1. What is the difference between a policy and a procedure?

a. Compliance to a policy is discretionary, and compliance to a procedure is mandatory.

b. A procedure provides discetionary advice to aid in decision making. The policy defines specific requirements to ensure compliance.

c. A policy is a high – level document signed by a person of authority, and compliance is mandatory. A procedure defines the mandatory steps to attain compliance.

d. A policy is a mid – level document issued to advise the reader of desired actions in the abcsence of a standard. The procedure describes suggested steps to use.

2. What does *fiduciary responbility* mean?

a. To use information gained for personal interests without breaching confidentiality of the client.

b. To act for the benefit of another person and place the responbilities to be fair and honest ahead of your own interest.

c. To follow the desires of the client and maintain total confidentiality even if illegal acts are discovered. The auditor shall never disclose information from an audit in order to protect the client.

d. None of the above.

3. What are common types of audits?

a. forensic, accounting, verification, regulatory

b. integrated, operational, compliance, administrative

c. financial, SAS-74, compliance, administrative

d. information system, SAS-70, regulatory, procedural

4. What is the difference between the word *should* and *shall* when used in regulations?

a. *shall* represents discretionary requirements, and *should* provides advice to the reader.

b. *should* indicates mandatory actions, whereas *shall* provides advisory information recommending actions when approproate.

c. *should* and *shall* are comparable in meaning. The difference is based on the individual circumstances faced by the audit.

d. *should* indicates actions that are discretionary according to need, whereas *shall* means the action is mandatory regardless of financial impact.

5. Which of following is *not* defined as a nonaudit role?

a. system designer

b. operational staff member

c. auditor

d. organizational manager

6. Why is it necessary to protect audit documentation and work papers?

a. the evidence gathered in an audit must be disclosed for regulatory compliance.

b. a paper trail is necessary to prove the auditor is right and the auditee is wrong.

c. the auditor will have to prove illegal activity in a court of law.

d. audit documentation work papers may reveal confidential information that should not be lost or diclosed.

7. What is the purpose of standard terms of reference?

a. to meet the legal requirement of regulatory compliance

b. to prove who is responsible

c. to ensure honest and unbiased communication

d. to ensure the requirements are clearly identified in a regulation

8. What does the term *auditor independence* relate to?

a. it is not an issue for auditors working for a consulting company.

b. it is required for and external audit.

c. an internal auditor must undergo certification training to be independent.

d. the audit committee bestows independence upon the auditor.

9. Which of the following is true concerning the roles of data owner, data user, and data custodian?

a. the data user implements controls as necessary.

b. the data custodian is responsible for specifying acceptable usage.

c. the data owner specifies controls.

d. the data custodian specifies security classification.

10. What is the definition of a standard as compared to a *guideline*?

a. standard are discretionary controls used with guidelines to aid the readers decision process.

b. standards are mandatory control designed to support a policy. Following guidelines is discretionary.

c. guidelines are recommended controls necessary to support standards, whics are discretionary.

d. guidelines are intended to designate a policy, whereas standard are used in the absence of a policy.

11. Who should issue the organizational policies?

a. policies should originate from the bottom and move up to the department manager for approval.

b. the auditor should issue the policies in accordance with standards and authorized by the highest level of management to ensure compliance.

c. the policy should be signed and enforced by any level of management.

d. the policy should be signed and enforced by the highest level of management.

12. The auditors final opinion is to be based on which of the following?

a. the objectives and verbal statements made by management

b. an understanding of managements desired audit results

c. the audit committees specifications

d. the results of evidence and testing

13. What is the purpose of ISACA's profesional ethics statement?

a. to clearly specify acceptable and unacceptable behavior

b. to provide procedural advisement to the new IS auditor

c. to provide instruction on how to deal with irregularities and illegal acts by the client

d. to provide advice on when it is acceptable for the auditor to deviate from audit standards

14. How does the auditor derive a final opinion?

a. from evidence gathered and the auditors observations

b. by representations and assurances of management

c. by testing the compliance of language used in organizational policies

d. under advice of the audit committee

15. What is the difference between a threat and a vulnerability?

a. threats are path that can be exploited by a vulnerability.

b. threats are risks and become a vulnerability if they occur.

c. vulnerabilities are a path that can be taken by a threat, resulting in a loss.

d. vulnerability is a negative event that will cause a loss if it occurs.

16. Which of the following statements is *not* true regarding the audit committee?

a. executives inside the organization oversee the audit committee and responsible for keeping the committee busy working on compliance programs.

b. executives can be hired and fired by the audit committee because this committee is responsible for management oversight.

c. the audit committee is composed of members from the board of directors. This committee has the authority to hire external auditors, and external auditors may meet with the committee on a quarterly basis without other executives present.

d. the audit committee provides senior executives a method of bringing problems into a confidential discussion for the purpose of exploring a resolution.

17. The type of audit checks attributes againt the design spesifications.

a. process

b. system

c. compliance

d. product

18. Assessments and audits have several points in common. Which of the following statements provides the best description of an assessment compared to an audit?

a. audits are more formal than assessments.

b. they are similar in nature; the difference is in wording.

c. both provide reports that can be used for licensing purposes.

d. assessment reports provide a high assurance of the situation.

19. The audit may uncover irregularities and illegal acts that require disclosure. The auditor is obligated to promptly disclose this information to the authorities.

a. true

b. false

20. Which of the following statements is true?

a. the auditee is the person running the audit, and the client is the subject of the audit.

b. the auditor is the person running the audit, and the client is the subject of the audit.

c. the client is the person setting the scope for the audit, and the auditor performs the work.

d. the client pays for the audit, and the auditor sets the scope of the audit that will follow.

21. How should the auditor assist in the remediation of problems found during the audit?

a. take ownership of the issue and participate in designing the plan for fixing the problem.

b. the auditor should decide whether the problem is major or minor, and then advise the auditee with a specific solution after considering the impact to the business.

c. the auditor should help the auditees. The auditor can add value by defining the spesific steps necessary for remediation of the problem.

d. the auditor should never take ownership of problems found. Auditor are encouraged the provide general advice to the auditee, including an explanation of what to look for during the audit.

22. Which of the following in a business organization will be held liable by the government for failures of internal controls?

a. president, vice presidents, and other true corporate officers.

b. board of directors, president, vice presidents, departement directors, and managers

c. all member of management

d. board of directors, CEO, CFO, CIO, and departement directors

23. Which of the following is the best description of an ongoing audit program for regulatory compliance?

a. an audit is performed once for the entire year, and then repeated by using the same information for each successive year.

b. an audit may be automated by using audit program software.

c. an audit is a series of unique projects of short duration that add up to cover all the steps necessary for annual compliance.

d. an audit is a series fo assessments performed by the auditee for the purpose of licensing and regulatory compliance.

24. What term simply means the right people of authority looked at the issue, made an intelligent decision, and took appropriate action?

a. leadership

b. corporate responsibility

c. chain of command

d. governance

25. Which of the following assurance methods is acceptable for external use, including licensing?

a. independent audit

b. assessment

c. external audit

d. internal audit

26. What is the primary purpose of the IT steering committee?

a. make technical recommendations

b. identify business issues and objectives

c. review vendor contracts

d. specify the IT organizational structure

27. Which of these strategies is used in business process reengineering with an incremental approach?

a. bottom – up

b. end – state

c. uncostrained

d. top – down

28. The Software Engineering Institute's Capability Maturity Model (CMM) is best described by which of the following statements?

a. measurement of resources necessary to ensure a reduction in coding defects

b. documentation of accomplishments achieved during program development

c. relationship of application performance to the user's stated requirement

d. baseline of the currect progress or regression

29. What would be the area of greatest interest during an audit of a business process reengineering (BPR) project?

a. the steering committee approves sufficient controls for fraud detection.

b. planning methods inclue program evaluation review technique (PERT).

c. risk management planning with alignment of the project to business objectives.

d. vendor participation including documentation, installation assistance, and training.

30. What is the correct sequence for benchmark processes in business process reengineering (BPR) projects?

a. plan, research, observe, analyze, adapt, improve

b. research, test, plan, adapt, analyze, improve

c. plan, observe, analyze, improve, test

d. observe, research, analyze, adapt, plan, implement

31. Which of the following statements is true concerning the steering committee?

a. steering committee membership is composed of directors from each departement.

b. the steering committee focuses the agenda on IT issues.

c. absence of a formal charter indicates a lack of controls.

d. the steering committee conducts formal management oversight reviews.

32. Which of the following is not an advantage of a mature project management office (PMO)?

a. advanced planning assistance

b. master project register

c. coordination of projects across departements

d. independent projects

33. The Capability Maturity Model (CMM) contains five levels of achievement. Which of the following answers contains three of the levels in proper sequence?

a. initial, managed, repeatable

b. initial, managed, defined

c. defined, managed, optimized

d. managed, defined, repeatable

34. The organization's   is focused on exploiting trends forecast in the next three to five years.

a. strategy

b. long – term planning

c. operational plan

d. managerial plan

35. Which of the following is the best example of mandatory controls?

a. user account permissions

b. corporate guidelines

c. acceptable use policy

d. government regulation

36. During the selection of a BPR project, which of the following is the ideal target with the highest return?

a. marginal process

b. nonworking process

c. working process

d. excluded process

37. Who sets the priorities and objectives of the IT balanced scorecard (BSC)?

a. chief information officer (CIO)

b. chief financial officer (CFO)

c. chief executive officer (CEO)

d. IT steering committee

38. Which of the following business process reengineering (BPR) risk are likely to occur during the design phase?

a. transition risk, skill risk, financial risk

b. management risk, technical risk, HR risk

c. technical risk, detection rreenginisk, audit risk

d. scope risk, skill risk, political risk

39. Which of the following answers contains the steps for business process reengineering (BPR) in proper sequence?

a. diagnose, envision, redesign, reconstruct

b. evaluate, envision, redesign, reconstruct, review

c. envision, initiate, diagnose, redesign, reconstruct, review

d. initiate, evaluate, diagnose, reconstruct, review

40. What is the name of the decentralized control method enabling someone to make a decision based on their own options?

a. executive

b. discretionary

c. detailed

d. mandatory