

1. Correct answer: A

The compliance test uses precision to describe the rate of occurrence out of the sample population. The compliance testing uses precision to describe the expected error rate of the sample compared to total population. Precision is usually expressed as a percentage.

2. Correct answer: D

Risk analysis is used to determine whether the audit has any chance of representing the truth. Nothing in the realm of IS auditing is absolute because of the abstract nature of technology implementations.

3. Correct answer: B

A detection risk is that you would fail to detect that a material error has occurred.

4. Correct answer: D

Difference estimation, stratified mean, and unstratified mean are valid sample types for substantive testing. Qualitative estimation is just a distractor.

5. Correct answer: A

Answer B is incorrect because compliance testing uses discovery sampling to detect fraud. C and D are distractors.

6. Correct answer: B

The audit charter's purpose is to grant the right to audit and delegate responsibility, authority, and accountability.

7. Correct answer: B

All of the statements are true except B. A CSA is not a substitute for a traditional audit

8. Correct answer: D

Undue restrictions on scope would be a major concern as would the lack of time or the inability to obtain sufficient reliable evidence.

9. Correct answer: C

The audit committee's purpose is to review and challenge assurances made, and to maintain a positive working relationship with management and the auditors.

10. Correct answer: D

Traditional independent audits are conducted with formality and adherence to standards necessary for regulatory licensing and external reporting. It's true that there is always a shady auditor ready to lie for a client. The world expects an independent audit to be conducted by a qualified auditor representing a high degree of truth. Assessments are too informal and therefore can be used only internally in the organization.

11. Correct answer: D

Interviewing selected personnel is the best technique. Surveys, document review, and observations generate a lower yield.

12. Correct answer: C

The answers including risk of strike, lack of control, and unknown are distracters.

13. Correct answer: A

Substantive testing checks the substance or integrity of a transaction. Compliance testing looks for presence of controls or control attributes.

14. Correct answer: B

CAATs are able to perform faster than humans and produce more-accurate data in functions such as system scanning. Cost, training, and security of output are major considerations.

15. Correct answer: D

Discovery sampling is used to find 100 percent of everything possible when fraud is suspected or the likelihood of finding evidence is low. All the other possible choices are valid sampling methods used in compliance testing.

16. Correct answer: B

Integrated auditing is a methodology that combines the operational audit function, the financial audit function, and the IS audit function. Therefore, answers C and D are incorrect because they do not list all three types of functions to be integrated. Answer A is incorrect because it describes the control self-assessment (CSA), which is used to verify the reliability of internal controls and places internal controls in the hands of management

17. Correct answer: D

Discovery sampling would best be used to uncover fraud or other attempts to bypass regulations. Answer A is incorrect because attribute sampling is used to determine the rate of occurrence. Answer B is incorrect because frequency sampling is another name for attribute sampling. Both describe the same sampling technique. Answer C is incorrect because stop-and-go sampling is used when the auditor believes that only a few errors will be found in a population.

18. Correct answer: D

A control risk is the risk caused by the failure of internal controls; it can result in a material error. Answer A is incorrect because the audit risk is the amount of risk the organization is willing to accept. Answer B is incorrect because the inherent risk is the risk that can occur because of the lack of compensating controls. Combined, inherent risks can create a material risk. Answer C is incorrect because detection risk is the risk if an auditor does not design tests in such a way as to detect a material risk.

19. Correct answer: A

Attending board meetings is not one of the best ways to gather evidence during an audit. The best ways to gather evidence include observing employee activity, examining and reviewing actual procedures and processes, verifying employee security awareness training and knowledge, and examining actual reporting relationships to verify segregation of duties.

20. Correct answer: B

Answers A, C, and D are all advantages of CSA. CSA is not an audit function replacement.

21. Correct answer: C

A variance report is the best example of a detective control. Detective controls attempt to detect problems. Answers A, B, and D are incorrect because they all describe preventive controls.

22. Correct answer: A

Internal accounting controls used to safeguard financial records are an example of a general control procedure. Answers B, C, and D all describe information system control procedures.

23. Correct answer: B

The word material describes a significant level of risk that the auditor is unwilling to accept. Answers A, C, and D do not define the term.

24. Correct answer: B

An integrated test facility is a type of substantive test that uses data represented by fake entities such as products, items, or departments. Answer A is incorrect because a parallel test compares real results to those generated by the auditor to compare the control function. Answer C is incorrect because embedded audit modules identify and report specific transactions or other information based on predetermined

criteria. Answer D is incorrect because test data uses theoretical transactions to validate program logic and control mechanisms.

25. Correct answer: D

Variable sampling would be the best sampling technique to review an organization's balance sheet for material transactions. It is also known as dollar estimation. Answer A is incorrect because attribute sampling is used to determine the rate of occurrence. Answer B is incorrect because frequency sampling is another name for attribute sampling. Both describe the same sampling technique. Answer C is incorrect because stop-and-go sampling is used when an auditor believes that only a few errors will be found in a population.

26. Correct answer: D

Seek competent legal advice. It is not the auditor's job to detect potentially illegal acts however, the auditor should seek the aid of a lawyer concerning liability and reporting requirements.

27. Correct answer: B

Standards are mandatory, and any deviation would require justification.

28. Correct answer: C

The engagement letter is used with independent auditors to define the relationship. This letter serves as a record to document the understanding and agreement between the audit committee and the independent auditor. It provides the independent auditor the responsibility, accountability, and authority to conduct the audit.

29. Correct answer: B

Every audit is paid for and requested by a client, who is responsible for setting the scope, granting authority, and providing access to the auditee.

30. Correct answer: C

The work can be outsourced; however, the liability for failure remains with the company. One example is the Firestone tire failure affecting Ford Motor Company. Another is the lead paint used by subcontractors forcing the giant toy recall of 2007. Liability cannot be outsourced.

31. Correct answer: D

Audits should adhere to standards, guidelines, and best practices. Answer A represents a restriction on scope. B and C are components of answer D.

32. Correct answer: A

A skills matrix is used to identify the skills of each person and to ensure that the right person is performing the task. Using a skills matrix in planning is an excellent method to justify proper funding for training or additional personnel.

33. Correct answer: C

Embedded audit module (EAM) processes dummy transactions during the processing of genuine transactions. The intention is to determine whether the system is functioning correctly.

34. Correct answer: B

The auditor should never base the decision on the job position of the other person. All of the other choices are vague but truthful. Always assess the independence of the provider, check their qualifications, agree on scope and procedures used, and supervise and review their work. Don't use it if the results are questionable or fail to follow very high adherence to audit standards.

35. Correct answer: A

Strong controls will implement multiple types of preventative, detective, and corrective controls using a combined approach of administrative methods, physical methods, and technical methods. This is referred to as depth of control, hopefully using all nine layers. Using the bare minimum would be a weak control.

36. Correct answer: C

Approved audit charter outlines the auditor's responsibility, authority and accountability. The audit scope is specific to one audit and does not grant authority to perform an audit. A request from management to perform an audit is not sufficient because it relates to a specific audit. The approved audit schedule does not grant authority to perform an audit.

37. Correct answer: C

Inherent risks' exist independently of an audit and can occur because of the nature of the business. To successfully conduct an audit, it is important to be aware of the related business processes. To perform the audit the IS auditor needs to understand the business process, and by understanding the business process, the IS auditor better understands the inherent risks.

38. Correct answer: A

A risk-based audit approach focuses on the understanding of the nature of the business and being able to identify and categorize risk. Business risks impact the long-term viability of a specific business. Thus, an IS auditor using a risk-based audit approach must be able to understand business processes.

39. Correct answer: C

The risk of an error existing that could be material or significant when combined with other errors encountered during the audit, there being no related compensating controls, is the inherent risk. Control risk is the risk that a material error exists that will not be prevented or detected in a timely manner by the system of internal controls.

40. Correct answer: D

The IS auditor is not expected to ignore control weaknesses just because they are outside the scope of a current review. Further, the conduct of a detailed systems software review may hamper the audit's schedule and the IS auditor may not be technically competent to do such a review at this time. If there are control weaknesses that have been discovered by the IS auditor, they should be disclosed. By issuing a disclaimer this responsibility would be waived. Hence, the appropriate option would be to review the

systems software as relevant to the review and recommend a detailed systems software review for which additional resources may be recommended.

41. Correct answer: B

Short and long-term issues that drive audit planning can be heavily impacted by changes to the risk environment, technologies and business processes of the enterprise. Planning for deployment of available audit resources is determined by the audit assignments planned, which is influenced by the planning process. The audit charter reflects the mandate of top management to the audit function and resides at a more abstract level. Applicability of IS audit standards, guidelines and procedures is universal to any audit engagement and is not influenced by short- and long-term issues.

42. Correct answer: B

Facilitated workshops work well within business units. Process flow narratives and data flow diagrams would not be as effective since they would not necessarily identify and assess all control issues. Informal peer reviews similarly would be less effective for the same reason.

43. Correct answer: C

The first step in audit planning is to gain an understanding of the business's mission, objectives and purpose which in turn identifies the relevant policies, standards, guidelines, procedures, and organization structure. All other choices are dependent upon having a thorough understanding of the business's objectives and purpose.

44. Correct answer: A

Standard S5, Planning, establishes standards and provides guidance on planning an audit. It requires a risk-based approach.

45. Correct answer: C



A corrective control helps to correct or minimize the impact of a problem. Backup tapes can be used for restoring the files in case of damage of files, thereby reducing the impact of a disruption. Preventive controls are those that prevent problems before they arise. Backup tapes cannot be used to prevent damage to files and hence cannot be classified as a preventive control. Management controls modify processing systems to minimize a repeat occurrence of the problem. Backup tapes do not modify processing systems and hence do not fit the definition of a management control. Detective controls help to detect and report problems as they occur. Backup tapes do not aid in detecting errors.

46. Correct answer: D

A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

47. Correct answer: A

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.

48. Correct answer: C

Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

49. Correct answer: A

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.

50. Correct answer: C

The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

51. Correct answer: B

Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning.

52. Correct answer: A

The use of statistical sampling procedures helps minimize detection risk.

53. Correct answer: B

Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

54. Correct answer: C

A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can identify high-risk areas that might need a detailed review later.

55. Correct answer: C

When trying to determine the existence of unauthorized access to data by a user or program, the IS auditor will often review the system logs.

56. Correct answer: A

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

57. Correct answer: D

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

58. Correct answer: C

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

59. Correct answer: C

An IS auditor must first understand relative business processes before performing an application audit.

60. Correct answer: B

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

61. Correct answer: B

If proper identification and authentication are not performed during access control, no accountability can exist for any action performed.

62. Correct answer: C

In planning an audit, the most critical step is identifying the areas of high risk.

63. Correct answer: C

When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of the point at which controls are exercised as data flows through the system.

64. Correct answer: D

When implementing continuous-monitoring systems, an IS auditor's first step is to identify high risk areas within the organization.

65. Correct answer: D

Inherent risk is associated with authorized program exits (trap doors).

66. Correct answer: A

Lack of reporting of a successful attack on the network is a great concern to an IS auditor.

67. Correct answer: A

It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

68. Correct answer: C

The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

69. Correct answer: B

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.

70. Correct answer: B

IS auditors should review access-control lists (ACL) to determine user permissions that have been granted for a particular resource.

71. Correct answer: B

IS auditors should always check to ensure that password files are encrypted. IS auditors should always check to ensure that password files are encrypted.

72. Correct answer: A

A major IS audit concern is users' ability to directly modify the database.

73. Correct answer: B

Instead of simply reviewing the effectiveness and utilization of assets, an IS auditor is more concerned with adequate access control, appropriate access policies, and effectiveness of safeguards and procedures.

74. Correct answer: B

Decision trees use questionnaires to lead the user through a series of choices to reach a conclusion.

75. Correct answer: A

Rapid application development (RAD) is used to develop strategically important systems faster, reduce development costs, and still maintain high quality.

76. Correct answer: B

Inadequate user participation during system requirements definition is the most common reason for information systems to fail to meet the needs of users.

77. Correct answer: B

The project steering committee is responsible for the overall direction, costs, and timetables for systems-development projects.

78. Correct answer: A

Using a statistical sample to inventory the tape library is an example of a substantive test.

79. Correct answer: C

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

80. Correct answer: B

Detection risks are directly affected by the auditor's selection of audit procedures and techniques. Inherent risks are not usually affected by an IS auditor. Control risks are controlled by the actions of the company's management. Business risks are not affected by an IS auditor.

81. Correct answer: D

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.

82. Correct answer: D

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.

83. Correct answer: C

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.

84. Correct answer: A

Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

85. Correct answer: C

The use of continuous auditing techniques can improve system security when used in time-sharing environments that process a large number of transactions, but leave a scarce paper trail. Choice A is incorrect since the continuous audit approach often does require an IS auditor to collect evidence on



system reliability while processing is taking place. Choice B is incorrect since an IS auditor normally would review and follow up only on material deficiencies or errors detected. Choice D is incorrect since the use of continuous audit techniques depends on the complexity of an organization's computer systems.

86. Correct answer: B

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.

87. Correct answer: B

In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage. Understanding whether appropriate controls required to mitigate risks are in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be done to compare the actual state to an expected or desirable state.

88. Correct answer: D

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.

89. Correct answer: A

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.

90. Correct answer: D

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

91. Correct answer: A

The ISACA IS Auditing Guideline G15 on planning the IS audit states, 'An assessment of risk should be made to provide reasonable assurance that material items will be adequately covered during the audit work. This assessment should identify areas with a relatively high risk of the existence of material problems.' Definite assurance that material items will be covered during the audit work is an impractical proposition. Reasonable assurance that all items will be covered during the audit work is not the correct answer, as material items need to be covered, not all items.

92. Correct answer: A

Given an expected error rate and confidence level, statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size and quantify the probability of error (confidence coefficient). Choice B is incorrect because sampling risk is the risk of a sample not being representative of the population. This risk exists for both judgment and statistical samples.

Choice C is incorrect because statistical sampling does not require the use of generalized audit software. Choice D is incorrect because the tolerable error rate must be predetermined for both judgment and statistical sampling.

93. Correct answer: A

ISACA auditing standards require that an IS auditor plan the audit work to address the audit objectives. Choice B is incorrect because the auditor does not collect evidence in the planning stage of an audit. Choices C and D are incorrect because they are not the primary goals of audit planning. The activities

described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

94. Correct answer: A

Procedures are processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising in the course of an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate and the auditor's past experience plays a key role in making a judgment. ISACA's guidelines provide information on how to meet the standards when performing IS audit work. Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit and not of professional judgment. Professional judgment is not a primary input to the financial aspects of the audit.

95. Correct answer: D

When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation and evaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths-to determine if the controls are functioning. Lastly, the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

96. Correct answer: A

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.

97. Correct answer: A

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

98. Correct answer: B

The primary purpose for meeting with auditee prior to formally closing a review is to gain agreement on the findings. The other choices, though related to the formal closure of an audit, are of secondary importance.

99. Correct answer: B

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them. Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

100. Correct answer: A

An IS auditor's responsibilities for detecting fraud include evaluating fraud indicators and deciding whether any additional action is necessary or whether an investigation should be recommended. The IS auditor should notify the appropriate authorities within the organization only if it has determined that the indicators of fraud are sufficient to recommend an investigation. Normally, the IS auditor does not have authority to consult with external legal counsel.

101. Correct answer: B

If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure. The goal should be to enlighten the auditee or uncover new information of which an IS auditor may not have been aware. Anything that appears to threaten the auditee will lessen effective communications and set up an adversarial relationship. By the same token, an IS auditor should not automatically agree just because the auditee expresses an alternate point of view.

102. Correct answer: D

ISACA's standard on 'reporting' requires the IS auditor have sufficient and appropriate audit evidence to support the reported results. Statements from IS management provide a basis for obtaining concurrence on matters that cannot be verified with empirical evidence. The report should be based on evidence collected during the course of the review even though the auditor may have access to the work papers of other auditors. The results of an organizational control self-assessment (CSA) could supplement the audit findings. Choices A, B and C might be referenced during an audit but, of themselves, would not be considered a sufficient basis for issuing a report.

103. Correct answer: C

The IS auditor should make the final decision about what to include or exclude from the audit report. The other choices would limit the independence of the auditor.

104. Correct answer: A

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

105. Correct answer: A

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a control self-assessment (CSA) program depends on the degree to which line managers assume responsibility for controls- Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

106. Correct answer: A

The objective of control self-assessment is to have business management become more aware of the importance of internal control and their responsibility in terms of corporate governance. Reducing audit expenses is not a key benefit of control self-assessment (CSA). Improved fraud detection is important, but not as important as ownership, and is not a principal objective of CSA. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

107. Correct answer: A

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.

108. Correct answer: D

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

109. Correct answer: B

Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff is trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to

prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently) of access privileges that have officially been granted.

110. Correct answer: C

Cross-training is a process of training more than one individual to perform a specific job or procedure. This practice helps decrease the dependence on a single person and assists in succession planning. This provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations. However, in using this approach, it is prudent to have first assessed the risk of any person knowing all parts of a system and the related potential exposures. Cross-training reduces the risks addressed in choices A, B and D.

111. Correct answer: C

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

112. Correct answer: B

Inclusion in job descriptions of security responsibilities is a form of security training and helps ensure that staff and management are aware of their roles with respect to information security.

The other three choices are not criterion for evaluating security awareness training. Awareness is a criterion for evaluating the importance that senior management attaches to information assets and their protection. Funding is a criterion that aids in evaluating whether security vulnerabilities are being addressed, while the number of incidents that have occurred is a criterion for evaluating the adequacy of the risk management program.

113. Correct answer: A

The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff

assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

114. Correct answer: B

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.

115. Correct answer: A

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.

116. Correct answer: A

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.

117. Correct answer: A



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.

118. Correct answer: D

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.

119. Correct answer: D

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

