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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.