Review Question bab 1

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

Review Question bab 2

1. 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

2. 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

3. 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

4. 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.

5. 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

6. 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.

7. 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

8. 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

9. 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

16. What is the primary purpose of employee contracts?

a. define the relationship as work for hire

b. prevent individuals from ever working for competitors

c. enforce the requirement to join a union

d. specify the terms of employee benefits

17. Which of the following is a governance problem that may occur when projects are funded under the “sponsor pays” method?

a. deliverables are determined by the sponsor.

b. the definition of quality may balanced be insufficient.

c. the sponsor may not implement the proper controls.

d. the sponsor may not have enough funding.

18. Which of the following is not a reason cited in the text balanced scorecard (BSC) implementations could fail?

a. politics of losing the department budget

b. top management provides full support

c. lack of BSC training and awareness

d. empire building by the department head

19. *Shadow organization* refers to two groups performing similar functions under different departments. What does the presence of a shadow organization indicate?

a. twice the support coverage

b. a relationship of trust and proper delegation of authority

c. executive distrust or failure to integrate

d. a sponsor who is ccoperating as a team player with separation of duties

20. Which type of charge – back scheme is notorious for violating separaion of duties or for attempting to exceed authority?

a. sponsor pays

b. actual usage billing

c. charge – back

d. budgeted cost

21. What is the advantage of using PERT analysis during project for business process reengineering (BPR)?

a. it charts a detailed sequence of individual activies.

b. it is a critical path methodology

c. it is used to perform root cause analysis

d. it enables the use of decision tree reporting

22. Which statement about the Capability Maturity Model is *not* true?

a. level 3 provides quantitative measurement of the process output.

b. level 3 processes have published objectives, measurements, and standards that are in effect across departmental boundaries.

c. level 5 provides maximum control in outsourcing because the definition of requirement is very specific.

d. level 5 maturity converts a product into a commodity and allows a company to payless and demand unquetionable aherence to management's authority.

23. Which of the following statements has the best correlation to the definition of *strategy*?

a. defines the techniques to be used in support of the business objective

b. defines the necessary procedures to accomplish the goal

c. defines guidelines to follow in a recipe for success

d. defines what business we are in for the next three years

24. Why is change control considered a governance issue?

a. it forces separation of duties to ensure that at least two people agree with the decision.

b. change control increases the number of people employed and therefore provides a valuable economic advantage.

c. it allows management to hire less – skilled personnel and still get the same results.

d. proper implementation of governance saves money by reducing the need for change control

25. Which of the following is *not* considered a control failure?

a. using a policy that lacks a detective mechanism to identify violations

b. modifying an ineffective procedure outside of change control

c. testing to discover how many policy violations have occured

d. implementing a policy or standard without consequences of failure

Review Questions bab 3

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. unstatified 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 ton an IS auditor?

a. control, detection, noncompliance, risk of strike

b. inherent, noninherent, 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 test 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 100 percent sample?

a. attribute

b. stop – and – go

c. cell

d. discovery

16. 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

17. The auditor is permitted to deviate from professional audit standard 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.

18. 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

19. Who has the responsibility of setting the scope of the audit?

a. auditor

b. client

c. audit manager

d. auditee

20. What is the biggest issue with the decision to transfer risk an outsourced contractor?

a. there is potensial 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. outsorcing shields the company from intrinsic risks.

21. 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 standars, guidelines, and best practices

22. During audit planning, severals document 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

23. 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

24. 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.

25. 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 occuring

c. using at least one control in each of the three categorie of preventative, detective, corrective

d. implementing comprehensive pervasive controls inside of an ERP application

Review Question bab 4

1. Which RAID level does not improve fault tolerance?

a. RAID level 0

b. RAID level 1

c. RAID level 2

d. RAID level 5

2. Which type of network device directs packets throught the Internet?

a. hubs

b. routers

c. repeaters

d. modems

3. Which of the following is a list of OSI model levels fromt the top down?

a. application, physical, session, transport, network, data – link, presentation

b. presentation, data – link, network, transport, session, physical, application

c. application, presentation, session, transport, network, data – link, physical

d. presentation, data – link, network, transport, session, physical, application

4. Which of the following is the most popular media for connecting workstation in a corporate environment?

a. coaxial

b. shielded twisted – pair

c. unshielded twisted – pair

d. fiber optics

5. What is one of the first priorities for an auditor reviewing security of the client's network?

a. checking firewall configuration settings

b. understandings details of network architecture and implementation

c. verifying the use of strong passwords

d. reviewing records to indicate systems are monitored and IDPS system are working properly

6. At which layer of the OSI model does a gateway operate?

a. layer 3

b. layer 5

c. layer 6

d. layer 7

7. Which of the following network topologies provides a redundant path for communication?

a. fiber – optic

b. star

c. ring

d. bus

8. What is the purpose of the address resolution protocol (ARP)?

a. find the ip address

b. find the mailing address

c. find the MAC address

d. find the domain name

9. What is the security issue regarding packet analyzers?

a. viewing passwords

b. special training

c. purchase cost

d. only for auditor's use

10. Which of the following is *not* a function of the operating system?

a. filing system for storage and retrieval

b. detection of system penetration

c. user interface (shell)

d. security functions with even logging

11. Which of the following protocols is likely to be used for monitoring the health of the network?

a. OSI

b. SNMP

c. SMTP

d. RIP

12. What is the difference between a router and a switch?

a. both operate at layer 2; the router routes traffic, and the switch connects various user to the network

b. both operate at layer 3; the router routes traffic, and the switch connects various user to the network

c. they operate at OSI layer 3 and layer 2, respectively

d. they operate at OSI layer 2 and layer 3, respectively

13. Which type of network cabling is relatively immune to interference, difficult to tap, and can run extended distances?

a. coaxial

b. shielded twisted – pair

c. unshielded twisted – pair

d. fiber – optic

14. Which type of memory is used to permanently record programs on solid – state chips and retains the data even after power is turned off?

a. random access memory

b. read – only memory

c. flash memory

d. optical memory

15. Network switches have frequently replaced the use of network hubs. What is the issue in regard to monitoring when using a network switch?

a. hubs will pass all traffic across ports.

b. SNMP must be configured properly.

c. switches operate at OSI layer 2.

d. switches filter traffic between ports.

16. Which of the following statements is false concerning the communication circuits used in wide area networking?

a. switched virtual circuits (SVCs) may use different routes to reach the destination.

b. digital circuit – swithced lines are dedicated between location.

c. packet – switched circuits are charged according to distance.

d. circuit – switched lines allow the user to transmit any amount of data.

17. The architectre of a computer with a single central processing unit (CPU) contains which of the following points that represents the biggest area of interests to the auditor?

a. time – sharing is used to service the different processing tasks one at time.

b. an upgrade to a multiprocessor system should be justified to improve response times.

c. system control software is halted between processing tasks.

d. a pipeline design should be implemented to minimize system idle time.

18. Which of the following RAID implementations is designed for the disk array to be configured into one large virtual disk partition using high – speed asynchronous data transfer?

a. RAID-1

b. RAID-7

c. RAID-5

d. RAID-6

19. In network communications, the transmission sends a single data packet to multiple addresses for applications such as Internet – based television.

a. broadcast

b. multicast

c. visicast

d. unicast

20. Which of the following network protocols uses the MAC address to find a computer's IP address?

a. domain name system (DNS) protocol

b. reserve domain name system (RDNS) protocol

c. reserve address resolution protocol (RARP)

d. address resolution protocol (ARP)

21. The Internet Protocol (IP) contains a special feature for separating different types of communication between network addresses. What is this feature called?

a. software port

b. hardware port

c. dynamic host configutation protocol

d. virtual communication protocol

22. Default settings are used by vendors to help users get the system up and running. What is the auditor's primary area of interest regarding default settings?

a. save time and money for the user

b. represent the manufacturer's recommended settings

c. indicate well – known settings published by the vendor

d. reduce supprot headaches, which increased operational uptime

23. The can be poisoned by a hacker to prevent the computer from converting computer names into network addresses.

a. address resolution protocol (ARP)

b. reverse address resolution protocol (RARP)

c. border gateway protocol (BGP)

d. domain name system (DNS)

24. Which of the following best describes ad hoc networks?

a. dynamic connection of remote devices

b. fixed connection of devices

c. active device host communication

d. wirelss connection using a static configuration

25. Except for the older plain old telephone service (POTS) lines, what is the primary issue of remote access over telephone company circuits?

a. the cost of service may be expensive.

b. the available bandwidth may be to slow.

c. a remote – access circuit is always active to accept communication.

d. remote access servers (RASs) may be used to create a dial – up modem pool.