

***DOMAIN 01: THE PROCESS OF AUDITING INFORMATION SYSTEMS***

**1. Which term best describes the difference between the audit sample and the total population?**

- A. Precision**
- B. Tolerable error rate**
- C. Level of risk**
- D. Analytic delta**

**2. Which is not a purpose of risk analysis?**

- A. Support risk-based audit decisions**
- B. Assist the auditor in determining audit objectives**
- C. Assist the auditor in identifying risks and threats**
- D. Ensure absolute safety during the audit**

**3. Failing to prevent or detect a material error would represent which type of risk?**

- A. Overall audit risk**
- B. Detection risk**
- C. Inherent risk**
- D. Control risk**

**4. Which of the following is not a type of quantitative sampling model?**

- A. Difference estimation**
- B. Stratified mean per unit**
- C. Unstratified mean per unit**
- D. Qualitative estimation per unit**

5. The two types of tests are referred to as \_\_\_\_\_ and \_\_\_\_\_ using \_\_\_\_\_ Sampling methods.
- A. Substantive tests, compliance tests, variable and attribute
  - B. Compliance tests, substantive tests, variable and discovery
  - C. Predictive tests, compliance tests, stop-and-go and difference estimation
  - D. Integrity tests, compliance tests, stratified mean and unstratified mean
6. What is the purpose of the audit charter?
- A. To engage external auditors
  - B. To grant responsibility, authority, and accountability
  - C. To authorize the creation of the audit committee
  - D. To provide detailed planning of the audit
7. Which of the following is false concerning a control self-assessment (CSA)?
- A. Empowers the user to take ownership and accountability
  - B. Eliminates the need for a traditional audit
  - C. May be used to identify high-risk areas for later review
  - D. Will not have the level of independence provided by an external auditor
8. Which of the following would be a concern of the auditor that should be explained in the Audit report along with their findings?
- A. Detailed list of audit objectives
  - B. The need by the current auditor to communicate with the prior auditor
  - C. Communicating results directly to the chairperson of the audit committee
  - D. Undue restrictions placed by management on evidence use or audit procedures

9. What is the purpose of the audit committee?
- A. To assist managers with training in auditing skills
  - B. To govern, control, and manage the organization
  - C. To challenge and review assurances
  - D. To provide daily coordination of all audit activities
10. Which type of audit may be used for regulatory licensing or external reporting?
- A. Qualified audit
  - B. Independent assessment
  - C. Control self-assessment
  - D. Traditional audit
11. What is the best data collection technique the auditor can use if the resources are available?
- A. Surveys that create a broad sample
  - B. Review of existing documentation
  - C. Auditor observation
  - D. Interviews
12. Which of the following types of risk are of the most interest to an IS auditor?
- A. Control, detection, noncompliance, risk of strike
  - B. Inherent, non-inherent, control, lack of control
  - C. Sampling, control, detection, inherent
  - D. Unknown, quantifiable, cumulative
13. Which of the following describes the relationship between compliance testing and substantive testing?

- A. Compliance testing checks for the presence of controls; substantive testing checks the integrity of internal contents.
- B. Substantive testing tests for presence; compliance testing tests actual contents.
- C. The tests are identical in nature; the difference is whether the audit subject is under the Sarbanes-Oxley Act.
- D. Compliance testing tests individual account balances; substantive testing checks for written corporate policies.

**14. What is the principal issue surrounding the use of CAAT?**

- A. The capability of the software vendor.
- B. Possible cost, complexity, and the security of output.
- C. Inability of automated tools to consider the human characteristics of the environment.
- D. Documentary evidence is more effective.

**15. Auditors base their report on findings, evidence, and the results of testing. It's more of a score than an opinion. Which of the following types of evidence sampling refer to a**

- A. Attribute
- B. Stop-and-go
- C. Cell
- D. Discovery

**16. Which of the following best describes integrated auditing?**

- A. Integrated auditing places internal control in the hands of management and reduces the time between the audit and the time of reporting.
- B. Integrated auditing combines the operational audit function, the financial audit function, and the IS audit function.
- C. Integrated auditing combines the operational audit function and the IS audit function.

- D. Integrated auditing combines the financial audit function and the IS audit function.**

**17. Which type of sampling would best be used to uncover fraud or other attempts to Bypass regulations?**

- A. Attribute sampling**
- B. Frequency estimating sampling**
- C. Stop-and-go sampling**
- D. Discovery sampling**

**18. Which of the following best describes this statement: This risk can be caused by the Failure of internal controls and can result in a material error.**

- A. Audit risk**
- B. Inherent risk**
- C. Detection risk**
- D. Control risk**

**19. Which of the following is not one of the best techniques for gathering evidence during an audit?**

- A. Attend board meetings**
- B. Examine and review actual procedures and processes**
- C. Verify employee security awareness training and knowledge**
- D. Examine actual reporting relationships to verify segregation of duties**

**20. Which of the following is not an advantage of the control self-assessment (CSA)?**

- A. CSA helps provide early detection of risks.**
- B. CSA is an audit function replacement.**
- C. CSA reduces control costs.**

**D. CSA provides increased levels of assurance.**

**21. Which of the following is the best example of a detective control?**

- A. Intrusion-prevention systems**
- B. User registration process**
- C. Variance reports**
- D. Access-control software**

**22. Which of the following is the best example of a general control procedure?**

- A. Internal accounting controls used to safeguard financial records**
- B. Business continuity and disaster-recovery procedures that provide reasonable assurance that the organization is secure against disasters**
- C. Procedures that provide reasonable assurance for the control of access to data and programs**
- D. Procedures providing reasonable assurance that have been developed to control and manage data-processing operations**

**23. Which of the following describes a significant level of risk that the organization is unwilling to accept?**

- A. Detection risk**
- B. Material risk**
- C. Business risk**
- D. Irregularities**

**24. Which of the following is the most accurate description of a substantive test in which the data Represents fake entities such as products, items, or departments?**

- A. Parallel tests**
- B. Integrated test facility**

- C. Embedded audit module
- D. Test data

**25. You need to review an organization's balance sheet for material transactions. Which of the following would be the best sampling technique?**

- A. Attribute sampling
- B. Frequency estimating sampling
- C. Stop-and-go sampling
- D. Variable sampling

**26. An IS auditor is performing a review of an application and finds something that might be illegal. The IS auditor should do which of the following?**

- A. Disregard or ignore the finding because this is beyond the scope of this review
- B. Conduct a detailed investigation to aid the authorities in catching the culprit
- C. Immediately notify the auditee of the finding
- D. Seek legal advice before finishing the audit

**27. The auditor is permitted to deviate from professional audit standards when they feel it is Necessary which of the following is true regarding such deviation?**

- A. Standards are designed for discretionary use.
- B. Deviation is almost unheard of and would require significant justification.
- C. Deviation depends on the authority granted in the audit charter.
- D. The unique characteristics of the client will require auditor flexibility.

**28. Which is the best document to help define the relationship of the independent auditor and provide evidence of the agreed-upon terms and conditions?**

- A. Audit charter

- B. Annual audit plan**
  - C. Engagement letter**
  - D. Auditor's report**
- 29. Who has the responsibility of setting the scope of the audit?**
- A. Auditor**
  - B. Client**
  - C. Audit manager**
  - D. Auditee**
- 30. What is the biggest issue with the decision to transfer risk to an outsourced contractor?**
- A. There is potential for uncontrollable increase in operating cost over time.**
  - B. Outsourcing shifts the entire risk to the contractor.**
  - C. The company still retains liability for whatever happens.**
  - D. Outsourcing shields the company from intrinsic risks.**
- 31. Audits are intended to be conducted in accordance with which of the following ideals?**
- A. Specific directives from management concerning evidence and procedure**
  - B. Reporting and communication**
  - C. Assessment of the organizational controls**
  - D. Adherence to standards, guidelines, and best practices**
- 32. During audit planning, several documents are produced in support of the project. Which of these is used to identify the person responsible for specific tasks in order to gain funding and ensure quality?**
- A. Skills matrix**
  - B. Procurement matrix**



- C. Task matrix
- D. Activities matrix

**33. Which of these types of computer-assisted audit tools (CAAT) is designed to process dummy transactions during the processing of genuine transactions?**

- A. Continuous and intermittent simulation
- B. Embedded program audit hooks
- C. Embedded audit module
- D. Online event monitor

**34. Which of the following conditions is false in regard to using the work of other people during your audit?**

- A. Ensure independence of the provider.
- B. Accept the work based on job position.
- C. Use agreed-upon scope and approach.
- D. Provide supervision and review.

**35. ISACA refers to testing for strong controls. What is the best description of a strong control?**

- A. Effective implementation of multiple controls targeting the same objective
- B. Preventative controls that stop the problem from ever occurring
- C. Using at least one control in each of the three categories of preventative, detective, corrective
- D. Implementing comprehensive pervasive controls inside of an ERP application.

**36. Which of the following outlines the overall authority to perform an IS audit?**

- A. The audit scope, with goals and objectives
- B. A request from management to perform an audit

- C. The approved audit charter
- D. The approved audit schedule

**37. In performing a risk-based audit, which risk assessment is completed initially by the IS auditor?**

- A. Detection risk assessment
- B. Control risk assessment
- C. Inherent risk assessment
- D. Fraud risk assessment

**38. While developing a risk-based' audit program on which of the following would the IS auditor MOST likely focus?**

- A. Business processes
- B. Critical IT applications
- C. Operational controls
- D. Business strategies

**39. Which of the following types of audit' risk assumes an absence of compensating controls in the area being reviewed?**

- A. Control risk
- B. Detection risk
- C. Inherent risk
- D. Sampling risk

**40. An IS auditor performing a review of an application's controls finds a weakness in System software that could materially impact the application. The IS auditor should?**

- A. disregard these control weaknesses since a system software review is beyond the scope of this review.
- B. Conduct a detailed system software review and report the control weaknesses.

- C. include in the report a statement that the audit was limited to a review of the application's controls.
- D. review the system software controls as relevant and recommend a detailed system Software review.

**41. Which of the following is the MOST important reason why an audit planning process should be reviewed at periodic intervals?**

- A. To plan for deployment of available audit resources
- B. To consider changes to the risk environment
- C. To provide inputs for documentation of the audit charter
- D. To identify the applicable IS audit standards

**42. Which of the following is MOST effective for implementing a control self- assessment (CSA) within business units?**

- A. Informal peer reviews
- B. Facilitated workshops
- C. Process flow narratives
- D. Data flow diagrams

**43. The FIRST step in planning an audit is to:**

- A. Define audit deliverables.
- B. Finalize the audit scope and audit objectives.
- C. Gain, an understanding of the business' objectives.
- D. Develop the audit approach or audit strategy.

**44. The approach an IS auditor should use to plan its audit coverage should be based on:**

- A. Risk.

- B. Materiality**
- C. Professional skepticism.**
- D. Sufficiency of audit evidence.**

**45. A company performs a daily backup of critical data and software files, and stores the backup tapes at an offsite location. The backup tapes are used to restore the files in case of a disruption. This is a:**

- A. Preventive control.**
- B. Management control,**
- C. Corrective control.**
- D. Detective control.**

**46. Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?**

- A. Field checks**
- B. Control totals**
- C. Reasonableness checks**
- D. A before-and-after maintenance report**

**47. Which of the following is a benefit of using call back devices?**

- A. Provide an audit trail**
- B. Can be used in a switchboard environment**
- C. Permit unlimited user mobility**
- D. Allow call forwarding**

**48. As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?**

- A. The same value.**
- B. Greater value.**
- C. Lesser value.**

**D. Prior audit reports are not relevant.**

**49. 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.**

**50. What is the PRIMARY purpose of audit trails?**

- A. To document auditing efforts**
- B. To correct data integrity errors**
- C. To establish accountability and responsibility for processed transactions**
- D. To prevent unauthorized access to data**

**51. How does the process of systems auditing benefit from using a risk-based approach to audit planning?**

- A. Controls testing starts earlier.**
- B. Auditing resources are allocated to the areas of highest concern.**
- C. Auditing risk is reduced.**
- D. Controls testing are more thorough.**

**52. The use of statistical sampling procedures helps minimize:**

- A. Detection risk**
- B. Business risk**
- C. Controls risk**
- D. Compliance risk**

**53. What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?**

- A. Business risk**
- B. Detection risk**
- C. Residual risk**
- D. Inherent risk**

**54. A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:**

- A. Identify high-risk areas that might need a detailed review later**
- B. Reduce audit costs**
- C. Reduce audit time**
- D. Increase audit accuracy**

**55. Why does the IS auditor often review the system logs?**

- A. To get evidence of password spoofing**
- B. To get evidence of data copy activities**
- C. To determine the existence of unauthorized access to data by a user or program**
- D. To get evidence of password sharing**

**56. What is a reliable technique for estimating the scope and cost of a software-development project?**

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

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

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

**58. If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.**

**A. Lack of IT documentation is not usually material to the controls tested in an IT audit.**

**B. The auditor should at least document the informal standards and policies.**

**Furthermore, the IS auditor should create formal documented policies to be implemented.**

**C. The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.**

**D. The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should create formal documented policies to be implemented.**

**59. What must an IS auditor understand before performing an application audit? Choose the BEST**

**A. The potential business impact of application risks.**

**B. Application risks must first be identified.**

**C. Relative business processes.**

**D. Relevant application risks.**

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

**A. Implementer**

**B. Facilitator**

- C. Developer
- D. Sponsor

**61. which of the following would prevent accountability for an action performed, thus allowing Non-repudiation?**

- A. Proper authentication
- B. Proper identification AND authentication
- C. Proper identification
- D. Proper identification, authentication, AND authorization

**62. Which of the following is the MOST critical step in planning an audit?**

- A. Implementing a prescribed auditing framework such as COBIT
- B. Identifying current controls
- C. Identifying high-risk audit targets
- D. Testing controls

**63. To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following? Choose the BEST answer.**

- A. The business objectives of the organization
- B. The effect of segregation of duties on internal controls
- C. The point at which controls are exercised as data flows through the system
- D. Organizational control policies

**64. What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?**

- A. Document existing internal controls
- B. Perform compliance testing on internal controls



- C. Establish a controls-monitoring steering committee
- D. Identify high-risk areas within the organization

65. What type of risk is associated with authorized program exits (trap doors)? Choose the BEST answer.

- A. Business risk
- B. Audit risk
- C. Detective risk
- D. Inherent risk

66. Which of the following is of greatest concern to the IS auditor?

- A. Failure to report a successful attack on the network
- B. Failure to prevent a successful attack on the network
- C. Failure to recover from a successful attack on the network
- D. Failure to detect a successful attack on the network

67. An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. Is it true or false?

- A. True
- B. False

68. Why does an IS auditor review an organization chart?

- A. To optimize the responsibilities and authority of individuals
- B. To control the responsibilities and authority of individuals
- C. To better understand the responsibilities and authority of individuals
- D. To identify project sponsors

**69. When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management Personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. Is it true or false?**

- A. True**
- B. False**

**70. Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.**

- A. Systems logs**
- B. Access control lists (ACL)**
- C. Application logs**
- D. Error logs**

**71. What should IS auditors always check when auditing password files?**

- A. That deleting password files is protected**
- B. That password files are encrypted**
- C. That password files are not accessible over the network**
- D. That password files are archived**

**72. Which of the following is of greatest concern when performing an IS audit?**

- A. Users' ability to directly modify the database**
- B. Users' ability to submit queries to the database**
- C. Users' ability to indirectly modify the database**
- D. Users' ability to directly view the database**

**73. Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. Is it true or false?**

- A. True**
- B. False**

**74. What uses questionnaires to lead the user through a series of choices to reach a conclusion?**

**Choose the BEST answer.**

- A. Logic trees**
- B. Decision trees**
- C. Decision algorithms**
- D. Logic algorithms**

**75. What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality? Choose the BEST answer.**

- A. Rapid application development (RAD)**
- B. GANTT**
- C. PERT**
- D. Decision trees**

**76. What is the most common reason for information systems to fail to meet the needs of users?**

**Choose the BEST answer.**

- A. Lack of funding**
- B. Inadequate user participation during system requirements definition**
- C. Inadequate senior management participation during system requirements definition**
- D. Poor IT strategic planning**

**77. Who is responsible for the overall direction, costs, and timetables for systems-development projects?**

- A. The project sponsor**
- B. The project steering committee**
- C. Senior management**
- D. The project team leader**

**78. An IS auditor is using a statistical sample to inventory the tape library. What type of test would this is considered?**

- A. Substantive**
- B. Compliance**
- C. Integrated**
- D. Continuous audit**

**79. 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.**

**80. 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**

**81. 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**

**82. An audit charter should:**

- A. be dynamic and change often to coincide with the changing nature of technology and the audit profession.**
- B. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.**
- C. document the audit procedures designed to achieve the planned audit objectives.**
- D. Outline the overall authority, scope and responsibilities of the audit function.**

**83. 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.**

**84. 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**

**85. 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.

86. 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

87. When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:

- A. controls needed to mitigate risks are in place.
- B. vulnerabilities and threats are identified.
- C. audit risks are considered.
- D. a gap analysis is appropriate.

88. 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.

**89. 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.**

**90. 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. Auditor's ability to find relevant evidence.**
- D. Purpose and scope of the audit being done.**

**91. 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.**

**92. An IS auditor should use statistical sampling and not judgment (non-statistical) sampling, when:**

- A. the probability of error must be objectively quantified.**
- B. the auditor wishes to avoid sampling risk.**
- C. generalized audit software is unavailable.**
- D. the tolerable error rate cannot be determined.**

**93. During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:**

- A. Address audit objectives.**

- B. Collect sufficient evidence.**
  - C. Specify appropriate tests.**
  - D. Minimize audit resources.**
- 94. When selecting audit procedures, an IS auditor should use professional judgment to ensure that:**
- A. sufficient evidence will be collected.**
  - B. all significant deficiencies identified will be corrected within a reasonable period.**
  - C. all material weaknesses will be identified.**
  - D. audit costs will be kept at a minimum level.**
- 95. An IS auditor evaluating logical access controls should FIRST:**
- A. document the controls applied to the potential access paths to the system.**
  - B. test controls over the access paths to determine if they are functional.**
  - C. evaluate the security environment in relation to written policies and practices**
  - D. Obtain an understanding of the security risks to information processing.**
- 96. 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**
- 97. Which of the following would normally be the MOST reliable evidence for an auditor?**
- A. A confirmation letter received from a third party verifying an account balance**
  - B. Assurance from line management that an application is working as designed**
  - C. Trend data obtained from World Wide Web (Internet) sources**



**D. Ratio analysts developed by the IS auditor from reports supplied by line management**

**98. The PRIMARY purpose for meeting with auditee prior to formally closing a review is to:**

- A. Confirm that the auditors did not overlook any important issues.**
- B. Gain agreement on the findings.**
- C. Receive feedback on the adequacy of the audit procedures.**
- D. Test the structure of the final presentation.**

**99. The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is**

**to:**

- A. Comply with regulatory requirements.**
- B. Provide a basis for drawing reasonable conclusions.**
- C. Ensure complete audit coverage.**
- D. Perform the audit according to the defined scope.**

**100. After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:**

- A. Expand activities to determine whether an investigation is warranted.**
- B. Report the matter to the audit committee.**
- C. Report the possibility of fraud to top management and ask how they would like to proceed.**
- D. Consult with external legal counsel to determine the course of action to be taken.**

**101. During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:**

- A. Ask the auditee to sign a release form accepting full legal responsibility.**

- B. Elaborate on the significance of the finding and the risks of not correcting it.**
  - C. Report the disagreement to the audit committee for resolution.**
  - D. Accept the auditee's position since they are the process owners.**
- 102. When preparing an audit report the IS auditor should ensure that the results are supported by:**
- A. statements from IS management.**
  - B. work papers of other auditors.**
  - C. An organizational control self-assessment.**
  - D. Sufficient and appropriate audit evidence.**
- 103. The final decision to include a material finding in an audit report should be made by the:**
- A. Audit committee.**
  - B. Auditee's manager.**
  - C. IS auditor.**
  - D. CEO of the organization**
- 104. 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.**
- 105. The success of control self-assessment (CSA) highly depends on:**
- A. having line managers assume a portion of the responsibility for control monitoring.**

- B. assigning staff managers the responsibility for building, but not monitoring, controls.**
- C. The implementation of a stringent control policy and rule-driven controls.**
- D. The implementation of supervision and the monitoring of controls of assigned duties.**

**106. Which of the following is the key benefit of control self-assessment (CSA)?**

- A. Management ownership of the internal controls supporting business objectives is reinforced.**
- B. Audit expenses are reduced when the assessment results are an input to external audit Work.**
- C. Improved fraud detection since internal business staff are engaged in testing controls**
- D. Internal auditors can shift to a consultative approach by using the results of the Assessment.**

**107. 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.**

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

- A. Length of service, since this will help ensure technical competence.**
- B. age, as training in audit techniques may be impractical.**
- C. IS knowledge, since this will bring enhanced credibility to the audit function.**

**D. ability, as an IS auditor, to be independent of existing IS relationships.**

**109. When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?**

- A. Restricting physical access to computing equipment**
- B. Reviewing transaction and application logs**
- C. Performing background checks prior to hiring IT staff**
- D. Locking user sessions after a specified period of inactivity**

**110. An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:**

- A. Dependency on a single person.**
- B. Inadequate succession planning.**
- C. One person knowing all parts of a system.**
- D. A disruption of operations.**

**111. Which of the following reduces the potential impact of social engineering attacks?**

- A. Compliance with regulatory requirements**
- B. Promoting ethical understanding**
- C. Security awareness programs**
- D. Effective performance incentives**

**112. Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?**

- A. Senior management is aware of critical information assets and demonstrates an adequate concern for their protection.**
- B. Job descriptions contain clear statements of accountability for information security.**

- C. In accordance with the degree of risk and business impact, there is adequate funding for security efforts.**
- D. No actual incidents have occurred that have caused a loss or a public embarrassment.**

**113. Which of the following is normally a responsibility of the chief security officer (CSO)?**

- A. Periodically reviewing and evaluating the security policy**
- B. Executing user application and software testing and evaluation**
- C. Granting and revoking user access to IT resources**
- D. Approving access to data and applications**

**114. To support an organization's goals, an IS department should have:**

- A. A low-cost philosophy.**
- B. Long- and short-range plans.**
- C. Leading-edge technology.**
- D. Plans to acquire new hardware and software.**

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

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

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

- A. Allocating resources**
- B. Keeping current with technology advances**

- C. Conducting control self-assessment
- D. Evaluating hardware needs

**117. 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.

**118. 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.

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

- A. Implementation.
- B. Compliance.
- C. Documentation.
- D. Sufficiency.