the client (management and staff) is

the participant in the CSA process. During a CSA workshop, instead of the IS auditor performing detailed audit procedures, they should lead and guide the clients in assessing their environment. Choices B, C and D should not be roles of the IS auditor. These roles are more appropriate for the client.

Area: 1

5. When communicating audit results, IS auditors should remember that ultimately they are responsible to:

A. senior management and/or the audit committee.
B. the manager of the audited entity.
C. the IS audit director.
D. legal authorities.

The correct answer is:
A. senior management and/or the audit committee.

Explanation:
The IS auditor is ultimately responsible to senior management and the audit committee of the board of directors. Even though the IS auditor should discuss the findings with the management staff of the audited entity (choice B), this is done only to gain agreement on the findings and to develop a course of corrective action. Choice C is incorrect because the IS audit director should review the report that the IS auditor prepared, but is not the person who will make the decisions regarding the findings and their potential consequences. Choice D is incorrect because the responsibility for reporting to legal authorities would rest with the board of directors and their legal counselors.

Area: 1

6. 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.

The correct answer is:
D. the threats/vulnerabilities affecting the assets.

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.

Area: 1

7. 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.

The correct answer is:
A. areas of high risk.

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.

Area: 1

8. Which of the following is the GREATEST challenge in using test data?

A. Ensuring the program version tested is the same as the production program
B. Creating test data that covers all possible valid and invalid conditions
C. Minimizing the impact of additional transactions on the application being tested
D. Processing the test data under an auditor's supervision

The correct answer is:
B. Creating test data that covers all possible valid and invalid conditions

Explanation:
The effectiveness of test data is determined by the comprehensiveness of the coverage of all the key controls to be tested. If the test data does not cover all valid and invalid conditions, there is a

risk that relevant control weakness may remain undetected. Changes in the program, for the period covered under audit, may have been done to remove bugs or for additional functionalities. However, as the test data approach involves testing of data for the audit period, changes in the program tested may have minimal impact. Applications with current technology are usually not impacted by additional transactions. Test data is developed by the auditor; however, it is not necessary that processing be under an auditor's supervision, since the input data will be verified by the outputs.

Area: 1

9. 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.

The correct answer is:
A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.

Explanation:
Choice A takes into consideration both 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.

Area: 1

10. 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

The correct answer is:
C. Using a statistical sample to inventory the tape library

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.

Area: 1

11. Which of the following should be the FIRST step of an IS audit?

A. Create a flowchart of the decision branches.
B. Gain an understanding of the environment under review.
C. Perform a risk assessment.
D. Develop the audit plan.

The correct answer is:
B. Gain an understanding of the environment under review.

Explanation:
An auditor needs to gain an understanding of the processes prior to creating a flowchart. Based on the scope of the audit, the IS auditor should gain an understanding of the environment under review, and then carry out a risk assessment. Finally, on the basis of understanding the environment under review and the risk assessment, the IS auditor should prepare an audit plan.

Area: 1

12. The use of statistical sampling procedures helps minimize:

A. sampling risk.
B. detection risk.
C. inherent risk.
D. control risk.

The correct answer is:
B. detection risk.

Explanation:
Detection risk is the risk that the IS auditor uses an inadequate test procedure and concludes that material errors do not exist, when in fact they do. Using statistical sampling, an IS auditor can quantify how closely the sample should represent the population and quantify the probability of error. Sampling risk is the risk that incorrect assumptions will be made about the characteristics

of a population from which a sample is selected. Assuming there are no related compensating controls, inherent risk is the risk that an error exists, which could be material or significant when combined with other errors found during the audit. Statistical sampling will not minimize this. Control risk is the risk that a material error exists, which will not be prevented or detected on a timely basis by the system of internal controls. This cannot be minimized using statistical sampling.

Area: 1

13. 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.

The correct answer is:
D. resources are allocated to the areas of highest concern.

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 risk-based 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.

Area: 1

14. 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.

The correct answer is:
A. include the finding in the final report because the IS auditor is responsible for an accurate report of all findings.

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.

Area: 1

15. The PRIMARY objective of an IS audit function is to:

A. determine whether everyone uses IS resources according to their job description.
B. determine whether information systems safeguard assets, and maintain data integrity.
C. examine books of accounts and relative documentary evidence for the computerized system.
D. determine the ability of the organization to detect fraud.

The correct answer is:
B. determine whether information systems safeguard assets, and maintain data integrity.

Explanation:
The primary reason for conducting IS audits is to determine whether a system safeguards assets and maintains data integrity. Examining books of accounts is one of the processes involved in IS audit, but it is not the primary purpose. Detecting frauds could be a result of an IS audit but is not the purpose for which an IS audit is performed.

Area: 1

16. In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, an 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.

The correct answer is:
D. identify and evaluate the existing controls.

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.

Area: 1

17. 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

The correct answer is:
A. Lack of reporting of a successful attack on the network

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.

Area: 1

18. Which of the following is an IS control objective?

A. Output reports are locked in a safe place.
B. Duplicate transactions do not occur.
C. System backup/recovery procedures are updated periodically.
D. System design and development meet users' requirements.

The correct answer is:
B. Duplicate transactions do not occur.

Explanation:
Preventing duplicate transactions is a control objective. Having output reports locked in a safe place is an internal accounting control system, backup/recovery procedures are an operational control, and system design and development meeting user requirement is an administrative control.

Area: 1

19. A key element in a risk analysis is/are:

A. audit planning.
B. controls.
C. vulnerabilities.
D. liabilities.

The correct answer is:
C. vulnerabilities.

Explanation:
Vulnerabilities are a key element in the conduct of a risk analysis. Audit planning consists of short- and longterm processes that may detect threats to the information assets. Controls mitigate risks associated with specific threats. Liabilities are part of business and are not inherently a risk.

Area: 1

20. 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 the delegation of authority for 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.

The correct answer is:
D. outline the overall authority, scope and responsibilities of the audit function.

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.

Area: 1

21. During a review of the controls over the process of defining IT service levels, an IS auditor would MOST likely interview the:

A. systems programmer.
B. legal staff.

C. business unit manager.
D. application programmer.

The correct answer is:
C. business unit manager.

Explanation:
Understanding the business requirements is key in defining the service levels. While each of the other entities listed may provide some definition, the best choice here is the business unit manager because of the knowledge this person has of the requirements of the organization.

Area: 1

22. In a risk-based audit approach, an IS auditor, in addition to risk, would be influenced by:

A. the availability of CAATs.
B. management's representation.
C. organizational structure and job responsibilities.
D. the existence of internal and operational controls

The correct answer is:
D. the existence of internal and operational controls

Explanation:
The existence of internal and operational controls will have a bearing on the IS auditor's approach to the audit. In a risk-based approach, the IS auditor is not just relying on risk, but also on internal and operational controls as well as knowledge of the company and the business. This type of risk assessment decision can help relate the cost-benefit analysis of the control to the known risk, allowing practical choices. The nature of available testing techniques and management's representations, have little impact on the risk-based audit approach. Although organizational structure and job responsibilities need to be considered, they are not directly considered unless they impact internal and operational controls.

Area: 1

23. 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.

The correct answer is:
C. appropriate levels of protection are applied to information assets.

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.

Area: 1

24. 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

The correct answer is:
A. Attribute sampling

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 or not. The other choices are used in substantive testing which involves testing of details or quantity.

Area: 1

25. The PRIMARY purpose of an audit charter is to:

A. document the audit process used by the enterprise.
B. formally document the audit department's plan of action.

C. document a code of professional conduct for the auditor.
D. describe the authority and responsibilities of the audit department.

The correct answer is:
D. describe the authority and responsibilities of the audit department.

Explanation:
The audit charter typically sets out the role and responsibility of the internal audit department. It should state management's objectives for and delegation of authority to the audit department. It is rarely changed and does not contain the audit plan or audit process, which is usually part of annual audit planning, nor does it describe a code of professional conduct, since such conduct is set by the profession and not by management.

Area: 1

26. Which of the following normally would 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 analysis developed by the IS auditor from reports supplied by line management

The correct answer is:
A. A confirmation letter received from a third party verifying an account balance

Explanation:
Evidence obtained from independent third parties almost always is considered to be the most reliable. Answers B, C and D would not be considered as reliable.

Area: 1

27. 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.

The correct answer is:
A. Multiple cycles of backup files remain available.

Explanation:
Backup files containing documents, which 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.

Area: 1

28. Which of the following BEST describes an integrated test facility?

A. A technique that enables the IS auditor to test a computer application for the purpose of verifying correct processing
B. The utilization of hardware and/or software to review and test the functioning of a computer system
C. A method of using special programming options to permit the printout of the path through a computer program taken to process a specific transaction
D. A procedure for tagging and extending transactions and master records that are used by an IS auditor for tests

The correct answer is:
A. A technique that enables the IS auditor to test a computer application for the purpose of verifying correct processing

Explanation:
Answer A best describes an integrated test facility, which is a specialized computer-assisted audit process that allows an IS auditor to test an application on a continuous basis. Answer B is an example of a systems control audit review file; answers C and D are examples of snapshots.

Area: 1

29. The IS department of an organization wants to ensure that the computer files, used in the information processing facility, are adequately backed up to allow for proper recovery. This is a/an:

A. control procedure.
B. control objective.
C. corrective control.
D. operational control.

The correct answer is:
B. control objective.

Explanation:
IS control objectives specify the minimum set of controls to ensure efficiency and effectiveness in the operations and functions within an organization. Control procedures are developed to provide reasonable assurance that specific objectives will be achieved. A corrective control is a category of controls, which aims to minimizing the threat and/or remedy problems that were not prevented or were not initially detected. Operational controls address the day-to-day operational functions and activities, and aid in ensuring that the operations are meeting the desired business objectives.

Area: 1

30. 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.

The correct answer is:
D. purpose and scope of the audit being done.

Explanation:
The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An audit with a narrow purpose and scope would result most likely in less data collection, than an audit with a wider purpose and scope. The scope of an IS audit should not be constrained by the ease of obtaining the information or by the auditor's familiarity with the area being audited. Collecting all the required evidence is a required element of an IS audit, and the scope of the audit should not be limited by the auditee's ability to find relevant evidence.

Area: 1

31. An IS auditor is assigned to perform a post-implementation review of an application system. Which of 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.

The correct answer is:
A. implemented a specific control during the development of the application system.

Explanation:
Independence may be impaired if the 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 the IS auditor's independence. Choice D is incorrect because the IS auditor's independence is not impaired by providing advice on known best practices.

Area: 1

32. When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware:

A. of the point at which controls are exercised as data flow through the system.
B. that only preventive and detective controls are relevant.
C. that corrective controls can only be regarded as compensating.
D. that classification allows an IS auditor to determine which controls are missing.

The correct answer is:
A. of the point at which controls are exercised as data flow through the system.

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.

Area: 1

33. 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.

The correct answer is:
C. can improve system security when used in time-sharing environments that process a large number of transactions.

Explanation:
The use of continuous auditing techniques can actually 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.

Area: 1

34. An IS auditor discovers evidence of fraud perpetrated with a manager's user ID. The manager had written the password, allocated by the system administrator, inside his/her desk drawer. The IS auditor should conclude that the:

A. manager's assistant perpetrated the fraud.
B. perpetrator cannot be established beyond doubt.
C. fraud must have been perpetrated by the manager.
D. system administrator perpetrated the fraud.

The correct answer is:
B. perpetrator cannot be established beyond doubt.

Explanation:
The password control weaknesses means that any of the other three options could be true. Password security would normally identify the perpetrator. In this case, it does not establish guilt beyond doubt.

Area: 1

35. Detection risk refers to:

A. concluding that material errors do not exist, when in fact they do.
B. controls that fail to detect an error.
C. controls that detect high-risk errors.
D. detecting an error but failing to report it.

The correct answer is:
A. concluding that material errors do not exist, when in fact they do.

Explanation:
Detection risk refers to the risk that an IS auditor may use an inadequate test procedure and conclude that no material error exists when in fact errors do exist.

Area: 1

36. 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

The correct answer is:
C. Observation and interviews

Explanation:
By observing the IS staff performing their tasks, the 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, and 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.

Area: 1

37. 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.

The correct answer is:
C. generalized audit software to search for address field duplications.

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. 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.

Area: 1

38. During an implementation review of a multiuser distributed application, the 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.

The correct answer is:
C. record the observations and the risk arising from the collective weaknesses.

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 the IS auditor to recognize the combined affect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

Area: 1

39. 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

The correct answer is:
D. Production library listings

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 time intensive. 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.

Area: 1

40. 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

The correct answer is:
B. A compliance test of program library controls

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.

Area: 1

41. 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.

The correct answer is:
C. compares processing output with independently calculated data.

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.

Area: 1

42. 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.

The correct answer is:
B. establish accountability and responsibility for processed transactions.

Explanation:
Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space. Choice D is also a valid reason; however, it is not the primary reason.

Area: 1

43. To identify the value of inventory that has been kept for more than eight weeks, an IS auditor would MOST likely use:

A. test data.
B. statistical sampling.
C. an integrated test facility.
D. generalized audit software.

The correct answer is:
D. generalized audit software.

Explanation:
Generalized audit software will facilitate reviewing the entire inventory file to look for those items that meet the selection criteria. Generalized audit software provides direct access to data and provides for features of computation, stratification, etc. Test data are used to verify programs, but will not confirm anything about the transactions in question. The use of statistical sampling methods is not intended to select specific conditions, but is intended to select samples from a file on a random basis. In this case, the IS auditor would want to check all of the items that meet the criteria and not just a sample of them. An integrated test facility allows the IS auditor to test transactions through the production system.

Area: 1

44. Dataflow 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.

The correct answer is:
C. graphically summarize data paths and storage.

Explanation:
Dataflow 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.

Area: 1

45. Which of the following is an objective of a control self-assessment (CSA) program?

A. Concentration on areas of high risk
B. Replacement of audit responsibilities
C. Completion of control questionnaires
D. Collaborative facilitative workshops

The correct answer is:
A. Concentration on areas of high risk

Explanation:
The objectives of CSA programs include education for line management in control responsibility and monitoring and concentration by all on areas of high risk. The objectives of CSA programs include the enhancement of audit responsibilities, not replacement of audit responsibilities. Choices C and D are tools of CSA, not objectives.

Area: 1

46. 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 auditee of the unauthorized software, and follow up to confirm deletion.
C. Report the use of the unauthorized software to auditee management and the need to prevent recurrence.
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

The correct answer is:
C. Report the use of the unauthorized software to auditee management and the need to prevent recurrence.

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. The 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.

Area: 1

47. The risk that an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when, in fact, they do, is an example of:

A. inherent risk.
B. control risk.
C. detection risk.
D. audit risk.

The correct answer is:
C. detection risk.

Explanation:
This is an example of detection risk.

Area: 1

48. A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

A. can identify high-risk areas that might need a detailed review later.
B. allows IS auditors to independently assess risk.
C. can be used as a replacement for traditional audits.
D. allows management to relinquish responsibility for control.

The correct answer is:
A. can identify high-risk areas that might need a detailed review later.

Explanation:
CSA is predicated on the review of high-risk areas that either need immediate attention, or a more thorough review at a later date. Answer B is incorrect because CSA requires the involvement of both auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Answer C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Answer D is incorrect because CSA does not allow management to relinquish its responsibility for control.

Area: 1

49. When implementing continuous monitoring systems, an IS auditor's first step is to identify:

A. reasonable target thresholds.
B. high-risk areas within the organization.
C. the location and format of output files.
D. applications that provide the highest potential payback.

The correct answer is:
B. high-risk areas within the organization.

Explanation:
The first and most critical step in the process is to identify high-risk areas within the organization. Business department managers and senior executives are in the best positions to offer insight into these areas. Once potential areas of implementation have been identified, an assessment of potential impact should be completed to identify applications that provide the highest potential payback to the organization. At this point, tests and reasonable target thresholds should be determined prior to programming. During systems development, the location and format of the output files generated by the monitoring programs should be defined.

Area: 1

50. In a risk-based audit approach, an IS auditor should FIRST complete a/an:

A. inherent risk assessment.
B. control risk assessment.
C. test of control assessment.
D. substantive test assessment.

The correct answer is:
A. inherent risk assessment.

Explanation:
The first step in a risk-based audit approach is to gather information about the business and industry to evaluate the inherent risks. After completing the assessment of the inherent risks, the next step is to complete an assessment of the internal control structure. The controls are then tested, and on the basis of the test results, substantive tests are carried out and assessed.

Area: 1

51. With regard to sampling, it can be said that:

A. sampling is generally applicable when the population relates to an intangible or undocumented control.
B. if an auditor knows internal controls are strong, the confidence coefficient may be lowered.
C. attribute sampling would help prevent excessive sampling of an attribute by stopping an audit test at the earliest possible moment.
D. variable sampling is a technique to estimate the rate of occurrence of a given control or set of related controls.

The correct answer is:
B. if an auditor knows internal controls are strong, the confidence coefficient may be lowered.

Explanation:
Statistical sampling quantifies how closely the sample should represent the population, usually as a percentage. If the auditor knows internal controls are strong, the confidence coefficient may be lowered. Sampling is generally applicable when the population relates to a tangible or documented control. Choice C is a description of stop-or-go sampling. Choice D is a definition of attribute sampling.

Area: 1

52. 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

The correct answer is:
D. A confirmation letter received from an outside source

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.

Area: 1

53. 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.

The correct answer is:
A. reasonable assurance that the audit will cover material items.

Explanation:
The IS auditing guideline 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.

Area: 1

54. Which of the following processes describes risk assessment? Risk assessment is:

A. subjective.
B. objective.
C. mathematical.
D. statistical.

The correct answer is:
A. subjective.

Explanation:
The IS auditing guideline on the use of a risk assessment in audit planning states, “All risk assessment methodologies rely on subjective judgments at some point in the process (e.g., for assigning weightings to the various parameters). The IS auditor should identify the subjective decisions required in order to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.”

Area: 1

55. The responsibility, authority and accountability of the IS audit function is appropriately documented in an audit charter and MUST be:

A. approved by the highest level of management.
B. approved by audit department management.
C. approved by user department management.
D. changed every year before commencement of IS audits.

The correct answer is:
A. approved by the highest level of management.

Explanation:
The standard on responsibility, authority and accountability states, “The responsibility, authority

and accountability of the information systems audit function are to be appropriately documented in an audit charter or engagement letter." Choice B and C are incorrect because the audit charter should be approved by the highest level of management, not merely by the information systems audit department or the user department. The resulting planning methodologies should be reviewed and approved by senior management and by the audit committee. Choice D is incorrect because the audit charter, once established, is not routinely revised and should be changed only if change can be, and is, thoroughly justified.

Area: 1

56. 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 is MOST suitable for performing that task?

A. CASE tools
B. Embedded data collection tools
C. Heuristic scanning tools
D. Trend/variance detection tools

The correct answer is:
D. Trend/variance detection tools

Explanation:
Trend/variance detection tools look for anomalies in user or system behavior, for example, determining for prenumbered documents whether the numbers 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.

Area: 1

57. An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

A. variable sampling.
B. substantive testing.
C. compliance testing.
D. stop-or-go sampling.

The correct answer is:
C. compliance testing.

Explanation:
Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

Area: 1

58. Which one of the following could an IS auditor use to validate the effectiveness of edit and validation routines?

A. Domain integrity test
B. Relational integrity test
C. Referential integrity test
D. Parity checks

The correct answer is:
A. Domain integrity test

Explanation:
Domain integrity testing is aimed at verifying that the data conform to definitions, i.e., the data items are all in the correct domains. The major objective of this exercise is to verify that the edit and validation routines are working satisfactorily. Relational integrity tests are performed at the record level and usually involve calculating and verifying various calculated fields, such as control totals. Referential integrity checks involve ensuring that all references to a primary key from another file actually exist in their original file. A parity check is a bit added to each character prior to transmission. The parity bit is a function of the bits making up the character. The recipient performs the same function on the received character and compares the result to the transmitted parity bit. If it is different, an error is assumed.

Area: 1

59. The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

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

The correct answer is:
B. Detection

Explanation:
A detection risk is directly affected by the auditor's selection of audit procedures and techniques. Inherent risks usually are not affected by the IS auditor. A control risk is controlled by the actions of the management of the company. Financial risks are not affected by the IS auditor.

Area: 1

60. An IS auditor has evaluated the controls for the integrity of the data in a financial application. Which of the following findings would be the MOST significant?

A. The application owner was unaware of several changes applied to the application by the IT department.
B. The application data are backed up only once a week.
C. The application development documentation is incomplete.
D. Information processing facilities are not protected by appropriate fire detection systems.

The correct answer is:
A. The application owner was unaware of several changes applied to the application by the IT department.

Explanation:
This is the most significant finding as it directly affects the integrity of the application's data and is evidence of an inadequate change control process and incorrect access rights to the processing environment. Although backing up the application data only once a week is a finding, it does not affect the integrity of the data in the system. Incomplete application development documentation does not affect integrity of the data. The lack of appropriate fire detection systems does not affect the integrity of the data but may affect the storage of the data.

Area: 1

61. An IS auditor discovers unlicensed or unauthorized software packages in numerous PCs. The auditor should:

A. report the finding to the management of the department being audited, advising of the risks involved.
B. uninstall the unlicensed or unauthorized software packages.
C. do nothing, as this is a common situation in many companies.
D. advise the involved PC users of the risks.

The correct answer is:

A. report the finding to the management of the department being audited, advising of the risks involved.

Explanation:

Since the situation indicates that there has been a failure in control, the auditor should inform management. The IT auditor should never intervene directly in corrective actions (choice B), because this is not his/her job and would compromise his/her impartiality for future audits. Choice C is an incorrect response to the situation, since no matter how common it is, it is improper, works to the detriment of the company (which should have a policy against it) and is illegal. Choice D is useful but insufficient and indicates there has been a failure in control.

Area: 1

62. 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.

The correct answer is:

D. Many user ids have identical passwords.

Explanation:

Exploitation of a known user id and password requires minimum 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 many user IDs having identical passwords 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 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.

Area: 1

63. In a critical server, an IS auditor discovers a Trojan horse that was produced by a known virus that exploits a vulnerability of an operating system. Which of the following should an IS auditor do FIRST?

A. Investigate the virus author.
B. Analyze the operating system log.
C. Ensure that the malicious code is removed.
D. Install the patch that eliminates the vulnerability.

The correct answer is:
C. Ensure that the malicious code is removed.

Explanation:
The priority is safeguarding the system; therefore, the IS auditor should suggest corrective controls, i.e., remove the code. The IS auditor is not responsible for investigating the virus. The IS auditor may analyze the virus information and determine if it has affected the operating system, but this is an investigative task that would take place after ensuring that the malicious code has been removed. Installing the patch that eliminates the vulnerability should be done by technical support.

Area: 1

64. Senior management has requested that an IS auditor assist the departmental management in the implementation of necessary controls. The IS auditor should:

A. refuse the assignment since it is not the role of the IS auditor.
B. inform management of his/her inability to conduct future audits.
C. perform the assignment and future audits with due professional care.
D. obtain the approval of user management to perform the implementation and follow-up.

The correct answer is:
B. inform management of his/her inability to conduct future audits.

Explanation:
In this situation the IS auditor should inform management of the impairment of independence in conducting further audits in the auditee area. An IS auditor can perform non-audit assignments where the IS auditor's expertise can be of use to the management; however, by performing the non-audit assignment, the IS auditor cannot conduct the future audits of the auditee as his/her independence may be compromised. However, the independence of the IS auditor will not be impaired when suggesting/recommending controls to the auditee after the audit.

Area: 1

65. 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
D. Ability to search for violations of intellectual property rights

The correct answer is:
A. The preservation of the chain of custody for electronic evidence

Explanation:
The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Time and cost savings, choice B, and efficiency and effectiveness, choice C, are legitimate concerns and differentiate good from poor forensic software packages. The ability to search for intellectual property rights violations, choice D, is an example of a use of forensic software.

Area: 1

66. The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

A. destruction policy.
B. security policy.
C. archive policy.
D. audit policy.

The correct answer is:
C. archive policy.

Explanation:
With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

Area: 2

67. Which of the following is the PRIMARY objective of an IT performance measurement process?

A. Minimize errors.
B. Gather performance data.
C. Establish performance baselines.
D. Optimize performance.

The correct answer is:
D. Optimize performance.

Explanation:
An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of the IT measurement process and would be used to evaluate the performance against previously established performance baselines.

Area: 2

68. 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.

The correct answer is:
B. are more likely to be derived as a result of a risk assessment.

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.

Area: 2

69. To support an organization's goals, the IS department should have:

A. a low-cost philosophy.
B. long- and short-range plans.
C. leading-edge technology.
D. planned to acquire new hardware and software.

The correct answer is:
B. long- and short-range plans.

Explanation:
To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

Area: 2

70. 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.

The correct answer is:
A. whether IT processes support business requirements.

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.

Area: 2

71. 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.

The correct answer is:
D. establish responsibility and accountability for the employee's actions.

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.

Area: 2

72. The MOST likely affect 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. that the technology will not be aligned with the organization's objectives.
D. an absence of control over technology contracts.

The correct answer is:
C. that the technology will not be aligned with the organization's objectives.

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.

Area: 2

73. 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 resumé

The correct answer is:
A. Background screening

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 resumé may not be accurate.

Area: 2

74. 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.

The correct answer is:
C. Unauthorized users may have access to originate, modify or delete data.

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.

Area: 2

75. 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.

The correct answer is:
B. security and control policies support business and IT objectives.

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.

Area: 2

76. 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.

The correct answer is:
A. desired result or purpose of implementing specific control procedures.

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.

Area: 2

77. In reviewing the IS short-range (tactical) plan, the IS auditor should determine whether:

A. there is an integration of IS and business staffs within projects.
B. there is a clear definition of the IS mission and vision.
C. there is a strategic information technology planning methodology in place.
D. the plan correlates business objectives to IS goals and objectives.

The correct answer is:
A. there is an integration of IS and business staffs within projects.

Explanation:
The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

Area: 2

78. Which of the following would be a compensating control to mitigate risks resulting from an inadequate segregation of duties?

A. Sequence check
B. Check digit
C. Source documentation retention
D. Batch control reconciliations

The correct answer is:
D. Batch control reconciliations

Explanation:
Batch control reconciliations are an example of compensating controls. Other examples of compensating controls are transaction logs, reasonableness tests, independent reviews and audit trails, such as console logs, library logs and job accounting date. Sequence checks and check digits are data validation edits, and source documentation retention is an example of a data file control.

Area: 2

79. 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

The correct answer is:
C. Approving and monitoring major projects, the status of IS plans and budgets

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.

Area: 2

80. 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.

The correct answer is:
B. implementing and enforcing good processes.

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.

Area: 2

81. An organization acquiring other businesses continues using its legacy EDI systems and uses three separate value-added network (VAN) providers. No written VAN agreements exist. The IS auditor should recommend that management:

A. obtains independent assurance of the third-party service providers.
B. sets up a process for monitoring the service delivery of the third party.
C. ensures that formal contracts are in place.
D. considers agreements with third-party service providers in the development of continuity plans.

The correct answer is:
C. ensures that formal contracts are in place.

Explanation:
Written agreements would assist management in ensuring compliance with external requirements. While management should obtain independent assurance of compliance, this cannot be achieved until there is a contract in place. One aspect of managing third-party services is to provide monitoring; however, this cannot be achieved until there is a contract. Ensuring that VAN agreements are available for review may assist in the development of continuity plans, if they are deemed critical IT resources. However, this cannot be achieved until a contract is in place.

Area: 2

82. Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?

A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports

The correct answer is:
D. Availability reports

Explanation:
IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

Area: 2

83. The implementation of cost-effective controls in an automated system is ultimately the responsibility of the:

A. system administrator.
B. quality assurance function.
C. business unit management.
D. chief of internal audit.

The correct answer is:
C. business unit management.

Explanation:
It is the business unit management's responsibility to implement cost-effective controls in an automated system. They are the best group in an organization to know which information assets need to be secured in terms of availability, confidentiality and integrity. System administrators take care of services related to the system requirements of the user management group. The quality assurance function addresses the overall quality of the systems. The audit group will assess or examine the compliance level of the controls with written policies, procedures or practices.

Area: 2

84. 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.

The correct answer is:
A. this lack of knowledge may lead to unintentional disclosure of sensitive information

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.

Area: 2

85. 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.

The correct answer is:
C. understanding the responsibilities and authority of individuals.

Explanation:
An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps the 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.

Area: 2

86. 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

The correct answer is:
B. Authorization of access to data

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.

Area: 2

87. 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 back up of the employee's work.
C. notify other employees of the termination.
D. disable the employee's logical access.

The correct answer is:
D. disable the employee's logical access.

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.

Area: 2

88. Which of the following would an IS auditor consider the MOST relevant to short-term planning for the IS department?

A. Allocating resources
B. Keeping current with technology advances
C. Conducting control self-assessment
D. Evaluating hardware needs

The correct answer is:
A. Allocating resources

Explanation:
The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department

Area: 2

89. Which of the following goals would you expect to find in an organization's strategic plan?

A. Test a new accounting package.
B. Perform an evaluation of information technology needs.
C. Implement a new project planning system within the next 12 months.
D. Become the supplier of choice for the product offered.

The correct answer is:
D. Become the supplier of choice for the product offered.

Explanation:
Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time- and project-oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

Area: 2

90. 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.

The correct answer is:
C. adoption of a corporate information security policy statement.

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.

Area: 2

91. Which of the following would normally be found in application run manuals?

A. Details of source documents
B. Error codes and their recovery actions
C. Program flowcharts and file definitions
D. Change records for the application source code

The correct answer is:
B. Error codes and their recovery actions

Explanation:
Application run manuals should include actions to be taken by an operator when an error occurs. Source documents and source code are irrelevant to the operator. Although dataflow diagrams may be useful, detailed program diagrams and file definitions are not.

Area: 2

92. Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider
B. Participating in systems design with the provider
C. Renegotiating the provider's fees
D. Monitoring the outsourcing provider's performance

The correct answer is:
D. Monitoring the outsourcing provider's performance

Explanation:
In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a by-product of monitoring the outsourcing provider's performance, while renegotiating fees is

usually a one-time activity.

Area: 2

93. Which of the following duties would be a concern if performed along with systems administration?

A. Access rule maintenance
B. System audit trail review
C. Data librarian
D. Performance monitoring

The correct answer is:
B. System audit trail review

Explanation:
A system administrator performs various functions by using the admin/root or an equivalent login. This login enables the system administrator to have unlimited access to the system resources. The only control over the system administrator's activities is the system audit trail; hence, it should be reviewed by someone other than the system administrator. Maintenance of access rules, data librarian functions and performance monitoring can be assigned to the system administrator.

Area: 2

94. The general ledger setup function in an enterprise resource package (ERP) allows for setting accounting periods. Access to this function has been permitted to users in finance, the warehouse and order entry. The MOST likely reason for such broad access is the:

A. need to change accounting periods on a regular basis.
B. requirement to post entries for a closed accounting period.
C. lack of policies and procedures for the proper segregation of duties.
D. need to create/modify the chart of accounts and its allocations.

The correct answer is:
C. lack of policies and procedures for the proper segregation of duties.

Explanation:
Setting of accounting periods is one of the critical activities of the finance function. Granting access to this function to warehouse and order entry personnel could be a result of a lack of proper policies and procedures for the adequate segregation of duties. Accounting periods should not be changed at regular intervals, but established permanently. The requirement to post entries

for a closed accounting period is a risk. If necessary, this should be done by someone in the finance or accounting area. The need to create/modify the chart of accounts and its allocations is the responsibility of the finance department and is not a function that should be performed by warehouse or order entry personnel.

Area: 2

95. Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

A. The use of diskless workstations
B. Periodic checking of hard drives
C. The use of current antivirus software
D. Policies that result in instant dismissal if violated

The correct answer is:
B. Periodic checking of hard drives

Explanation:
The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software unless the software contains a virus. Diskless workstations act as a preventative control and are not effective since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

Area: 2

96. When an information security policy has been designed, it is MOST important that the information security policy be:

A. stored offsite.
B. written by IS management.
C. circulated to users.
D. updated frequently.

The correct answer is:
C. circulated to users.

Explanation:
To be effective, an information security policy should reach all members of the staff. Storing the security policy offsite or in a safe place may be desirable but of little value if its contents are not

known to the organization’s employees. The information security policy should be written by business unit managers including IS, but not exclusively IS managers. Updating the information security policy is important but will not assure its dissemination.

Area: 2

97. 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.

The correct answer is:
C. data and systems owners.

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.

Area: 2

98. An IS auditor performing a review of the IS department discovers that formal project approval procedures do not exist. In the absence of these procedures, the IS manager has been arbitrarily approving projects that can be completed in a short duration and referring other, more complicated projects to higher levels of management for approval. The IS auditor should recommend as a FIRST course of action that:

A. users participate in the review and approval process.
B. formal approval procedures be adopted and documented.
C. projects be referred to appropriate levels of management for approval.
D. the IS manager’s job description be changed to include approval authority.

The correct answer is:
B. formal approval procedures be adopted and documented.

Explanation:
It is imperative that formal, written approval procedures be established to set accountability. This

is true of the IS manager and higher levels of management. Choices A, C and D would be subsequent recommendations once authority has been established.

Area: 2

99. Responsibility and reporting lines cannot always be established when auditing automated systems since:

A. diversified control makes ownership irrelevant.
B. staff traditionally changes jobs with greater frequency.
C. ownership is difficult to establish where resources are shared.
D. duties change frequently in the rapid development of technology.

The correct answer is:
C. ownership is difficult to establish where resources are shared.

Explanation:
Because of the diversified nature of both data and application systems, the actual owner of data and applications may be hard to establish.

Area: 2

100. Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line management.
B. does not vary from the IS department's preliminary budget.
C. complies with procurement procedures.
D. supports the business objectives of the organization.

The correct answer is:
D. supports the business objectives of the organization.

Explanation:
Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Answer A is incorrect since line management prepared the plans.

Area: 2

101. 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.

The correct answer is:
B. defining data elements, data names and their relationship.

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)

Area: 2

102. 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.

The correct answer is:
D. board of directors.

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.

Area: 2

103. 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

The correct answer is:
A. Response

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.

Area: 2

104. Which of the following would provide a mechanism whereby IS management can determine if the activities of the organization have deviated from the planned or expected levels?

A. Quality management
B. IS assessment methods
C. Management principles
D. Industry standards/benchmarking

The correct answer is:
B. IS assessment methods

Explanation:
Assessment methods provide a mechanism, whereby IS management can determine if the activities of the organization have deviated from planned or expected levels. These methods include IS budgets, capacity and growth planning, industry standards/benchmarking, financial management practices, and goal accomplishment. Quality management is the means by which the IS department processes are controlled, measured and improved. Management principles focus on areas such as people, change, processes and security. Industry standards/benchmarking provide a means of determining the level of performance provided by similar information processing facility environments.

Area: 2

105. Which of the following situations would increase the likelihood of fraud?

A. Application programmers are implementing changes to production programs.
B. Application programmers are implementing changes to test programs.
C. Operations support staff are implementing changes to batch schedules.
D. Database administrators are implementing changes to data structures.

The correct answer is:
A. Application programmers are implementing changes to production programs.

Explanation:
Production programs are used for processing an enterprise's data. It is imperative that controls on changes to production programs be stringent. Lack of control in this area could result in application programs being modified to manipulate the data. Application programmers are required to implement changes to test programs. These are used only in development and do not directly impact the live processing of data. The implementation of changes to batch schedules by operations support staff will affect the scheduling of the batches only; it does not impact the live data. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.

Area: 2

106. An IS auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late-night shift a month as the senior computer operator. The MOST appropriate course of action for the IS auditor is to:

A. advise senior management of the risk involved.
B. agree to work with the security officer on these shifts as a form of preventative control.
C. develop a computer-assisted audit technique to detect instances of abuses of this arrangement.
D. review the system log for each of the late-night shifts to determine whether any irregular actions occurred.

The correct answer is:
A. advise senior management of the risk involved.

Explanation:
The IS auditor's first and foremost responsibility is to advise senior management of the risk involved in having the security administrator perform an operations function. This is a violation of separation of duties. The IS auditor should not get involved in processing.

Area: 2

107. Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a 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.

The correct answer is:
B. reduce the opportunity for an employee to commit an improper or illegal act.

Explanation:
Required vacations/holidays of a week or more duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions. This reduces the opportunity to commit improper or illegal acts, and 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.

Area: 2

108. The quality assurance group is typically responsible for:

A. ensuring that the output received from system processing is complete.
B. monitoring the execution of computer processing tasks.
C. ensuring that programs and program changes and documentation adhere to established standards.
D. designing procedures to protect data against accidental disclosure, modification or destruction.

The correct answer is:
C. ensuring that programs and program changes and documentation adhere to established standards.

Explanation:
The quality assurance group is typically responsible for ensuring that programs, program changes and documentation adhere to established standards. Choice A is the responsibility of the data control group, choice B is the responsibility of computer operations, and choice D is the responsibility of data security.

Area: 2

109. 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

The correct answer is:
C. Degaussing the tapes

Explanation:
The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

Area: 2

110. 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.

The correct answer is:
C. have formal terms of reference and maintain minutes of its meetings.

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 on a timely basis. Choice A is incorrect because only senior management, or high staff levels should be members of 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.

Area: 2

111. 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.

The correct answer is:
C. creating the logical and physical database.

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.

Area: 2

112. Involvement of senior management is MOST important in the development of:

A. strategic plans.
B. IS policies.
C. IS procedures.
D. standards and guidelines.

The correct answer is:
A. strategic plans.

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.

Area: 2

113. Which of the following data entry controls provides the GREATEST assurance that the data are entered correctly?

A. Using key verification
B. Segregating the data entry function from data entry verification
C. Maintaining a log/record that details the time, date, employee's initials/user ID and progress of various data preparation and verification tasks
D. Adding check digits

The correct answer is:
A. Using key verification

Explanation:
Key verification or one-to-one verification will yield the highest degree of confidence that data entered are error-free. However, this could be impractical for large amounts of data. The segregation of the data entry function from data entry verification is an additional data entry control but does not address accuracy. Maintaining a log/record that details the time, date, employee's initials/user ID and progress of various data preparation and verification tasks provides an audit trail. A check digit is added to data to ensure that original data have not been altered. If a check digit is wrongly keyed, this would lead to accepting incorrect data but would only apply to those data elements with a check digit.

Area: 2

114. A local area network (LAN) administrator normally would be restricted from:

A. having end-user responsibilities.
B. reporting to the end-user manager.
C. having programming responsibilities.
D. being responsible for LAN security administration.

The correct answer is:
C. having programming responsibilities.

Explanation:
A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.

Area: 2

115. An IS auditor is reviewing the database administration (DBA) function to ascertain whether adequate provision has been made for controlling data. The IS auditor should determine that the:

A. function reports to data processing operations.
B. responsibilities of the function are well defined.
C. database administrator is a competent systems programmer.
D. audit software has the capability of efficiently accessing the database.

The correct answer is:
B. responsibilities of the function are well defined.

Explanation:
The IS auditor should determine that the responsibilities of the DBA function are not only well defined but also assure that the DBA reports directly to the IS manager or executive to provide independence, authority and responsibility. The DBA should not report to either data processing operations or systems development management. The DBA need not be a competent systems programmer. Choice D is not as important as choice A.

Area: 2

116. A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

A. the length of service since this will help ensure technical competence.
B. age as training in audit techniques may be impractical.
C. IS knowledge since this will bring enhanced credibility to the audit function.
D. ability, as an IS auditor, to be independent of existing IS relationships.

The correct answer is:
D. ability, as an IS auditor, to be independent of existing IS relationships.

Explanation:
Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. The fact that the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any candidate should be evaluated against those requirements. In addition, the length of service will not ensure technical competency, and evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

Area: 2

117. Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

A. Yes, because the IS auditor will evaluate the adequacy of the service bureau's plan and assist his/her company in implementing a complementary plan.
B. Yes, because based on the plan, the IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract.

C. No, because the backup to be provided should be specified adequately in the contract.
D. No, because the service bureau's business continuity plan is proprietary information.

The correct answer is:
A. Yes, because the IS auditor will evaluate the adequacy of the service bureau's plan and assist his/her company in implementing a complementary plan.

Explanation:
The primary responsibility of the IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

Area: 2

118. A probable advantage to an organization that has outsourced its data processing services is that:

A. needed IS expertise can be obtained from the outside.
B. greater control can be exercised over processing.
C. processing priorities can be established and enforced internally.
D. greater user involvement is required to communicate user needs.

The correct answer is:
A. needed IS expertise can be obtained from the outside.

Explanation:
Outsourcing is a contractual arrangement whereby the organization relinquishes control over part or all of the information processing to an external party. This is frequently done to acquire additional resources or expertise that is not obtainable from inside the organization.

Area: 2

119. An IS auditor should be concerned when a telecommunication analyst:

A. monitors systems performance and tracks problems resulting from program changes.
B. reviews network load requirements in terms of current and future transaction volumes.
C. assesses the impact of the network load on terminal response times and network data transfer rates.
D. recommends network balancing procedures and improvements.

The correct answer is:
A. monitors systems performance and tracks problems resulting from program changes.

Explanation:
The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes (choice B), assessing the impact of network load or terminal response times and network data transfer rates (choice C) and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes (choice A) would put the analyst in a self-monitoring role.

Area: 2

120. Which of the following is a control over database administration activities?

A. A database checkpoint to restart processing after a system failure
B. Database compression to reduce unused space
C. Supervisory review of access logs
D. Backup and recovery procedures to ensure database availability

The correct answer is:
C. Supervisory review of access logs

Explanation:
To ensure management approval of database administration activities and to exercise control over the use of database tools, there should be a supervisory review of access logs. Database administration activities include among others, database checkpoints, database compression techniques, and data backup and recovery procedures established and implemented to ensure database availability.

Area: 2

121. An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

A. hardware configuration.
B. access control software.
C. ownership of intellectual property.
D. application development methodology.

The correct answer is:
C. ownership of intellectual property.

Explanation:
Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be of no real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

Area: 2

122. Without compensating controls, which of the following functions would represent a risk if combined with that of a systems analyst?

A. Application programming
B. Data entry
C. Quality assurance
D. Database administrator

The correct answer is:
C. Quality assurance

Explanation:
A systems analyst should not perform quality assurance (QA) duties as independence would be impaired, since the systems analyst is part of the team developing/designing the software. A systems analyst can perform the other functions. The best example is a citizen programmer. A citizen programmer (name related to citizen, since they have the right to do anything and everything) who has access to development tools can perform all activities while developing software (including design, development, testing, implementation). Only good compensatory controls would be able to monitor/control these activities. Compensating controls will ensure these functions have been effectively performed. If an analyst compromises on functions in these roles, it can be immediately detected with the help of compensating controls. However, a system analyst should be discouraged from performing the role of QA, because quality assurance levels could be compromised if the agreed standards are not met.

Area: 2

123. An IS auditor reviewing an organization’s IT strategic plan should FIRST review:

A. the existing IT environment.
B. the business plan.
C. the present IT budget.
D. current technology trends.

The correct answer is:
B. the business plan.

Explanation:
The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, the IS auditor would first need to familiarize him/herself with the business plan.

Area: 2

124. In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries
B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

The correct answer is:
C. Procedures that verify that only approved program changes are implemented

Explanation:
While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited, as suggested in choice B, this practice is not always possible in small organizations. The IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

Area: 2

125. 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

The correct answer is:
B. The basis for access authorization

Explanation:
The security policy provides the broad framework of security, as laid down and approved by the 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.

Area: 2

126. 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.

The correct answer is:
B. retention.

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.

Area: 2

127. An organization has outsourced its software development. Which of the following is the responsibility of the organization's IT management?

A. Paying for provider services
B. Participating in systems design with the provider
C. Managing compliance with the contract for the outsourced services
D. Negotiating contractual agreement with the provider

The correct answer is:
C. Managing compliance with the contract for the outsourced services

Explanation:
Actively managing compliance with the contract terms for the outsourced services is the responsibility of IT management. Payment of invoices is a finance responsibility. Negotiation of the contractual agreement would have already taken place and is usually a shared responsibility of the legal department and other departments, such as IT.

Area: 2

128. In an organization where an IT security baseline has been defined, the IS auditor should FIRST ensure:

A. implementation.
B. compliance.
C. documentation.
D. sufficiency.

The correct answer is:
D. sufficiency.

Explanation:
The auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

Area: 2

129. IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
B. The service provider does not have incident handling procedures.
C. Recently a corrupted database could not be recovered because of library management problems.
D. Incident logs are not being reviewed.

The correct answer is:
A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.

Explanation:
The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

Area: 2

130. An organization has outsourced IT operations to a service provider. The organization's IS auditor makes the following observations:

- **Key servers located at the outsourcing organization are about to be moved to the service provider.**
- **Critical systems are backed up, but recovery is inefficient.**
- **Disaster recovery is not covered by the outsourcing contract.**
- **The service provider backs up data to the building next to it.**

Which of the following should the IS auditor recommend be done immediately?
A. Improve the backup of critical systems.
B. Delay moving the servers.
C. Incorporate disaster recovery in the contract.
D. Back up data to a location further away from the service provider.

The correct answer is:
B. Delay moving the servers.

Explanation:
Moving the servers may cause a business interruption and should be postponed until disaster recovery is included in the outsourcing contract. Choices A, C and D should be addressed during the development of viable disaster recovery provisions and after the server move is postponed.

Area: 2

131. Which of the following is MOST important when assessing services provided by an Internet service provider (ISP)?

A. Performance reports generated by the ISP
B. The service level agreement (SLA)
C. Interviews with the provider
D. Interviews with other clients of the ISP

The correct answer is:
B. The service level agreement (SLA)

Explanation:
A service level agreement provides the basis for an adequate assessment of the degree to which the provider is meeting the level of agreed service. Choices A, C and D would not be the basis for an independent evaluation of the service.

Area: 2

132. Implementation of access control FIRST requires:

A. a classification of IS resources.
B. the labeling of IS resources.
C. the creation of an access control list.
D. an inventory of IS resources.

The correct answer is:
D. an inventory of IS resources.

Explanation:
The first step in implementing access control is an inventory of IS resources, which is the basis for classification. Labeling of resources cannot be done without first determining the resources' classifications. The access control list (ACL) would not be done without a meaningful classification of resources.

Area: 2

133. An IS auditor performing a general controls review of IS management practices relating to personnel should pay particular attention to:

A. mandatory vacation policies and compliance.
B. staff classifications and fair compensation policies.
C. staff training.
D. the functions assigned to staff.

The correct answer is:
D. the functions assigned to staff.

Explanation:

When performing a general controls review it is important for an IS auditor to pay attention to the issue of segregation of duties, which is affected by vacation/holiday practices. Mandatory vacation policies and compliance may vary depending on the country and industry. Staff classifications and fair compensation policies may be a morale issue, not a controls issue. Staff training is desirable, but not as critical as an appropriate segregation of duties.

Area: 2

134. An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

A. References from other customers
B. Service level agreement (SLA) template
C. Maintenance agreement
D. Conversion plan

The correct answer is:
A. References from other customers

Explanation:
The IS auditor should look for an independent verification that the ISP can perform the tasks being contracted. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows-issues which would be of concern to the IS auditor. Checking references is a means of obtaining an independent verification that the vendor can perform the services it says it can. A maintenance agreement relates more to equipment than to services, and a conversion plan, while important, is less important than verification that the ISP can provide the services they propose.

Area: 2

135. When reviewing IS strategies, the IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

A. has all the personnel and equipment it needs.
B. plans are consistent with management strategy.
C. uses its equipment and personnel efficiently and effectively.
D. has sufficient excess capacity to respond to changing directions.

The correct answer is:
B. plans are consistent with management strategy.

Explanation:
Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

Area: 2

136. To ensure an organization is complying with privacy requirements, the IS auditor should FIRST review:

A. the IT infrastructure.
B. the organization's policies, standards and procedures.
C. legal and regulatory requirements.
D. the adherence to the organizational policies, standards and procedures.

The correct answer is:
C. legal and regulatory requirements.

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, the 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.

Area: 2

137. 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.

The correct answer is:
D. Access to a network port is not restricted.

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.

Area: 3

138. 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 Socket Layers (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned, if a hacker:

A. compromised the Wireless Application Protocol (WAP) gateway.
B. installed a sniffing program in front of the server.
C. stole a customer's PDA.
D. listened to the wireless transmission.

The correct answer is:
A. compromised the Wireless Application Protocol (WAP) gateway.

Explanation:
In a WAP gateway, the encrypted messages from customers must be decrypted to transmit to 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.

Area: 3

139. To maximize the performance of a large database in a parallel processing environment, which of the following is used for separating indexes?

A. Disk partitioning
B. Mirroring
C. Hashing
D. Duplexing

The correct answer is:
C. Hashing

Explanation:
An essential part of designing a database for parallel processing is the partitioning scheme. Because large databases are indexed, independent indexes must also be partitioned to maximize performance. Hashing is a method used for index partitioning. It associates data to disks based

on a hash key. Disk partitioning creates logical drives on the single disk for better management of the contents. Disk mirroring uses two identical disks. All operations on the two disks are performed so that each disk is a mirror image of the other. This provides redundancy in case of failure of one of the disks. Disk duplexing makes use of more than one disk with two separate controllers providing redundancy in case of a disk failure or a controller card failure.

Area: 3

140. Which of the following will prevent dangling tuples in a database?

A. Cyclic integrity
B. Domain integrity
C. Relational integrity
D. Referential integrity

The correct answer is:
D. Referential integrity

Explanation:
Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., for existence of all foreign keys in the original tables. If this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized source documentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

Area: 3

141. 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

The correct answer is:
B. Switches

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.

Area: 3

142. The objective of concurrency control in a database system is to:

A. restrict updating of the database to authorized users.
B. prevent integrity problems, when two processes attempt to update the same data at the same time.
C. prevent inadvertent or unauthorized disclosure of data in the database.
D. ensure the accuracy, completeness and consistency of data.

The correct answer is:
B. prevent integrity problems, when two processes attempt to update the same data at the same time.

Explanation:
Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users and controls, such as passwords, prevent the inadvertent or unauthorized disclosure of data from the database. Quality controls, such as edits, ensure the accuracy, completeness and consistency of data maintained in the database.

Area: 3

143. In a database management system (DBMS), the location of data and the method of accessing the data are provided by the:

A. data dictionary.
B. metadata.
C. directory system.
D. data definition language.

The correct answer is:
C. directory system.

Explanation:
A directory system describes the location of data and the access method. A data dictionary contains an index and description of all the items stored in the database. Metadata are the data elements required to define an enterprisewide data warehouse. The data definition language processor allows the database administrator (DBA) to create/modify a data definition for mapping between external and conceptual schemes.

Area: 3

144. 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

The correct answer is:
C. Network monitoring devices

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 environmentwide, logical facilities that can differentiate among users, before providing access to systems.

Area: 3

145. A benefit of quality of service (QoS) is that the:

A. entire networks availability and performance will be significantly improved.
B. telecom carrier will provide the company with accurate service level compliance reports.
C. participating applications will have guaranteed service levels.
D. communications link will be supported by security controls to perform secure online transactions.

The correct answer is:
C. participating applications will have guaranteed service levels.

Explanation:
The main function of QoS is to optimize network performance by assigning priority to business applications and end users through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved, while the speed of data exchange for specific applications could be faster. Availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

Area: 3

146. 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.

The correct answer is:
A. they are set to meet security and performance requirements.

Explanation:
The primary concern is to find the balance between security and performance. Recording changes in an audit trail and periodically reviewing it 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.

Area: 3

147. 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.

The correct answer is:
A. make unauthorized changes to the database directly, without an audit trail.

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.

Area: 3

148. By establishing a network session through an appropriate application, a sender transmits a message by breaking it into packets, but the packets may reach the receiver out of sequence. Which OSI layer addresses the out-of-sequence message through segment sequencing?

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

The correct answer is:
D. Transport layer

Explanation:
The function of resequencing packets (segment) received out of order is taken care of by the transport layer. Neither the network, session or application layers address resequencing.

Area: 3

149. Checking for authorized software baselines is an activity addressed within which of the following?

A. Project management
B. Configuration management
C. Problem management
D. Risk management

The correct answer is:
B. Configuration management

Explanation:
Configuration management accounts for all IT components, including software. Project management is about scheduling, resource management and progress tracking of software development. Problem management records and monitors incidents. Risk management involves risk identification, impact analysis, an action plan, etc.

Area: 3

150. To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

A. System access log files
B. Enabled access control software parameters
C. Logs of access control violations
D. System configuration files for control options used

The correct answer is:
D. System configuration files for control options used

Explanation:
Review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

Area: 3

151. 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

The correct answer is:
A. Availability of online network documentation

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 among which the following are included: supporting terminal access to remote hosts, handling file transfer between hosts and interuser communications.

Area: 3

152. 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

The correct answer is:
C. Providing network redundancy

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/echo checks to detect line errors, parity checks, error correction codes and sequence checks. Choices A, B and D are communication network controls

Area: 3

153. 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

The correct answer is:
D. Attenuation

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.

Area: 3

154. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called:

A. alternative routing.
B. diverse routing.
C. redundancy.
D. circular routing.

The correct answer is:
B. diverse routing.

Explanation:
Diverse routing is the method of routing traffic through split-cable facilities or duplicate-cable facilities, which can be accomplished with different/duplicate cable sheaths. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics. Redundancy involves providing extra capacity, with an option to use such excess capacity in the event the primary transmission capability is not available. Circular routing is the logical path of a message in a communication network based on a series of gates at the physical network layer in the open system interconnection.

Area: 3

155. A Ping command is used to measure:

A. attenuation.
B. throughput.
C. delay distortion.
D. latency.

The correct answer is:
D. latency.

Explanation:
Latency, which is measured using a Ping command, represents the delay that a message/packet will have in traveling from source to destination. A decrease in amplitude as a signal propagates

through a transmission medium is called attenuation. Throughput, which is the quantity of work per unit of time, is measured in bytes per second. Delay distortion represents delay in transmission because the rate of propagation of a signal along a transmission line varies with the frequency.

Area: 3

156. Which of the following would BEST support 24/7 availability?

A. Daily backup
B. Offsite storage
C. Mirroring
D. Periodic testing

The correct answer is:
C. Mirroring

Explanation:
Mirroring of critical elements is a tool that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not, of themselves, support continuous availability.

Area: 3

157. Analysis of which of the following would MOST likely enable the IS auditor to determine if an unapproved program attempted to access sensitive data?

A. Abnormal job termination reports
B. Operator problem reports
C. System logs
D. Operator work schedules

The correct answer is:
C. System logs

Explanation:
System logs are automated reports that identify most of the activities performed on the computer. Many programs that analyze the system log to report on specifically defined items have been developed. Abnormal job termination reports identify application jobs that were terminated before successful completion. Operator problem reports are used by operators to log computer operations problems and their solutions. Operator work schedules are maintained by IS

management to assist in human resource planning.

Area: 3

158. When assessing the portability of a database application, the IS auditor should verify that:

A. a structured query language (SQL) is used.
B. information import and export procedures exist with other systems.
C. indexes are used.
D. all entities have a significant name and identified primary and foreign keys.

The correct answer is:
A. a structured query language (SQL) is used.

Explanation:
The use of an SQL is a key element for database portability. Import and export of information with other systems is an objective of a database interfaces review. The use of an index is an objective of a database access review, and the fact that all entities have a significant name and identified primary and foreign keys is an objective of a database design review.

Area: 3

159. In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

A. isolation.
B. consistency.
C. atomicity.
D. durability.

The correct answer is:
C. atomicity.

Explanation:
The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the database be maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions, and hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that, when a transaction has been reported back to a user as complete, the resultant changes to the database

will survive subsequent hardware or software failures.

Area: 3

160. 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

The correct answer is:
C. False-negative reporting

Explanation:
False-negative reporting on weaknesses means the control weaknesses in the network are not identified and, hence, 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.

Area: 3

161. In a LAN environment, which of the following minimizes the risk of data corruption during transmission?

A. Using end-to-end encryption for data communication
B. Using separate conduits for electrical and data cables
C. Using check sums for checking the corruption of data
D. Connecting the terminals using a star topology

The correct answer is:
B. Using separate conduits for electrical and data cables

Explanation:
Using separate conduits for data cables and electrical cables, minimizes the risk of data corruption due to an induced magnetic field created by electrical current. Data encryption minimizes the risk of data leakage in case of wire tapping; however, it cannot prevent corruption. A check sum will help detect the data corruption during communication, but will not prevent it. Using a star topology will increase the speed of communication, but will not detect the

corruption.

Area: 3

162. Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

A. A system downtime log
B. Vendors' reliability figures
C. Regularly scheduled maintenance log
D. A written preventive maintenance schedule

The correct answer is:
A. A system downtime log

Explanation:
A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

Area: 3

163. Which of the following is the MOST effective means of determining which controls are functioning properly in an operating system?

A. Consulting with the vendor
B. Reviewing the vendor installation guide
C. Consulting with the system programmer
D. Reviewing the system generation parameters

The correct answer is:
D. Reviewing the system generation parameters

Explanation:
System generation parameters determine how a system runs, the physical configuration and its interaction with the workload.

Area: 3

164. Congestion control is BEST handled by which OSI layer?

A. Data link layer
B. Session layer

C. Transport layer
D. Network layer

The correct answer is:
C. Transport layer

Explanation:
The transport layer is responsible for reliable data delivery. This layer implements a flow control mechanism that can detect congestion, reduce data transmission rates and increase transmission rates when the network appears to no longer be congested (e.g., TCP flow controls). The network layer is not correct because congestion control occurs based on router implementations of flow control at the subnet level (i.e., source quench messages sent out when router memory or the buffer reaches capacity); however, no message exists to cancel or discard messages, which actually may increase congestion problems. The session and data link layers do not have any functionality for network management.

Area: 3

165. Utility programs that assemble software modules needed to execute a machine instruction application program version are:

A. text editors.
B. program library managers.
C. linkage editors and loaders.
D. debuggers and development aids.

The correct answer is:
C. linkage editors and loaders.

Explanation:
Utility programs that assemble software modules needed to execute a machine instruction application program version are linkage editors and loaders.

Area: 3

166. Capacity monitoring software is used to ensure:

A. maximum use of available capacity.
B. that future acquisitions meet user needs.
C. concurrent use by a large number of users.
D. continuity of efficient operations.

The correct answer is:
D. continuity of efficient operations.

Explanation:
Capacity monitoring software shows the actual usage of online systems vs. their maximum capacity. The aim is to enable software support staff to ensure that efficient operation, in the form of response times, is maintained in the event that use begins to approach the maximum available capacity. Systems should never be allowed to operate at maximum capacity. Monitoring software is intended to prevent this. Although the software reports may be used to support a business case for future acquisitions, it would not provide information on the effect of user requirements and it would not ensure concurrent usage of the system by users, other than to highlight levels of user access.

Area: 3

167. A referential integrity constraint consists of:

A. ensuring the integrity of transaction processing.
B. ensuring that data are updated through triggers.
C. ensuring controlled user updates to the database.
D. rules for designing tables and queries.

The correct answer is:
B. ensuring that data are updated through triggers.

Explanation:
Referential integrity constraints ensure that a change in a primary key of one table is automatically updated in a matching foreign key of other tables. This is done using triggers.

Area: 3

168. Which of the following exposures associated with the spooling of sensitive reports for offline printing would an IS auditor consider to be the MOST serious?

A. Sensitive data can be read by operators.
B. Data can be amended without authorization.
C. Unauthorized report copies can be printed.
D. Output can be lost in the event of system failure.

The correct answer is:
C. Unauthorized report copies can be printed.

Explanation:
Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure

Area: 3

169. Which of the following is critical to the selection and acquisition of the correct operating system software?

A. Competitive bids
B. User department approval
C. Hardware-configuration analysis
D. Purchasing department approval

The correct answer is:
C. Hardware-configuration analysis

Explanation:
The purchase of operating system software is dependent on the fact that software is compatible with the existing hardware. Choices A and D, although important, are not as important as choice C. Users do not normally approve the acquisition of operating systems software.

Area: 3

170. 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

The correct answer is:
D. Dedicated lines

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.

Area: 3

171. 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

The correct answer is:
A. Screened subnet firewall

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 only 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.

Area: 3

172. A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies
B Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
C Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
D. Reengineering the existing processing and redesigning the existing system

The correct answer is:
C Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format

Explanation:
EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls) EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

Area: 3

173. Which of the following is widely accepted as one of the critical components in networking management?

A. Configuration management
B. Topological mappings
C. Application of monitoring tools
D. Proxy server trouble shooting

The correct answer is:
A. Configuration management

Explanation:
Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function both internally and externally. It also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network and its connectivity. Application monitoring is not essential and proxy server trouble shooting is used for trouble-shooting purposes.

Area: 3

174. Applying a retention date on a file will ensure that:

A. data cannot be read until the date is set.
B. data will not be deleted before that date.
C. backup copies are not retained after that date.
D. datasets having the same name are differentiated.

The correct answer is:
B. data will not be deleted before that date.

Explanation:
A retention date will ensure that a file cannot be overwritten before that date has passed. The

retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and, therefore, may well be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

Area: 3

175. 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.

The correct answer is:
C. attack problems that require consideration of a large number of input variables.

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, and 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.

Area: 3

176. 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

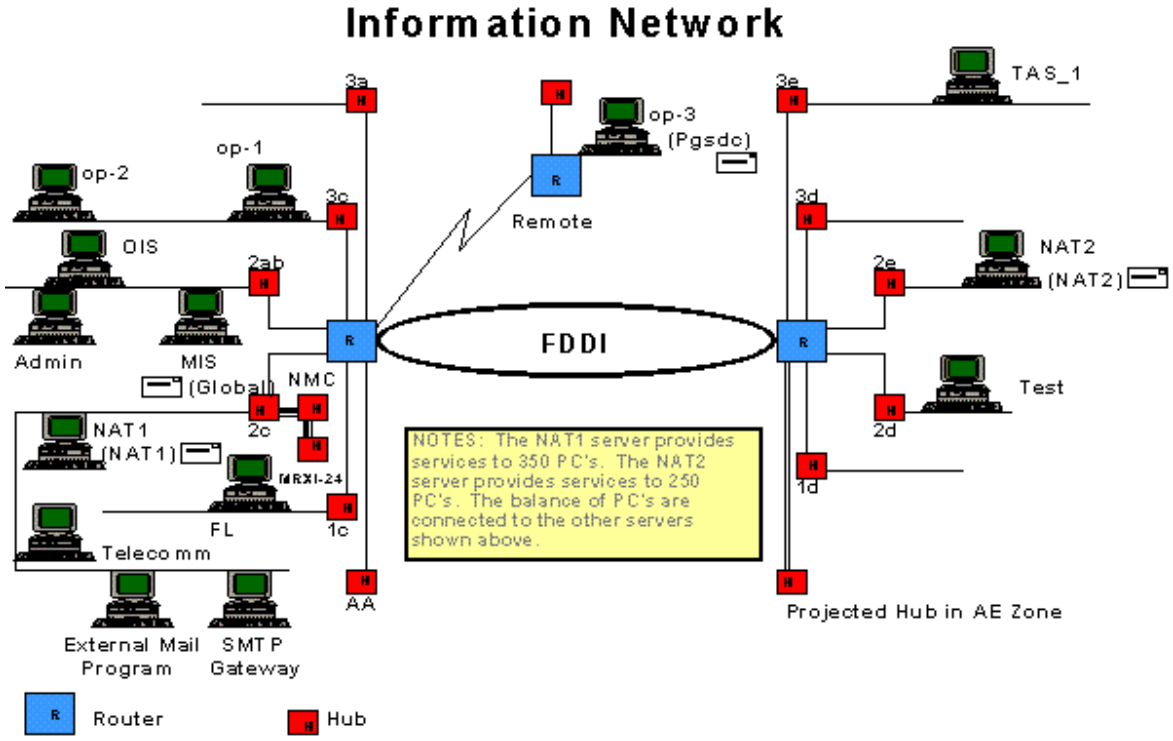
The correct answer is:
A. Gateway

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. A protocol converter is a hardware device that converts between two different types of transmissions, such as asynchronous and synchronous transmissions. A front-end communication processor connects all network

communication lines to a central computer to relieve the central computer from performing network control, format conversion and message handling tasks. A concentrator/multiplexor is a device used for combining several lower-speed channels into a higher-speed channel.

Area: 3

177. The following question refers to the diagram below.



Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?

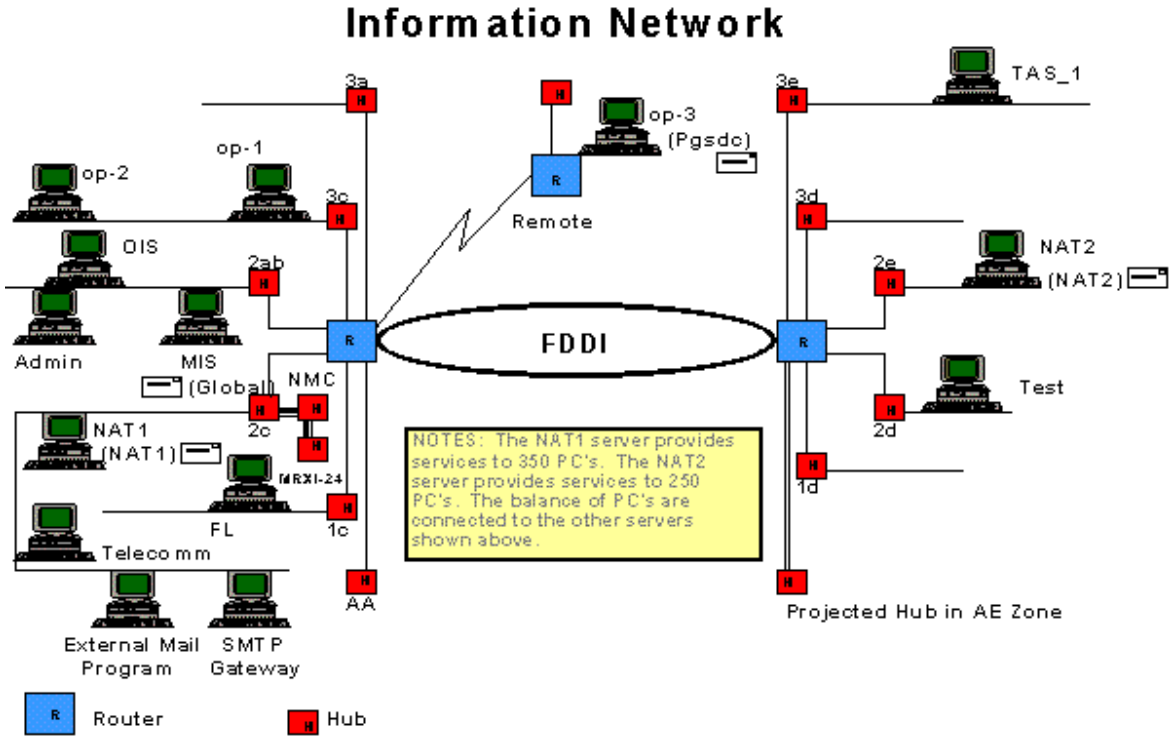
A. No firewalls are needed.
B. Op-3 location only
C. MIS (Global) and NAT2
D. SMTP Gateway and op-3

The correct answer is:
D. SMTP Gateway and op-3

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.

Area: 3

178. The following question refers to the diagram below.



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(s), if any, should be recommended to mitigate this weakness?

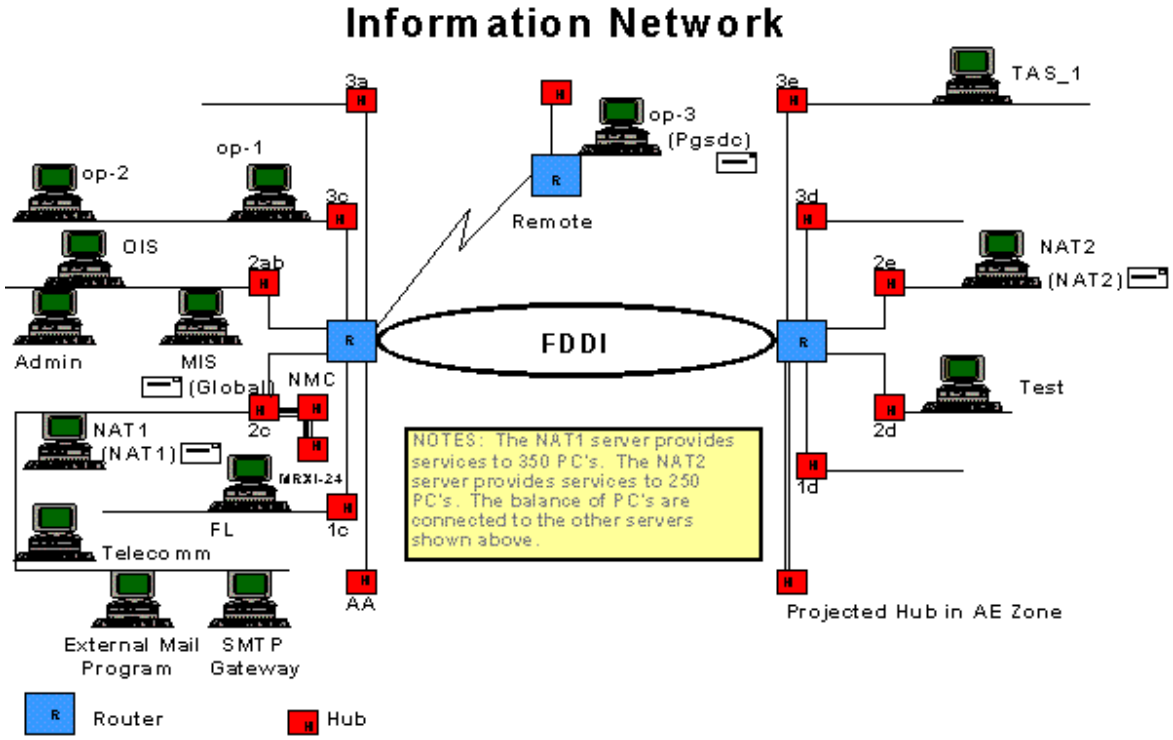
A. Intelligent hub
B. Physical security over the hubs
C. Physical security and an intelligent hub
D. No controls are necessary since this is not a weakness.

The correct answer is:
C. Physical security and an intelligent hub

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 a reasonable protection over hubs with active ports.

Area: 3

179. The following question refers to the diagram below.



In the 2c area on the diagram, there are three hubs connected to each other. What potential risk might this indicate?

A. Virus attack
B. Performance degradation
C. Poor management controls
D. Vulnerability to external hackers

The correct answer is:

B. Performance degradation

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.

Area: 3

180. When a PC that has been used for the storage of confidential data is sold on the open market the:

A. hard disk should be demagnetized.
B. hard disk should be mid-level formatted.
C. data on the hard disk should be deleted.
D. data on the hard disk should be defragmented.

The correct answer is:
A. hard disk should be demagnetized.

Explanation:
The hard disk should be demagnetized, since this will cause all of the bits to be set to zero, eliminating any chance of retrieving information that was previously stored on the disk. A mid-level format does not delete information from the hard disk. It only resets the directory pointers. While the deletion of data from the disk removes the pointer to the file, the data remains in place, so with the proper tools, the information can be retrieved. The defragmentation of the disk does not cause information to be deleted, but simply moves it around to make it more efficient to access.

Area: 3

181. A universal serial bus (USB) port:

A. connects the network without a network card.
B. connects the network with an Ethernet adapter.
C. replaces all existing connections.
D. connects the monitor.

The correct answer is:
B. connects the network with an Ethernet adapter.

Explanation:
The USB port connects the network without having to install a separate network interface card inside a computer by using a USB Ethernet adapter.

Area: 3

182. Which of the following would enable an enterprise to provide access to its intranet (i.e., extranet) to its business partners across the Internet?

A. Virtual private network
B. Client-server
C. Dial-in access
D. Network service provider

The correct answer is:
A. Virtual private network

Explanation:
A virtual private network (VPN) allows external partners to securely participate in the extranet using public networks as a transport or shared private networks. Because of its low cost, using public networks (Internet) as a transport is the principal method. VPNs rely on tunneling/encapsulation techniques, which allow the Internet protocol (IP) to carry a variety of different protocols (e.g., SNA, IPX, NETBEUI). A client-server (choice B) does not address extending the network to business partners (i.e., client-server refers to a group of computers within an organization connected by a communications network where the client is the requesting machine and the server is the supplying machine). Choice C refers to remote users accessing a secured environment. It is the means, not the method, of providing access to a network. A network service provider (choice D) may provide services to a shared private network by providing Internet services, but it does not extend to an organization's intranet.

Area: 3

183. 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. On the basis of changing requirements, firewall policies are updated.
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.

The correct answer is:
D. The firewall is placed on top of the commercial operating system with all installation options.

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, 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).

Area: 3

184. 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.

The correct answer is:
D. two segments of a single LAN.

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. A bridge operates at level 2 of the OSI layer and is used to connect two LANs using different protocols (e.g., joining an ethernet and token network) to form a logical network. A gateway, which is a level 7 device, is used to connect a LAN to a WAN. A LAN is connected with a MAN, which operates in the network layer using a router.

Area: 3

185. Which of the following would help to ensure the portability of an application connected to a database? The:

A. verification of database import and export procedures.
B. usage of a structured query language (SQL).
C. analysis of stored procedures/triggers.
D. synchronization of the entity-relation model with the database physical schema.

The correct answer is:
B. usage of a structured query language (SQL).

Explanation:
The use of SQL facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design entity-relation model will all be helpful but do not contribute to the portability of an application connecting to a database.

Area: 3

186. 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

The correct answer is:
D. Front-end processor

Explanation:
A front-end processor is a hardware device that connects all communication lines to a central computer to relieve the central computer.

Area: 3

187. Which of the following can be used to verify output results and control totals by matching them against the input data and control totals?

A. Batch header forms
B. Batch balancing
C. Data conversion error corrections
D. Access controls over print spools

The correct answer is:
B. Batch balancing

Explanation:
Batch balancing is used to verify output results and control totals by matching them against the input data and control totals. Batch header forms control data preparation; data conversion error corrections correct errors that occur due to duplication of transactions and inaccurate data entry; and access controls over print spools prevent reports from being accidentally deleted from print spools or directed to a different printer.

Area: 3

188. Which of the following would an IS auditor expect to find in a console log?

A. Names of system users
B. Shift supervisor identification

C. System errors
D. Data edit errors

The correct answer is:
C. System errors

Explanation:
System errors are the only ones that you would expect to find in the console log.

Area: 3

189. 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

The correct answer is:
A. A neural network

Explanation:
A neural network will monitor and learn patterns, reporting exceptions for investigation. Database management software is a method of storing and retrieving data. Management information systems provide management statistics but do not normally have a monitoring and detection function. Computer-assisted audit techniques detect specific situations, but are not intended to learn patterns and detect abnormalities.

Area: 3

190. An IS auditor needs to link his/her microcomputer to a mainframe system that uses binary synchronous data communications with block data transmission. However, the IS auditor's microcomputer, as presently configured, is capable of only asynchronous ASCII character data communications. Which of the following must be added to the IS auditor's computer to enable it to communicate with the mainframe system?

A. Buffer capacity and parallel port
B. Network controller and buffer capacity
C. Parallel port and protocol conversion
D. Protocol conversion and buffer capability

The correct answer is:
D. Protocol conversion and buffer capability

Explanation:
For the IS auditor's microcomputer to communicate with the mainframe, the IS auditor must use a protocol converter to convert the asynchronous and synchronous transmission. Additionally, the message must be spooled to the buffer to compensate for different rates of data flow.

Area: 3

191. The interface that allows access to lower- or higher-level network services is called:

A. firmware.
B. middleware.
C. X.25 interface.
D. utilities.

The correct answer is:
B. middleware.

Explanation:
Middleware, a class of software employed by client-server applications, provides services, such as identification, authentication, directories and security. It facilitates client-server connections over the network and allows client applications to access and update remote databases and mainframe files. Firmware consists of memory chips with embedded program code that hold their content when the power is turned off. X.25 interface is the interface between data terminal equipment and data circuit terminating equipment for terminals operating in the packet mode on some public data networks. Utilities are system software used to perform system maintenance and routines that are required during normal processing, such as sorting or backup.

Area: 3

192. Which of the following controls will detect MOST effectively the presence of bursts of errors in network transmissions?

A. Parity check
B. Echo check
C. Block sum check
D. Cyclic redundancy check

The correct answer is:
D. Cyclic redundancy check

Explanation:

The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. If both of them are equal, then the block is assumed error free. In this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. In higher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data back to the sending device for comparison with the original transmission.

Area: 3

193. Which of the following types of firewalls provide the GREATEST degree and granularity of control?

A. Screening router
B. Packet filter
C. Application gateway
D. Circuit gateway

The correct answer is:

C. Application gateway

Explanation:

The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This means that it not only checks the packet IP addresses (layer 3) and the ports it is directed to (in this case port 80, layer 4), it also checks every http command (layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and B) basically work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4 (not from higher levels). A circuit gateway (choice D) is based on a proxy or program that acts as an intermediary between external and internal accesses. This means that, during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external server to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

Area: 3

194. Which of the ISO/OSI model layers provides for routing packets between nodes?

A. Data link
B. Network
C. Transport
D. Session

The correct answer is:
B. Network

Explanation:
The network layer switches and routes information (network layer header). Node-to-node data link services are extended across a network by this layer. The network layer provides service for routing packets (units of information at the network layer) between nodes connected through an arbitrary network. The data link layer transmits information as groups-of-bits (logical units called a frame) to adjacent computer systems (node-to-node). The bits in a frame are divided into an address field (media access control-MAC-48-bit hardware address), control field, data field and error-control field. The transport layer, provides end-to-end data integrity. To ensure reliable delivery, the transport layer builds on the error-control mechanisms provided by lower layers. If lower layers are not adequate, the transport layer is the last chance for error recovery. The session layer provides the control structure for communications between applications. It establishes, manages and terminates connections (sessions) between cooperating applications, and performs access security checking.

Area: 3

195. In a TCP/IP-based network, an IP address specifies a:

A. network connection.
B. router/gateway.
C. computer in the network.
D. device on the network.

The correct answer is:
A. network connection.

Explanation:
An IP address specifies a network connection. An IP address encodes both a network and a host on that network; it does not specify an individual computer, but provides a connection to a network. A router/gateway connects two networks and has two IP addresses. Hence, an IP address cannot specify a router. A computer in the network can be connected to other networks as well. It will then use many IP addresses. Such computers are called multihomed hosts. Here,

again, an IP address cannot refer to the computer. IP addresses do not refer to individual devices on the network, but refer to the connections by which they are connected to the network.

Area: 3

196. 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

The correct answer is:
B. Bridge

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 forwarding device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet. Routers are switching devices that operate at the OSI network layer by examining network addresses (i.e., routing information encoded in an IP packet). The router, by examining the IP address, can make intelligent decisions in directing the packet to its destination. Repeaters amplify transmission signals to reach remote devices by taking a signal from a LAN, reconditioning and retiming it, and sending it to another. This functionality is hardware-encoded and occurs at the OSI physical layer. Gateways provide access paths to foreign networks.

Area: 3

197. 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.

The correct answer is:
B. resolution service for the name/address.

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.

Area: 3

198. In a web server, a common gateway interface (CGI) is MOST often used as a(n):

A. consistent way for transferring data to the application program and back to the user.
B. computer graphics imaging method for movies and TV.
C. graphic user interface for web design.
D. interface to access the private gateway domain.

The correct answer is:
A. consistent way for transferring data to the application program and back to the user.

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 or entering 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.

Area: 3

199. 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.

The correct answer is:
B. routing verification procedures.

Explanation:
The communication's interface stage requires routing verification procedures. EDI or ANSI X12 is a standard that must be interpreted by an application for transactions to be processed and then to be invoiced, paid and sent, whether they are for merchandise or services. There is no point in 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.

Area: 3

200. For an online transaction processing system, transactions per second is a measure of:

A. throughput.
B. response time.
C. turnaround time.
D. uptime.

The correct answer is:
A. throughput.

Explanation:
Throughput measures how much work is done by a system over a period of time; it measures the productivity of the system. In an online transaction processing system, transactions per second is a throughput index. Response time is defined as the length of time that elapsed between submission of an input and receipt of the first character of output in an online system. Turnaround time is the length of time that elapsed between submission of a job and receipt of a completed output. It is a measure of timeliness in a batch system. The percentage of time that the system is available for processing is called uptime or a reliability index; thus, this is not the correct answer.

Area: 3

201. 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.

The correct answer is:
A. Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.

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.

Area: 3

202. Which of the following would be considered an essential feature of a network management system?

A. A graphical interface to map the network topology
B. Capacity to interact with the Internet to solve the problems
C. Connectivity to a help desk for advice on difficult issues
D. An export facility for piping data to spreadsheets

The correct answer is:
A. A graphical interface to map the network topology

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, and the ability to export to a spreadsheet is not an essential element.

Area: 3

203. 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.

The correct answer is:
A. incorrectly configuring the access lists.

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.

Area: 3

204. Which of the following LAN physical layouts is subject to total loss if one device fails?

A. Star
B. Bus
C. Ring
D. Completely connected

The correct answer is:
B. Bus

Explanation:
The bus topology is vulnerable to failure if one device fails. In line and bus networks, which are essentially the same thing, terminals are connected to a single cable. If this cable is severed, all terminals beyond the point of severance will be unavailable.

Area: 3

205. A network diagnostic tool that monitors and records network information is a/an:

A. online monitor.
B. downtime report.
C. help desk report.
D. protocol analyzer.

The correct answer is:
D. protocol analyzer.

Explanation:
Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

Area: 3

206. Which of the following will help detect changes made by an intruder to the system log of a server?

A. Mirroring the system log on another server
B. Simultaneously duplicating the system log on a write-once disk
C. Write protecting the directory containing the system log
D. Storing the backup of the system log offsite

The correct answer is:
B. Simultaneously duplicating the system log on a write-once disk

Explanation:
A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

Area: 3

207. When reviewing the implementation of a LAN, the IS auditor should FIRST review the:

A. node list.
B. acceptance test report.
C. network diagram.
D. user's list.

The correct answer is:
C. network diagram.

Explanation:
To properly review a LAN implementation, the 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.

Area: 3

208. Which of the following is an example of the defense in-depth security principle?

A. Using two firewalls of different vendors to consecutively check the incoming network traffic
B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic
C. Having no physical signs on the outside of a computer center building
D. Using two firewalls in parallel to check different types of incoming traffic

The correct answer is:
B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic

Explanation:
Defense in-depth means using different security mechanisms that back up each other. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

Area: 3

209. Which of the following BEST ensures the integrity of a server's operating system?

A. Protecting the server in a secure location
B. Setting a boot password
C. Hardening the server configuration
D. Implementing activity logging

The correct answer is:
C. Hardening the server configuration

Explanation:
Hardening a system means to configure it in the most secure manner (install latest security patches, properly define the access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenario-it is a detective

control (not a preventive one) and the attacker who already gained privileged access can modify logs or disable them.

Area: 3

210. 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

The correct answer is:
A. Firewalls

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.

Area: 3

211. To evaluate the referential integrity of a database, an IS auditor should review the:

A. composite keys.
B. indexed fields.
C. physical schema.
D. foreign keys.

The correct answer is:
D. foreign keys.

Explanation:
A foreign key is a column in a table that references a primary key of another table, thus providing the referential integrity. Composite keys consist of two or more columns designated

together as a table's primary key. Field indexing speeds up searches, but does not ensure referential integrity. Referential integrity is related to the logical schema, not the physical schema.

Area: 3

212. An IS auditor detected that several PCs connected to the Internet have a low security level that is allowing for the free recording of cookies. This creates a risk because cookies locally store:

A. information about the Internet site.
B. information about the user.
C. information for the Internet connection.
D. Internet pages.

The correct answer is:
B. information about the user.

Explanation:
The cookie file resides on the client machine. It contains data passed from web sites, so that web sites can communicate with this file when the same client returns. The web site only has access to that part of the cookie file that represents the interaction with that particular web site. Cookie files have caused some issues with respect to privacy. The four choices all relate to a cookie, but the fact that the cookie stores information about the user is the risk.

Area: 3

213. Which of the following is the MOST probable cause for a mail server being used to send spam?

A. Installing an open relay server
B. Enabling Post Office Protocol (POP3)
C. Using Simple Mail Transfer Protocol (SMTP)
D. Activating user accounting

The correct answer is:
A. Installing an open relay server

Explanation:
An open proxy (or open relay) allows unauthorized people to route their spam through someone else's mail server. POP3 and SMTP are commonly used mail protocols. Activating user accounting does not relate to using a server to send spam.

Area: 3

214. The MOST significant security concern when using flash memory (e.g., USB removable disk) is that the:

A. contents are highly volatile.
B. data cannot be backed up.
C. data can be copied.
D. device may not be compatible with other peripherals.

The correct answer is:
C. data can be copied.

Explanation:
Unless properly controlled, flash memory provides an avenue anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other periphereal; therefore, compatibility is not an issue.

Area: 3

215. An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

A. Analyze the need for the structural change.
B. Recommend restoration to the originally designed structure.
C. Recommend the implementation of a change control process.
D. Determine if the modifications were properly approved.

The correct answer is:
D. Determine if the modifications were properly approved.

Explanation:
The IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the auditor find that the structural modification had not been approved.

Area: 3

216. The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentiality.
B. increased redundancy.
C. unauthorized accesses.
D. application malfunctions.

The correct answer is:
B. increased redundancy.

Explanation:
Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy (Redundancy which is usually considered positive when it is a question of resource availability is negative in a database environment, since it demands additional, otherwise unnecessary, data handling efforts.) Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

Area: 3

217. Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits a 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.

The correct answer is:
D. Stop the service until an appropriate security fix is installed.

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 every software that utilizes it from working between segments.

Area: 3

218. Which of the following operating system mechanisms checks each request by a subject (user process) to access and use an object (e.g., file, device, program) to ensure that the request complies with a security policy?

A. Address Resolution Protocol
B. Access control analyzer
C. Reference monitor
D. Concurrent monitor

The correct answer is:
C. Reference monitor

Explanation:
A reference monitor is an abstract mechanism that checks each request by a subject (user process) to access and uses an object (e.g., file, device, program) to ensure that the request complies with a security policy. A reference monitor is implemented via a security kernel, which is a hardware/software/firmware mechanism. Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol (IP) address to a physical machine address that is recognized in the local network. An access control analyzer is an audit utility for analyzing how well access controls have been implemented and maintained within an access control package. A concurrent monitor is an audit utility that captures selected events as application systems are running to facilitate assessing program quality.

Area: 3

219. Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

A. protect the organization from viruses and nonbusiness materials.
B. maximize employee performance.
C. safeguard the organization's image.
D. assist the organization in preventing legal issues

The correct answer is:
A. protect the organization from viruses and nonbusiness materials.

Explanation:
The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e-mail. Choice B could be true in some circumstances (i.e., it would need to be implemented along with an awareness program, so that employee performance can be significantly improved); however, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect

benefits.

Area: 3

220. Which of the following is the GREATEST risk related to the monitoring of audit logs?

A. Logs are not backed up periodically.
B. Routine events are recorded.
C. Procedures for enabling logs are not documented.
D. Unauthorized system actions are recorded but not investigated.

The correct answer is:
D. Unauthorized system actions are recorded but not investigated.

Explanation:
If unauthorized system actions are not investigated, the log is useless. Not backing up logs periodically is a risk but not as critical as the need to investigate questionable actions. Recording routine events can make it more difficult to recognize unauthorized actions, but the critical events are still recorded. Procedures for enabling and reviewing logs should be documented, but documentation does not ensure investigation.

Area: 3

221. Who is principally responsible for periodically reviewing users' access to systems?

A. Computer operators
B. Security administrators
C. Data owners
D. IS auditors

The correct answer is:
C. Data owners

Explanation:
The data owners, who are responsible for the use and reporting of information under their control, should provide written authorization for users to gain access to that information. The data owner should periodically review and evaluate authorized (granted) access to ensure these authorizations are still valid.

Area: 4

222. Which of the following intrusion detection systems (IDS) monitors the general patterns of activity and traffic on a network and creates a database?

A. Signature-based
B. Neural networks
C. Statistical-based
D. Host-based

The correct answer is:
B. Neural networks

Explanation:
The neural networks-based IDS monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but has the added function of self-learning. Signature-based systems are a type of IDS in which the intrusive patterns identified are stored in the form of signatures. These IDS systems protect against detected intrusion patterns. Statistical-based systems need a comprehensive definition of the known and expected behavior of systems. Host-based systems are not a type of IDS, but a category of IDS and are configured for a specific environment. They will monitor various internal resources of the operating system to warn of a possible attack.

Area: 4

223. The MOST important difference between hashing and encryption is that hashing:

A. is irreversible.
B. output is the same length as the original message.
C. is concerned with integrity and security.
D. is the same at the sending and receiving end.

The correct answer is:
A. is irreversible.

Explanation:
Hashing works one way. By applying a hashing algorithm to a message, a message hash/digest is created. If the same hashing algorithm is applied to the message digest, it will not result in the original message. As such, hashing is irreversible, while encryption is reversible. This is the basic difference between hashing and encryption. Hashing creates an output that is smaller than the original message, and encryption creates an output of the same length as the original message. Hashing is used to verify the integrity of the message and does not address security. The same hashing algorithm is used at the sending and receiving ends to generate and verify the massage hash/digest. Encryption will not necessarily use the same algorithm at the sending and

receiving end to encrypt and decrypt.

Area: 4

224. Which of the following cryptography options would increase overhead/cost?

A. The encryption is symmetric rather than asymmetric.
B. A long asymmetric encryption key is used.
C. The hash is encrypted rather than the message.
D. A secret key is used.

The correct answer is:
B. A long asymmetric encryption key is used.

Explanation:
Computer processing time is increased for longer asymmetric encryption keys, and the increase may be disproportionate. For example, one benchmark showed that doubling the length of an RSA key from 512 bits to 1,024 bits caused the decrypt time to increase nearly six-fold. An asymmetric algorithm requires more processing time than symmetric algorithms. A hash is shorter than the original message; hence, a smaller overhead is required if the hash is encrypted rather than the message. Use of a secret key, as a symmetric encryption key, is generally small and used for the purpose of encrypting user data.

Area: 4

225. The MOST important key success factor in planning a penetration test is:

A. the documentation of the planned testing procedure.
B. scheduling and deciding on the timed length of the test.
C. the involvement of the management of the client organization.
D. the qualifications and experience of staff involved in the test.

The correct answer is:
C. the involvement of the management of the client organization.

Explanation:
The most important part of planning any penetration test is the involvement of the management of the client organization. Penetration testing without management approval could reasonably be considered espionage and is illegal in many jurisdictions.

Area: 4

226. To determine who has been given permission to use a particular system resource, the IS auditor should review?

A. Activity lists
B. Access control lists
C. Logon ID lists
D. Password lists

The correct answer is:
B. Access control lists

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.

Area: 4

227. Which of the following virus prevention techniques can be implemented through hardware?

A. Remote booting
B. Heuristic scanners
C. Behavior blockers
D. Immunizers

The correct answer is:
A. Remote booting

Explanation:
Remote booting (e.g., diskless workstations) is a method of preventing viruses, and can be implemented through hardware. Choice C is a detection, not a prevention, although it is hardware-based. Choices B and D are not hardware-based.

Area: 4

228. Which of the following append themselves to files as a protection against viruses?

A. Behavior blockers
B. Cyclical redundancy checkers (CRCs)

C. Immunizers
D. Active monitors

The correct answer is:
C. Immunizers

Explanation:
Immunizers defend against viruses by appending sections of themselves to files. They continuously check the file for changes and report changes as possible viral behavior. Behavior blockers focus on detecting potentially abnormal behavior, such as writing to the boot sector or the master boot record, or making changes to executable files. Cyclical redundancy checkers compute a binary number on a known virus-free program that is then stored in a database file. When that program is subsequently called to be executed, the checkers look for changes to the files, compare it to the database and report possible infection if changes have occurred. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions.

Area: 4

229. Vendors have released patches fixing security flaws in their software. Which of the following should the IS auditor recommend in this situation?

A. Assess the impact of patches prior to installation.
B. Ask the vendors for a new software version with all fixes included.
C. Install the security patch immediately.
D. Decline to deal with these vendors in the future.

The correct answer is:
A. Assess the impact of patches prior to installation.

Explanation:
The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. To install the patch without knowing what it might affect could easily cause problems. New software versions with all fixes included are not always available and a full installation could be time-consuming. Declining to deal with vendors does not take care of the flaw.

Area: 4

230. Which of the following acts as a decoy to detect active Internet attacks?

A. Honeypots
B. Firewalls
C. Trapdoors
D. Traffic analysis

The correct answer is:
A. Honeypots

Explanation:
Honeypots are computer systems that are expressly set up to attract and trap individuals who attempt to penetrate other individuals' computer systems. The concept of a honeypot is to learn from intruder's actions. A properly designed and configured honeypot provides data on methods used to attack systems. The data are then used to improve measures that could curb future attacks. A firewall is basically a preventive measure. Trapdoors create a vulnerability that provides an opportunity for the insertion of unauthorized code into a system. Traffic analysis is a type of passive attack.

Area: 4

231. 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.

The correct answer is:
B. User accounts are created with expiration dates and are based on services provided.

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 IDs after the work is completed is necessary, but if not automated, the deletion could be overlooked.

Area: 4

232. During a logical access controls review, the 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.

The correct answer is:
D. user accountability may not be established.

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.

Area: 4

233. A certifying authority (CA) can delegate the processes of:

A. revocation and suspension of a subscriber's certificate.
B. generation and distribution of the CA public key.
C. establishing a link between the requesting entity and its public key.
D. issuing and distributing subscriber certificates.

The correct answer is:
C. establishing a link between the requesting entity and its public key.

Explanation:
Establishing a link between the requesting entity and its public key is a function of a registration authority. This may or may not be performed by a CA; therefore, this function can be delegated. Revocation and suspension and issuance and distribution of the subscriber certificate are functions of the subscriber certificate life cycle management, which the CA must perform. Generation and distribution of the CA public key is a part of the CA key life cycle management process and, as such, cannot be delegated.

Area: 4

234. Which of the following results in a denial-of-service attack?

A. Brute-force attack
B. Ping of death
C. Leapfrog attack
D. Negative acknowledgement (NAK) attack

The correct answer is:
B. Ping of death

Explanation:
The use of Ping with a packet size higher than 65 KB and no fragmentation flag on will cause a denial of service. A brute-force attack is typically a text attack that exhausts all possible key combinations. A leapfrog attack, the act of telneting through one or more hosts to preclude a trace, makes use of user id and password information obtained illicitly from one host to compromise another host. A negative acknowledgement attack is a penetration technique that capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly, leaving the system in an unprotected state during such interrupts.

Area: 4

235. When reviewing a firewall, which of the following should be of MOST concern to an IS auditor?

A. A well-defined security policy
B Implementation of a firewall with the latest and most secure algorithm
C. The effectiveness of the firewall in enforcing the security policy
D. The security of the platform in which the firewall resides

The correct answer is:
C. The effectiveness of the firewall in enforcing the security policy

Explanation:
The existence of a good security policy is important, but if the firewall has not been implemented so as to effectively enforce the policy, then the policy is of little value. Although the other choices are concerns, they are not as great a concern as the effectiveness of the firewall in enforcing the security policy.

Area: 4

236. Which of the following is an advantage of elliptic curve encryption over RSA encryption?

A. Computation speed
B. Ability to support digital signatures
C. Simpler key distribution
D. Greater strength for a given key length

The correct answer is:
A. Computation speed

Explanation:
The main advantage of elliptic curve encryption over RSA encryption is its computation speed. This method was developed by Diffie and Martin E. Hellman, who were the first to conceive of the concept of public key encryption. Both encyption methods support digital signatures, are used for public key encryption and distribution, and are of similar strength.

Area: 4

237. 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)

The correct answer is:
A. False-acceptance rate (FAR)

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.

Area: 4

238. 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

The correct answer is:
A. Statistical-based

Explanation:
A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal network activity may include, at times, 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 an IDS. Either of the three IDSs above may be host- or network-based.

Area: 4

239. 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

The correct answer is:
B. Screened-subnet firewall

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 utilizies a packet filtering router and a bastion host. This approach implements basic network layer security (packet filting) 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.

Area: 4

240. Which of the following would be the BEST overall control for an Internet business, looking for confidentiality, reliability and integrity of data?

A. Secure Sockets Layer (SSL)
B. Intrusion detection system (IDS)
C. Public key infrastructure (PKI)
D. Virtual private network (VPN)

The correct answer is:
C. Public key infrastructure (PKI)

Explanation:
PKI would be the best overall technology because cryptography provides for encryption, digital signatures and nonrepudiation controls for confidentiality and reliability. SSL can provide confidentiality. IDS is a detective control. A VPN would provide confidentiality and authentication (reliability).

Area: 4

241. The risk of gaining unauthorized access through social engineering can BEST be addressed by:

A. security awareness programs.
B. asymmetric encryption.
C. intrusion detection systems.
D. a demilitarized zone.

The correct answer is:
A. security awareness programs.

Explanation:
The human factor is the weakest link in the information security chain. Social engineering is the human side of breaking into an enterprise's network. It relies on interpersonal relations and deception. Organizations with technical security countermeasures, such as an authentication process, encryption, intrusion detection systems or firewalls, may still be vulnerable if an employee gives away confidential information. The best means of defense for social engineering is an ongoing security awareness program wherein all employees are educated about the dangers of social engineering.

Area: 4

242. To ensure message integrity, confidentiality and nonrepudiation between two parties, the MOST effective method would be to create a message digest by applying a cryptographic hashing algorithm against:

A. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key by using the receiver's public key.
B. any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key using the receiver's public key.
C. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the symetric key using the receiver's public key.
D. the entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

The correct answer is:
A. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key by using the receiver's public key.

Explanation:
Applying a cryptographic hashing algorithm against the entire message addresses the message integrity issue. Enciphering the message digest using the sender's private key addresses nonrepudiation. Encrypting the message with a symmetric key and, thereafter, the key is enciphered using the receiver's public key addresses the confidentiality of the message as well as the receiver's nonrepudiation most efficiently. The other choices would address only a portion of the requirements.

Area: 4

243. Which of the following antivirus software implementation strategies would be the MOST effective in an interconnected corporate network?

A. Server antivirus software
B. Virus walls
C. Workstation antivirus software
D. Virus signature updating

The correct answer is:
B. Virus walls

Explanation:
An important means of controlling the spread of viruses is to detect the virus at the point of entry, before it has an opportunity to cause damage. In an interconnected corporate network, virus scanning software, used as an integral part of firewall technologies, is referred to as a virus wall. Virus walls scan incoming traffic with the intent of detecting and removing viruses before they enter the protected network. The presence of virus walls does not preclude the necessity for installing virus detection software on servers and workstations within the network, but network-level protection is most effective the earlier the virus is detected. Virus signature updating is a must in all circumstances, be it networked or not.

Area: 4

244. 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.

The correct answer is:
D. a deadman door.

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.

Area: 4

245. An IS auditor observed that some data entry operators leave their computers in the midst of data entry without logging off. Which of the following controls should be suggested to prevent unauthorized access?

A. Encryption
B. Switch off the computer when leaving
C. Password control
D. Screen saver password

The correct answer is:
D. Screen saver password

Explanation:
Since data entry operators have to attend to other assignments in the midst of data entry and the nature of the assignments are such that they do not logoff the computer, a screen saver password is the only effective control to guard against unauthorized access. Encryption does not prevent access to the computer, it only guards against disclosure of the confidential contents of the files. Switching off the computer without properly shutting it down is not advisable. Password control takes place when logging on to an application and is not effective in this scenario.

Area: 4

246. 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

The correct answer is:
C. A smart card requiring the user's PIN

Explanation:
A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a key board 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.

Area: 4

247. A single digitally signed instruction was given to a financial institution to credit a customer's account. The financial institution received the instruction three times and credited the account three times. Which of the following would be the MOST appropriate control against such multiple credits?

A. Encrypting the hash of the payment instruction with the public key of the financial institution
B. Affixing a time stamp to the instruction and using it to check for duplicate payments
C. Encrypting the hash of the payment instruction with the private key of the instructor
D. Affixing a time stamp to the hash of the instruction before having it digitally signed by the instructor

The correct answer is:
B. Affixing a time stamp to the instruction and using it to check for duplicate payments

Explanation:
Affixing a time stamp to the instruction and using it to check for duplicate payments makes the instruction unique. The financial institution can check that the instruction was not intercepted and replayed, and thus, it could prevent crediting the account three times. Encrypting the hash of the payment instruction with the public key of the financial institution does not protect replay, it only protects confidentiality and integrity of the instruction. Encrypting the hash of the payment instruction with the private key of the instructor ensures integrity of the instruction and nonrepudiation of the issued instruction. The process of creating a message digest requires applying a cryptographic hashing algorithm to the entire message. The receiver, upon decrypting the message digest, will recompute the hash using the same hashing algorithm and compare the result with what was sent. Hence, affixing a time stamp into the hash of the instruction before being digitally signed by the instructor would violate the integrity requirements of a digital signature.

Area: 4

248. Which of the following would be of MOST concern to an IS auditor reviewing a VPN implementation? Computers on the network that are located:

A. on the enterprise's facilities.
B. at the backup site.
C. in employees' homes.
D. at the enterprise's remote offices.

The correct answer is:
C. in employees' homes.

Explanation:
One risk of a VPN implementation is the chance of allowing high-risk computers onto the enterprise's network. All machines that are allowed onto the virtual network should be subject to the same security policy. Home computers are least subject to the corporate security policies and, hence, are high-risk computers. Once a computer is hacked and "owned," any network that trusts that computer is at risk. Implementation and adherence to corporate security policy is easier when all computers on the network are on the enterprise's campus. Internally to an enterprise's physical network, there should be security policies in place to detect and halt an outside attack that uses an internal machine as a staging platform. Computers at the backup site are subject to the corporate security policy and, hence, are not high-risk computers. Computers on the network that are at the enterprise's remote offices, perhaps with different IS and security employees who have different ideas about security, are more risky than choices A and B, but obviously less risky

than home computers.

Area: 4

249. The PRIMARY reason for using digital signatures is to ensure data:

A. confidentiality.
B. integrity.
C. availability.
D. timeliness.

The correct answer is:
B. integrity.

Explanation:
Digital signatures provide integrity because the digital signature of a signed message (file, mail, document, etc.) changes every time a single bit of the document changes; thus, a signed document cannot be altered. Depending on the mechanism chosen to implement a digital signature, the mechanism might be able to ensure data confidentiality or even timeliness, but this is not assured. Availability is not related to digital signatures.

Area: 4

250. The PKI element that manages the certificate life cycle, including certificate directory maintenance and certificate revocation list (CRL) maintenance and publication, is the:

A. certificate authority (CA).
B. digital certificate.
C. certification practice statement (CPS).
D. registration authority.

The correct answer is:
A. certificate authority (CA).

Explanation:
The certificate authority manages the certificate life cycle, including certificate directory maintenance and CRL maintenance and publication. The CA attests, as a trusted provider of the public/private key pairs, to the authenticity of the owner to whom a public/private key pair has been given. The digital certificate is composed of a public key and identifying information about the owner of the public key. It associates a public key with an individual's identity. Certificates are e-documents, digitally signed by a trusted entity and containing information on individuals. The process entails the sender, who is digitally signing a document with the digital certificate

attached issued by a trusted entity where the receiver relies on the public key that is included in the digital certificate, to authenticate the message. The certification practice statement is the governance process for CA operations. A CPS documents the high-level practices, procedures and controls of a CA. The registration authority attests, as a trusted provider of the public/private key pairs, to the authenticity of the owner to whom a public/private key pair has been provided. In other words, the registration authority performs the process of identification and authentication by establishing a link between the identity of the requesting person or organization and the public key. As a brief note, a CA manages and issues certificates, whereas a RA is responsible for identifying and authenticating subscribers, but does not sign or issue certificates. Definitions can be found in a glossary posted at: http://sig.nfc.usda.gov/pki/glossary/glossary.html and http://www.cio-dpi.gc.ca/pki-icp/beginners/glossary/glossary_e.asp?format=print and in "Auditing and Certification of a Public Key Infrastructure," by Ronald Koorn, Peter Walsen, Mark Lund, Information Systems Control Journal, Volume 5, 2002, p. 28-29.

Area: 4

251. Which of the following is an example of a passive attack initiated through the Internet?

A. Traffic analysis
B. Masquerading
C. Denial of service
D. E-mail spoofing

The correct answer is:
A. Traffic analysis

Explanation:
Internet security threats/vulnerabilities are divided into passive and active attacks. Examples of passive attacks include network analysis, eavesdropping and traffic analysis. Active attacks include brute-force attacks, masquerading, packet replay, message modification, unauthorized access through the Internet or web-based services, denial-of-service attacks, dial-in penetration attacks, e-mail bombing and spamming, and e-mail spoofing.

Area: 4

252. 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.

The correct answer is:
C. equal-error rate.

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 false-rejection rates or low false-acceptance rates alone do not measure the efficiency of the device. Estimated-error rate is nonexisting and hence irrelevant.

Area: 4

253. Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called a:

A. feedback error control.
B. block sum check.
C. forward error control.
D. cyclic redundancy check.

The correct answer is:
C. forward error control.

Explanation:
Forward error control involves transmitting additional redundant information with each character or frame to facilitate detection and correction of errors. In feedback error control, only enough additional information is transmitted so the receiver can identify that an error has occurred. Choices B and D are both error detection methods but not error correction methods. Block sum check is an extension of parity check wherein an additional set of parity bits is computed for a block of characters. A cyclic redundancy check is a technique wherein a single set of check digits is generated, based on the contents of the frame, for each frame transmitted.

Area: 4

254. 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.

The correct answer is:
D. polymorphic virus.

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. A logic bomb is code that is hidden in a program or system which will cause something to happen when the user performs a certain action or when certain conditions are met. A logic bomb, which can be downloaded along with a corrupted shareware or freeware program, may destroy data, violate system security or erase the hard drive. A stealth virus is a virus that hides itself by intercepting disk access requests. When an antivirus program tries to read files or boot sectors to find the virus, the stealth virus feeds the antivirus program a clean image of the file or boot sector. A Trojan horse is a virus program that appears to be useful and harmless but which has harmful side effects such as destroying data or breaking the security of the system on which it is run.

Area: 4

255. 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 shutoff switch.
B. Install protective covers.
C. Escort visitors.
D. Log environmental failures.

The correct answer is:
B. Install protective covers.

Explanation:
A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation. Relocating the shutoff switch would defeat the purpose of having it readily accessible. Escorting the personnel who move the equipment may not have prevented this incident, and logging of environmental failures would provide management with a report of incidents, but reporting alone would not prevent a reoccurrence.

Area: 4

256. The process of using interpersonal communication skills to get unauthorized access to company assets is called:

A. wire tapping.
B. trapdoors.
C. war dialing.
D. social engineering.

The correct answer is:
D. social engineering.

Explanation:
Social engineering is a term that describes a nontechnical kind of intrusion that relies heavily on human interaction and often involves tricking other people into breaking normal security procedures. Wire tapping is a technique used for getting the signals transmitted over cables without disturbing the flow between the source and destination. Trapdoors are a break in the software source code deliberately left by programmers to enable the insertion of additional debugging code, and they may be used later for some unwanted purposes. War dialing involves trying out all the published phone numbers of the company to find one that is connected to a modem and subsequently using that as an entry point into the corporate databases.

Area: 4

257. 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

The correct answer is:
B. Identification of network applications to be externally accessed

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.

Area: 4

258. The security level of a private key system depends on the number of:

A. encryption key bits.
B. messages sent.
C. keys.
D. channels used.

The correct answer is:
A. encryption key bits.

Explanation:
The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, it's the algorithm and its complexity that make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

Area: 4

259. 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

The correct answer is:
B. Application gateway

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.

Area: 4

260. A callback 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 and using a telephone number from its database.
B. dials back to the user machine based on the user id and password and using a telephone number provided by the user during the original connection.
C. waits for a redial from the user machine for confirmation and then verifies the user id and password using its database.
D. waits for a redial from the user machine for confirmation and then verifies the user id and password using the sender's database.

The correct answer is:
A. dials back to the user machine based on the user id and password and using a telephone number from its database.

Explanation:
A callback 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.

Area: 4

261. The act that describes a computer intruder capturing a stream of data packets and inserting these packets into the network as if it were another genuine message stream is called:

A. eavesdropping.
B. message modification.
C. a brute-force attack.
D. packet replay.

The correct answer is:
D. packet replay.

Explanation:
Packet replay is a combination of passive and active modes of attack. This form of attack is particularly effective when the receiving end of the communication channel is automated and acts on the receipt and interpretation of information packets without human intervention.

Area: 4

262. Which of the following can consume valuable network bandwidth?

A. Trojan horses
B. Trapdoors
C. Worms
D. Vaccines

The correct answer is:
C. Worms

Explanation:
Worms are destructive programs that may destroy data or utilize tremendous computer and communication resources. Trojan horses can capture and transmit private information to the attacker's computer. Trapdoors are exits out of an authorized program. Vaccines are programs designed to detect computer viruses.

Area: 4

263. The review of router access control lists should be conducted during a/an:

A. environmental review.
B. network security review.
C. business continuity review.
D. data integrity review.

The correct answer is:
B. network security review.

Explanation:
Network security reviews include reviewing router access control lists, port scanning, internal and external connections to the system, etc. Environmental reviews, business continuity reviews and data integrity reviews do not require a review of the router access control lists.

Area: 4

264. Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

A. Analyzer
B. Administration console
C. User interface
D. Sensor

The correct answer is:
D. Sensor

Explanation:
Sensors are responsible for collecting data. Analyzers receive input from sensors and determine intrusive activity. An administration console and a user interface are components of an IDS.

Area: 4

265. Which of the following steps would an IS auditor normally perform FIRST in a data center security review?

A. Evaluate physical access test results.
B. Determine the risks/threats to the data center site.
C. Review business continuity procedures.
D. Test for evidence of physical access at suspect locations.

The correct answer is:
B. Determine the risks/threats to the data center site.

Explanation:
During planning, the IS auditor should get an overview of the functions being audited and evaluate the audit and business risks. Choices A and D are part of the audit fieldwork process that occurs subsequent to this planning and preparation. Choice C is not part of a security review.

Area: 4

266. An enterprisewide network security architecture of a public key infrastructure (PKI) would be comprised of:

A. A public key cryptosystem, private key cryptosystem and digital certificate
B. A public key cryptosystem, symmetric encryption and certificate authorities
C. A symmetric encryption, digital certificate and kerberos authentication
D. A public key cryptosystem, digital certificate and certificate authorities

The correct answer is:
D. A public key cryptosystem, digital certificate and certificate authorities

Explanation:
These three elements make up a complete system. The other choices are combinations that do not

make a complete system.

Area: 4

267. Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

A. Unauthorized access from outside the organization
B. Unauthorized access from within the organization
C. A delay in Internet connectivity
D. A delay in downloading using File Transfer Protocol (FTP)

The correct answer is:
A. Unauthorized access from outside the organization

Explanation:
Firewalls are meant to prevent outsiders from gaining access to an organization's computer systems through the Internet gateway. They form a barrier with the outside world, but are not intended to address access by internal users, and are more likely to cause delays than address such concerns.

Area: 4

268. The MOST effective method of preventing unauthorized use of data files is:

A. automated file entry.
B. tape librarian.
C. access control software.
D. locked library.

The correct answer is:
C. access control software.

Explanation:
Access control software is an active control designed to prevent unauthorized access to data.

Area: 4

269. A digital signature contains a message digest to:

A. show if the message has been altered after transmission.
B. define the encryption algorithm.

C. confirm the identity of the originator.
D. enable message transmission in a digital format.

The correct answer is:
A. show if the message has been altered after transmission.

Explanation:
The message digest is calculated and included in a digital signature to prove that the message has not been altered. It should be the same value as a recalculation performed upon receipt. It does not define the algorithm or enable the transmission in digital format and has no effect on the identity of the user; it is there to ensure integrity rather than identity.

Area: 4

270. Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

A. Registration authority
B. Certificate authority (CA)
C. Certification relocation list
D. Certification practice statement

The correct answer is:
B. Certificate authority (CA)

Explanation:
The certificate authority maintains a directory of digital certificates for the reference of those receiving them. It manages the certificate life cycle, including certificate directory maintenance and certificate revocation list maintenance and publication. Choice A is not correct because a registration authority is an optional entity that is responsible for the administrative tasks associated with registering the end entity that is the subject of the certificate issued by the CA. Choice C is incorrect since a CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. Choice D is incorrect because a certification practice statement is a detailed set of rules governing the certificate authority's operations.

Area: 4

271. Which of the following is the MOST effective control procedure for security of a stand-alone small business computer environment?

A. Supervision of computer usage
B. Daily management review of the trouble log

C. Storage of computer media in a locked cabinet
D. Independent review of an application system design

The correct answer is:
A. Supervision of computer usage

Explanation:
Since small, stand-alone business computer environments normally lack basic controls, such as access control software and a strict segregation of duties, strong compensating controls should be applied. In this situation, supervision of computer usage must be relied upon. This takes the form of monitoring office activity, reviewing key control reports, and sampling employee work to ensure it is appropriate and authorized.

Area: 4

272. Which of the following logical access exposures involves changing data before, or as, it is entered into the computer?

A. Data diddling
B. Trojan horse
C. Worm
D. Salami technique

The correct answer is:
A. Data diddling

Explanation:
Data diddling involves changing data before, or as, it is entered into the computer. A Trojan horse involves unauthorized changes to a computer program. A worm is a destructive program that destroys data. The salami technique is a program modification that slices off small amounts of money from a computerized transaction.

Area: 4

273. A TCP/IP-based environment is exposed to the Internet. Which of the following BEST ensures that complete encryption and authentication protocols exist for protecting information while transmitted?

A. Work is completed in tunnel mode with IP security using the nested services of authentication header (AH) and encapsulating security payload (ESP).
B. A digital signature with RSA has been implemented.

C. Digital certificates with RSA are being used.
D. Work is being completed in TCP services.

The correct answer is:
A. Work is completed in tunnel mode with IP security using the nested services of authentication header (AH) and encapsulating security payload (ESP).

Explanation:
Tunnel mode with IP security provides encryption and authentication of the complete IP package. To accomplish this, the AH and ESP services can be nested. Choices B and C provide authentication and integrity. TCP services do not provide encryption and authentication.

Area: 4

274. Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?

A. Security awareness
B. Reading the security policy
C. Security committee
D. Logical access controls

The correct answer is:
D. Logical access controls

Explanation:
To retain a competitive advantage and meet basic business requirements, organizations must ensure the integrity of the information stored on their computer systems, preserve the confidentiality of sensitive data and ensure the continued availability of their information systems. To meet these goals, logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy (choice B), which should be known by the organization's employees, would help to protect information, but would not prevent the unauthorized access of information. A security committee (choice C) is key to the protection of information assets, but would address security issues within a broader perspective.

Area: 4

275. Which of the following is the MOST effective technique for providing security during data transmission?

A. Communication log
B. Systems software log
C. Encryption
D. Standard protocol

The correct answer is:
C. Encryption

Explanation:
Encryption provides security for data during transmission. The other choices do not provide protection during data transmission.

Area: 4

276. Digital signatures require the:

A. signer to have a public key and the receiver to have a private key.
B. signer to have a private key and the receiver to have a public key.
C. signer and receiver to have a public key.
D. signer and receiver to have a private key.

The correct answer is:
B. signer to have a private key and the receiver to have a public key.

Explanation:
Digital signatures are intended to verify to a recipient the integrity of the data and the identity of the sender. The digital signature standard is a public key algorithm. This requires the signer to have a private key, and the receiver to have a public key.

Area: 4

277. Which of the following is a benefit of using a callback device?

A. Provides an audit trail.
B. Can be used in a switchboard environment.
C. Permits unlimited user mobility.
D. Allows call forwarding.

The correct answer is:
A. Provides an audit trail.

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.

Area: 4

278. When reviewing an organization's logical access security, which of the following would be of MOST concern to an IS auditor?

A. Passwords are not shared.
B. Password files are not encrypted.
C. Redundant logon IDs are deleted.
D. The allocation of logon IDs is controlled.

The correct answer is:
B. Password files are not encrypted.

Explanation:
When evaluating the technical aspects of logical security, unencrypted files represent the greatest risk. The sharing of passwords, checking for the redundancy of logon ids, and proper logon ID procedures are essential, but they are less important than ensuring that the password files are encrypted.

Area: 4

279. In the ISO/OSI model, which of the following protocols is the FIRST to establish security for the user application?

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

The correct answer is:
A. Session layer

Explanation:

The session layer provides functions that allow two applications to communicate across the network. The functions include security, recognition of names, logons and so on. The session layer is the first layer where security is established for user applications. The transportation layer provides transparent transfer of data between end points. The network layer controls the packet routing and switching within the network, as well as to any other network. The presentation layer provides common communication services, such as encryption, text compression and reformatting.

Area: 4

280. The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is:

A. data integrity.
B. authentication.
C. nonrepudiation.
D. replay protection.

The correct answer is:
C. nonrepudiation.

Explanation:
All of the above are features of a digital signature. Nonrepudiation ensures that the claimed sender cannot later deny generating and sending the message. Data integrity refers to changes in the plaintext message that would result in the recipient failing to compute the same message hash. Since only the claimed sender has the key, authentication ensures that the message has been sent by the claimed sender. Replay protection is a method that a recipient can use to check that the message was not intercepted and replayed.

Area: 4

281. An IS auditor doing penetration testing during an audit of Internet connections would:

A. evaluate configurations.
B. examine security settings.
C. ensure virus-scanning software is in use.
D. use tools and techniques that are available to a hacker.

The correct answer is:
D. use tools and techniques that are available to a hacker.

Explanation:
Penetration testing is a technique used to mimic an experienced hacker attacking a live site by using tools and techniques available to a hacker. The other choices are procedures that an IS auditor would consider undertaking during an audit of Internet connections, but are not aspects of penetration testing techniques.

Area: 4

282. 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.

The correct answer is:
A. Visitors are escorted.

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.

Area: 4

283. Which of the following should concern an IS auditor when reviewing security in a client-server environment?

A. Protecting data using an encryption technique
B. Preventing unauthorized access using a diskless workstation
C. Ability of users to access and modify the database directly
D. Disabling floppy drives on the users' machines

The correct answer is:
C. Ability of users to access and modify the database directly

Explanation:
For the purpose of data security in a client-server environment, an IS auditor should be concerned with the users ability to access and modify a database directly. This could affect the integrity of the data in the database. Data protected by encryption aid in securing the data.

Diskless workstations prevent copying of data into local disks and thus help to maintain the integrity and confidentiality of data. Disabling floppy drives is a physical access control, which helps to maintain the confidentiality of data by preventing it from being copied onto a disk.

Area: 4

284. Passwords should be:

A. assigned by the security administrator for first time logon.
B. changed every 30 days at the discretion of the user.
C. reused often to ensure the user does not forget the password.
D. displayed on the screen so that the user can ensure that it has been entered properly.

The correct answer is:
A. assigned by the security administrator for first time logon.

Explanation:
Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days); however, changing should not be voluntary, it should be required by the system. Systems should not permit previous passwords to be used again; old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

Area: 4

285. Which of the following can identify attacks and penetration attempts to a network?

A. Firewall
B. Packet filters
C. Stateful inspection
D. Intrusion detection system (IDs)

The correct answer is:
D. Intrusion detection system (IDs)

Explanation:
An IDS has a large database of attack signatures, which is used to ward off attacks. Packet filter and stateful inspection are types of firewalls. A firewall is a fence around a network designed to block certain types of communications routed or passing through specific ports. It is not designed to discover someone bypassing or going under the firewall.

Area: 4

286. Which of the following is a technique that could be used to capture network user passwords?

A. Encryption
B. Sniffing
C. Spoofing
D. Data destruction

The correct answer is:
B. Sniffing

Explanation:
Sniffing is an attack that can be used to capture sensitive pieces of information (password), passing through the network. Encryption is a method of scrambling information to prevent unauthorized individuals from understanding the transmission. Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication. Data destruction is erasing information or removing it from its original location.

Area: 4

287. When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?

A. Read access to data
B. Delete access to transaction data files
C. Logged read/execute access to programs
D. Update access to job control language/script files

The correct answer is:
B. Delete access to transaction data files

Explanation:
Deletion of transaction data files should be a function of the application support team, not operations staff. Read access to production data is a normal requirement of a computer operator, as is logged access to programs and access to JCL in order to control job execution.

Area: 4

288. To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

A. online terminals be placed in restricted areas.
B. online terminals be equipped with key locks.
C. ID cards be required to gain access to online terminals.
D. online access be terminated after a specified number of unsuccessful attempts.

The correct answer is:
D. online access be terminated after a specified number of unsuccessful attempts.

Explanation:
The most appropriate control to prevent unauthorized entry is to terminate connection after a specified number of attempts. This will deter access through the guessing of ids and passwords. The other choices are physical controls, which are not effective in deterring unauthorized accesses via the telephone lines.

Area: 4

289. Which of the following controls would BEST detect intrusion?

A. User ids and user privileges are granted through authorized procedures.
B. Automatic logoff is used when a workstation is inactive for a particular period of time.
C. Automatic logoff of the system after a specified number of unsuccessful attempts.
D. Unsuccessful logon attempts are monitored by the security administrator.

The correct answer is:
D. Unsuccessful logon attempts are monitored by the security administrator.

Explanation:
Intrusion is detected by the active monitoring and review of unsuccessful logons. User ids and the granting of user privileges defines a policy, not a control. Automatic logoff is a method of preventing access on inactive terminals and is not a detective control. Unsuccessful attempts to log on are a method for preventing intrusion, not detecting.

Area: 4

290. Programs that can run independently and travel from machine to machine across network connections, with the ability to destroy data or utilize tremendous computer and communication resources, are referred to as:

A. Trojan horses.
B. viruses.
C. worms.
D. logic bombs.

The correct answer is:
C. worms.

Explanation:
Worms are nonreplicating programs that can run independently and travel from machine to machine. A Trojan horse resembles a commonly used authorized program that does something unrelated to its stated or intended purpose causing a malicious or fraudulent action or event to occur. Viruses are malicious program code inserted into other executable code that can self-replicate and spread from computer to computer. Logic bombs are programmed threats that lie dormant in commonly used software for an extended period of time until they are triggered.

Area: 4

291. 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

The correct answer is:
D. Applets opening connections from the client machine

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.

Area: 4

292. Which of the following is a feature of an intrusion detection system (IDS)?

A. Gathering evidence on attack attempts
B. Identifying weaknesses in the policy definition

C. Blocking access to particular sites on the Internet
D. Preventing certain users from accessing specific servers

The correct answer is:
A. Gathering evidence on attack attempts

Explanation:
An IDS can gather evidence on intrusive activity like an attack or penetration attempt. Identifying weaknesses in the policy definition is a limitation of an IDS. Choices C and D are features of firewalls, and choice B requires a manual review and, therefore, is outside the functionality of an IDS.

Area: 4

293. An IS auditor conducting an access controls review in a client-server environment discovers that all printing options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:

A. exposure is greater since information is available to unauthorized users.
B. operating efficiency is enhanced since anyone can print any report at any time.
C. operating procedures are more effective since information is easily available.
D. user friendliness and flexibility is facilitated since there is a smooth flow of information among users.

The correct answer is:
A. exposure is greater since information is available to unauthorized users.

Explanation:
Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside, as electronic files, without printing because print options allow for printing in an electronic form as well.

Area: 4

294. An IS auditor performing a telecommunication access control review should be concerned PRIMARILY with the:

A. maintenance of access logs of usage of various system resources.
B. authorization and authentication of the user prior to granting access to system resources.

C. adequate protection of stored data on servers by encryption or other means.
D. accountability system and the ability to identify any terminal accessing system resources.

The correct answer is:
B. authorization and authentication of the user prior to granting access to system resources.

Explanation:
The authorization and authentication of users is the most significant aspect in a telecommunications access control review, as it is a preventive control. Weak controls at this level can affect all other aspects. The maintenance of access logs of usage of system resources is a detective control. The adequate protection of data being transmitted to and from servers by encryption or other means is a method of protecting information during transmission and is not an access issue. The accountability system and the ability to identify any terminal accessing system resources deal with controlling access through the identification of a terminal.

Area: 4

295. Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:

A. change the company's security policy.
B. educate users about the risk of weak passwords.
C. build in validations to prevent this during user creation and password change.
D. require a periodic review of matching user ID and passwords for detection and correction.

The correct answer is:
C. build in validations to prevent this during user creation and password change.

Explanation:
The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risks of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

Area: 4

296. The PRIMARY objective of a logical access controls review is to:

A. review access controls provided through software.
B. ensure access is granted per the organization's authorities.
C. walk through and assess the access provided in the IT environment.
D. provide assurance that computer hardware is adequately protected against abuse.

The correct answer is:
B. ensure access is granted per the organization's authorities.

Explanation:
The scope of a logical access controls' review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical access controls' review, rather than objectives. Choice D is relevant to a physical access control review.

Area: 4

297. Which of the following is the MOST important objective of data protection?

A. Identifying persons who need access to information
B. Ensuring the integrity of information
C. Denying or authorizing access to the IS system
D. Monitoring logical accesses

The correct answer is:
B. Ensuring the integrity of information

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.

Area: 4

298. Naming conventions for system resources are important for access control because they:

A. ensure that resource names are not ambiguous.
B. reduce the number of rules required to adequately protect resources.
C. ensure that user access to resources is clearly and uniquely identified.
D. ensure that internationally recognized names are used to protect resources.

The correct answer is:
B. reduce the number of rules required to adequately protect resources.

Explanation:
Naming conventions for system resources are important for efficient administration of security controls. The conventions can be structured so resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous cannot be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

Area: 4

299. Which of the following exposures could be caused by a line-grabbing technique?

A. Unauthorized data access
B. Excessive CPU cycle usage
C. Lockout of terminal polling
D. Multiplexor control dysfunction

The correct answer is:
A. Unauthorized data access

Explanation:
Line grabbing will enable eavesdropping, thus allowing unauthorized data access. It will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

Area: 4

300. The creation of an electronic signature:

A. encrypts the message.
B. verifies from where the message came.
C. cannot be compromised when using a private key.
D. cannot be used with e-mail systems.

The correct answer is:
B. verifies from where the message came.

Explanation:
The creation of an electronic signature does not in itself encrypt the message or secure it from compromise. It only verifies the message's origination.

Area: 4

301. Which of the following reports is a measure of telecommunication transmissions and determines whether transmissions are completed accurately?

A. Online monitor reports
B. Downtime reports
C. Help desk reports
D. Response-time reports

The correct answer is:
A. Online monitor reports

Explanation:
Online monitors measure telecommunication transmissions and determine whether transmissions are completed accurately. Downtime reports track the availability of telecommunication lines and circuits; help desk reports handle problems occurring in the normal course of operations; and response-time reports identify the time it takes for a command entered at a terminal to be answered by the computer.

Area: 4

302. 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

The correct answer is:
A. Simple Network Management Protocol

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.

Area: 4

303. Which of the following is the MOST effective type of antivirus software?

A. Scanners
B. Active monitors
C. Integrity checkers
D. Vaccines

The correct answer is:
C. Integrity checkers

Explanation:
Integrity checkers compute a binary number on a known virus-free program that is then stored in a database file. The number is called a cyclical redundancy check (CRC). When that program is called to execute, the checker computes the CRC on the program about to be executed and compares it to the number in the database. A match means no infection; a mismatch means that a change in the program has occurred. A change in the program could mean a virus. Scanners look for sequences of bits called signatures that are typical of virus programs. They examine memory, disk boot sectors, executables and command files for bit patterns that match a known virus. Therefore, scanners need to be updated periodically to remain effective. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions. Active monitors can be misleading, because they cannot distinguish between a user request and a program or virus request. As a result, users are asked to confirm actions like formatting a disk or deleting a file or set of files. Vaccines are known to be good antivirus software. However, they also need to be updated periodically to remain effective.

Area: 4

304. When using public key encryption to secure data being transmitted across a network:

A. both the key used to encrypt and decrypt the data are public.
B. the key used to encrypt is private, but the key used to decrypt the data is public.

C. the key used to encrypt is public, but the key used to decrypt the data is private.
D. both the key used to encrypt and decrypt the data are private.

The correct answer is:
C. the key used to encrypt is public, but the key used to decrypt the data is private.

Explanation:
Public key encryption, also known as asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.

Area: 4

305. The technique used to ensure security in virtual private networks (VPNs) is:

A. encapsulation.
B. wrapping.
C. transform.
D. encryption.

The correct answer is:
A. encapsulation.

Explanation:
Encapsulation or tunneling is a technique used to carry the traffic of one protocol over a network that does not support that protocol directly. The original packet is wrapped in another packet. The other choices are not security techniques specific to VPNs.

Area: 4

306. During an audit of a telecommunications system, the IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:

A. encryption.
B. callback modems.
C. message authentication.
D. dedicated leased lines.

The correct answer is:
A. encryption.

Explanation:
Encryption of data is the most secure method. The other methods are less secure, with leased lines being possibly the least secure method.

Area: 4

307. An Internet-based attack using password sniffing can:

A. enable one party to act as if they are another party.
B. cause modification to the contents of certain transactions.
C. be used to gain access to systems containing proprietary information.
D. result in major problems with billing systems and transaction processing agreements.

The correct answer is:
C. be used to gain access to systems containing proprietary information.

Explanation:
Password sniffing attacks can be used to gain access to systems on which proprietary information is stored. Spoofing attacks can be used to enable one party to act as if they are another party. Data modification attacks can be used to modify the contents of certain transactions. Repudiation of transactions can cause major problems with billing systems and transaction processing agreements.

Area: 4

308. Which of the following controls would be the MOST comprehensive in a remote access network with multiple and diverse subsystems?

A. Proxy server
B. Firewall installation
C. Network administrator
D. Password implementation and administration

The correct answer is:
D. Password implementation and administration

Explanation:
The most comprehensive control in this situation is password implementation and administration. While firewall installations are the primary line of defense, they cannot protect all access and, therefore, an element of risk remains. A proxy server is a type of firewall installation and thus the same rules apply. The network administrator may serve as a control, but typically this would

not be comprehensive enough to serve on multiple and diverse systems.

Area: 4

309. 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.

The correct answer is:
C server used to connect authorized users to private, trusted network resources.

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 to 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.

Area: 4

310. During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, the IS auditor must prove that which of the following is used?

A. A biometric, digitalized and encrypted parameter with the customer's public key
B. A hash of the data that is transmitted and encrypted with the customer's private key
C. A hash of the data that is transmitted and encrypted with the customer's public key
D. The customer's scanned signature, encrypted with the customer's public key

The correct answer is:
B. A hash of the data that is transmitted and encrypted with the customer's private key

Explanation:
The calculation of a hash or digest of the data that are transmitted and its encryption require the public key of the client (receiver) and are called a signature of the message or digital signature.

The receiver performs the same process and then compares the received hash, once it has been decrypted with his/her private key, to the hash that he/she calculates with the received data. If they are the same, the conclusion would be that there is integrity in the data that have arrived and the origin is authenticated. The concept of encrypting the hash with the private key of the originator provides nonrepudiation, as it can only be decrypted with their public key and, as the CD suggests, the private key would not be known to the recipient. Simply put, in a key-pair situation, anything that can be decrypted by a sender's public key must have been encrypted with his/her private key, so he/she must have been the sender, i.e., nonrepudiation. Choice C is wrong because, if this were the case, the hash could not be decrypted by the recipient, so the benefit of nonrepudiation would be lost and there could be no verification that the message had not been intercepted and amended. A digital signature is created by encrypting with ones private key. The person creating the signature uses its own private key, otherwise everyone would be able to create a signature with any public key. Therefore, the signature of the client is created with the clients private key, and this can be verified-by the enterprise-using the clients public key. Choice B is the correct answer because, in this case, the customer uses his/her private key to sign the hash data.

Area: 4

311. When planning an audit of a network set up, the IS auditor should give highest priority to obtaining which of the following network documentation?

A. Wiring and schematic diagram
B. Users' lists and responsibilities
C. Application lists and their details
D. Backup and recovery procedures

The correct answer is:
A. Wiring and schematic diagram

Explanation:
The wiring and schematic diagram of the network is necessary to carry out a network audit. A network audit may not be feasible if a network wiring and schematic diagram is not available. All other documents are important but not necessary.

Area: 4

312. Which of the following is MOST directly affected by network performance monitoring tools?

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

The correct answer is:
B. Availability

Explanation:
In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

Area: 4

313. 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 is certain.
D. the host web site is part of the organization.

The correct answer is:
C. the source of the executable is certain.

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 are considered external defenses. A firewall will find it more difficult to filter a specific file from a trusted source. A secure web connection provides confidentiality. Neither can identify an executable as friendly. Hosting the web site as part of the organization is impractical. Enabling the acceptance of Java and/or Active X is an all-or-nothing proposition. The client will accept the program, if the parameters are established to do so.

Area: 4

314. Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity and nonrepudiation by either sender or recipient?

A. The recipient uses his/her private key to decrypt the secret key.
B The encrypted pre-hash code and the message are encrypted using a secret key.

C. The encrypted pre-hash code is derived mathematically from the message to be sent.
D. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the pre-hash code.

The correct answer is:
D. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the pre-hash code.

Explanation:
Most encrypted transactions today use a combination of private keys, public keys, secret keys, hash functions and digital certificates to achieve confidentiality, message integrity and nonrepudiation by either sender or recipient. The recipient uses the sender's public key to decrypt the pre-hash code into a post-hash code, which when equaling the pre-hash code, verifies the identity of the sender and that the message has not been changed in route; this would provide the greatest assurance. Each sender and recipient has a private key, known only to him/her and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key and both must be from the same party. A single, secret key is used to encrypt the message, because secret key encryption requires less processing power than using public and private keys. A digital certificate, signed by a certificate authority, validates senders' and recipients' public keys.

Area: 4

315. Which of the following controls would provide the GREATEST assurance of database integrity?

A. Audit log procedures
B. Table link/reference checks
C. Query/table access time checks
D. Rollback and rollforward database features

The correct answer is:
B. Table link/reference checks

Explanation:
Performing table link/reference checks serves to detect table linking errors (such as completeness and accuracy of the contents of the database) and thus provides the greatest assurance of database integrity. Audit log procedures enable recording of all events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the database's contents. Querying/monitoring table access time checks helps designers improve database performance, but not integrity. Rollback and rollforward database features ensure recovery from an abnormal disruption. They assure the

integrity of the transaction that was being processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

Area: 4

316. Use of asymmetric encryption in an Internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:

A. customer over the authenticity of the hosting organization.
B. hosting organization over the authenticity of the customer.
C customer over the confidentiality of messages from the hosting organization.
D. hosting organization over the confidentiality of messages passed to the customer.

The correct answer is:
A. customer over the authenticity of the hosting organization.

Explanation:
Any false site will not be able to encrypt using the private key of the real site, so the customer would not be able to decrypt the message using the public key. Many customers have access to the same public key so the host cannot use this mechanism to ensure the authenticity of the customer. The customer cannot be assured of the confidentiality of messages from the host as many people have access to the public key and can decrypt the messages from the host. The host cannot be assured of the confidentiality of messages sent out, as many people have access to the public key and can decrypt it.

Area: 4

317. The database administrator has recently informed you of the decision to disable certain normalization controls in the database management system (DBMS) software to provide users with increased query performance. This will MOST likely increase the risk of:

A. loss of audit trails.
B. redundancy of data.
C. loss of data integrity.
D. unauthorized access to data.

The correct answer is:
B. redundancy of data.

Explanation:

Normalization is the removal of redundant data elements from the database structure. Disabling features of normalization in relational databases will increase the likelihood of data redundancy. Audit trails are a feature of DBMS software that can be lost by not enabling them. These are not connected to normalization controls. The integrity of data is not directly affected by disabling normalization controls. Access to data is set through defining user rights and controlling access to information, and is not affected by normalization controls.

Area: 4

318. E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

A. sender's private key and encrypting the message using the receiver's public key.
B. sender's public key and encrypting the message using the receiver's private key.
C. the receiver's private key and encrypting the message using the sender's public key.
D. the receiver's public key and encrypting the message using the sender's private key.

The correct answer is:
A. sender's private key and encrypting the message using the receiver's public key.

Explanation:
By signing the message with the sender's private key, the receiver can verify its authenticity using the sender's public key. By encrypting the message with the receiver's public key, only the receiver can decrypt the message using his/her own private key. The receiver's private key is confidential and, therefore, unknown to the sender. Messages encrypted using the sender's private key can be read by anyone (with the sender's public key).

Area: 4

319. Confidential data residing on a PC are BEST protected by:

A. a password.
B. file encryption.
C. removable diskettes.
D. a key-operated power source.

The correct answer is:
B. file encryption.

Explanation:
File encryption is the best means of protecting confidential data in a PC. A key-operated power source, password or removable diskettes will only restrict access, and the data will still be

viewable using electronic eavesdropping techniques. Only encryption provides confidentiality. A password also may not be the best method of protection since passwords can be compromised. Removable diskettes do provide some security for information if they are locked away so only authorized individuals can gain access. However, if obtained by unauthorized individuals, information can be easily accessed. A key-operated power source can be bypassed by obtaining power from another source.

Area: 4

320. 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.

The correct answer is:
A. hardware is protected against power surges.

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.

Area: 4

321. Electromagnetic emissions from a terminal represent an exposure because they:

A. affect noise pollution.
B. disrupt processor functions.
C. produce dangerous levels of electric current.
D. can be detected and displayed.

The correct answer is:
D. can be detected and displayed.

Explanation:
Emissions can be detected by sophisticated equipment and displayed, thus giving access to data to unauthorized persons. They should not cause disruption of CPUs or effect noise pollution.

Area: 4

322. An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the BEST protection against hacking?

A. An application-level gateway
B. A remote access server
C. A proxy server
D. Port scanning

The correct answer is:
A. An application-level gateway

Explanation:
An application-level gateway is the best way to protect against hacking because it can define with detail rules that describe the type of user or connection that is or is not permitted. It analyzes in detail each package, not only in layers one through four of the OSI model but also layers five through seven, which means that it reviews the commands of each higher level protocol (HTTP, FTP, SNMP, etc.) For a remote access server, there is a device (server) that asks for a username and password before entering the network. This is good when accessing private networks, but it can be mapped or scanned from the Internet creating security exposure. Proxy servers can provide protection based on the IP address and ports. However, an individual is needed who really knows how to do this, and applications can use different ports for the different sections of the program. Port scanning works when there is a very specific task to complete, but not when trying to control what comes from the Internet (or when all the ports available need to be controlled). For example, the port for Ping (echo request) could be blocked and the IP addresses would be available for the application and browsing, but would not respond to Ping.

Area: 4

323. 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 sprinklers
C. Dry-pipe sprinklers
D. Carbon dioxide gas

The correct answer is:
C. Dry-pipe sprinklers

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.

Area: 4

324. Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

A. Power line conditioners
B. A surge protective device
C. An alternative power supply
D. An interruptible power supply

The correct answer is:
A. Power line conditioners

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.

Area: 4

325. 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

The correct answer is:
A. Appliances

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.

Area: 4

326. Which of the following physical access controls would provide the highest degree of security over unauthorized access?

A. Bolting door lock
B. Cipher lock
C. Electronic door lock
D. Fingerprint scanner

The correct answer is:
D. Fingerprint scanner

Explanation:
All are physical access controls designed to protect the organization from unauthorized access. However, biometric door locks, such as a fingerprint scanner, provide advantages, since they are harder to duplicate, easier to deactivate and individually identified. Biometric door locks, using an individual's unique body features, are used for access when extremely sensitive facilities must be protected.

Area: 4

327. Security administration procedures require read-only access to:

A. access control tables.
B. security log files.
C. logging options.
D. user profiles.

The correct answer is:
B. security log files.

Explanation:
Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access, to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update the way the transactions and user activities are monitored, captured, stored, processed and reported.

Area: 4

328. A MAJOR risk of using single sign-on (SSO) is that it:

A. has a single authentication point.
B. represents a single point of failure.
C. causes an administrative bottleneck.
D. leads to a lockout of valid users.

The correct answer is:
A. has a single authentication point.

Explanation:
The primary risk associated with single sign-on is the single authentication point. If a password is compromised, access to many applications can be obtained without further verification. A single point of failure provides a similar redundancy to the single authentication point. However, failure can occur at multiple points in resources, such as data, process or network. An administrative bottleneck may result when the administration is centralized in a single-step entry system. This is, therefore, an advantage. User lockout can occur with any password authentication system and is normally remedied swiftly by the security administrator resetting the account.

Area: 4

329. With the help of the security officer, granting access to data is the responsibility of:

A. data owners.
B. programmers.
C. system analysts.
D. librarians.

The correct answer is:
A. data owners.

Explanation:
Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (e.g., read or update).

Area: 4

330. Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

A. Virtual private network
B. Dedicated line
C. Leased line
D. Integrated services digital network

The correct answer is:
A. Virtual private network

Explanation:
The most secure method is a virtual private network (VPN), using encryption, authentication and tunneling to allow data to travel securely from a private network to the Internet. Choices B, C and D are network connectivity options that are normally too expensive to be practical for small- to medium-sized organizations.

Area: 4

331. The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

A. connecting points are available in the facility to connect laptops to the network.
B. users take precautions to keep their passwords confidential.
C. terminals with password protection are located in insecure locations.
D. terminals are located within the facility in small clusters under the supervision of an administrator.

The correct answer is:
A. connecting points are available in the facility to connect laptops to the network.

Explanation:
Any person with wrongful intentions can connect a laptop to the network. The insecure connecting points make unauthorized access possible if the individual has knowledge of a valid

user id and password. The other choices are controls for preventing unauthorized network access. If system passwords are not readily available for intruders to use, they must guess, which introduces an additional factor and requires time. System passwords provide protection against unauthorized use of terminals located in insecure locations. Supervision is a very effective control when used to monitor access to a small operating unit or production resources.

Area: 4

332. Which of the following functions is performed by a virtual private network (VPN)?

A. Hiding information from sniffers on the net
B. Enforcing security policies
C. Detecting misuse or mistakes
D. Regulating access

The correct answer is:
A. Hiding information from sniffers on the net

Explanation:
A VPN hides information from sniffers on the net, using encryption. It works based on tunneling. A VPN does not analyze information packets and, therefore, cannot enforce security policies; it does not check the content of packets and, therefore, cannot detect misuse or mistakes; and it does not perform an authentication function and, hence, cannot regulate access.

Area: 4

333. Applying a digital signature to data traveling in a network provides:

A. confidentiality and integrity.
B. security and nonrepudiation.
C. integrity and nonrepudiation.
D. confidentiality and nonrepudiation.

The correct answer is:
C. integrity and nonrepudiation.

Explanation:
The process of applying a mathematical algorithm to the data that travel in the network and placing the results of this operation with the hash data is used for controlling data integrity, since any unauthorized modification to this data would result in a be different hash. The application of a digital signature would accomplish the nonrepudiation of the delivery of the message. The term security is a broad concept and not a specific one. In addition to a hash and a digital signature,

confidentiality is applied when an encryption process exists.

Area: 4

334. Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital certificates for its business-to-consumer transactions via the Internet?

A. Customers are widely dispersed geographically, but the certificate authorities are not.
B Customers can make their transactions from any computer or mobile device.
C. The certificate authority has several data processing subcenters to administer certificates.
D. The organization is the owner of the certificate authority.

The correct answer is:
D. The organization is the owner of the certificate authority.

Explanation:
If the certificate authority belongs to the same organization, this would generate a conflict of interest. That is, if a customer wanted to repudiate a transaction, he/she could allege that because of the shared interests an unlawful agreement exists between the parties generating the certificates. If a customer wanted to repudiate a transaction, he/she could argue that there exists a bribery between the parties to generate the certificates, as there exist shared interests. The other options are not weaknesses.

Area: 4

335. Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the Internet?

A. Transport mode with authentication header plus encapsulating security payload (ESP)
B. Secure sockets layer (SSL) mode
C. Tunnel mode with AH plus ESP
D. Triple-DES encryption mode

The correct answer is:
C. Tunnel mode with AH plus ESP

Explanation:
Tunnel mode provides protection to the entire IP package. To accomplish this, AH and ESP services can be nested. The transport mode provides primary protection for the higher layers of the protocols by extending protection to the data fields (payload) of an IP package. The SSL

(Secure Sockets Layer) mode, provides security to the higher communication layers (transport layer). The triple-DES encryption mode is an algorithm that provides confidentiality.

Area: 4

336. Which of the following is the MOST reliable sender authentication method?

A. Digital signatures
B. Asymmetric cryptography
C. Digital certificates
D. Message authentication code

The correct answer is:
C. Digital certificates

Explanation:
Digital certificates are issued by a trusted third party. The message sender attaches the certificate rather than the public key and can verify authenticity with the certificate repository. Asymmetric cryptography is vulnerable to a man-in-the-middle attack. Digital certificates are used for confidentiality. Message authentication code is used for message integrity verification.

Area: 4

337. Which of the following provides the GREATEST assurance of message authenticity?

A. The pre-hash code is derived mathematically from the message being sent.
B. The pre-hash code is encrypted using the sender's private key.
C. The pre-hash code and the message are encrypted using the secret key.
D. The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

The correct answer is:
B. The pre-hash code is encrypted using the sender's private key.

Explanation:
Encrypting the pre-hash code using the sender's private key provides assurance of the authenticity of the message. Mathematically deriving the pre-hash code provides integrity to the message. Encrypting the pre-hash code and the message using the secret key provides confidentiality.

Area: 4

338. Which of the following Internet security threats could compromise integrity?

A. Theft of data from the client
B. Exposure of network configuration information
C. A Trojan horse browser
D. Eavesdropping on the net

The correct answer is:
C. A Trojan horse browser

Explanation:
Internet security threats/vulnerabilities to integrity include a Trojan horse, which could modify user data, memory and messages, found in client-browser software. The other options compromise confidentiality.

Area: 4

339. The FIRST step in data classification is to:

A. establish ownership.
B. perform a criticality analysis.
C. define access rules.
D. create a data dictionary.

The correct answer is:
A. establish ownership.

Explanation:
Data classification is necessary to define access rules based on a need-to-do and need-to-know basis. The data owner is responsible for defining the access rules; hence, establishing of ownership is the first step in data classification. The other choices are incorrect. A criticality analysis is required for protection of data, which takes input from data classification. Access definition is complete after data classification and input for a data dictionary is prepared from the data classification process.

Area: 4

340. Which of the following types of transmission media provide the BEST security against unauthorized access?

A. Copper wire
B. Twisted pair

C. Fiber-optic cables
D. Coaxial cables

The correct answer is:
C. Fiber-optic cables

Explanation:
Fiber-optic 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.

Area: 4

341. 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.

The correct answer is:
A. Review the parameter settings.

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 as strong audit evidence as choice A.

Area: 4

342. Which of the following is a concern when data is transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

A. The organization does not have control over encryption.
B. Messages are subjected to wire tapping.
C. Data might not reach the intended recipient.
D. The communication may not be secure.

The correct answer is:
A. The organization does not have control over encryption.

Explanation:
The SSL security protocol provides data encryption, server authentication, message integrity and optional client authentication. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on the SSL capabilities. SSL encrypts the datum while it is being transmitted over the Internet. The encryption is done in the background, without any interaction from the user, consequently there is no password to remember either. The other choices are incorrect. Since the communication between client and server is encrypted, the confidentiality of information is not affected by wire tapping. Since SSL does the client authentication, only the intended recipient will receive the decrypted data. All data sent over an encrypted SSL connection are protected with a mechanism to detect tampering, i.e., automatically determining whether data has been altered in transit.

Area: 4

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.

The correct answer is:
B. interview programmers about the procedures currently being followed.

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.

Area: 4

344. Authentication is the process by which the:

A. system verifies that the user is entitled to input the transaction requested.
B. system verifies the identity of the user.
C. user identifies him/herself to the system.
D. user indicates to the system that the transaction was processed correctly.

The correct answer is:
B. system verifies the identity of the user.

Explanation:
Authentication is the process by which the system verifies the identity of the user. Choice A is not the best answer because authentication refers to verifying who the user is to a security table of users authorized to access the system, not necessarily the functions which the user can perform. Choice C is incorrect because this does not imply that the system has verified the identity of the user. Choice D is not correct because this is an application control for accuracy.

Area: 4

345. If inadequate, which of the following would be the MOST likely contributor to a denial-of-service attack?

A. Router configuration and rules
B. Design of the internal network
C. Updates to the router system software
D. Audit testing and review techniques

The correct answer is:
A. Router configuration and rules

Explanation:
Inadequate router configuration and rules would lead to an exposure to denial-of-service attacks. Choices B and C would be lesser contributors. Choice D is incorrect because audit testing and review techniques are applied after the fact.

Area: 4

346. The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

A. symmetric encryption.
B. message authentication code.
C. hash function.
D. digital signature certificates.

The correct answer is:
A. symmetric encryption.

Explanation:
SSL uses a symmetric key for message encryption. A message authentication code is used for ensuring data integrity. Hash function is used for generating a message digest; it does not use public key encryption for message encryption. Digital signature certificates are used by SSL for server authentication.

Area: 4

347. A dry-pipe fire extinguisher system is a system that uses:

A. water, but in which water does not enter the pipes until a fire has been detected.
B. water, but in which the pipes are coated with special water-tight sealants.
C. carbon dioxide instead of water.
D. halon instead of water.

The correct answer is:
A. water, but in which water does not enter the pipes until a fire has been detected.

Explanation:
The dry-pipe sprinkler is an effective and environmentally friendly method of suppressing fire. Water sprinklers with an automatic power shutoff system can be set to automatic release without threat to life. Sprinklers must be dry-pipe to prevent the risk of leakage. Halon or carbon dioxide are also used to extinguish fire, but are not used through a dry pipe.

Area: 4

348. During the review of a biometrics system operation, the IS auditor should FIRST review the stage of:

A. enrollment.
B. identification.
C. verification.
D. storage.

The correct answer is:
A. enrollment.

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.

Area: 4

349. The PRIMARY goal of a web site certificate is:

A. authentication of the web site that will be surfed.
B. authentication of the user who surfs through that site.
C. preventing surfing of the web site by hackers.
D. the same purpose as that of a digital certificate.

The correct answer is:
A. authentication of the web site that will be surfed.

Explanation:
Authenticating the site to be surfed is the primary goal of a web certificate. Authentication of a user is achieved through passwords and not by a web site certificate. The site certificate does not prevent hacking nor does it authenticate a person.

Area: 4

350. Which of the following provides the framework for designing and developing logical access controls?

A. Information systems security policy
B. Access control lists
C. Password management
D. System configuration files

The correct answer is:
A. Information systems security policy

Explanation:
The information systems security policy developed and approved by the top management in an organization is the basis upon which logical access control is designed and developed. Access control lists, password management and systems configuration files are all tools for implementing the access controls.

Area: 4

351. 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

The correct answer is:
D. Training provided on a regular basis to all current and new employees

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.

Area: 4

352. Which of the following is the 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

The correct answer is:
A. Assimilation of the framework and intent of a written security policy by all appropriate parties

Explanation:
Assimilation of the framework and intent of a written security policy by the users of the systems is critical to the successful implementation and maintenance of security policy. A good password system may exist, but if the users of the system keep passwords written on his/her table, the password system 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 also are required along with the user's education on the importance of security.

Area: 4

353. IS auditors, in performing detailed network assessments and access control reviews, should FIRST:

A. determine the points of entry.
B. evaluate users' access authorization.
C. assess users' identification and authorization.
D. evaluate the domain-controlling server configuration.

The correct answer is:
A. determine the points of entry.

Explanation:
In performing detailed network assessments and access control reviews, IS auditors should first determine the points of entry to the system and accordingly review the points of entry for appropriate controls. Evaluation of user access authorization, assessment of user identification and authorization, and evaluation of the domain-controlling server configuration are all implementation issues for appropriate controls for the points of entry.

Area: 4

354. A hacker could obtain passwords without the use of computer tools or programs through the technique of:

A. social engineering.
B. sniffers.
C. backdoors.
D. Trojan horses.

The correct answer is:
A. social engineering.

Explanation:
Social engineering is based on the divulgence of private information through dialogues, interviews, inquiries, etc., in which a user may be indiscreet regarding his/her or other's personal data. A sniffer is a computer tool to monitor the traffic in networks. Backdoors are computer programs left by hackers to exploit vulnerabilities. Trojan horses are computer programs that pretend to supplant a real program; thus, the functionality of the program is not authorized and is usually malicious in nature.

Area: 4

355. The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:

A. searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.
B. and penetration tests are different names for the same activity.
C. is executed by automated tools, whereas penetration testing is a totally manual process.
D. is executed by commercial tools, whereas penetration testing is executed by public processes.

The correct answer is:
A. searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.

Explanation:
The objective of a vulnerability assessment is to find the security holds in the computers and elements analyzed and its intent is not to damage the infrastructure. The intent of penetration testing is to imitate a hacker's activities and determine how far they could go into the network. They are not the same; they have different approaches. Vulnerability assessments and penetration testing can be executed by automated or manual tools or processes and can be executed by commercial or free tools.

Area: 4

356. The most common problem in the operation of an intrusion detection system (IDS) is:

A. the detection of false positives.
B. receiving trap messages.
C. reject-error rates.
D. denial-of-service attacks.

The correct answer is:
A. the detection of false positives.

Explanation:
Because of the configuration and the way IDS technology operates, the main problem in operating IDSs is the recognition (detection) of events that are not really security incidents-false

positives (equivalent of a false alarm). The IS auditor needs to be aware of this and should check for implementation of related controls, such as IDS tuning, incident handling procedures (such as the screening process to know if an event is a security incident or a false positive). Trap messages are generated by the Simple Network Management Protocol (SNMP) agents when an important event happens, but are not particularly related to security or IDSs. Reject-error rate is related to biometric technology and is not related to IDSs. Denial of service is a type of attack and is not a problem in the operation of IDSs.

Area: 4

357. Which of the following provides nonrepudiation services for e-commerce transactions?

A. Public key infrastructure (PKI)
B. Data encryption standard (DES)
C. Message authentication code (MAC)
D. Personal identification number (PIN)

The correct answer is:
A. Public key infrastructure (PKI)

Explanation:
PKI is the administrative infrastructure for digital certificates and encryption key pairs. The qualities of an acceptable digital signature are: it is unique to the person using it, it is capable of verification, it is under the sole control of the person using it, and it is linked to data in such a manner that if data are changed, the digital signature is invalidated. PKI meets these tests. The data encryption standard (DES) is the most common private key cryptographic system. DES does not address nonrepudiation. A MAC is a cryptographic value calculated by passing an entire message through a cipher system. The sender attaches the MAC before transmission and the receiver recalculates the MAC and compares it to the sent MAC. If the two MACs are not equal, this indicates that the message has been altered during transmission. It has nothing to do with nonrepudiation. A PIN is a type of password, a secret number assigned to an individual that, in conjunction with some other means of identification, serves to verify the authenticity of the individual.

Area: 4

358. The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:

A. only the sender and receiver are able to encrypt/decrypt the data.
B. the sender and receiver can authenticate their respective identities.
C. the alteration of transmitted data can be detected.
D. the ability to identify the sender by generating a one time session key.

The correct answer is:
A. only the sender and receiver are able to encrypt/decrypt the data.

Explanation:
SSL generates a session key used to encrypt/decrypt the transmitted data, thus ensuring its confidentiality. Although SSL allows the exchange of X509 certificates to provide for identification and authentication, this feature along with choices C and D are not the primary objectives.

Area: 4

359. The role of the CA (certification authority) 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.

The correct answer is:
D. confirm the identity of the entity owning a certificate issued by that CA.

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.

Area: 4

360. 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.

The correct answer is:
B. Both fire suppression systems present a risk of suffocation when used in a closed room.

Explanation:
Protecting people's life should always be of highest priority in fire suppression activities. CO2 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 CO2 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.

Area: 4

361. Which of the following would be the BEST access control procedure?

A. The data owner formally authorizes access and an administrator implements the user authorization tables.
B. Authorized staff implement the user authorization tables and the data owner sanctions them.
C. The data owner and an IS manager jointly create and update the user authorization tables.
D. The data owner creates and updates the user authorization tables.

The correct answer is:
A. The data owner formally authorizes access and an administrator implements the user authorization tables.

Explanation:
The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedure for authorizing access.

Area: 4

362. Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

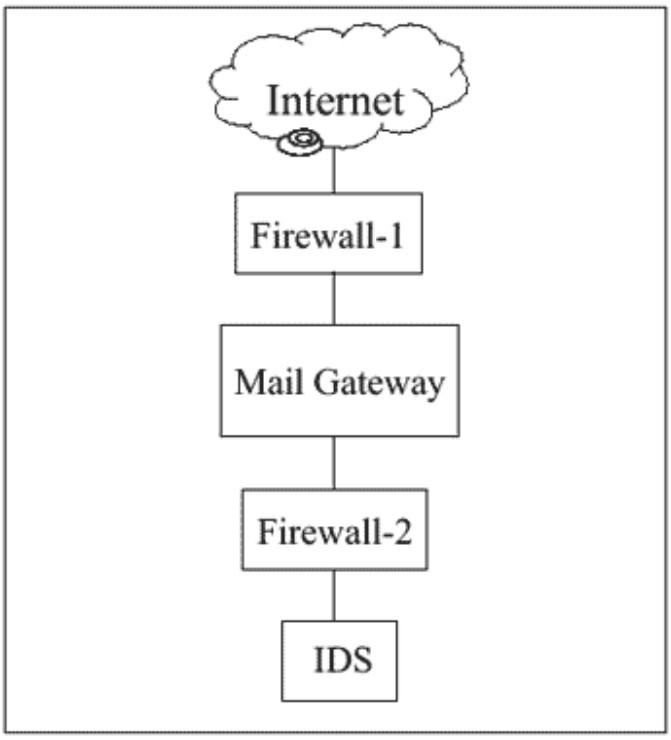
A. The buyer is assured that neither the merchant nor any other party can misuse his/her credit card data.
B. All personal SET certificates are stored securely in the buyer's computer.
C. The buyer is liable for any transaction involving his/her personal SET certificates.
D. The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

The correct answer is:
C. The buyer is liable for any transaction involving his/her personal SET certificates.

Explanation:
The usual agreement between the credit card issuer and the card holder stipulates that the card holder assumes responsibility for any use of his/her 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 his/her credit card data, he/she will have to handle the wallet software.

Area: 4

363. This question refers to the following diagram.



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.

The correct answer is:
C. close firewall-2.

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 be 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.

Area: 4

364. Which of the following is an operating system access control function?

A. Logging user activities
B. Logging data communication access activities
C. Verifying user authorization at the field level
D. Changing data files

The correct answer is:
A. Logging user activities

Explanation:
General operating system access control functions include log user activities, log events, etc. Choice B is a network control feature. Choices C and D are database- and/or application-level access control functions.

Area: 4

365. Which of the following would MOST effectively reduce social engineering incidents?

A. Security awareness training
B. Increased physical security measures
C. E-mail monitoring policy
D. Intrusion detection systems

The correct answer is:
A. Security awareness training

Explanation:
Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the intrusion. An e-mail monitoring policy informs users that all e-mail in the organization is subject to monitoring. It does not protect the users from potential security incidents and intruders. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

Area: 4

366. An accuracy measure for a biometric system is:

A. system response time.
B. registration time.
C. input file size.
D. false-acceptance rate.

The correct answer is:
D. false-acceptance rate.

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.

Area: 4

367. 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.

The correct answer is:
C. The risk that the honeypot could be used to launch further attacks on the organization's infrastructure.

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.

Area: 4

368. An information security policy stating that "the display of passwords must be masked or suppressed" addresses which of the following attack methods?

A. Piggybacking
B. Dumpster diving
C. Shoulder surfing
D. Impersonation

The correct answer is:
C. Shoulder surfing

Explanation:
If a password is displayed on a monitor, any person nearby could "look over the shoulder" of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to "the display of passwords." If the policy referred to "the display and printing of

passwords" then it would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information). Impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

Area: 4

369. Which of the following should be a concern to an IS auditor reviewing a wireless network?

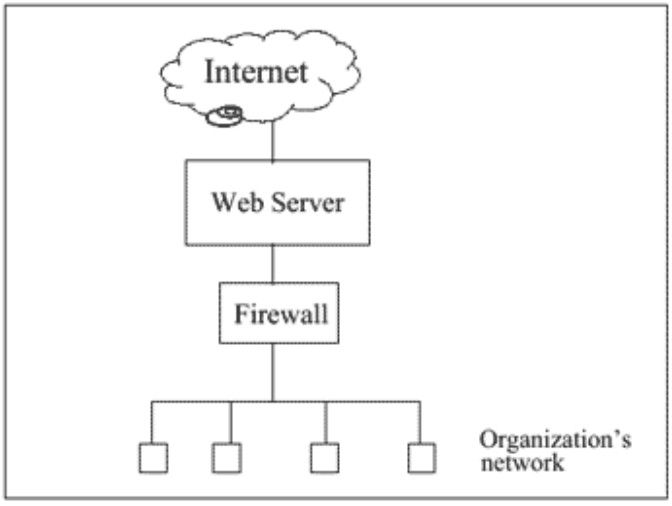
A. 128-bit-static-key WEP (Wired Equivalent Privacy) encryption is enabled.
B. SSID (Service Set IDentifier) broadcasting has been enabled.
C. Antivirus software has been installed in all wireless clients.
D. MAC (Media Access Control) access control filtering has been deployed.

The correct answer is:
B. SSID (Service Set IDentifier) broadcasting has been enabled.

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.

Area: 4

370. This question refers to the following diagram.



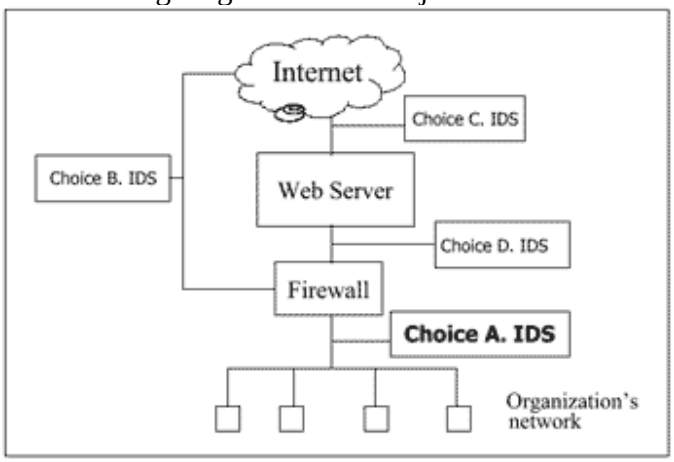
To detect attack attempts that the firewall is unable to recognize, the IS auditor should recommend placing a network intrusion detection system (IDS) between the:

A. firewall and the organization's network.
B. Internet and the firewall.

C. Internet and the web server.
D. web server and the firewall.

The correct answer is:
A. firewall and the organization's network.

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.
The following diagram shows the justification for this question.



Area: 4

371. 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

The correct answer is:
C. Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key

Explanation:
To ensure authenticity and confidentiality, a message must be encrypted twice-first with the sender's private key and second 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.

Area: 4

372. An efficient use of PKI should encrypt the:

A. entire message.
B. private key.
C. public key.
D. symmetric session key.

The correct answer is:
D. symmetric session key.

Explanation:
Public key (asymmetric) cryptographic systems require larger keys (1024 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.

Area: 4

373. 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

The correct answer is:
B. AES

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.

Area: 4

374. An IS auditor is PRIMARILY concerned about electromagnetic emissions from a cathode ray tube (CRT) because they may:

A. cause health disorders (such as headaches) and diseases.
B. be intercepted and information may be obtained from them.
C. cause interference in communications.
D. cause errors in the motherboard.

The correct answer is:
B. be intercepted and information may be obtained from them.

Explanation:
The greatest risk, although infrequent, due to the expensive technology required is choice B. The expense would be justified only if the value of the information to be obtained was high. CRTs can be intercepted, and information obtained can be from them. This is called a Tempest attack, taken from the code name of the first secret project in which such an interception was studied. These weak signals can be radiated and intercepted with the proper equipment or transmitted, for example, via power leads. The signals fade rapidly as distance increases. The first line of defense is to create a physical security zone (PSZ) to keep receivers at a distance. They can cause health disorders, such as headaches and diseases; however, no studies have confirmed that these risks are higher than those posed by the natural radiation found in certain zones (e.g., mountain areas). The intensity of the radiation is so low that, with normal technology, they can not cause interference with communications.

Area: 4

375. To ensure compliance with the security policy requirement that passwords be a combination of letters and numbers, the IS auditor should recommend that:

A. the company policy be changed.
B. passwords be periodically changed.
C. an automated password management tool be used.
D. security awareness training be delivered.

The correct answer is:
C. an automated password management tool be used.

Explanation:
The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing his/her old password for a designated period of time. Choices A, B and D do not enforce compliance.

Area: 4

376. 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

The correct answer is:
D. SSID (service set identifier) broadcasting

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.

Area: 4

377. An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

A. more than one individual can claim to be a specific user.
B. there is no way to limit the functions assigned to users.
C. user accounts can be shared.
D. users have a need-to-know privilege.

The correct answer is:
B. there is no way to limit the functions assigned to users.

Explanation:
Without an appropriate authorization process, it will be impossible to establish functional limits and accountability. The risk that more than one individual can claim to be a specific user is associated with the authentication processes, rather than with authorization. The risk that user accounts can be shared is associated with identification processes, rather than with authorization. The need-to-know basis is the best approach to assigning privileges during the authorization process.

Area: 4

378. 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

The correct answer is:
C. Web of trust

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. 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.

Area: 4

379. An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

A. Digitalized signatures
B. Hashing

C. Parsing
D. Steganography

The correct answer is:
D. Steganography

Explanation:
Steganography is a technique for concealing the existence of messages or information. An increasingly important steganographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes, and it is widely applied in the design of programming languages or in data entry editing.

Area: 4

380. Which of the following is the MOST important action in recovering from a cyberattack?

A. Creation of an incident response team
B. Use of cyberforensic investigators
C. Execution of a business continuity plan
D. Filing an insurance claim

The correct answer is:
C. Execution of a business continuity plan

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, cyberforensics 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.

Area: 4

381. 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

The correct answer is:
C. War driving

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 user's passwords by trying combinations and dictionary words.

Area: 4

382. The information security policy that states "each individual must have their badge read at every controlled door" addresses which of the following attack methods?

A. Piggybacking
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

The correct answer is:
A. Piggybacking

Explanation:
Piggybacking refers to unauthorized persons, following authorized persons, either physically or virtually, into restricted areas. This policy addresses the "polite behavior" problem of holding doors open for a stranger. If every employee must have his/her badge read at every controlled door no unauthorized person could enter the sensitive area. Looking over the shoulder of a user to obtain sensitive information, could be done by an unauthorized person, who has gained access to areas using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter. Therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and

piggybacking, but this information security policy does not address the impersonation attack.

Area: 4

383. After completing the business impact analysis (BIA) which of the following 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.

The correct answer is:
C. Develop recovery strategies.

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.

Area: 5

384. A structured walk-through test of a disaster recovery plan involves:

A. representatives from each of the functional areas coming together to go over the plan.
B. all employees who participate in the day-to-day operations coming together to practice executing the plan.
C. moving the systems to the alternate processing site and performing processing operations.
D. distributing copies of the plan to the various functional areas for review.

The correct answer is:
A. representatives from each of the functional areas coming together to go over the plan.

Explanation:
A structured walk-through test of a disaster recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete and can be implemented when required. Choice B is a simulation test to prepare and train the personnel who will be required to respond to disasters and disruptions. Choice C is a form of parallel testing to ensure that critical systems will perform satisfactorily in the alternate site. Choice D is a checklist test.

Area: 5

385. 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

The correct answer is:
B. Paper

Explanation:
A paper test is appropriate for testing a BCP. It is a walk-through 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.

Area: 5

386. In a contract with a hot, warm or cold site, contractual provisions should cover which of the following considerations?

A. Physical security measures
B. Total number of subscribers
C. Number of subscribers permitted to use a site at one time
D. References by other users

The correct answer is:
C. Number of subscribers permitted to use a site at one time

Explanation:
The contract should specify the number of subscribers permitted to use the site at any one time. Physical security measures are not a part of the contract, although they are an important consideration when choosing a third-party site. The total number of subscribers is not a consideration; what is important is whether the agreement limits the number of subscribers in a building or in a specific area. The references that other users can provide is a consideration taken before signing the contract, it is by no means part of the contractual provisions.

Area: 5

387. An IS auditor evaluating the resilience of a high-availability network would 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.

The correct answer is:
B. the network servers are clustered in a site.

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 backups if a site has been destroyed. A hot site would also be a good alternative for a single-point-of-failure site.

Area: 5

388. Which of the following is the GREATEST concern when an organization's backup facility is at a warm site?

A. Timely availability of hardware
B. Availability of heat, humidity and air conditioning equipment
C. Adequacy of electrical power connections
D. Effectiveness of the telecommunications network

The correct answer is:
A. Timely availability of hardware

Explanation:
A warm site has the basic infrastructure facilities, such as power, air conditioning and networking, implemented but is normally lacking computing equipment. Therefore, the availability of hardware becomes a primary concern.

Area: 5

389. 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

The correct answer is:
B. Absence of a backup for the network backbone

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.

Area: 5

390. Which of the following recovery strategies is MOST appropriate for a business having multiple offices within a region and a limited recovery budget?

A. A hot site maintained by the business
B. A commercial cold site
C. Reciprocal arrangement between its offices
D. A third-party hot site

The correct answer is:
C. Reciprocal arrangement between its offices

Explanation:
For a business having many offices within a region, a reciprocal arrangement among its offices would be most appropriate. Each office could be designated as a recovery site for some other office. This would be the least expensive approach to providing an acceptable level of confidence. A hot site maintained by the business would be a costly solution but would provide a high degree of confidence. Multiple cold sites leased for the multiple offices would lead to a costly solution with a high degree of confidence. A third-party facility for recovery is provided by a traditional hot site. This would be a costly approach providing a high degree of confidence.

Area: 5

391. The PRIMARY purpose of implementing Redundent Array of Inexpensive Disks (RAID) level 1 in a file server is to:

A. achieve performance improvement.
B. provide user authentication.
C. ensure availability of data.
D. ensure the confidentiality of data.

The correct answer is:
C. ensure availability of data.

Explanation:
RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk. If disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication and does nothing to provide for data confidentiality.

Area: 5

392. The PRIMARY purpose of a business impact analysis (BIA) is to:

A. provide a plan for resuming operations after a disaster.
B. identify the events that could impact the continuity of an organization's operations.
C. publicize the commitment of the organization to physical and logical security.
D. provide the framework for an effective disaster recovery plan (DRP).

The correct answer is:
B. identify the events that could impact the continuity of an organization's operations.

Explanation:
A business impact analysis (BIA) is one of the key steps in the development of a business continuity plan (BCP). A BIA will identify the diverse events that could impact the continuity of the operations of an organization.

Area: 5

393. 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

The correct answer is:
C. Critical business processes for ascertaining the priority for recovery

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.

Area: 5

394. Which of the following would not prevent the loss of an asset but would assist in recovery by transferring part of the risk to a third party?

A. Full system backups
B. Insurance
C. Testing
D. Business impact analysis (BIA)

The correct answer is:
B. Insurance

Explanation:
Insurance assists by involving a third party in sharing the risks. In case of the destruction of an asset, the third party would compensate for the loss based on the contract. This would assist in reinstating the asset to the predisaster condition. A BIA is the first step in developing a business continuity plan. This step would assist in the classification of assets based on risk and would not assist in either preventing a disaster or reinstating an asset to a predisaster condition. Backups would assist in recovering a system in case of a disaster but do not necessarily involve a third party. Testing the plan would help to ensure that the business continuity plan works as intended, but testing would not reinstate an asset to a predisaster condition.

Area: 5

395. Which of the following would contribute MOST to an effective business continuity plan (BCP)? The BCP:

A. document is circulated to all interested parties.
B. planning involves all user departments.
C. is approved by senior management.
D. is audited by an external IS auditor.

The correct answer is:
B. planning involves all user departments.

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.

Area: 5

396. After implementation of a disaster recovery plan (DRP), predisaster and post-disaster operational cost for an organization will:

A. decrease.
B. not change (remain the same).
C. increase.
D. increase or decrease depending upon the nature of the business.

The correct answer is:
C. increase.

Explanation:
There are costs associated with all activities and DRP is not an exception. Although there are costs associated with a DRP, there are unknown costs that are incurred if a DRP is not implemented.

Area: 5

397. Which of the following is the MOST important criterion for the selection of a location for an offsite storage facility for IS backup files? The offsite facility must be:

A. physically separated from the data center and not subject to the same risks.
B. given the same level of protection as that of the computer data center.
C. outsourced to a reliable third party.
D. equipped with surveillance capabilities.

The correct answer is:
A. physically separated from the data center and not subject to the same risks.

Explanation:
It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

Area: 5

398. The FIRST step in developing a business continuity plan (BCP) is to:

A. classify the importance of systems.
B. establish a disaster recovery strategy.
C. determine the critical recovery time period.
D. perform a risk ranking.

The correct answer is:
A. classify the importance of systems.

Explanation:
Determining the classification of systems is the foremost step in a BCP exercise. Without determining the classification of the systems, the other steps cannot be performed. Choices B, C and D are carried out later in the process.

Area: 5

399. 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

The correct answer is:
C. Business impact analysis (BIA)

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.

Area: 5

400. Which of the following is the MOST reasonable option for recovering a noncritical system?

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

The correct answer is:
D. Cold site

Explanation:
Generally a cold site is contracted for a longer period at a lower cost. Since it requires more time to make a cold site operational, it is generally used for noncritical applications. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations. A mobile site is a vehicle ready with all necessary computer equipment, and it can be moved to any cold or warm site depending upon the need. The need for a mobile site depends upon the scale of operations and a hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.

Area: 5

401. 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

The correct answer is:
B. Preparedness test

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 DRP 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 DRP test and is used in software maintenance.

Area: 5

402. If a database is restored using before-image dumps, where should the process be started following an interruption?

A. Before the last transaction
B. After the last transaction
C. As the first transaction after the latest checkpoint
D. As the last transaction before the latest checkpoint

The correct answer is:
A. Before the last transaction

Explanation:
If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

Area: 5

403. In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

A. Maintaining system software parameters
B. Ensuring periodic dumps of transaction logs
C. Ensuring grandfather-father-son file backups
D. Maintaining important data at an offsite location

The correct answer is:
B. Ensuring periodic dumps of transaction logs

Explanation:
Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historical data. The volume of activity usually associated with an online system makes other more traditional methods of backup impractical.

Area: 5

404. As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following are necessary to restore these files?

A. The previous day's backup file and the current transaction tape
B. The previous day's transaction file and the current transaction tape
C. The current transaction tape and the current hard copy transaction log
D. The current hard copy transaction log and the previous day's transaction file

The correct answer is:
A. The previous day's backup file and the current transaction tape

Explanation:
The previous day's backup will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

Area: 5

405. An organization's disaster recovery plan should address early recovery of:

A. all information systems processes.
B. all financial processing applications.
C. only those applications designated by the IS manager.
D. processing in priority order, as defined by business management.

The correct answer is:
D. processing in priority order, as defined by business management.

Explanation:
Business management should know which systems are critical and when they need to process well in advance of a disaster. It is management's responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organizations that exist for the purpose of assisting the general user management in successfully performing their jobs.

Area: 5

406. An offsite information processing facility:

A. should have the same amount of physical access restrictions as the primary processing site.
B. should be easily identified from the outside so that, in the event of an emergency, it can be easily found.
C. should be located in proximity to the originating site, so it can quickly be made operational.
D. need not have the same level of environmental monitoring as the originating site.

The correct answer is:
A. should have the same amount of physical access restrictions as the primary processing site.

Explanation:
An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity of the original site, and the offsite facility should possess the same level of environmental monitoring and control as the originating site.

Area: 5

407. An advantage of the use of hot sites as a backup alternative is that:

A. the costs associated with hot sites are low.
B. hot sites can be used for an extended amount of time.
C. hot sites can be made ready for operation within a short period of time.
D. they do not require that equipment and systems software be compatible with the primary site.

The correct answer is:
C. hot sites can be made ready for operation within a short period of time.

Explanation:
Hot sites can be made ready for operation normally within hours. However, the use of hot sites is expensive, should not be considered as a long-term solution, and does require that equipment and systems software be compatible with the primary installation being backed up.

Area: 5

408. Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?

A. Invite client participation.
B. Involve all technical staff.
C. Rotate recovery managers.
D. Install locally stored backup.

The correct answer is:
C. Rotate recovery managers.

Explanation:
Recovery managers should be rotated to ensure the experience of the recovery plan is spread among the managers. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or offsite backup should always be used.

Area: 5

409. An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

A. adequate fire insurance exists.
B. regular hardware maintenance is performed.
C. offsite storage of transaction and master files exists.
D. backup processing facilities are fully tested.

The correct answer is:
C. offsite storage of transaction and master files exists.

Explanation:
Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

Area: 5

410. Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

A. Reviewing program code
B. Reviewing operations documentation
C. Turning off the UPS, then the power
D. Reviewing program documentation

The correct answer is:
B. Reviewing operations documentation

Explanation:
Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

Area: 5

411. A company performs full backup of data and programs on a regular basis. The primary purpose of this practice is to:

A. maintain data integrity in the applications.
B. restore application processing after a disruption.
C. prevent unauthorized changes to programs and data.
D. ensure recovery of data processing in case of a disaster.

The correct answer is:
B. restore application processing after a disruption.

Explanation:
Backup procedures are designed to restore programs and data to a previous state prior to computer or system disruption. These backup procedures merely copy data and do not test or validate integrity. Backup procedures will also not prevent changes to program and data. On the contrary, changes will simply be copied. Although backup procedures are a necessary part of the recovery process following a disaster, they are not sufficient in themselves.

Area: 5

412. Disaster recovery planning addresses the:

A. technological aspect of business continuity planning.
B. operational piece of business continuity planning.
C. functional aspect of business continuity planning.
D. overall coordination of business continuity planning.

The correct answer is:
A. technological aspect of business continuity planning.

Explanation:
Disaster recovery planning is the technological aspect of business continuity planning. Business resumption planning addresses the operational part of business continuity planning.

Area: 5

413. This question refers to the following information.
An IS auditor conducting a review of disaster recovery planning at a financial processing organization has discovered the following:

- **The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.**
- **The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his/her attention.**
- **The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.**

The IS auditor's report should recommend that:
A. the deputy CEO is censured for his/her failure to approve the plan.
B. a board of senior managers is set up to review the existing plan.
C. the existing plan is approved and circulated to all key management and staff.
D. a manager coordinates the creation of a new or revised plan within a defined time limit.

The correct answer is:
D. a manager coordinates the creation of a new or revised plan within a defined time limit.

Explanation:
The primary concern is to establish a workable disaster recovery plan, which reflects current processing volumes to protect the organization from any disruptive incident. Censuring the deputy CEO will not achieve this and is generally not within the scope of an IS auditor to recommend. Establishing a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short timescale is to make an experienced manager responsible for coordinating the knowledge of other managers into a single, formal document within a defined time limit.

Area: 5

414. This question refers to the following information.
An IS auditor conducting a review of disaster recovery planning at a financial processing organization has discovered the following:

- **The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.**
- **The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his/her attention.**
- **The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.**

The basis of an organization's disaster recovery plan is to reestablish live processing at an alternative site where a similar, but not identical, hardware configuration is already established. The IS auditor should:
A. take no action as the lack of a current plan is the only significant finding.
B. recommend that the hardware configuration at each site is identical.
C. perform a review to verify that the second configuration can support live processing.
D. report that the financial expenditure on the alternative site is wasted without an effective plan.

The correct answer is:
C. perform a review to verify that the second configuration can support live processing.

Explanation:
The IS auditor does not have a finding unless it can be shown that the alternative hardware cannot support the live processing system. Even though the primary finding is the lack of a proven and communicated disaster recovery plan, it is essential that this aspect of recovery is included in the audit. If it is found to be inadequate, the finding will materially support the overall audit opinion. It is certainly not appropriate to take no action at all, leaving this important factor untested, and unless it is shown that the alternative site is inadequate, there can be no comment on the expenditure (even if this is considered a proper comment for the IS auditor to make). Similarly, there is no need for the configurations to be identical. The alternative site could actually exceed the recovery requirements if it is also used for other work, such as other processing or systems development and testing. The only proper course of action at this point would be to find out if the recovery site can actually cope with a recovery.

Area: 5

415. Which of the following processes is the FIRST step in developing a business continuity and disaster recovery plan for an organization?

A. Alternate site selection
B. Business impact analysis
C. Test procedures and frequency
D. Information classification

The correct answer is:
B. Business impact analysis

Explanation:
All four processes are essential for developing the business continuity plan; however, a business impact analysis is the first process used to determine the impact of a disaster on the business operations. Information classification helps to determine the priorities of application recovery while recovering from a disaster event. Alternate site requirements are decided and the site is selected based on the business impact analysis and recovery priorities. The testing of the plan is completed after the above processes are complete.

Area: 5

416. Disaster recovery planning for a company's computer system usually focuses on:

A. operations turnover procedures.
B. strategic long-range planning.
C. the probability that a disaster will occur.
D. alternative procedures to process transactions.

The correct answer is:
D. alternative procedures to process transactions.

Explanation:
It is important that disaster recovery identifies alternative processes that can be put in place while the system is not available.

Area: 5

417. Of the following, the MAIN purpose for periodically testing offsite facilities is to:

A. ensure the integrity of the data in the database.
B. eliminate the need to develop detailed contingency plans.
C. ensure the continued compatibility of the contingency facilities.
D. ensure that program and system documentation remains current.

The correct answer is:
C. ensure the continued compatibility of the contingency facilities.

Explanation:
The main purpose of offsite hardware testing is to ensure the continued compatibility of the contingency facilities. Specific software tools are available to ensure the ongoing integrity of the database. Contingency plans should not be eliminated and program and system documentation should be reviewed continuously for currency.

Area: 5

418. A large chain of shops with electronic funds transfer (EFT) at point-of-sale devices has a central communications processor for connecting to the banking network. Which of the following is the BEST disaster recovery plan for the communications processor?

A. Offsite storage of daily backups
B. Alternative standby processor onsite
C. Installation of duplex communication links
D. Alternative standby processor at another network node

The correct answer is:
D. Alternative standby processor at another network node

Explanation:
Having an alternative standby processor at another network node would be the best. The unavailability of the central communications processor would disrupt all access to the banking network, resulting in the disruption of operations for all of the shops. This could be caused by failure of equipment, power or communications. Offsite storage of backups would not help, since EFT tends to be an online process and offsite storage will not replace the dysfunctional processor. The provision of an alternate processor onsite would be fine if it were an equipment problem, but would not help if the outage were caused by power, for example. Installation of duplex communication links would be most appropriate if it were only the communication link that failed.

Area: 5

419. Facilitating telecommunications continuity by providing redundant combinations of local carrier T-1 lines, microwaves and/or coaxial cables to access the local communication loop is:

A. last-mile circuit protection.
B. long-haul network diversity.

C. diverse routing.
D. alternative routing.

The correct answer is:
A. last-mile circuit protection.

Explanation:
The method of providing telecommunication continuity through the use of many recovery facilities, providing redundant combinations of local carrier T-1s, microwave and/or coaxial cable to access the local communication loop in the event of a disaster, is called last-mile circuit protection. Providing diverse longdistance network availability utilizing T-1 circuits among major long-distance carriers is called long-haul network diversity. This ensures long-distance access should any one carrier experience a network failure. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics.

Area: 5

420. 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 is contracted for 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.

The correct answer is:
D. Media backups are performed on a timely basis and stored offsite.

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.

Area: 5

421. Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

A. Developments may result in hardware and software incompatibility.
B. Resources may not be available when needed.

C. The recovery plan cannot be tested.
D. The security infrastructures in each company may be different.

The correct answer is:
A. Developments may result in hardware and software incompatibility.

Explanation:
If one organization updates its hardware and software configuration, it may mean that it is no longer compatible with the systems of the other party in the agreement. This may mean that each company is unable to use the facilities at the other company to recover their processing following a disaster. Resources being unavailable when needed are an intrinsic risk in any reciprocal agreement, but this is a contractual matter and is not the greatest risk. The plan can be tested by paper-based walk-throughs and, possibly, by agreement between the companies. The difference in security infrastructures, while a risk, is not insurmountable.

Area: 5

422. The PRIMARY objective of a business continuity and disaster recovery plan 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.

The correct answer is:
D. protect human life.

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.

Area: 5

423. Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization?

A. Built-in alternative routing
B. Completing full system backup daily
C. A repair contract with a service provider
D. A duplicate machine alongside each server

The correct answer is:
A. Built-in alternative routing

Explanation:
Alternative routing would ensure the network would continue if a server is lost or if a link is severed as message rerouting could be automatic. System backup will not afford immediate protection. The repair contract is not as effective as permanent alternative routing. Standby servers will not provide continuity if a link is severed.

Area: 5

424. An IS auditor reviewing an organization's IS disaster recovery plan should verify that it is:

A. tested every six months.
B. regularly reviewed and updated.
C. approved by the chief executive officer (CEO).
D. communicated to every departmental head in the organization.

The correct answer is:
B. regularly reviewed and updated.

Explanation:
The plan should be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel. Otherwise, it may become out of date and may no longer be effective. The plan must be subjected to regular testing, but the period between tests will again depend on the nature of the organization and the relative importance of IS. Three months or even annually may be appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan. Similarly, although a business continuity plan is likely to be circulated throughout an organization, the IS disaster recovery plan will usually be a technical document and only relevant to IS and communications staff .

Area: 5

425. There are several methods of providing telecommunications continuity. The method of routing traffic through split cable or duplicate cable facilities is:

A. alternative routing.
B. diverse routing.

C. long-haul network diversity.
D. last-mile circuit protection.

The correct answer is:
B. diverse routing.

Explanation:
Diverse routing routes traffic through split-cable facilities or duplicate-cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual-entrance facilities. This type of access is timeconsuming and costly. Alternative routing is a method of routing information via an alternate medium, such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Long-haul network diversity is a diverse, long-distance network utilizing T-1 circuits among the major long-distance carriers. It ensures long-distance access should any carrier experience a network failure. Last-mile circuit protection is a redundant combination of local carrier T-1s, microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local-carrier routing is also utilized.

Area: 5

426. After a full operational contingency test, the IS auditor performs a review of the recovery steps. He 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.

The correct answer is:
A. Perform an integral review of the recovery tasks.

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.

Area: 5

427. Which of the following is MOST important to provide for in a disaster recovery plan?

A. Backup of compiled object programs
B. Reciprocal processing agreement
C. Phone contact list
D. Supply of special forms

The correct answer is:
A. Backup of compiled object programs

Explanation:
Of the choices, a backup of compiled object programs is the most important in a successful recovery. A reciprocal processing agreement is not as important, because alternative equipment can be found after a disaster occurs. A phone contact list may aid in the immediate aftermath, as would an accessible supply of special forms, but neither is as important as having access to required programs.

Area: 5

428. The responsibilities of a disaster recovery relocation team include:

A. obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule.
B. locating a recovery site, if one has not been predetermined, and coordinating the transport of company employees to the recovery site.
C. managing the relocation project and conducting a more detailed assessment of the damage to the facilities and equipment.
D. coordinating the process of moving from the hot site to a new location or to the restored original location.

The correct answer is:
D. coordinating the process of moving from the hot site to a new location or to the restored original location.

Explanation:
Choice A describes an offsite storage team, choice B defines a transportation team and choice C defines a salvage team

Area: 5

429. While reviewing the business continuity plan of an organization, the IS auditor observed that the organization's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?

A. Deterrence
B. Mitigation
C. Recovery
D. Response

The correct answer is:
B. Mitigation

Explanation:
An effective business continuity plan includes steps to mitigate the effects of a disaster. Files must be restored on a timely basis for a backup plan to be effective. An example of deterrence is when a plan includes installation of firewalls for information systems. An example of recovery is when a plan includes an organization's hot site to restore normal business operations.

Area: 5

430. Which of the following disaster recovery/continuity plan components provides the GREATEST assurance of recovery after a disaster?

A. The alternate facility will be available until the original information processing facility is restored.
B. User management is involved in the identification of critical systems and their associated critical recovery times.
C. Copies of the plan are kept at the homes of key decision-making personnel.
D. Feedback is provided to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

The correct answer is:
A. The alternate facility will be available until the original information processing facility is restored.

Explanation:
The alternate facility should be made available until the original site is restored to provide the greatest assurance of recovery after a disaster. Without this assurance, the plan will not be successful. All other choices ensure prioritization or the execution of the plan.

Area: 5

431. Which of the following must exist to ensure the viability of a duplicate information processing facility?

A. The site is near the primary site to ensure quick and efficient recovery.
B. The site contains the most advanced hardware available.
C. The workload of the primary site is monitored to ensure adequate backup is available.
D. The hardware is tested when it is installed to ensure it is working properly.

The correct answer is:
C. The workload of the primary site is monitored to ensure adequate backup is available.

Explanation:
Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need. Testing the hardware when the site is established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.

Area: 5

432. Which of the following is a continuity plan test that uses actual resources to simulate a system crash to costeffectively obtain evidence about the plan's effectiveness?

A. Paper test
B. Post test
C. Preparedness test
D. Walk-through

The correct answer is:
C. Preparedness test

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 walk-through 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 walk-through is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

Area: 5

433. An offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

A. cold site.
B. warm site.
C. dial-up site.
D. duplicate processing facility.

The correct answer is:
A. cold site.

Explanation:
A cold site is ready to receive equipment but does not offer any components at the site in advance of the need. A warm site is an offsite backup facility that is partially configured with network connections and selected peripheral equipment, such as disk and tape units, controllers and CPUs, to operate an information processing facility. A duplicate information processing facility is a dedicated, self-developed recovery site that can back up critical applications.

Area: 5

434. 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.

The correct answer is:
A. shadow file processing.

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.

Area: 5

435. Which of the following findings would an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

A. There are three individuals with a key to enter the area.
B. Paper documents are also stored in the offsite vault.
C. Data files that are stored in the vault are synchronized.
D. The offsite vault is located in a separate facility.

The correct answer is:
C. Data files that are stored in the vault are synchronized.

Explanation:
Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because the IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

Area: 5

436. A disaster recovery plan (DRP) for an organization should:

A. reduce the length of the recovery time and the cost of recovery.
B. increase the length of the recovery time and the cost of recovery.
C. reduce the duration of the recovery time and increase the cost of recovery.
D. not affect the recovery time nor the cost of recovery.

The correct answer is:
A. reduce the length of the recovery time and the cost of recovery.

Explanation:

One of the objectives of a DRP is to reduce both the duration and cost of recovering from a disaster. DRP would increase the cost of operations before and after the disaster occurs, but should reduce the time to return to normal operations and the cost that could result from a disaster.

Area: 5

437. 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 DRP.
D. Update the IS assets inventory.

The correct answer is:
D. Update the IS assets inventory.

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.

Area: 5

438. A disaster recovery plan (DRP) for an organization's financial system specifies that the recovery point objective (RPO) is no data loss and the recovery time objective (RTO) is 72 hours. Which of the following is the MOST cost-effective solution?

A. A hot site that can be operational in eight hours with asynchronous backup of the transaction logs
B. Distributed database systems in multiple locations updated asynchronously
C. Synchronous updates of the data and standby active systems in a hot site
D. Synchronous remote copy of the data in a warm site that can be operational in 48 hours

The correct answer is:
D. Synchronous remote copy of the data in a warm site that can be operational in 48 hours

Explanation:
The synchronous copy of the storage achieves the RPO objective and a warm site operational in 48 hours meets the required RTO. Asynchronous updates of the database in distributed locations

do not meet the RPO. Synchronous updates of the data and standby active systems in a hot site meet the RPO and RTO requirements but are more costly than a warm site solution.

Area: 5

439. When developing a backup strategy the FIRST step is to:

A. identify the data.
B. select the storage location.
C. specify the storage media.
D. define the retention period.

The correct answer is:
A. identify the data.

Explanation:
Archiving data and backups is essential for the continuity of business. Selection of the data to be backed up is the first step in the process. Once the data has been identified an appropriate retention period, storage media and location can be selected.

Area: 5

440. A financial institution that processes millions of transactions each day has a central communications processor (switch) for connecting to ATMs (automated teller machines). Which of the following would be the BEST contingency plan for the communications processor?

A. Reciprocal agreement with another organization
B. Alternate processor in the same location
C. Alternate processor at another network node
D. Installation of duplex communication links

The correct answer is:
C. Alternate processor at another network node

Explanation:
The unavailability of the central communications processor would disrupt all access to the banking network. This could be caused by an equipment, power or communications failure. Reciprocal agreements make an organization dependent on the other organization and raise privacy, competition and regulatory issues. Having an alternate processor in the same location, resolves the equipment problem, but would not be effective if the failure was caused by environmental conditions (i.e., power disruption). The installation of duplex communication

links would only be appropriate if the failure were limited to the communication link.

Area: 5

441. To provide protection for media backup stored at an offsite location the storage site should be:

A. located on a different floor of the building.
B. easily accessible by everyone.
C. clearly labeled for emergency access.
D. protected from unauthorized access.

The correct answer is:
D. protected from unauthorized access.

Explanation:
The offsite storage site should always be protected against unauthorized accesses and at least have the same security requirements as the primary site. Choice A is incorrect because, if the backup is in the same building, it may suffer the same event and may be inaccessible. Choices B and C represent access risks.

Area: 5

442. Which of the following ensures the availability of transactions in the event of a disaster?

A. Send tapes hourly containing transactions offsite.
B. Send tapes daily containing transactions offsite.
C. Capture transactions to multiple storage devices.
D. Transmit transactions offsite in real time.

The correct answer is:
D. Transmit transactions offsite in real time.

Explanation:
The only way to ensure availability of all transactions is to perform a real-time transmission to an offsite facility. Choices A and B are not in real time and, therefore, would not include all the transactions. Choice C does not ensure availability at an offsite location.

Area: 5

443. The cost of ongoing operations when a disaster recovery plan (DRP) is in place, compared to not having a DRP, will MOST likely:

A. increase.
B. decrease.
C. remain the same.
D. be unpredictable.

The correct answer is:
A. increase.

Explanation:
Due to the additional cost of DRP measures, the cost of normal operations for any organization will always increase after a DRP implementation, i.e., the cost of normal operations during a nondisaster period will be more than the cost of operations during a nondisaster period when no DRP was in place.

Area: 5

444. Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

A. Resuming critical processes
B. Recovering sensitive processes
C. Restoring the site
D. Relocating operations to an alternative site

The correct answer is:
A. Resuming critical processes

Explanation:
The resumption of critical processes has the highest priority as it enables business processes to begin immediately after the interruption and not later than the declared mean time between failures (MTBF). Recovery of sensitive processes refers to recovering the vital and sensitive processes that can be performed manually at a tolerable cost for an extended period of time and those that are not marked as high priority. Repairing and restoring the site to original status and resuming the business operations is a time-consuming operation and is not the highest priority. Relocating operations to an alternative site, either temporarily or permanently depending on the interruption, is a time-consuming process and moreover relocation may not be required.

Area: 5

445. Which of the following tasks should be performed FIRST when preparing a disaster recovery plan?

A. Develop a recovery strategy.
B. Perform a business impact analysis.
C. Map software systems, hardware and network components.
D. Appoint recovery teams with defined personnel, roles and hierarchy.

The correct answer is:
B. Perform a business impact analysis.

Explanation:
The first step in any disaster recovery plan is to perform a business impact analysis. All other tasks come afterwards.

Area: 5

446. IS management has decided to install a level 1 Redundant Array of Inexpensive Disks (RAID) system in all servers to compensate for the elimination of offsite backups. The IS auditor should recommend:

A. upgrading to a level 5 RAID.
B. increasing the frequency of onsite backups.
C. reinstating the offsite backups.
D. establishing a cold site in a secure location.

The correct answer is:
C. reinstating the offsite backups.

Explanation:
A RAID system, at any level, will not protect against a natural disaster. The problem will not be alleviated without offsite backups, more frequent onsite backups or even setting up a cold site. Choices A, B and D do not compensate for the lack of offsite backup.

Area: 5

447. Which of the following provides the BEST evidence of an organization's disaster recovery readiness?

A. The disaster recovery plan
B. Customer references for the alternate site provider

C. The process for maintaining the disaster recovery plan
D. The results of tests and drills

The correct answer is:
D. The results of tests and drills

Explanation:
Plans are important, but mere plans do not provide reasonable assurance unless tested. References for the alternate site provider and the existence and maintenance of a disaster recovery plan are important but only tests and drills would demonstrate the adequacy of the plans and provide reasonable assurance of an organization's disaster recovery readiness.

Area: 5

448. Which of the following types of testing would determine whether a new or modified 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

The correct answer is:
D. Sociability testing

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.

Area: 6

449. An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

A. continuous improvement.
B. quantitative quality goals.
C. a documented process.
D. a process tailored to specific projects.

The correct answer is:
A. continuous improvement.

Explanation:
An organization would have reached the highest level of the software CMM at level 5, optimizing. Quantitative quality goals can be reached at level 4 and below, a documented process is executed at level 3 and below, and a process tailored to specific projects can be achieved at level 3 or below.

Area: 6

450. Which of the following risks could result from inadequate software baselining?

A. Scope creep
B. Sign-off delays
C. Software integrity violations
D. Inadequate controls

The correct answer is:
A. Scope creep

Explanation:
A software baseline is the cut-off point in the design and development of a system beyond which additional requirements or modifications to the design do not or cannot occur without undergoing formal strict procedures for approval based on a business cost-benefit analysis. Failure to adequately manage the requirements of a system through baselining can result in a number of risks. Foremost among these risks is scope creep, the process through which requirements change during development. Choices B, C and D may not always result, but choice A is inevitable.

Area: 6

451. Which of the following is often an advantage of using prototyping for systems development?

A. The finished system will have adequate controls.
B. The system will have adequate security/audit trail.
C. It reduces time to deployment.
D. It is easy to achieve change control.

The correct answer is:
C. It reduces time to deployment.

Explanation:
Prototyping is the process of creating systems through controlled trial and error. This method of system development can provide the organization with significant time and cost savings. By focusing mainly on what the user wants and sees, developers may miss some of the controls that come from the traditional systems development approach; therefore, a potential risk is that the finished system will have poor controls. In prototyping, changes in the designs and requirements occur quickly and are seldom documented or approved; hence, change control becomes more complicated with prototyped systems.

Area: 6

452. Business units are concerned about the performance of a newly implemented system. Which of the following should the IS auditor recommend?

A. Develop a baseline and monitor system usage.
B. Define alternate processing procedures.
C. Prepare the maintenance manual.
D. Implement the changes users have suggested.

The correct answer is:
A. Develop a baseline and monitor system usage.

Explanation:
The IS auditor should recommend the development of a performance baseline and monitor the system’s performance, against the baseline, to develop empirical data upon which decisions for modifying the system can be made. Alternate processing procedures and a maintenance manual will not alter a system’s performance. Implementing changes without knowledge of the cause(s) for the perceived poor performance may not result in a more efficient system.

Area: 6

453. Which of the following would be the MOST likely to ensure that business requirements are met during software development?

A. Adequate training
B. Programmers that clearly understand the business processes
C. Documentation of business rules
D. Early engagement of key users

The correct answer is:
D. Early engagement of key users

Explanation:
Key users, since they are familiar with the daily needs, are the individuals that can provide the requirements to ensure the application developed will meet the business needs. Training would aid in learning how to use the system but would not provide the business requirements. Choices B and C are important; however, they will not, by themselves, ensure that requirements are met.

Area: 6

454. An IS auditor that participates in the testing stage of a software development project establishes that the individual modules perform correctly. The IS auditor should:

A. conclude that the individual modules running as a group will be correct.
B. document the test as positive proof that the system can produce the desired results.
C. inform management and recommend an integrated test.
D. provide additional test data.

The correct answer is:
C. inform management and recommend an integrated test.

Explanation:
Modules that have been tested individually can have interface problems, causing adverse affects on other modules. Therefore, the most appropriate action for the IS auditor is to recommend that management carry out an integrated test, which will demonstrate whether the modules working together can produce the desired output. Running additional test data against individual modules will not prove the ability of the modules to work together.

Area: 6

455. During the audit of an acquired software package the IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

A. test the software for compatibility with existing hardware.
B. perform a gap analysis.
C. review the licensing policy.
D. ensure that the procedure had been approved.

The correct answer is:
D. ensure that the procedure had been approved.

Explanation:
In the case of a deviation from the predefined procedures, the IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions the IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

Area: 6

456. Who of the following is ultimately responsible for providing requirement specifications to the software development project team?

A. Team leader
B. Project sponsor
C. System analyst
D. Steering committee

The correct answer is:
B. Project sponsor

Explanation:
The project sponsor is the manager in charge of the business function, the owner of the data and the owner of the system under development. Providing functional specifications through functional users is the responsibility of the project sponsor. The other choices are incorrect. The team leader or project manager working with the project sponsor is responsible for the overall control of the project. The steering committee provides the overall direction and ensures representation of all areas impacted by the new system. The steering committee is responsible for monitoring the overall progress of the project, but is not responsible for the function being automated and, therefore, cannot provide requirement specifications. The system analyst working from the specifications designs the new application system.

Area: 6

457. The request for proposal (RFP) for the acquisition of an application system would MOST likely be approved by the:

A. project steering committee.
B. project sponsor.
C. project manager.
D. user project team.

The correct answer is:
A. project steering committee.

Explanation:
A project steering committee usually consists of senior representative from each function that will be affected by the new system and would be the most appropriate group to approve the RFP. The project sponsor provides funding for the project. The project manager and user project team are responsible for drafting the RFP.

Area: 6

458. Procedures to prevent scope creep should be baselined in which of the following systems development life cycle (SDLC) phases?

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

The correct answer is:
C. Design

Explanation:
To prevent uncontrolled entry of new requirements into a system being developed, a standard process for authorization, approval, testing and documentation is necessary. Such procedures are baselined in the design phase and modified in accordance with the needs of the organization. In the development phase, the design specifications are used to program the system that will support specific organizational processes. The implementation phase is too late and the feasibility phase is too early for establishing scope creep procedures.

Area: 6

459. A programmer, using firecall IDs, as provided in the manufacture's manual, gained access to the production environment and made an unauthorized change. Which of the following could have prevented this from happening?

A. Deactivationt
B. Monitoring
C. Authorization
D. Resetting

The correct answer is:
D. Resetting

Explanation:
The vendor supplied firecall IDs should be reset at the time of implementing the system and new IDs generated. Deactivation may cause the disruption of a critical production job. Without resetting the vendor provided firecall IDs, monitoring and authorization of such IDs are not effective controls.

Area: 6

460. Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

A. System testing
B. Acceptance testing
C. Integration testing
D. Unit testing

The correct answer is:
B. Acceptance testing

Explanation:
Acceptance testing is the final stage before the software is installed and is available for use. The greatest impact would occur if the software fails at the acceptance testing level, as this could result in delays and cost overruns. System testing is undertaken by the developer team to determine if the software meets user requirements per specifications. Integration testing examines the units/modules as one integrated system and unit testing examine the individual units or components of the software. System, integration and unit testing are all performed by the developers at various stages of development, and the impact of failure is comparatively less for each, than failure at the acceptance testing stage.

Area: 6

461. The PRIMARY objective of conducting a post-implementation review is to assess whether the system:

A. achieved the desired objectives.
B. provides for backup and recovery.
C. provides for information security.
D. documentation is clear and understandable.

The correct answer is:
A. achieved the desired objectives.

Explanation:
The primary objective of a post-implementation review of a system is to assess whether the system's objectives have been achieved. The other choices may be subobjectives of a post-implementation review but are not the primary purpose.

Area: 6

462. Regression testing is the process of testing a program to determine if:

A. the new code contains errors.
B. discrepancies exist between functional specifications and performance.
C. new requirements have been met.
D. changes have introduced any errors in the unchanged code.

The correct answer is:
D. changes have introduced any errors in the unchanged code.

Explanation:
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 the same as the data used in the original test. Unit testing is used to determine if a new code contains errors or does not meet requirements.

Area: 6

463. A debugging tool, which reports on the sequence of steps executed by a program, is called a/an:

A. output analyzer.
B. memory dump.

C. compiler.
D. logic path monitor.

The correct answer is:
D. logic path monitor.

Explanation:
Logic path monitors report on the sequence of steps executed by a program. This provides the programmer with clues to logic errors, if any, in the program. An output analyzer checks the results of a program for accuracy by comparing the expected results with the actual results. A memory dump provides a picture of the content of a computer's internal memory at any point in time, often when the program is aborted, thus providing information on inconsistencies in data or parameter values. Though compilers have some potential to provide feedback to a programmer, they are not generally considered a debugging tool.

Area: 6

464. Which of the following capability maturity model levels ensures achievement of basic project management controls?

A. Repeatable (level 2)
B. Defined (level 3)
C. Managed (level 4)
D. Optimizing (level 5)

The correct answer is:
A. Repeatable (level 2)

Explanation:
Level 2 has the characteristics of basic project management controls. Level 3 ensures a documented process, level 4 ensures quantitative quality goals, and level 5 ensures continuous process improvement.

Area: 6

465. An organization has an integrated development environment (IDE) on which the program libraries reside on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an integrated development environment?

A. Controls the proliferation of multiple versions of programs
B. Expands the programming resources and aids available

C. Increases program and processing integrity
D. Prevents valid changes from being overwritten by other changes

The correct answer is:
B. Expands the programming resources and aids available

Explanation:
A strength of an integrated development environment is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

Area: 6

466. When selecting software, which of the following business and technical issues is the MOST important to be considered?

A. Vendor reputation
B. Requirements of the organization
C. Cost factors
D. An installed base

The correct answer is:
B. Requirements of the organization

Explanation:
Establishing the requirements of the organization is a task that should be completed early in the process. Cost factors are a part of the analysis in the evaluation of software alternatives. A vendor's reputation and the installed base become important only after the requirements are met.

Area: 6

467. 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.

The correct answer is:
C. recommend that problem resolution be escalated.

Explanation:
When an 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.

Area: 6

468. Which of the following facilitates program maintenance?

A. More cohesive and loosely coupled programs
B. Less cohesive and loosely coupled programs
C. More cohesive and strongly coupled programs
D. Less cohesive and strongly coupled programs

The correct answer is:
A. More cohesive and loosely coupled programs

Explanation:
Cohesion refers to the performance of a single dedicated function by each program. Coupling refers to the independence of the comparable units. Loosely coupled units, when the program code is changed, will reduce the probability of affecting other program units. More cohesive and loosely coupled units are best for maintenance.

Area: 6

469. An organization wants to enforce data integrity principles and achieve faster performance/execution in a database application. Which of the following design principles should be applied?

A. User (customized) triggers
B. Data validation at the front end
C. Data validation at the back end
D. Referential integrity

The correct answer is:
D. Referential integrity

Explanation:
Referential integrity should be implemented at the time of the design of the database to provide a

faster execution mechanism. All other options are implemented at the application coding stage.

Area: 6

470. What data should be used for regression testing?

A. Different data than used in the previous test
B. The most current production data
C. The data used in previous tests
D. Data produced by a test data generator

The correct answer is:
C. The data used in previous tests

Explanation:
Regression testing ensures that changes or corrections in a program have not introduced new errors. Therefore, this would be achieved only if the data used for regression testing are the same as the data used in previous tests.

Area: 6

471. An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

A. reverse engineering.
B. prototyping.
C. software reuse.
D. reengineering.

The correct answer is:
D. reengineering.

Explanation:
Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remains maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

Area: 6

472. During unit testing, the test strategy applied is:

A. black box.
B. white box.
C. bottom-up.
D. top-down.

The correct answer is:
B. white box.

Explanation:
White box testing examines the internal structure of a module. A programmer should perform this test for each module prior to integrating the module with others. Black box testing focuses on the functional requirements and does not consider the control structure of the module. Choices C and D are not correct because these tests require that several modules have already been assembled and tested.

Area: 6

473. Which of the following is the most important element in the design of a data warehouse?

A. Quality of the metadata
B. Speed of the transactions
C. Volatility of the data
D. Vulnerability of the system

The correct answer is:
A. Quality of the metadata

Explanation:
Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for query and analysis. Metadata aim to provide a table of contents to the information stored in the data warehouse. Companies that have built warehouses believe that metadata are the most important component of the warehouse.

Area: 6

474. Assumptions while planning an IS project involve a high degree of risk because they are:

A. based on known constraints.
B. based on objective past data.
C. a result of a lack of information.
D. often made by unqualified people.

The correct answer is:
C. a result of a lack of information.

Explanation:
Assumptions are made when adequate information is not available. When an IS project manager makes an assumption, there is a high degree of risk because the lack of proper information can cause unexpected loss to an IS project. Assumptions are not based on “known” constraints. When constraints are known in advance, a project manager can plan according to those constraints rather than assuming the constraints will not affect the project. Having objective data about past IS projects will not lead to making assumptions, but rather helps the IS project manager in planning the project. Hence, if objective past data are available and the project manager makes use of them, risk to the project is less. Regardless of whether they are made by qualified people or unqualified people, assumptions are risky.

Area: 6

475. One of the purposes of library control software is to allow:

A. programmers access to production source and object libraries.
B. batch program updating.
C. operators to update the control library with the production version before testing is completed.
D. read-only access to source code.

The correct answer is:
D. read-only access to source code.

Explanation:
An important purpose of library control software is to allow read-only access to source code. Choices A, B and C are activities which library control software should help to prevent or prohibit.

Area: 6

476. The responsibility for designing, implementing and maintaining a system of internal control lies with:

A. the IS auditor.
B. management.
C. the external auditor.
D. the programming staff.

The correct answer is:
B. management.

Explanation:
Designing, implementing and maintaining a system of internal controls, including the prevention and detection of fraud is the responsibility of management. The IS auditor assesses the risks and performs tests to detect irregularities created by weaknesses in the structure of internal controls.

Area: 6

477. Which of the following is a strength of the program evaluation review technique (PERT) over other techniques? PERT:

A. considers different scenarios for planning and control projects.
B. allows the user to input program and system parameters.
C. tests system maintenance processes accurately.
D. estimates costs of system projects.

The correct answer is:
A. considers different scenarios for planning and control projects.

Explanation:
PERT considers different scenarios for planning and controlling projects. Three time estimates—optimistic, pessimistic and most likely—are used to create a level of uncertainty in the estimation of the time for individual activities.

Area: 6

478. An organization is moving its application maintenance in-house from an outside source. Which of the following should be the main concern of an IS auditor?

A. Regression testing
B. Job scheduling

C. User manuals
D. Change control procedures

The correct answer is:
D. Change control procedures

Explanation:
It is essential for the maintenance and control of software that change control procedures be in place. Regression testing is completed after changes are made to the software, and since the software is already being used, the job schedule must be in place and may be reviewed later. This change does not affect user manuals and any associated risks.

Area: 6

479. Ideally, stress testing should be carried out in a:

A. test environment using test data.
B. production environment using live workloads.
C. production environment using live workloads.
D. production environment using test data.

The correct answer is:
C. production environment using live workloads.

Explanation:
Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices B and D), and if only test data is used, there is no certainty that the system was stress tested adequately.

Area: 6

480. Which of the following represents a typical prototype of an interactive application?

A. Screens and process programs
B. Screens, interactive edits and sample reports
C. Interactive edits, process programs and sample reports
D. Screens, interactive edits, process programs and sample reports

The correct answer is:
B. Screens, interactive edits and sample reports

Explanation:
Process programs are not produced by a prototyping tool. This often leads to confusion for the end user who expects quick implementation of programs that accomplish the results that these tools produce.

Area: 6

481. When auditing the proposed acquisition of a new computer system, the IS auditor should FIRST establish that:

A. a clear business case has been approved by management.
B.
C. users will be involved in the implementation plan.
D. the new system will meet all required user functionality.

The correct answer is:
A. a clear business case has been approved by management.

Explanation:
The first concern of the IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as are meeting the needs of the users and having users involved in the implementation process, it is too early in the procurement process for these to be the IS auditor's first concern.

Area: 6

482. Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

A. Inheritance
B. Dynamic warehousing
C. Encapsulation
D. Polymorphism

The correct answer is:
C. Encapsulation

Explanation:
Encapsulation is a property of objects, and it prevents accessing either properties or methods that

have not been previously defined as public. This means that any implementation of the behavior of an object is not accessible. An object defines a communication interface with the exterior and only that which belongs to that interface can be accessed.

Area: 6

483. The most common reason for the failure of information systems to meet the needs of users is that:

A. user needs are constantly changing.
B. the growth of user requirements was forecast inaccurately.
C. the hardware system limits the number of concurrent users.
D. user participation in defining the system's requirements was inadequate.

The correct answer is:
D. user participation in defining the system's requirements was inadequate.

Explanation:
Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a system that does not fully or adequately address the needs of the user. Only users can define what their needs are and, therefore, what the system should accomplish.

Area: 6

484. Which of the following BEST describes the objectives of following a standard system development methodology?

A. To ensure that appropriate staffing is assigned and to provide a method of controlling costs and schedules
B. To provide a method of controlling costs and schedules and to ensure communication among users, IS auditors, management and IS personnel
C. To provide a method of controlling costs and schedules and an effective means of auditing project development
D. To ensure communication among users, IS auditors, management and personnel, and to ensure that appropriate staffing is assigned

The correct answer is:
B. To provide a method of controlling costs and schedules and to ensure communication among users, IS auditors, management and IS personnel

Explanation:
A well-defined systems development methodology will facilitate effective management of the

project since costs and schedules will be monitored consistently. Also, design methodologies require various approvals and sign-offs from different functional groups. This facilitates adequate communications between these groups.

Area: 6

485. Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Black box test
B. Desk checking
C. Structured walk-through
D. Design and code

The correct answer is:
A. Black box test

Explanation:
A black box test is a dynamic analysis tool for testing software modules. During the testing of software modules a black box test works first in a cohesive manner as a 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 somebody closely examines it by applying his/her mind, without actually activating the software. Hence, these cannot be referred to as dynamic analysis tools.

Area: 6

486. Which of the following groups should assume ownership of a systems development project and the resulting system?

A. User management
B. Senior management
C. Project steering committee
D. Systems development management

The correct answer is:
A. User management

Explanation:
User management assumes ownership of the project and resulting system. They should review and approve deliverables as they are defined and accomplished. Senior management approves

the project and the resources needed to complete it. The project steering committee provides overall direction and is responsible for monitoring costs and timetables. Systems development management provides technical support.

Area: 6

487. The primary purpose of a system test is to:

A. test the generation of the designed control totals.
B. determine whether the documentation of the system is accurate.
C. evaluate the system functionally.
D. ensure that the system operators become familiar with the new system.

The correct answer is:
C. evaluate the system functionally.

Explanation:
The primary reason why a system is tested is to evaluate the entire system functionality.

Area: 6

488. The phases and deliverables of a system development life cycle (SDLC) project should be determined:

A. during the initial planning stages of the project.
B. after early planning has been completed, but before work has begun.
C. through out the work stages, based on risks and exposures.
D. only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.

The correct answer is:
A. during the initial planning stages of the project.

Explanation:
It is extremely important that the project be planned properly and that the specific phases and deliverables be identified during the early stages of the project.

Area: 6

489. Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?

A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique

The correct answer is:
C. Rapid application development

Explanation:
Rapid application development is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality. The program evaluation review technique (PERT) and critical path methodology (CPM) are both planning and control techniques, while function point analysis is used for estimating the complexity of developing business applications.

Area: 6

490. When implementing an application software package, which of the following presents the GREATEST risk?

A. Uncontrolled multiple software versions
B. Source programs that are not synchronized with object code
C. Incorrectly set parameters
D. Programming errors

The correct answer is:
C. Incorrectly set parameters

Explanation:
Parameters that are not set correctly would be the greatest concern when implementing an application software package. The other choices, though important, are a concern of the provider, not the organization that is implementing the software itself.

Area: 6

491. Which of the following is an advantage of prototyping?

A. The finished system normally has strong internal controls.
B. Prototype systems can provide significant time and cost savings.
C. Change control is often less complicated with prototype systems.
D. It ensures that functions or extras are not added to the intended system.

The correct answer is:
B. Prototype systems can provide significant time and cost savings.

Explanation:
Prototype systems can provide significant time and cost savings; however, they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated, and it often leads to functions or extras being added to the system that were not originally intended.

Area: 6

492. The use of fourth-generation languages (4GLs) should be weighed carefully against using traditional languages, because 4GLs:

A. can lack lower level detail commands necessary to perform data intensive operations.
B. cannot be implemented on both the mainframe processors and microcomputers.
C. generally contain complex language subsets that must be used by skilled users.
D. cannot access database records and produce complex online outputs.

The correct answer is:
A. can lack lower level detail commands necessary to perform data intensive operations.

Explanation:
All of the answers are advantages of using 4GLs except that they can lack lower-level detail commands necessary to perform data intensive operations. These operations are usually required when developing major applications.

Area: 6

493. When reviewing a system development project at the project initiation stage, an IS auditor finds that the project team is following the organization's quality manual. To meet critical deadlines the project team proposes to fast track the validation and verification processes, commencing some elements before the previous deliverable is signed off. Under these circumstances, the IS auditor would MOST likely:

A. report this as a critical finding to senior management.
B. accept that different quality processes can be adopted for each project.
C. report to IS management the team's failure to follow quality procedures.
D. report the risks associated with fast tracking to the project steering committee.

The correct answer is:
D. report the risks associated with fast tracking to the project steering committee.

Explanation:
It is important that quality processes are appropriate to individual projects. Attempts to apply inappropriate processes will often find their abandonment under pressure. A fast-tracking process is an acceptable option under certain circumstances; however, it is important that the project steering committee is informed of the risks associated with this (i.e., possibility of rework if changes are required).

Area: 6

494. A decision support system (DSS):

A. is aimed at solving highly structured problems.
B. combines the use of models with nontraditional data access and retrieval functions.
C. emphasizes flexibility in the decision-making approach of users.
D. supports only structured decision-making tasks.

The correct answer is:
C. emphasizes flexibility in the decision-making approach of users.

Explanation:
DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less-structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semistructured decision-making tasks.

Area: 6

495. A request for a change to a report format in a module (subsystem) was made. After making the required changes, the programmer should carry out:

A. unit testing.
B. unit and module testing.
C. unit, module and regression testing.
D. module testing.

The correct answer is:
C. unit, module and regression testing.

Explanation:
Unit, module and regression testing will ensure that the specific unit, module or subsystem and

the complete system work as expected. Regression testing is required for any changes carried out at any level. The unit testing will ensure that the unit is working as expected. The unit and module testing will ensure that the unit and the module work as expected. Unit testing and module testing will ensure that the report or the unit and the module or the subsystem are working as expected, but will not ensure that there has not been an impact on the complete system. Regression testing is required for any changes carried out at any level.

Area: 6

496. The PRIMARY role of an IS auditor during the system design phase of an application development project is to:

A. advise on specific and detailed control procedures.
B. ensure the design accurately reflects the requirement.
C. ensure all necessary controls are included in the initial design.
D. advise the development manager on adherence to the schedule.

The correct answer is:
C. ensure all necessary controls are included in the initial design.

Explanation:
The duty of the IS auditor is to ensure that required controls are included. Unless specifically present as a consultant, the IS auditor should not be involved in detailed designs. During the design phase, the IS auditor's primary role is to ensure controls are included. Unless there is any potential slippage to report, the IS auditor is not concerned with project control at this stage.

Area: 6

497. 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.

The correct answer is:
D. test transactions are representative of live processing.

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.

Area: 6

498. 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.

The correct answer is:
B. unauthorized access to sensitive data may result.

Explanation:
Unless the data are sanitized, there is a risk of disclosing sensitive data.

Area: 6

499. 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

The correct answer is:
D. To ensure the new system meets user requirements

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 testing will be completed before parallel testing. Errors in program interfaces with files will be tested during system testing.

Area: 6

500. Which of the following audit procedures would an IS auditor normally perform FIRST when reviewing an organization's systems development methodology?

A. Determine procedural adequacy.
B. Analyze procedural effectiveness.

C. Evaluate the level of compliance with procedures.
D. Compare established standards to observed procedures.

The correct answer is:
D. Compare established standards to observed procedures.

Explanation:
The first step should be to establish that the entity being audited meets best practice. The adequacy of the procedures observed should follow confirmation that they meet best practice. Effectiveness analysis will follow establishment of standards. Compliance tests will follow establishment of standards.

Area: 6

501. Good quality software is BEST achieved:

A. through thorough testing.
B. by finding and quickly correcting programming errors.
C. by determining the amount of testing using the available time and budget.
D. by applying well-defined processes and structured reviews throughout the project.

The correct answer is:
D. by applying well-defined processes and structured reviews throughout the project.

Explanation:
Testing can point to quality deficiencies, However, it cannot by itself fix them. Corrective action at this point in the project is expensive. While it is necessary to detect and correct program errors, the bigger return comes from detecting defects as they occur in upstream phases, such as requirements and design. Choice C is representative of the most common mistake when applying quality management to a software project. It is seen as overhead, instead early removal of defects has a substantial payback. Rework is actually the largest cost driver on most software projects. Choice D represents the core of achieving quality, that is, following a well-defined, consistent process and effectively reviewing key deliverables.

Area: 6

502. Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

A. Release-to-release source and object comparison reports
B. Library control software restricting changes to source code

C. Restricted access to source code and object code
D. Date and time-stamp reviews of source and object code

The correct answer is:
D. Date and time-stamp reviews of source and object code

Explanation:
Date and time-stamp reviews of source and object code would ensure that source code, which has been compiled, matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is the one being used.

Area: 6

503. Which of the following group/individuals should assume overall direction and responsibility for costs and timetables of system development projects?

A. User management
B. Project steering committee
C. Senior management
D. Systems development management

The correct answer is:
B. Project steering committee

Explanation:
The project steering committee is ultimately responsible for all costs and timetables. User management assumes ownership of the project and the resulting system. Senior management commits to the project and approves the resources necessary to complete the project. System development management provides technical support for the hardware and software environments by developing, installing and operating the requested system.

Area: 6

504. In planning a software development project, which of the following is the MOST difficult to determine?

A. Project slack times
B. The project's critical path
C. Time and resource requirements for individual tasks
D. Relationships that preclude the start of an activity before others are complete

The correct answer is:
C. Time and resource requirements for individual tasks

Explanation:
The most difficult problem is effectively estimating a project's slack time and/or resource requirements for individual tasks or development activities. This is commonly done through direct software measures (sizeoriented SLOC—source lines of code; KLOC—thousand lines of code) or indirect software measures (function points—values for number of user inputs, outputs, inquiries; number of files and interfaces). The other choices are project management methods and techniques employed that are dependent on the effectiveness of methods used in deriving accurate and reliable software development productivity and performance measures.

Area: 6

505. During a post-implementation review of an enterprise resource management system, an IS auditor would MOST likely:

A. review access control configuration.
B. evaluate interface testing.
C. review detailed design documentation.
D. evaluate system testing.

The correct answer is:
A. review access control configuration.

Explanation:
Reviewing access control configuration would be the first task performed to determine whether security has been appropriately mapped in the system. Since a post-implementation review is done after user acceptance testing and actual implementation, one would not engage in interface testing or detailed design documentation. Evaluating interface testing would be part of the implementation process. The issue of reviewing detailed design documentation is not generally relevant to an enterprise resource management system, since these are usually vendor packages with user manuals. System testing should be performed before final user sign-off.

Area: 6

506. 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.

The correct answer is:
B. decision trees.

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.

Area: 6

507. Peer reviews to detect software errors during a program development activity are called:

A. emulation techniques.
B. structured walk-throughs.
C. modular program techniques.
D. top-down program construction.

The correct answer is:
B. structured walk-throughs.

Explanation:
A structured walk-through is a management tool for improving productivity. Structured walk-throughs can detect an incorrect or improper interpretation of the program specifications. This, in turn, improves the quality of system testing and acceptance of it. The other choices are methods or tools in the overall systems development process.

Area: 6

508. Testing the connection of two or more system components that pass information from one area to another is:

A. pilot testing.
B. parallel testing
C. interface testing.
D. regression testing.

The correct answer is:
C. interface testing.

Explanation:
Interface testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. Pilot testing is a preliminary test that focuses on specific and predetermined aspects of a system and is not meant to replace other methods. Parallel testing is the process of feeding test data into two systems—the modified system and an alternative system—and comparing the results. 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 is the same as the data used in the original test.

Area: 6

509. 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.

The correct answer is:
C. errors in critical modules are detected earlier.

Explanation:
The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upwards until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing is 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.

Area: 6

510. Which of the following is MOST likely to occur when a system development project is in the middle of the programming/coding phase?

A. Unit tests
B. Stress tests

C. Regression tests
D. Acceptance tests

The correct answer is:
A. Unit tests

Explanation:
During the programming phase, the development team should have mechanisms in place to ensure that coding is being developed to standard and is working correctly. Unit tests are key elements of that process in that they ensure that individual programs are working correctly. They would normally be supported by code reviews. Stress tests, regression tests and acceptance tests would normally occur later in the development and testing phases. As part of the process of assessing compliance with quality processes, IS auditors should verify that such reviews are undertaken.

Area: 6

511. 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

The correct answer is:
B. Integration testing

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.

Area: 6

512. A distinguishing feature of fourth-generation languages (4GLs) is portability, which means?

A. Environmental independence
B. Workbench concepts (i.e., temporary storage, test editing, etc.)
C. Ability to design screen formats and develop graphical outputs
D. Ability to execute online operations

The correct answer is:
A. Environmental independence

Explanation:
Portability describes the ability of 4GLs to execute across computer architectures, operating systems, mainframe processors and personal computers. Choices B, C and D are other attributes of 4GLs.

Area: 6

513. The PRIMARY reason for separating the test and development environments is to:

A. restrict access to systems under test.
B. segregate user and development staff.
C. control the stability of the test environment.
D. secure access to systems under development.

The correct answer is:
C. control the stability of the test environment.

Explanation:
The test environment must be controlled and stable to ensure that development projects are tested in a realistic environment that, as far as possible, mirrors the live environment. Restricting access to test and development systems can be achieved easily by normal access control methods, and the mere separation of the environments will not provide adequate segregation of duties. The IS auditor must be aware of the benefits of separating these environments wherever possible.

Area: 6

514. 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. Post-implementation review

The correct answer is:
B. Requirements definition

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 how the system functionality can be tested to 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. The IS auditor should know at what point user testing should be planned in order to ensure it is most effective and efficient.

Area: 6

515. 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.

The correct answer is:
A. facilitate the ability to reuse modules.

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 object-oriented technique.

Area: 6

516. Which of the following development methods uses a prototype that can be updated continually to meet changing user or business requirements?

A. Data-oriented development (DOD)
B. Object-oriented development (OOD)
C. Business process reengineering (BPR)
D.Rapid application development (RAD)

The correct answer is:
D.Rapid application development (RAD)

Explanation:
Only RAD uses prototyping as its core development tool. OOD and DOD use continuously developing models, and BPR attempts to convert an existing business process rather than make dynamic changes.

Area: 6

517. 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

The correct answer is:
C. The necessary communication protocols

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.

Area: 6

518. When reviewing the quality of an IS department's development process, the IS auditor finds that he/she does not use any formal, documented methodology and standards. The IS auditor's MOST appropriate action would be to:

A. complete the audit and report the finding.
B. investigate and recommend appropriate formal standards.
C. document the informal standards and test for compliance.
D. withdraw and recommend a further audit when standards are implemented.

The correct answer is:
C. document the informal standards and test for compliance.

Explanation:
The IS auditor's first concern would be to ensure that projects are consistently managed. Where

it is claimed that an internal standard exists, it is important to ensure that it is operated correctly, even when this means documenting the claimed standards first. Merely reporting the issue as a weakness and closing the audit without findings would not help the organization in any way and investigating formal methodologies may be unnecessary if the existing, informal standards prove to be adequate and effective.

Area: 6

519. Which of the following testing methods is MOST effective during the initial phases of prototyping?

A. System
B. Parallel
C. Volume
D. Top-down

The correct answer is:
D. Top-down

Explanation:
Top-down testing starts with the system's major functions and works downwards. The initial emphasis when using prototyping is to create screens and reports, thus shaping most of the proposed system's features in a short period. Volume and system testing is performed during final system testing phases. Parallel testing is not necessarily needed, especially if there is no old system with which to compare.

Area: 6

520. 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.

The correct answer is:
B. perform user acceptance testing.

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 requirements.

Area: 6

521. 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.

The correct answer is:
D. source code of the ETCS application be placed in escrow.

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.

Area: 6

522. Which of the following is a measure of the size of an information system based on the number and complexity of a system's inputs, outputs and files?

A. Program evaluation review technique (PERT)
B. Rapid application development (RAD)
C. Function point analysis (FPA)
D. Critical path method (CPM)

The correct answer is:
C. Function point analysis (FPA)

Explanation:
Function point analysis is a measure of the size of an information system based on the number

and complexity of the inputs, outputs and files that a user sees and with which it interacts. Function points are used in a manner analogous to lines of code as a measure of software productivity, quality and other attributes. PERT is a network management technique used in both the planning and control of projects. RAD is a methodology that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality. CPM is used by network management techniques, such as PERT, in computing a critical path.

Area: 6

523. 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 both 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.

The correct answer is:
C. they improve the performance of both the web server and network.

Explanation:
An applet is a JAVA program that is sent over the network from the web server, through a web browser, to the client machine. Then the code is run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on both 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.

Area: 6

524. A company 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.

The correct answer is:
B. A quality plan is not part of the contracted deliverables.

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.

Area: 6

525. Change management procedures are established by IS management to:

A. control the movement of applications from the test environment to the production environment.
B. control the interruption of business operations from lack of attention to unresolved problems.
C. ensure the uninterrupted operation of the business in the event of a disaster.
D. verify that system changes are properly documented.

The correct answer is:
A. control the movement of applications from the test environment to the production environment.

Explanation:
Change management procedures are established by IS management to control the movement of applications from the test environment to the production environment. Problem escalation procedures control the interruption of business operations from lack of attention to unresolved problems, and quality assurance procedures verify that system changes are authorized and tested.

Area: 6

526. An enterprise has established a steering committee to oversee its e-business program. The steering committee would MOST likely be involved in the:

A. documentation of requirements.
B. escalation of project issues.
C. design of interface controls.
D. specification of reports.

The correct answer is:
B. escalation of project issues.

Explanation:
The function of the steering committee is to ensure the success of the project. If there are factors or issues that potentially could affect planned results, the steering committee should escalate them. Activities such as documentation of requirements, design of interface controls and specification of reports are the responsibility of the project team.

Area: 6

527. Which of the following is a control to detect an unauthorized change in a production environment?

A. Denying programmers access to production data
B. Requiring change requests to include benefits and costs
C. Periodically comparing control and current object and source programs
D. Establishing procedures for emergency changes

The correct answer is:
C. Periodically comparing control and current object and source programs

Explanation:
Running the code comparison program on the control and current object and source programs allows for the detection of unauthorized changes in the production environment. Choices A, B and D are preventive controls that are effective as long as they are being applied consistently.

Area: 6

528. Which of the following is MOST effective in controlling application maintenance?

A. Informing users of the status of changes
B. Establishing priorities on program changes
C. Obtaining user approval of program changes
D. Requiring documented user specifications for changes

The correct answer is:
C. Obtaining user approval of program changes

Explanation:

User approvals of program changes will ensure that changes are correct as specified by the user and that they are authorized. Therefore, erroneous or unauthorized changes are less likely to occur, minimizing system downtime and errors.

Area: 6

529. The purpose of debugging programs is to:

A. generate random data that can be used to test programs before implementing them.
B. protect valid changes from being overwritten by other changes during programming.
C. define the program development and maintenance costs to be include in the feasibility study.
D. ensure that abnormal terminations and coding flaws are detected and corrected.

The correct answer is:
D. ensure that abnormal terminations and coding flaws are detected and corrected.

Explanation:
The purpose of debugging programs is to ensure that program abends and coding flaws are detected and corrected before the final program goes into production. There are special tools, such as logic path monitors, memory dumps and output analyzers, to aid the debugging efforts.

Area: 6

530. Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

A. Function point analysis
B. PERT chart
C. Rapid application development
D. Object-oriented system development

The correct answer is:
B. PERT chart

Explanation:
Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many overlapping tasks. A PERT chart will help determine project duration once all the activities and the work involved in the activities

are known. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality, and object-oriented system development is the process of solution specification and modeling.

Area: 6

531. In regard to moving an application program from the test environment to the production environment, the BEST control would be provided by having the:

A. application programmer copy the source program to the production libraries and then have the production control group compile the program.
B. application programmer copy the source program to the production libraries and then have the production control group compile the program.
C. production control group compile the object module to the production libraries using the source program in the test environment.
D. production control group copy the source program to the production libraries and then compile the program.

The correct answer is:
D. production control group copy the source program to the production libraries and then compile the program.

Explanation:
The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program.

Area: 6

532. Utilizing audit software to compare the object code of two programs is an audit technique used to test program:

A. logic.
B. changes.
C. efficiency.
D. computations.

The correct answer is:
B. changes.

Explanation:
The use of audit software to compare programs is an audit technique used to test change control.

Area: 6

533. The program evaluation review technique (PERT):

A. assumes that activities cannot be started and stopped independently.
B. assumes a perfect knowledge of the times of individual activities.
C. starts with a definition of the project activities and their relative sequence.
D. events, marking the start or end of an activity, have time of their own and expend resources.

The correct answer is:
C. starts with a definition of the project activities and their relative sequence.

Explanation:
When designing a PERT network, the first step is to identify all the activities of the project and their relative sequence. The analyst must be careful not to overlook any activity. The list of activities determines the detail of the PERT network. Choice A is not correct, as PERT assumes that the project is a collection of activities or tasks, where the activities can be started and stopped independently of each other, in contrast to a sequential flow of processing. Choice B is not correct because PERT assumes an imperfect knowledge of the times of individual activities and, therefore, incorporates a level of uncertainty in the estimation of such times. Choice D is incorrect as each activity in PERT begins and ends with an event. The event has no time of its own and expends no resources. An event or result may be the completion of the operational feasibility study or the point at which the user accepts the detailed design.

Area: 6

534. The difference between whitebox testing and black box testing is that white box testing:

A. involves the IS auditor.
B. is performed by an independent programmer team.
C. examines a program's internal logical structure.
D. uses the bottom-up approach.

The correct answer is:
C. examines a program's internal logical structure.

Explanation:
Black box testing observes a system's external behavior, while white box testing is a detailed exam of a logical path, checking the possible conditions. The IS auditor need not be involved in

either testing method. The bottom-up approach can be used in both tests. White box testing requires knowledge of the internals of the program or the module to be implemented/tested. Black box testing requires that the functionality of the program be known. The independent programmer team would not be aware of the application of a program in which they have not been involved; hence, the independent programmer team cannot provide any assistance in either of these testing approaches.

Area: 6

535. The reason for establishing a stop or freezing point on the design of a new system is to:

A. prevent further changes to a project in process.
B. indicate the point at which the design is to be completed.
C. require that changes after that point be evaluated for cost-effectiveness.
D. provide the project management team with more control over the project design.

The correct answer is:
C. require that changes after that point be evaluated for cost-effectiveness.

Explanation:
Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs it is recommended that the project be stopped or frozen to allow a rereview of all of the cost-benefits and the payback period.

Area: 6

536. Which is the first software capability maturity model (CMM) level to include a standard software development process?

A. Initial (level 1)
B. Repeatable (level 2)
C. Defined (level 3)
D. Optimizing (level 5)

The correct answer is:
C. Defined (level 3)

Explanation:
Based on lessons learned from level 1 (initial) and level 2 (repeatable), level 3 (defined) initiates documentation to provide standardized software processes across the organization. Level 1

(initial) is characterized as ad hoc and reliance is placed on key personnel and processes are not documented. After level 1, level 2 (repeatable) creates a learning environment where disciplined processes can be repeated successfully on other projects of similar size and scope. The ability to quantitatively control software projects arises on attaining the final level (5) of CMM. At level 5, an organization is in a position to use continuous process improvement strategies in applying innovative solutions and state-of-the-art technologies to its software projects.

Area: 6

537. If an application program is modified and proper system maintenance procedures are in place, which of the following should be tested? The:

A. integrity of the database.
B. access controls for the applications programmer.
C. complete program, including any interface systems.
D. segment of the program containing the revised code.

The correct answer is:
C. complete program, including any interface systems.

Explanation:
The complete program with all interfaces needs to be tested to determine the full impact of a change to program code. Usually, the more complex the program, the more testing is required.

Area: 6

538. An objective of a post-implementation review of a new or extensively modified business application system is to:

A. determine whether test data covered all scenarios.
B. conduct a certification and accreditation process.
C. assess whether expected project benefits were received.
D. design audit trail reports.

The correct answer is:
C. assess whether expected project benefits were received.

Explanation:
Assessing whether expected project benefits were achieved would be one of the objectives of a post-implementation review. Determining whether test data covered all scenarios and conducting a certification and accreditation process are objectives of the implementation phase of application systems development. Designing audit trails is part of the design phase of the

development.

Area: 6

539. Change control for business application systems being developed using prototyping could be complicated by the:

A. iterative nature of prototyping.
B. rapid pace of modifications in requirements and design.
C. emphasis on reports and screens.
D. lack of integrated tools.

The correct answer is:
B. rapid pace of modifications in requirements and design.

Explanation:
Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

Area: 6

540. The MAJOR concern for an IS auditor reviewing a CASE environment should be that the use of CASE does not automatically:

A. result in a correct capture of requirements.
B. ensure that desirable application controls have been implemented.
C. produce ergonomic and user-friendly interfaces.
D. generate efficient code.

The correct answer is:
A. result in a correct capture of requirements.

Explanation:
The principal concern should be to ensure an alignment of the application with business needs and user requirements. While the CASE being used may provide tools to cover this crucial initial phase, a cooperative user-analyst interaction is always needed. Choice B should be the next concern. If the system meets business needs and user requirements, it should also incorporate all desirable controls. Controls have to be specified since CASE can only automatically incorporate certain, rather low-level, controls (such as type of input data, e.g., date, expected). CASE will not (choice C) automatically generate ergonomic and user-friendly interfaces, but it should provide tools for easy (and automatically documented) tuning. CASE applications (choice D) generally

come short of optimizing the use of hardware and software resources, precisely because they are designed to optimize other elements, such as developers effort or documentation.

Area: 6

541. 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.

The correct answer is:
C. inadequate functional testing.

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.

Area: 6

542. Which of the following is a control weakness that can jeopardize a system replacement project?

A. The project initiation document has not been updated to reflect changes in the system scope.
B. A gap analysis comparing the chosen solution to the original specification has revealed a number of significant changes in functionality.
C. The project has been subject to a number of requirement specifications changes.
D. The organization has decided that a project steering committee is not required.

The correct answer is:
D. The organization has decided that a project steering committee is not required.

Explanation:
Even in a small project, the lack of a project steering committee represents the absence of a fundamental control. The project initiation document captures the initial scope and structure of the project, and it is not practical to keep it updated, as changes to the project can be captured through change control procedures and committee decisions. A gap analysis is a process that enables differences to be identified and addressed. Changes of scope and requirements are

significant risks that can have a major effect on project success; however, of themselves, they are not control weaknesses. They should be controlled by change control procedures.

Area: 6

543. A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

A. Comparing source code
B. Reviewing system log files
C. Comparing object code
D. Reviewing executable and source code integrity

The correct answer is:
B. Reviewing system log files

Explanation:
Reviewing system log files is the only trail that may provide information about the unauthorized activities in the production library. Source and object code comparisons are ineffective because the original programs were restored and do not exist. Reviewing executable and source code integrity is an ineffective control because integrity between the executable and source code is automatically maintained.

Area: 6

544. An organization planning to purchase a software package asks the IS auditor for a risk assessment. Which of the following is the MAJOR risk?

A. Unavailability of the source code
B. Lack of a vendor-quality certification
C. Absence of vendor/client references
D. Little vendor experience with the package

The correct answer is:
A. Unavailability of the source code

Explanation:
If the vendor goes out of business, not having the source code available would make it impossible to update the (software) package. Lack of a vendor-quality certification, absence of vendor/client references and little vendor experience with the package are important issues but not critical.

Area: 6

545. After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?

A. Stress
B. Black box
C. Interface
D. System

The correct answer is:
D. System

Explanation:
Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.

Area: 6

546. 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.

The correct answer is:
D. shortens the development time frame.

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.

Area: 6

547. 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 cut-over
D. Phased

The correct answer is:
C. Direct cut-over

Explanation:
Direct cut-over 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.

Area: 6

548. Which of the following is the GREATEST risk when implementing a data warehouse?

A. Increased response time on the production systems
B. Access controls that are not adequate to prevent data modification
C. Data duplication
D. Data that is not updated or current

The correct answer is:
B. Access controls that are not adequate to prevent data modification

Explanation:
Once the data is in a warehouse, no modifications should be made to it and access controls should be in place to prevent data modification. Increased response time on the production systems is not a risk, because a data warehouse does not impact production data. Based on data replication, data duplication is inherent in a data warehouse. Transformation of data from operational systems to a data warehouse is done at predefined intervals, and as such, data may not be current.

Area: 6

549. Which of the following should be done by an IS auditor when a source code comparison indicates modifications were made?

A. Determine whether modifications were authorized.
B. Update the control copy of the source code.
C. Manually review the source code.
D. Insert remarks in the source code describing the modifications.

The correct answer is:
A. Determine whether modifications were authorized.

Explanation:
The IS auditor's primary objective should be to determine if the changes were authorized. A manual review of the source code may be done in some instances, but this would not answer the question of whether the changes were authorized. Choices B and D would not be proper actions.

Area: 6

550. 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.

The correct answer is:
D. products are compatible with the current or planned OS.

Explanation:
Choices A, B and C are incorrect because none of them is 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).

Area: 6

551. The IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could the IS auditor use to estimate the size of the development effort?

A. Program evaluation review technique (PERT)
B. Counting source lines of code (SLOC)
C. Function point analysis
D. White box testing

The correct answer is:
C. Function point analysis

Explanation:
Function point analysis is an indirect method of measuring the size of an application by considering the number and complexity of its inputs, outputs and files. It is useful for evaluating complex applications. PERT is a project management technique that helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behavior of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

Area: 6

552. Which of the following phases represents the optimum point for software baselining to occur?

A. Testing
B. Design
C. Requirement
D. Development

The correct answer is:
B. Design

Explanation:
Software baselining is the cut-off point in the design and development of an application, beyond which change should not occur without undergoing formal procedures for approval and should be supported by a business cost-benefit impact analysis. The optimum point for software baselining to occur is the design phase.

Area: 6

553. When implementing an acquired system in a client-server environment, which of the following tests would confirm that the modifications in the Windows registry do not adversely impact the desktop environment?

A. Sociability testing
B. Parallel testing
C. White box testing
D. Validation testing

The correct answer is:
A. Sociability testing

Explanation:
When implementing an acquired system in an client-server environment, sociability testing would confirm that the system can operate in the target environment without adversely impacting other systems. Parallel testing is the process of feeding test data to both the old and new system and comparing the results. White box testing is based on a close examination of procedural details, and validation testing tests the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Area: 6

554. In an artificial intelligence system, access to which of the following components should be strictly controlled?

A. Inference engine
B. Explanation module
C. Knowledge base
D. Data interface

The correct answer is:
C. Knowledge base

Explanation:
The knowledge base contains specific information or fact patterns associated with a particular subject matter and the rules for interpreting these facts; therefore, strict access controls should be implemented and monitored to ensure the integrity of the decision rules. The inference engine is a program that uses the knowledge base and determines the most appropriate outcome based on the information supplied by the user. The data interface enables the expert system to collect data from nonhuman sources. For example, measurement instruments in a power plant and the explanation module aid the user in addressing the problem to be analyzed and provides the expert conclusion.

Area: 7

555. The output of the risk management process is an input for making:

A. business plans.
B. business plans.

C. security policy decisions.
D. software design decisions.

The correct answer is:
C. security policy decisions.

Explanation:
The risk management process is about making specific security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk management process.

Area: 7

556. 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.

The correct answer is:
A. business plan.

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, and the security plan should be at a corporate level.

Area: 7

557. A data validation edit that matches input data to an occurrence rate is a:

A. limit check.
B. reasonableness check.
C. range check.
D. validity check.

The correct answer is:
B. reasonableness check.

Explanation:
A reasonableness check is an edit check, wherein input data are matched to predetermined reasonable limits or occurrence rates. Limit checks verifiy that data does not exceed a predetermined amount. Range checks verifiy that data is within a predetermined range of values. Validity checks test for data validity in accordance with predetermined criteria.

Area: 7

558. The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

A. integrity.
B. authenticity.
C. authorization.
D. nonrepudiation.

The correct answer is:
A. integrity.

Explanation:
A checksum calculated on an amount field and included in the EDI communication can be used to identify unauthorized modifications. Authenticity and authorization cannot be established by a checksum alone and need other controls. Nonrepudiation can be ensured by using digital signatures.

Area: 7

559. The IS auditor's FIRST step in an application audit is to:

A. identify the risks of using the software.
B. assess access controls.
C. review the policies of the IS organization.
D. understand the business processes.

The correct answer is:
D. understand the business processes.

Explanation:
The audit of application software should start with the IS auditor gaining a knowledge and understanding of the business. This can be done through the study of the operating procedures of the organization. Choices A and B are performed after the auditor has an understanding of the

business processes. Likewise, a review of IS policies, choice C, would occur after having gained a basic understanding of the operation. Policies would be a part of audit compliance testing.

Area: 7

560. The FIRST step in managing the risk of a cyberattack is to:

A. assess the vulnerability impact.
B. evaluate the likelihood of threats.
C. identify critical information assets.
D. estimate potential damage.

The correct answer is:
C. identify critical information assets.

Explanation:
The first step in 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.

Area: 7

561. An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. Which would be the next task?

A. Report the risks to the CIO and CEO immediately.
B. Examine e-business application in development.
C. Identify threats and likelihood of occurrence.
D. Check the budget available for risk management.

The correct answer is:
C. Identify threats and likelihood of occurrence.

Explanation:
The IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

Area: 7

562. 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.

The correct answer is:
B. senior business management.

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.

Area: 7

563. Before implementing controls, management should FIRST ensure that the controls:

A. satisfy a requirement in addressing a risk issue.
B. do not reduce productivity.
C. are based on a cost-benefit analysis.
D. are detective or corrective.

The correct answer is:
A. satisfy a requirement in addressing a risk issue.

Explanation:
When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventative controls that attack the cause of a threat.

Area: 7

564. A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be the IS auditor's main concern about the new process?

A. Are key controls in place to protect assets and information resources?
B. Does it address the corporate customer requirements?

C. Does the system meet the performance goals (time and resources)?
D. Have owners been identified who will be responsible for the process?

The correct answer is:
A. Are key controls in place to protect assets and information resources?

Explanation:
The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the BPR process should achieve, but they are not the auditor's primary concern.

Area: 7

565. Which of the following tasks occurs during the research stage of the benchmarking process?

A. Critical processes are identified.
B. Benchmarking partners are visited.
C. Findings are translated into core principles.
D. Benchmarking partners are identified.

The correct answer is:
D. Benchmarking partners are identified.

Explanation:
During the research stage, the team collects data and identifies the benchmarking partners. In the planning stage, the team identifies the critical processes to be benchmarked. Visiting the benchmarking partners is performed in the observation stage. Translating the findings into core principles is performed during the adaptation stage.

Area: 7

566. An IS auditor assigned to audit a reorganized process should FIRST review which of the following?

A. A map of existing controls
B. Eliminated controls
C. Process charts
D. Compensating controls

The correct answer is:
C. Process charts

Explanation:
To ensure adequate control over the business process, the auditor should first review the flow charts showing the before and after processes. The process charts aid in analyzing the changes in the processes. The other choices—analyzing eliminated controls, ensuring that compensating controls are in place and analyzing the existing controls—are incorrect as each, performed individually, would not be as effective and all encompassing as reviewing the process charts.

Area: 7

567. Which of the following is a mechanism for mitigating risks?

A. Security and control practices
B. Property and liability insurance
C. Audit and certification
D. Contracts and service level agreements (SLAs)

The correct answer is:
A. Security and control practices

Explanation:
Risks are mitigated by implementing appropriate security and control practices. Insurance is a mechanism for transferring risk. Audit and certification are mechanisms of risk assurance, and contracts and SLAs are mechanisms of risk allocation.

Area: 7

568. IT governance is PRIMARILY the responsibility of the:

A. chief executive officer.
B. board of directors.
C. IT steering committee.
D.audit committee.

The correct answer is:
B. board of directors.

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.

Area: 7

569. Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

A. database integrity checks.
B. validation checks.
C. input controls.
D. database commits and rollbacks.

The correct answer is:
D. database commits and rollbacks.

Explanation:
Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

Area: 7

570. 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. It eliminates the need to prepare test data.

The correct answer is:
B. Periodic testing does not require separate test processes.

Explanation:
An integrated test facility creates a fictitious 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.

Area: 7

571. Which of the following audit tools is MOST useful to an IS auditor when an audit trail is required?

A. Integrated test facility (ITF)
B. Continuous and intermittent simulation (CIS)
C. Audit hooks
D. Snapshots

The correct answer is:
D. Snapshots

Explanation:
A snapshot tool is most useful when an audit trail is required. ITF can be used to incorporate test transactions into a normal production run of a system. CIS is useful when transactions meeting certain criteria need to be examined. Audit hooks are useful when only select transactions or processes need to be examined.

Area: 7

572. An IS auditor evaluating data integrity in a transaction-driven system environment should review atomicity to determine whether:

A. the database survives failures (hardware or software).
B. each transaction is separated from other transactions.
C. integrity conditions are maintained.
D. a transaction is completed, or a database is updated.

The correct answer is:
D. a transaction is completed, or a database is updated.

Explanation:
This concept is included in the atomicity, completeness, isolation and durability (ACID) principle. Durabilitymeans that the database survives failures (hardware or software). Isolation means that each transaction is separated from other transactions. Consistency means that integrity conditions are maintained.

Area: 7

573. To make an electronic funds transfer (EFT), one employee enters the amount field and another employee reenters the same data again, before the money is transferred. The control adopted by the organization in this case is:

A. sequence check.
B. key verification.
C. check digit.
D. completeness check.

The correct answer is:
B. key verification.

Explanation:
Key verification is a process in which keying-in is repeated by a separate individual using a machine that compares the original entry to the repeated entry. Sequence check refers to the continuity in serial numbers within the number range on documents. A check digit is a numeric value that has been calculated mathematically and added to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. Completeness checks ensure that all the characters required for a field have been input.

Area: 7

574. When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

A. There could be a question with regards to the legal jurisdiction.
B. Having a provider abroad will cause excesive costs in future audits.
C. The auditing process will be difficult because of the distances.
D. There could be different auditing norms.

The correct answer is:
A. There could be a question with regards to the legal jurisdiction.

Explanation:
In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

Area: 7

575. To share data in a multivendor network environment, it is essential to implement program-to-program communication. With respect to program-to-program communication features, that can be implemented in this environment, which of the following makes implementation and maintenance difficult?

A. User isolation
B. Controlled remote access
C. Transparent remote access
D. The network environments

The correct answer is:
D. The network environments

Explanation:
Depending on the complexity of the network environment, implementation of program-to-program communication features becomes progressively more difficult. It is possible to implement program-toprogram communication to isolate a user in the multivendor network. Program-to-program communication can be implemented to control and monitor the files that a user can transfer between systems, and the remote program-to-program communication will be transparent to the end user. All of these are security features.

Area: 7

576. When developing a risk management program, the FIRST activity to be performed is a/an:

A. threat assessment.
B. classification of data.
C. inventory of assets.
D. criticality analysis.

The correct answer is:
C. inventory of assets.

Explanation:
Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

Area: 7

577. 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

The correct answer is:
B. Data mining techniques

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, than it is a flag that the transaction may have resulted from a fraudulent use of the card.

Area: 7

578. A retail company recently installed data warehousing client software at geographically diverse sites. Due to time zone differences between the sites, updates to the warehouse are not synchronized. Which of the following will be affected the MOST?

A. Data availability
B. Data completeness
C. Data redundancy
D. Data inaccuracy

The correct answer is:
B. Data completeness

Explanation:
Unsynchronized updates will generally cause data completeness to be affected, for example, sales data from one site do not necessarily match costs incurred in another site.

Area: 7

579. A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility.

Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

A. Verifying production to customer orders
B. Logging all customer orders in the ERP system
C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production

The correct answer is:
A. Verifying production to customer orders

Explanation:
Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processing centrally. Production supervisory approval is a time-consuming, manual process that does not guarantee proper control.

Area: 7

580. 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.

The correct answer is:
C. Examine some of the test cases to confirm the results.

Explanation:
The 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.

Area: 7

581. Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printout.
B. transaction journal.
C. automated suspense file listing.
D. user error report.

The correct answer is:
B. transaction journal.

Explanation:
The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, and the user error report would only list input that resulted in an edit error.

Area: 7

582. As a business process reengineering (BPR) project takes hold it is expected that:

A. business priorities will remain stable.
B. information technologies will not change.
C. the process will improve product, service and profitability.
D. input from clients and customers will no longer be necessary.

The correct answer is:
C. the process will improve product, service and profitability.

Explanation:
As a reengineering process takes hold, certain key results will begin to emerge, including a concentration on process as a means of improving product, service and profitability. In addition, new business priorities and approaches to the use of information as well as powerful and more accessible information technologies will emerge. Often, the roles of client and customers will be redefined providing them with more direct and active participation in the enterprise's business process.

Area: 7

583. 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.

The correct answer is:
C. digital signature.

Explanation:
A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. A digest signature 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.

Area: 7

584. Which of the following is a check (control) for completeness?

A. Check digits
B. Parity bits
C. One-for-one checking
D. Prerecorded input

The correct answer is:
B. Parity bits

Explanation:
Parity bits are used to check for completeness of data transmissions. Choice A is incorrect because check digits are a control check for accuracy. Choice C is incorrect because, in one-for-one checking, individual documents are matched to a detailed listing of documents processed by the computer, but do not ensure that all documents have been received for processing. Choice D (prerecorded input) is a data file control for which selected information fields are preprinted on blank input forms to reduce the chance of input errors.

Area: 7

585. 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

The correct answer is:
C. Completeness check

Explanation:
A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteria. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

Area: 7

586. Which of the following types of controls is designed to provide the ability to verify data and record values through the stages of application processing?

A. Range checks
B. Run-to-run totals
C. Limit checks on calculated amounts
D. Exception reports

The correct answer is:
B. Run-to-run totals

Explanation:
Run-to-run totals provide the ability to verify data values through the stages of application processing. Runto- run total verification ensures that data read into the computer was accepted and then applied to the updating process.

Area: 7

587. The reliability of an application system's audit trail may be questionable if:

A. user IDs are recorded in the audit trail.
B. the security administrator has read-only rights to the audit file.
C. date and time stamps are recorded when an action occurs.
D. users can amend audit trail records when correcting system errors.

The correct answer is:
D. users can amend audit trail records when correcting system errors.

Explanation:
An audit trail is not effective if the details in it can be amended.

Area: 7

588. Which of the following is the FIRST thing an IS auditor should do after the discovery of a Trojan horse program in a computer system?

A. Investigate the author.
B. Remove any underlying threats.
C. Establish compensating controls.
D. Have the offending code removed.

The correct answer is:
D. Have the offending code removed.

Explanation:
The IS auditor's first duty is to prevent the Trojan horse from causing further damage. After removing the offending code, follow up actions would include investigation and recommendations (choices B and C).

Area: 7

589. The editing/validation of data entered at a remote site would be performed MOST effectively at the:

A. central processing site after running the application system.
B. central processing site during the running of the application system.
C. remote processing site after transmission of the data to the central processing site.
D. remote processing site prior to transmission of the data to the central processing site.

The correct answer is:
D. remote processing site prior to transmission of the data to the central processing site.

Explanation:
remote processing site prior to transmission of the data to the central processing site.

Area: 7

590. 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.

The correct answer is:
C. preparing simulated transactions for processing and comparing the results to predetermined results.

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.

Area: 7

591. A programmer included a routine into a payroll application to search for his/her own payroll number. As a result, if this payroll number does not appear during the payroll run, a routine will generate and place random numbers onto every paycheck. This routine is known as:

A. scavenging.
B. data leakage.
C. piggybacking.
D. a Trojan horse.

The correct answer is:
D. a Trojan horse.

Explanation:
A Trojan horse is malicious code hidden in an authorized computer program. The hidden code will be executed whenever the authorized program is executed. In this case, as long as the perpetrator’s payroll number is part of the payroll process nothing happens, but as soon as the payroll number is gone havoc occurs.

Area: 7

592. 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. the application's optimization.

The correct answer is:
B. impact of any exposures discovered.

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.

Area: 7

593. To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

A. during data preparation.
B. in transit to the computer.
C. between related computer runs.
D. during the return of the data to the user department.

The correct answer is:
A. during data preparation.

Explanation:
During data preparation is the best answer, because it establishes control at the earliest point.

Area: 7

594. While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

A. A scan of all floppy disks before use
B. A virus monitor on the network file server
C. Scheduled daily scans of all network drives
D. A virus monitor on the user's personal computer

The correct answer is:
C. Scheduled daily scans of all network drives

Explanation:
Scheduled daily scans of all network drives will detect the presence of a virus after the infection has occurred. All of the other choices are controls designed to prevent a computer virus from infecting the system.

Area: 7

595. When two or more systems are integrated, input/output controls must be reviewed by the IS auditor in the:

A. systems receiving the output of other systems.
B. systems sending output to other systems.
C. systems sending and receiving data.
D. interfaces between the two systems.

The correct answer is:
C. systems sending and receiving data.

Explanation:
Both of the systems must be reviewed for input/output controls, since the output for one system is the input for the other.

Area: 7

596. Functional acknowledgements are used:

A. as an audit trail for EDI transactions.
B. to functionally describe the IS department.
C. to document user roles and responsibilities.
D. as a functional description of application software.

The correct answer is:
A. as an audit trail for EDI transactions.

Explanation:
Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and therefore can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

Area: 7

597. An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

A. EDI trading partner agreements.
B. physical controls for terminals.
C. authentication techniques for sending and receiving messages.
D. program change control procedures.

The correct answer is:
C. authentication techniques for sending and receiving messages.

Explanation:
Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

Area: 7

598. The impact of EDI on internal controls will be:

A. that fewer opportunities for review and authorization will exist.
B. an inherent authentication.
C. a proper distribution of EDI transactions while in the possession of third parties.
D. that IPF management will have increased responsibilities over data center controls.

The correct answer is:
A. that fewer opportunities for review and authorization will exist.

Explanation:
EDI promotes a more efficient paperless environment, but at the same time, less human intervention makes it more difficult for reviewing and authorizing. Choice B is incorrect; since the interaction between parties is electronic, there is no inherent authentication occurring. Computerized data can look the same no matter what the source and does not include any distinguishing human element or signature. Choice C is incorrect because this is a security risk associated with EDI. Choice D is incorrect because there are relatively few, if any, additional data center controls associated with the implementation of EDI applications. Instead, more control will need to be exercised by the user's application system to replace manual controls, such as site reviews of documents. More emphasis will need to be placed on control over data transmission (network management controls).

Area: 7

599. Which of the following user profiles should be of MOST concern to the IS auditor, when performing an audit of an EFT system?

A. Three users with the ability to capture and verify their own messages
B. Five users with the ability to capture and send their own messages
C. Five users with the ability to verify other users and to send their own messages
D. Three users with the ability to capture and verify the messages of other users and to send their own messages

The correct answer is:
A. Three users with the ability to capture and verify their own messages

Explanation:
The ability of one individual to capture and verify messages represents an inadequate segregation, since messages can be taken as correct and as if they had already been verified.

Area: 7

600. 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

The correct answer is:
B. Reasonableness checks

Explanation:
A reasonableness check is a data validation edit and control, used to ensure that data conform to predetermined criteria. Before and after image reporting is a control over data files that makes it possible to trace changes. Online access controls are designed to prevent unauthorized access to the system and data. A hash total is a total of any numeric data field or series of data elements in a data file. This total is checked against a control total of the same field (or fields) to ensure completeness of processing.

Area: 7

601. A tax calculation program maintains several hundred tax rates. The BEST control to ensure that tax rates entered into the program are accurate is:

A. an independent review of the transaction listing.
B. a programmed edit check to prevent entry of invalid data.
C. programmed reasonableness checks with 20 percent data entry range.
D. a visual verification of data entered by the processing department.

The correct answer is:
A. an independent review of the transaction listing.

Explanation:
Tax rates represent critical data that will be used in numerous calculations and should be independently verified by someone other than the entry person before they are used in processing. Choices B and C are programmed controls that are useful for preventing gross errors, that is, errors such as an added zero or alpha instead of a numeric. A tax table must be 100 percent accurate, not just readable. Choice D will allow the data entry person to check input accuracy, but it is not sufficient.

Area: 7

602. During an audit of the tape management system at a data center, an IS auditor discovered that parameters are set to bypass or ignore the labels written on tape header records. The IS auditor also determined that effective staging and job setup procedures were in place. In this situation, the IS auditor should conclude that the:

A. tape headers should be manually logged and checked by the operators.
B. staging and job setup procedures are not appropriate compensating controls.
C. staging and job setup procedures compensate for the tape label control weakness.
D. tape management system parameters must be set to check all labels.

The correct answer is:
C. staging and job setup procedures compensate for the tape label control weakness.

Explanation:
Compensating controls are an important part of a control structure. They are considered adequate if they help to achieve the control objective and are cost-effective. In this situation the IS auditor is most likely to conclude that staging and job setup procedures compensate for the tape label control weakness.

Area: 7

603. An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

A. Allow changes to be made only with the DBA user account.
B. Make changes to the database after granting access to a normal user account
C. Use the DBA user account to make changes, log the changes and review the change log the following day.
D. Use the normal user account to make changes, log the changes and review the change log the following day.

The correct answer is:
C. Use the DBA user account to make changes, log the changes and review the change log the following day.

Explanation:
The use of a database administrator (DBA) user account is (should be) normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

Area: 7

604. With reference to the risk management process, which of the following statements is correct?

A. Vulnerabilities can be exploited by a threat.
B. Vulnerabilities are events with the potential to cause harm to IS resources.
C. Vulnerability exists because of threats associated with use of information resources.
D. Lack of user knowledge is an example of a threat.

The correct answer is:
A. Vulnerabilities can be exploited by a threat.

Explanation:
Vulnerabilities are characteristics of IS resources that can be exploited, resulting in some harm.

Threats not vulnerabilities are events with the potential to cause harm. A threat occurs because of a vulnerability associated with the use of information resources. Lack of user knowledge is an example of a vulnerability.

Area: 7

605. IS management has recently informed the IS auditor of its decision to disable certain referential integrity controls in the payroll system to provide users with a faster report generator. This will MOST likely increase the risk of:

A. data entry by unauthorized users.
B. a nonexistent employee being paid.
C. an employee receiving an unauthorized raise.
D. duplicate data entry by authorized users.

The correct answer is:
B. a nonexistent employee being paid.

Explanation:
Referential integrity controls prevent the occurrence of unmatched foreign key values. Given that a nonexistent employee does not appear in the employees' table, it will never have a corresponding entry in the salary payment's table. The other choices cannot be detected by referential integrity controls.

Area: 7

606. Which of the following message services provides the strongest protection that a specific action has occurred?

A. Proof of delivery
B. Nonrepudiation
C. Proof of submission
D. Message origin authentication

The correct answer is:
B. Nonrepudiation

Explanation:
Nonrepudiation services provide evidence that a specific action occurred. Nonrepudiation services are similar to their weaker proof counterparts (i.e., proof of submission, proof of delivery, and message origin authentication); however, nonrepudiation provides stronger protection because the proof can be demonstrated to a third party. Digital signatures are used to

provide nonrepudiation. Message origination authentication will only confirm the source of the message and does not confirm the specific action that has been completed.

Area: 7

607. An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:

A. check to ensure the type of transaction is valid for that card type.
B. verify the format of the number entered then locate it on the database.
C. ensure that the transaction entered is within the cardholder's credit limit.
D. confirm that the card is not shown as lost or stolen on the master file.

The correct answer is:
B. verify the format of the number entered then locate it on the database.

Explanation:
The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed. A validation control in data capture will ensure that the data entered is valid (i.e., it can be processed by the system). If the data captured in the initial validation is not valid (if the card number or PIN do not match with the database), then the card will be rejected or captured per the controls in place. Once initial validation is completed, then other validations specific to the card and cardholder would be performed.

Area: 7

608. A proposed transaction processing application will have many data capture sources and outputs in both paper and electronic form. To ensure that transactions are not lost during processing, the IS auditor should recommend the inclusion of:

A. validation controls.
B. internal credibility checks.
C. clerical control procedures.
D. automated systems balancing.

The correct answer is:
D. automated systems balancing.

Explanation:
Automated system's balancing would be the best way to ensure that no transactions are lost as

any imbalance between total inputs and total outputs would be reported for investigation and correction. Validation controls and internal credibility checks are certainly valid controls, but will not detect and report lost transactions. In addition, although a clerical procedure could be used to sum and compare inputs and outputs, an automated process is less susceptible to error.

Area: 7

609. Following a reorganization of a company's legacy database, it was discovered that records were accidentally deleted. Which of the following controls would have MOST effectively detected this occurrence?

A. Range check
B. Table lookups
C. Run-to-run totals
D. One-for-one checking

The correct answer is:
C. Run-to-run totals

Explanation:
Run-to-run totals would have been an effective detective control over processing in this situation. Table lookups and range checks are used for data validation before input, or as close to the point of origination as possible. One-for-one checking is time-consuming and, therefore, less effective.

Area: 7

610. A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

A. Key verification
B. One-for-one checking
C. Manual recalculations
D. Functional acknowledgements

The correct answer is:
D. Functional acknowledgements

Explanation:
Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. All the other choices are manual input controls, whereas data mapping deals with automatic integration of data in the receiving company.

Area: 7

611. In a data warehouse, data quality is achieved by:

A. cleansing.
B. restructuring.
C. source data credibility.
D. transformation.

The correct answer is:
C. source data credibility.

Explanation:
In a data warehouse system, the quality of data depends on the quality of the originating source. Choices A, B and D relate to the composition of a data warehouse and do not affect data quality. Restructuring, transformation and cleansing all relate to reorganization of existing data within the database.

Area: 7

612. Sales orders are automatically numbered sequentially at each of a retailer's multiple outlets. Small orders are processed directly at the outlets, with large orders sent to a central production facility. The MOST appropriate control to ensure that all orders transmitted to production are received and processed would be to:

A. send and reconcile transaction counts and totals.
B. have data transmitted back to the local site for comparison.
C. compare data communications protocols with parity checking.
D. track and account for the numerical sequence of sales orders at the production facility.

The correct answer is:
A. send and reconcile transaction counts and totals.

Explanation:
Sending and reconciling transaction totals not only ensure that the orders were received, but also processed by the central production location. Transmission back to the local site confirms that the central location received it, but not that they have actually processed it. Tracking and accounting for the numerical sequence only confirms what orders are on hand, and not whether they actually have been completed. The use of parity checking would only confirm that the order was not changed during transmission.

Area: 7

613. Which of the following is a control to compensate for a programmer having access to accounts payable production data?

A. Processing controls such as range checks and logic edits
B. Reviewing accounts payable output reports by data entry
C. Reviewing system-produced reports for checks (cheques) over a stated amount
D. Having the accounts payable supervisor match all checks (cheques) to approved invoices

The correct answer is:
D. Having the accounts payable supervisor match all checks (cheques) to approved invoices

Explanation:
To ensure that the programmer could not have a check (cheque) generated, it would be necessary for someone to confirm all of the checks (cheques) generated by the system. Range and logic checks could easily be bypassed by a programmer since they are privy to the controls that have been built into the system. The review of the accounts payable reports by data entry would only identify changes that might have been made to the data input. It would not identify information that might have been changed on the master files. Reviewing reports for checks (cheques) over a certain amount would not allow for the identification of any unauthorized, low-value checks (cheques) or catch alterations to the actual checks (cheques) themselves.

Area: 7

614. A data warehouse is:

A. object-oriented.
B. subject-oriented.
C. departmental specific.
D. a volatile database

The correct answer is:
B. subject-oriented.

Explanation:
Data warehouses are subject-oriented. The data warehouse is meant to help make decisions when the function(s) to be affected by the decision transgresses across departments within an organization. They are nonvolatile. Object orientation and volatility are irrelevant to a data warehouse system.

Area: 7

615. 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.

The correct answer is:
A. aid in scheduling project tasks.

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.

Area: 7

616. Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

A. Review software migration records and verify approvals.
B. Identify changes that have occurred and verify approvals.
C. Review change control documentation and verify approvals.
D. Ensure that only appropriate staff can migrate changes into production.

The correct answer is:
B. Identify changes that have occurred and verify approvals.

Explanation:
The most effective method is to determine through code comparisons what changes have been made and then verify that they have been approved. Change control records and software migration records may not have all changes listed. Ensuring that only appropriate staff can migrate changes into production is a key control process, but in itself does not verify compliance.

Area: 7

617. 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

The correct answer is:
C. Inability to specify purpose and usage patterns

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 DSS.

Area: 7

618. An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

A. critical.
B. vital.
C. sensitive.
D. noncritical.

The correct answer is:
C. sensitive.

Explanation:
Sensitive functions are best described as those that can be performed manually at a tolerable cost for an extended period of time. Critical functions are those that cannot be performed unless they are replaced by identical capabilities and cannot be replaced by manual methods. Vital functions refer to those that can be performed manually but only for a brief period of time. This is associated with lower costs of disruption than critical functions. Noncritical functions may be interrupted for an extended period of time, at little or no cost to the company, and require little time or cost to restore.

Area: 7

619. Once an organization has finished the business process reengineering (BPR) of all its critical operations, the IS auditor would MOST likely focus on a review of:

A. pre-BPR process flowcharts.
B. post-BPR process flowcharts.
C. BPR project plans.
D. continuous improvement and monitoring plans.

The correct answer is:
B. post-BPR process flowcharts.

Explanation:
The IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Choice A is incorrect because an IS auditor must review the process as it is today, not as it was in the past. Choices C and D are incorrect because they are steps within a BPR project.

Area: 7

620. An IS auditor performing a review of the EFT operations of a retailing company would verify that the customers credit limit is checked before funds are transferred by reviewing the EFT:

A. system's interface.
B. switch facility.
C. personal identification number generating procedure.
D. operation backup procedures.

The correct answer is:
A. system's interface.

Explanation:
At the application processing level, the IS auditor should review the interface between the EFT system and the application system that processes the accounts from which funds are transferred. Choice B is incorrect because an EFT switch is the facility that provides the communication linkage for all equipment in the network. Choices C and D are procedures that would not help determine if the customer's credit limit is verified before the funds are transferred.

Area: 7

621. A manufacturer has been purchasing materials and supplies for its business through an e-commerce application. Which of the following should this manufacturer rely on to prove that the transactions were actually made?

A. Reputation
B. Authentication
C. Encryption
D. Nonrepudiation

The correct answer is:
D. Nonrepudiation

Explanation:
Nonrepudiation may ensure that a transaction is enforceable. It involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient of the data's receipt, or vice versa. Choice A is incorrect because the company's reputation would not, of itself, prove a deal was made via the Internet. Choice B is not correct as authentication controls are necessary to establish the identification of all parties to a communication. Choice C is incorrect since encryption may protect the data transmitted over the Internet, but may not prove that the transactions were made.

Area: 7

622. A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

A. payroll reports should be compared to input forms.
B. gross payroll should be recalculated manually.
C. checks (cheques) should be compared to input forms.
D. checks (cheques) should be reconciled with output reports.

The correct answer is:
A. payroll reports should be compared to input forms.

Explanation:
The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the input (payroll reports). Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques) have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

Area: 7

623. Prices are charged on the basis of a standard master file rate that changes as volume increases. Any exceptions must be manually approved. What is the MOST effective automated control to help ensure that all price exceptions are approved?

A. All amounts are displayed back to the data entry clerk, who must verify them visually.
B. Prices outside the normal range should be entered twice to verify data entry accuracy.
C. The system beeps when price exceptions are entered and prints such occurrences on a report.
D. A second-level password must be entered before a price exception can be processed.

The correct answer is:
D. A second-level password must be entered before a price exception can be processed.

Explanation:
Automated control should ensure that the system processes the price exceptions only upon approval of another user who is authorized to approve such exceptions. A second-level password would ensure that price exceptions will be approved by a user who has been authorized by management. Visual verification of all amounts by a data entry clerk is not a control, but a basic requirement for any data entry. The user's ability to visually verify what has been entered is a basic manual control. Entry of price exceptions twice, is an input control. This does not ensure, that exceptions will be verified automatically by another user. The system beeping on entry of a price exception is only a warning to the data entry clerk; it does not prevent proceeding further. Printing of these exceptions on a report is a detective (manual) control.

Area: 7

624. An independent software program that connects two otherwise separate applications sharing computing resources across heterogeneous technologies is known as:

A. middleware.
B. firmware.
C. application software.
D. embedded systems.

The correct answer is:
A. middleware.

Explanation:
Middleware is independent software that connects two otherwise separate applications sharing

computing resources across heterogeneous technologies. Firmware is software (programs or data) that has been written onto read-only memory (ROM). It is a memory chip with embedded program code that holds its content when power is turned off. Firmware is a combination of software and hardware. Application software are programs that address an organization's processes and functions as opposed to system software, which enables the computer to function. Embedded systems are built-in modules for a specific purpose, e.g., SCARF.

Area: 7

625. Using test data as part of a comprehensive test of program controls in a continuous online manner is called a/an:

A. test data/deck.
B. base-case system evaluation.
C. integrated test facility (ITF).
D. parallel simulation.

The correct answer is:
B. base-case system evaluation.

Explanation:
Base-case system evaluation uses test data sets developed as part of comprehensive testing programs. It is used to verify correct systems operations before acceptance, as well as periodic validation. Test data/deck simulates transactions through real programs. An ITF creates fictitious files in the database with test transactions processed simultaneously with live input. Parallel simulation is the production of data processed using computer programs that simulate application program logic.

Area: 7

626. Which of the following ensures completeness and accuracy of accumulated data?

A. Processing control procedures
B. Data file control procedures
C. Output controls
D. Application controls

The correct answer is:
A. Processing control procedures

Explanation:
Processing controls ensure the completeness and accuracy of accumulated data, for example,

editing and runto- run totals. Data file control procedures ensure that only authorized processing occurs to stored data, for example, transaction logs. Output controls ensure that data delivered to users will be presented, formatted and delivered in a consistent and secure manner, for example, using report distribution. Application controls are a general terminology comprising all kinds of controls used in an application.

Area: 7

627. Which of the following represents the GREATEST potential risk in an EDI environment?

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

The correct answer is:
A. Transaction authorization

Explanation:
Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk. Choices B and D are examples of risks, but the impact is not as great as that of unauthorized transactions. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed; however, there will be no loss of data.

Area: 7

628. Which of the following is the FIRST step in a business process reengineering (BPR) project?

A. Defining the areas to be reviewed
B. Developing a project plan
C. Understanding the process under review
D. Reengineering and streamlining the process under review

The correct answer is:
A. Defining the areas to be reviewed

Explanation:
On the basis of the evaluation of the entire business process, correctly defining the areas to be

reviewed is the first step in a BPR project. On the basis of the definition of the areas to be reviewed, the project plan is developed. Understanding the process under review is important, but the subject of the review must first be defined. Thereafter, the process can be reengineered, streamlined, implemented and monitored for continuous improvement.

Area: 7

629. Which of the following is the MOST critical and contributes the MOST to the quality of data in a data warehouse?

A. Accuracy of the source data
B. Credibility of the data source
C. Accuracy of the extraction process
D. Accuracy of the data transformation

The correct answer is:
A. Accuracy of the source data

Explanation:
Accuracy of source data is a prerequisite for the quality of the data in a data warehouse. Credibility of the data source is important, accurate extraction processes are important and accurate transformation routines are important but would not change inaccurate data into quality (accurate) data.

Area: 7

630. A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses the team should:

A. compute the amortization of the related assets.
B. calculate a return on investment (ROI).
C. apply a qualitative approach.
D. spend the time needed to define exactly the loss amount.

The correct answer is:
C. apply a qualitative approach.

Explanation:
The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor (e.g., one is a very low impact to the business and five is a very high impact). A ROI is computed when there is predictable savings or revenues, which can be compared to the

investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack) that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

Area: 7

631. 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.

The correct answer is:
A. communications handler.

Explanation:
A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs). An EDI translator translates data between the standard format and a trading partner's proprietary format. An application interface moves electronic transactions to or from the application system and performs data mapping. An EDI interface manipulates and routes data between the application system and the communications handler.

Area: 7

632. 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.

The correct answer is:
C. redundancy check.

Explanation:
A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data. A reasonableness check compares data to predefined reasonability limits

or occurrence rates established for the data. A parity check is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

Area: 7

633. Which of the following integrity tests examines the accuracy, completeness, consistency and authorization of data?

A. Data
B. Relational
C. Domain
D. Referential

The correct answer is:
A. Data

Explanation:
Data integrity testing examines the accuracy, completeness, consistency and authorization of data. Relational integrity testing detects modification to sensitive data by the use of control totals. Domain integrity testing verifies that data conforms to specifications. Referential integrity testing ensures that data exists in its parent or original file before it exists in the child or another file.

Area: 7

634. 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

The correct answer is:
B. Check digit

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, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

Area: 7

635. 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.

The correct answer is:
A. existence of a set of functions and their specified properties.

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.

Area: 7

636. Which of the following is the BEST control to detect internal attacks on IT resources?

A. Checking of activity logs
B. Reviewing firewall logs
C. Implementing a security policy
D. Implementing appropriate segregation of duties

The correct answer is:
A. Checking of activity logs

Explanation:
Verification of individual activity logs will detect the misuse of IT resources. Depending on the configuration, firewall logs can help in detecting attacks passing through the firewall. Implementation of a security policy and segregation of duties are deterrent controls that might prevent the misuse of IT resources.

Area: 7

637. Which of the following is used to ensure that batch data is completely and accurately transferred between two systems?

A. Control total
B. Check digit
C. Check sum
D. Control account

The correct answer is:
A. Control total

Explanation:
A control total is frequently used as an easily recalculated control. The number of invoices in a batch or the value of invoices in a batch are examples of control totals. They provide a simple way of following an audit trail from a general ledger summary item to an individual transaction, and back. A check digit is a method of verifying the accuracy of a single data item, such as a credit card number. Although a check sum is an excellent control over batch completeness and accuracy, it is not easily recalculated and, therefore, is not as commonly used in financial systems as a control total. Check sums are frequently used in data transfer as part of encryption protocols. Control accounts are used in financial systems to ensure that components that exchange summary information, such as a sales register and a general ledger, can be reconciled.

Area: 7

638. In an electronic fund transfer (EFT) system, which of the following controls would be useful in detecting a duplication of messages?

A. Message authentication code
B. Digital signature
C. Authorization sequence number
D. Segregation of authorization

The correct answer is:
C. Authorization sequence number

Explanation:
All the controls are necessary in an EFT system; however, the authorization sequence number is the control that will detect the duplication of a message. A message authentication code detects unauthorized modifications, a digital signature ensures nonrepudiation, and the segregation of the creation of the message and the authorization will avoid dummy messages.

Area: 7

639. When auditing the conversion of an accounting system an IS auditor should verify the existence of a:

A. control total check.
B. validation check.
C. completeness check.
D. limit check.

The correct answer is:
A. control total check.

Explanation:
Tallying a control total of all accounts before and after conversion will assure the IS auditor that all amount data has been taken into the new system. Later one-to-one checking by users will assure that all the data has been converted. The other choices are incorrect. Validation checks, completeness checks and limit checks would be applied at the point at which the data are/were originally entered into the accounting system.

Area: 7

640. An employee is responsible for updating daily the interest rates in a finance application, including interest rate exceptions for preferred customers. Which of the following is the BEST control to ensure that all rates exceptions are approved?

A. A supervisor must enter his/her password before a rate exception is validated.
B. Rates outside the normal range require prior management approval.
C. The system beeps an alarm when rate exceptions are entered.
D. All interest rates must be logged and verified every 30 days.

The correct answer is:
B. Rates outside the normal range require prior management approval.

Explanation:
Prior approval of management for rates outside the normal range would be a proper control. Entering the password of a supervisor does not ensure authorization. A system alarm on entry of a rate exception is only a warning and logging of exceptions is a detective control.

Area: 7

641. The lack of adequate security controls represents an:

A. threat.
B. asset.
C. impact.
D. vulnerability.

The correct answer is:
D. vulnerability.

Explanation:
The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers, resulting in loss of sensitive information, which could lead to the loss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the "Potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets". The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionality in this context is a vulnerability.

Area: 7

642. Which of the following data validation edits could be used by a bank, to ensure the correctness of bank account numbers assigned to customers, thereby helping to avoid transposition and transcription errors?

A. Sequence Check
B. Validity Check
C. Check Digit
D. Existence Check

The correct answer is:
C. Check Digit

Explanation:
A check digit is a mathematically calculated value that is added to data to ensure that the original data has not been altered or an incorrect but correct value substituted. This helps in avoiding transposition and transcription errors. Thus, a check digit can be added to an account number to check for accuracy. Sequence checks ensure that a number follows sequentially and any out of sequence or duplicate control numbers are rejected or noted on an exception report. Validity checks and existence checks match data against predetermined criteria to ensure accuracy.

Area: 7

643. The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

A. financial results.
B. customer satisfaction.
C. internal process efficiency.
D. innovation capacity.

The correct answer is:
A. financial results.

Explanation:
Financial results have traditionally been the sole overall performance metric. The IT Balanced Scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

Area: 7

644. Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient services.
B. define key performance indicators.
C. provide business value to IT projects.
D. control IT expenses.

The correct answer is:
B. define key performance indicators.

Explanation:
A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

Area: 7

645. During an application audit, the IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

A. Implement data backup and recovery procedures.
B. Define standards and closely monitor for compliance.

C. Ensure that only authorized personnel can update the database.
D. Establish controls to handle concurrent access problems.

The correct answer is:
A. Implement data backup and recovery procedures.

Explanation:
Implementing data backup and recovery procedure is a corrective control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, and monitoring for compliance is a detective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is a preventive control.

Area: 7

646. An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

A. Log all table update transactions.
B. Implement before-and-after image reporting.
C. Use tracing and tagging.
D. Implement integrity constraints in the database.

The correct answer is:
D. Implement integrity constraints in the database.

Explanation:
Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

Area: 7

647. Which of the following presents an inherent risk, with no distinct identifiable preventive controls?

A. Piggybacking
B. Viruses
C. Data diddling
D. Unauthorized application shutdown

The correct answer is:
C. Data diddling

Explanation:
Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses, because it requires limited technical knowledge and occurs before computer security can protect the data. There are only compensating controls for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-replicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdown of an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which is effective if there are proper access controls.

Area: 7

648. An IS auditor has imported data from the client's database. The next step of 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 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.

The correct answer is:
A. matching control totals of the imported data to control totals of the original data.

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.

Area: 7

649. A financial institution is using an expert system for managing credit limits. An IS auditor reviewing the system should be MOST concerned with the:

A. validation of data inputs into the system.
B. level of experience and skills contained in the knowledge base.
C. access control settings.
D. implemented processing controls.

The correct answer is:
B. level of experience and skills contained in the knowledge base.

Explanation:
The level of experience or intelligence in the knowledge base is a key concern for the IS auditor as decision errors, based on a lack of knowledge, could have a severe impact on the organization. Choices A, C and D are not as important as B.

Area: 7

650. 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.

The correct answer is:
A. capturing of the knowledge and experience of individuals in an organization.

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.

Area: 7