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

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.

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.

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.

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.

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.

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.

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

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.

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

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.

12. The use of statistical sampling procedures helps minimize:

A. sampling risk.

B. detection risk.

C. inherent risk.

D. control risk.

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.

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.

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.

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.

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

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.

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

A. audit planning.

B. controls.

C. vulnerabilities.

D. liabilities.

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.

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.

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

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.

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

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.

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

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.

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

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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

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

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.

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.

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.

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.

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

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.

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.

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.

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.

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.