CISA EXAM PRACTICE - LATIHAN SOAL CISA

By Hery Purnama

1. For an auditor, it is very important to understand the different forms of project organization and their implication in the control of project management activities. In which of the following project organization form is management authority shared between the project manager and the department head?

- ○ Influence project organization
- ○ Pure project organization
- ● Matrix project organization
- ○ Forward project organization

2. Which of the following type of testing validate functioning of the application under test with other system, where a set of data is transferred from one system to another?

- ● Interface testing
- ○ Unit Testing
- ○ System Testing
- ○ Final acceptance testing

3. Which of the following statement correctly describes the difference between black box testing and white box testing?

- ● Black box testing focuses on functional operative effectiveness where as white box assesses the effectiveness of software program logic
- ○ White box testing focuses on functional operative effectiveness where as black box assesses the effectiveness of software program logic
- ○ White box and black box testing focuses on functional operative effectiveness of an information systems without regard to any internal program structure
- ○ White box and black box testing focuses on the effectiveness of the software program logic

4. Which of the following risk handling technique involves the practice of being proactive so that the risk in question is not realized?

- ○ Risk Mitigation

- ○ Risk Acceptance
- ● Risk Avoidance
- ○ Risk transfer

5. What are the different types of Audits?

- ● Compliance, financial, operational, forensic and integrated
- ○ Compliance, financial, operational, G9 and integrated
- ○ Compliance, financial, SA1, forensic and integrated
- ○ Compliance, financial, operational, forensic and capability

6. In which of the following cloud computing service model are applications hosted by the service provider and made available to the customers over a network?

- ● Software as a service
- ○ Data as a service
- ○ Platform as a service
- ○ Infrastructure as a service

7. Who is responsible for reviewing the result and deliverables within and at the end of each phase, as well as confirming compliance with requirements?

- ○ Project Sponsor
- ● Quality Assurance
- ○ User Management
- ○ Senior Management

8. As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains a significant change or addition of new functionality?

- ● Major software Release
- ○ Minor software Release
- ○ Emergency software release
- ○ General software Release

9. Why would a database be renormalized?

- ○ To ensure data integrity
- ● To increase processing efficiency
- ○ To prevent duplication of data
- ○ To save storage space

10. Which of the following is not a common method of multiplexing data?

- ● Analytical multiplexing
- ○ Time-division multiplexing
- ○ Asynchronous time-division multiplexing
- ○ Frequency division multiplexing

11. Which of the following is the BEST way to detect software license violations?

- ○ Implementing a corporate policy on copyright infringements and software use.
- ○ Requiring that all PCs be diskless workstations.
- ○ Installing metering software on the LAN so applications can be accessed through the metered software
- ● Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.

12. Who is responsible for providing technical support for the hardware and software environment by developing, installing and operating the requested system?

- ● System Development Management
- ○ Quality Assurance
- ○ User Management
- ○ Senior Management

13. Which of the following type of testing uses a set of test cases that focus on control structure of the procedural design?

- ○ Interface testing

- [x] Unit Testing
- [ ] System Testing
- [ ] Final acceptance testing

14. Which of the following type of testing has two major categories: QAT and UAT?

- [ ] Interface testing
- [ ] Unit Testing
- [x] System Testing
- [ ] Final acceptance testing

15. Which of the following data validation control validates input data against predefined range values?

- [x] Range Check
- [ ] Table lookups
- [ ] Existence check
- [ ] Reasonableness check

16. Which of the following audit risk is related to material error exist that would not be prevented or detected on timely basis by the system of internal controls?

- [x] Inherent Risk
- [ ] Control Risk
- [ ] Detection Risk
- [ ] Overall Audit Risk

17. In which of the following payment mode, the payer creates payment transfer instructions, signs it digitally and sends it to issuer?

- [ ] Electronic Money Model
- [ ] Electronics Checks model
- [x] Electronic transfer model
- [ ] Electronic withdraw model

18. Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a pattern of behaviors, effects, assumptions, attitude and ways of doing things?

- ○ Governing
- ● Culture
- ○ Enabling and support
- ○ Emergence

19. Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management?

- ○ Governing
- ○ Culture
- ○ Enabling and Support
- ● Emergence

20. Which of the following transmission media would NOT be affected by cross talk or interference?

- ○ Copper cable
- ○ Radio System
- ○ Satellite radio link
- ● Fiber optic cables

21. Which of the following factor is LEAST important in the measurement of critical success factors of productivity in the SDLC phases?

- ○ Dollar Spent per use
- ○ Number of transactions per month
- ○ Number of transactions per user
- ● Number of occurrences of fraud/misuse detection

22. Which of the following is NOT an example of preventive control?

- ○ Physical access control like locks and door

○ User login screen which allows only authorize user to access website

○ Encrypt the data so that only authorize user can view the same

● Duplicate checking of a calculations

23. Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?

○ Initial, Managed, Defined, Quantitatively managed, optimized

○ Initial, Managed, Defined, optimized, Quantitatively managed

● Initial, Defined, Managed, Quantitatively managed, optimized

○ Initial, Managed, Quantitatively managed, Defined, optimized

24. Identify the INCORRECT statement from below mentioned testing types

● Recovery Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems

○ Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour

○ Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process

○ Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process

25. In which of the following database model is the data organized into a tree-like structure, implying a single parent for each record?

● Hierarchical database model

○ Network database model

○ Relational database model

○ Object-relational database model

26. Which of the following type of a computer network covers a limited area such as a home, office or campus?

- [x] LAN
- [ ] WAN
- [ ] SAN
- [ ] PAN

27. Which of the following would BEST maintain the integrity of a firewall log?

- [ ] Granting access to log information only to administrators
- [ ] Capturing log events in the operating system layer
- [ ] Writing dual logs onto separate storage media
- [x] Sending log information to a dedicated third-party log server

28. When performing a database review, an IS auditor notices that some tables in the database are not normalized. The IS auditor should next:

- [ ] recommend that the database be normalized
- [ ] review the conceptual data model
- [ ] review the stored procedures.
- [x] review the justification.

29. Which of the following step of PDCA request a corrective actions on significant differences between the actual versus the planned result?

- [ ] Plan
- [ ] Do
- [ ] Check
- [x] Act

30. Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?

- [ ] Initial, Managed, Defined, Quantitatively managed, optimized
- [ ] Initial, Managed, Defined, optimized, Quantitatively managed
- [x] Initial, Defined, Managed, Quantitatively managed, optimized

- ○ Initial, Managed, Quantitatively managed, Defined, optimized

31. Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?

- ○ Bridge
- ○ Repeater
- ○ Router
- ● Gateway

32. Which of the following ISO/OSI layers performs transformations on data to provide a standardized application interface and to provide common communication services such as encryption?

- ○ Application layer
- ○ Session layer
- ● Presentation layer
- ○ Transport layer

33. Which of the following is NOT a defined ISO basic task related to network management?

- ○ Fault management
- ○ Accounting resources
- ○ Security management
- ● Communications management

34. Who provides the funding to the project and works closely with the project manager to define critical success factor (CSF)?

- ● Project Sponsor
- ○ Security Officer
- ○ User Management
- ○ Senior Management

35. Identify the INCORRECT statement from below mentioned testing types

● Recovery Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems

○ Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour

○ Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process

○ Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process

36. Which of the following audit include specific tests of control to demonstrate adherence to specific regulatory or industry standard?

● Compliance Audit

○ Financial Audit

○ Operational Audit

○ Forensic audit

37. Why would a database be renormalized?

○ To ensure data integrity

● To increase processing efficiency

○ To prevent duplication of data

○ To save storage space

38. Which of the following type of testing uses a set of test cases that focus on control structure of the procedural design?

○ Interface testing

● Unit Testing

○ System Testing

○ Final acceptance testing

39. Which of the following ACID property in DBMS requires that each transaction is "all or nothing"?

- ● Atomicity
- ○ Consistency
- ○ Isolation
- ○ Durability

40. Which of the following database model allow many-to-many relationships in a tree-like structure that allows multiple parents?

- ○ Hierarchical database model
- ● Network database model
- ○ Relational database model
- ○ Object-relational database model

41. Which of the following is a telecommunication device that translates data from digital to analog form and back to digital?

- ○ Multiplexer
- ● Modem
- ○ Protocol converter
- ○ Concentrator

42. What is the most effective means of determining that controls are functioning properly within an operating system?

- ○ Interview with computer operator
- ● Review of software control features and/or parameters
- ○ Review of operating system manual
- ○ Interview with product vendor

43. Which of the following characteristics pertaining to databases is not true?

- ○ A data model should exist and all entities should have a significant name
- ● Justifications must exist for normalized data.

- ○ No NULLs should be allowed for primary keys.
- ○ All relations must have a specific cardinality

44. Who is responsible for ensuring that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures?

- ○ Project Sponsor
- ● Security Officer
- ○ User Management
- ○ Senior Management

45. Who is responsible for reviewing the result and deliverables within and at the end of each phase, as well as confirming compliance with requirements?

- ○ Project Sponsor
- ● Quality Assurance
- ○ User Management
- ○ Senior Management

46. Which of the following statement correctly describes the difference between QAT and UAT?

- ● QAT focuses on technical aspect of the application and UAT focuses on functional aspect of the application
- ○ UAT focuses on technical aspect of the application and QAT focuses on functional aspect of the application
- ○ UAT and QAT both focuses on functional aspect of the application
- ○ UAT and QAT both focuses on technical aspect of the application

47. Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?

- ○ Parallel Test
- ○ Black box testing
- ● Regression Testing

- ○ Pilot Testing

48. Which of the following is the process of feeding test data into two systems – the modified system and alternative system and comparing the result?

- ● Parallel Test
- ○ Black box testing
- ○ Regression Testing
- ○ Pilot Testing

49. Which of the following control make sure that input data comply with predefined criteria maintained in computerized table of possible values?

- ○ Range Check
- ● Table lookups
- ○ Existence check
- ○ Reasonableness check

50. Which of the following control is intended to discourage a potential attacker?

- ● Deterrent
- ○ Preventive
- ○ Corrective
- ○ Recovery

51. Which of the following step of PDCA establishes the objectives and processes necessary to deliver results in accordance with the expected output?

- ● Plan
- ○ do
- ○ check
- ○ act

52. For an auditor, it is very important to understand the different forms of project organization and their implication in the control of project management activities. In which of the following

project organization form is management authority shared between the project manager and the department head?

- ○ Influence project organization
- ○ Pure project organization
- ● Matrix project organization
- ○ Forward project organization

53. Which of the following layer of the OSI model provides a standard interface for applications to communicate with devices on a network?

- ● Application layer
- ○ Presentation layer
- ○ Session layer
- ○ Transport layer

54. Which of the following is the BEST type of program for an organization to implement to aggregate, correlate and store different log and event files, and then produce weekly and monthly reports for IS auditors?

- ○ A security information event management (SIEM) product
- ○ An open-source correlation engine
- ● A log management tool
- ○ An extract, transform, load (ETL) system

55. An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

- ○ Consistency
- ○ Isolation
- ○ Durability
- ● Atomicity

56. Which is the best party to conduct access reviews?

○ A. Users’ managers

○ B. Information security manager

○ C. IT service desk

● D. Department head

57. Which of the following BEST provides access control to payroll data being processed on a local server?

○ A. Logging access to personal information

○ B. Using separate passwords for sensitive transactions

● C. Using software that restricts access rules to authorized staff

○ D. Restricting system access to business hours

58. An organization is proposing to install a single sign-on facility giving access to all systems. The organization should be aware that:

● A. maximum unauthorized access would be possible if a password is disclosed.

○ B. user access rights would be restricted by the additional security parameters.

○ C. the security administrator’s workload would increase.

○ D. user access rights would be increased.

59. Michael wants to improve the risk management process in his organization by creating content that will help management understand when certain risks should be accepted and when certain risks should be mitigated. The policy that Michael needs to create is known as:

- ○ A. A security policy
- ○ B. A control framework
- ● C. A risk appetite statement
- ○ D. A control testing procedure

60. In a typical risk management process, the best person(s) to make a risk treatment decision is:

- ○ A. The chief risk officer (CRO)
- ○ B. The chief information officer (CIO)
- ● C. The department head associated with the risk
- ○ D. The chief information security officer (CISO)

61. The ultimate responsibility for an organization's cybersecurity program lies with:

- ● A. The board of directors
- ○ B. The chief executive officer (CEO)
- ○ C. The chief information officer (CIO)

○ D. The chief information security officer (CISO)

62. Which of the following BEST determines whether complete encryption and authentication protocols for protecting information while being transmitted exist?

○ A. A digital signature with RSA has been implemented.

● B. Work is being done in tunnel mode with the nested services of authentication header (AH) and encapsulating security payload (ESP).

○ C. Digital certificates with RSA are being used.

○ D. Work is being done in transport mode with the nested services of AH and ESP.

63. Which of the following is the MOST effective preventive antivirus control?

○ A. Scanning email attachments on the mail server

○ B. Restoring systems from clean copies

○ C. Disabling universal serial bus ports

● D. An online antivirus scan with up-to-date virus definitions

64. The best person or group to make risk treatment decisions is:

○ A. The chief information security officer (CISO)

○ B. The audit committee of the board of directors

● C. The cybersecurity steering committee

○ D. External auditors

65. An IS auditor has just completed a review of an organization that has a mainframe computer and two database servers where all production data reside. Which of the following weaknesses would be considered the MOST serious?

○ A. The security officer also serves as the database administrator.

● B. Password controls are not administered over the two database servers.

○ C. There is no business continuity plan for the mainframe system's noncritical applications.

○ D. Most local area networks do not back up file-server-fixed disks regularly.

66. Which of the following characterizes a distributed denial-of-service attack?

● A. Central initiation of intermediary computers to direct simultaneous spurious message traffic at a specified target site

○ B. Local initiation of intermediary computers to direct simultaneous spurious message traffic at a specified target site

○ C. Central initiation of a primary computer to direct simultaneous spurious message traffic at multiple target sites

○ D. Local initiation of intermediary computers to direct staggered spurious message traffic at a specified target site

67. Which of the following concerns about the security of an electronic message would be addressed by digital signatures?

○ A. Unauthorized reading

● B. Theft

○ C. Unauthorized copying

○ D. Alteration

68. 1. Management's control of information technology processes is best described as:

○ A. Information technology policies

○ B. Information technology policies along with audits of those policies

● C. Information technology governance

○ D. Metrics as compared to similar organizations

69. In a U.S. public company, a CIO will generally report the state of the organization's IT function to:

○ A. The Treadway Commission

○ B. Independent auditors

○ C. The U.S. Securities and Exchange Commission

● D. The board of directors

70. An IS auditor reviewing the configuration of a signature-based intrusion detection system would be MOST concerned if which of the following is discovered?

● A. Auto-update is turned off.

○ B. Scanning for application vulnerabilities is disabled.

○ C. Analysis of encrypted data packets is disabled.

○ D. The IDS is placed between the demilitarized zone and the firewall.

71. What is the best method for ensuring that an organization's IT department achieves adequate business alignment?

○ A. Find and read the organization's articles of incorporation.

● B. Understand the organization's vision, mission statement, and objectives.

○ C. Determine who the CIO reports to in the organization.

○ D. Study the organization's application portfolio.

72. Roberta has located her organization's mission statement and a list of strategic objectives. What steps should Roberta take to ensure that the IT department aligns with the business?

● A. Discuss strategic objectives with business leaders to better understand what they wish to accomplish and what steps are being taken to achieve them.

○ B. Develop a list of activities that will support the organization's strategic objectives, and determine the cost of each.

○ C. Select those controls from the organization's control framework that align to each objective, and then ensure that those controls are effective.

○ D. Select the policies from the organization's information security policy that are relevant to each objective, and ensure that those policies are current.

73. A new CIO in an organization is building its formal IT department from the ground up. In order to ensure collaboration among business leaders and department heads in the organization, the CIO should form and manage:

○ A. A technology committee of the board of directors

● B. An IT steering committee

○ C. An audit committee of the board of directors

○ D. A business-aligned IT policy

74. An organization processes payroll and expense reports in an SaaS-based environment to thousands of corporate customers. Those customers want assurance that the organization's processes are effective. What kind of an audit should the organization undertake?

○ A. Compliance audit

○ B. Operational audit

- [x] C. Service provider audit
- [ ] D. IS audit

75. An auditor is auditing an organization's user account request and fulfillment process. What is the first type of evidence collection the auditor will likely want to examine?

- [ ] A. Observation
- [x] B. Document review
- [ ] C. Walkthrough
- [ ] D. Corroborative inquiry

76. A lead auditor is building an audit plan for a client's financial transaction processing system. The audit will take approximately three months. Which of the following is the best approach for reporting audit exceptions to the audit client?

- [ ] A. Report the exceptions to the audit committee.
- [ ] B. List the exceptions in the final audit report.

○ C. Include the exceptions in a weekly status report.

● D. Advise the client of exceptions as they are discovered and confirmed.

77. Which of the following is true about the ISACA Audit Standards and Audit Guidelines?

● A. ISACA Audit Standards are mandatory.

○ B. ISACA Audit Standards are optional.

○ C. ISACA Audit Guidelines are mandatory.

○ D. ISACA Audit Standards are only mandatory for SOX audits.

78. The classification based on criticality of a software application as part of an IS business continuity plan is determined by the:

● A. nature of the business and the value of the application to the business.

○ B. replacement cost of the application.

○ C. vendor support available for the application.

○ D. associated threats and vulnerabilities of the application.

79. An IS auditor should be involved in:

● A. observing tests of the disaster recovery plan.

○ B. developing the disaster recovery plan.

○ C. maintaining the disaster recovery plan.

○ D. reviewing the disaster recovery requirements of supplier contracts.

80. An auditor is auditing an organization's identity and access management program. The auditor has found that automated workflows are used to receive and track access requests and approvals. However, the auditor has identified a number of exceptions where subjects were granted access without the necessary requests and approvals. What remedy should the auditor recommend?

○ A. Monthly review of access approvers

○ B. Annual review of access approvers

○ C. Annual user access reviews

● D. Monthly user access reviews

81. Which of the following would allow an enterprise to extend its intranet across the Internet to its business partners?

● A. Virtual private network

○ B. Client-server

○ C. Dial-up access

○ D. Network service provider

82. Data mirroring should be implemented as a recovery strategy when:

● A. recovery point objective (RPO) is low.

○ B. recovery point objective (RPO) is high.

○ C. recovery time objective (RTO) is high.

○ D. disaster tolerance is high.

83. Which of the following components of a business continuity plan is PRIMARILY the responsibility of an organization's IS department?

○ A. Developing the business continuity plan

○ B. Selecting and approving the recovery strategies used in the business continuity plan

○ C. Declaring a disaster

● D. Restoring the IT systems and data after a disaster

84. A lead auditor is building an audit plan for a client's financial accounting system. The plan calls for

periodic testing of a large number of transactions throughout the audit project. What is the best approach for accomplishing this?

○ A. Reperform randomly selected transactions.

○ B. Periodically submit test transactions to the audit client.

● C. Develop one or more CAATs.

○ D. Request a list of all transactions to analyze.

85. Why are preventive controls preferred over detective controls?

○ A. Preventive controls are easier to justify and implement than detective controls.

○ B. Preventive controls are less expensive to implement than detective controls.

● C. Preventive controls stop unwanted events from occurring, while detective controls only record them.

○ D. Detective controls stop unwanted events from occurring, while preventive controls only record them.

86. Which one of the following provides the BEST method for determining the level of performance provided by similar information processing facility environments?

- A. User satisfaction
- B. Goal accomplishment
- C. Benchmarking
- D. Capacity and growth planning

87. For mission critical systems with a low tolerance to interruption and a high cost of recovery, the IS auditor, in principle, recommends the use of which of the following recovery options?

- A. Mobile site
- B. Warm site
- C. Cold site
- D. Hot site

88. An auditor is examining an IT organization's change control process. The auditor has determined that change advisory board (CAB) meetings take place on Tuesdays and Fridays, where planned changes are discussed and approved. The CAB does not discuss emergency changes that are not approved in advance. What opinion should the auditor reach

concerning emergency changes?

○ A. The CAB should not be discussing changes made in the past.

● B. The CAB should be discussing recent emergency changes.

○ C. Personnel should not be making emergency changes without CAB permission.

○ D. Change control is concerned only with planned changes, not emergency changes.

89. An audit project has been taking far too long, and management is beginning to ask questions about its schedule and completion. This audit may be lacking:

● A. Effective project management

○ B. Cooperation from individual auditees

○ C. Enough skilled auditors

○ D. Clearly stated scope and objectives

90. An auditor is auditing the user account request and fulfillment process. The event population consists of

hundreds of transactions, so the auditor cannot view them all. The auditor wants to view a random selection of transactions. This type of sampling is known as:

- ○ A. Judgmental sampling
- ○ B. Random sampling
- ○ C. Stratified sampling
- ● D. Statistical sampling

91. An organization processes payroll and expense reports in an SaaS-based environment to thousands of corporate customers. Those customers want assurance that the organization's processes are effective. What kind of an audit should the organization undertake?

- ○ A. AUP
- ○ B. PA-DSS
- ○ C. PCI-DSS
- ● D. SSAE18

92. When conducting an audit of client-server database security, the IS auditor should be MOST concerned about the availability of:

- ● A. system utilities.
- ○ B. application program generators.
- ○ C. systems security documentation.
- ○ D. access to stored procedures.

93. The IT Assurance Framework consists of all of the following except:

- ○ A. ISACA Code of Professional Ethics
- ○ B. IS audit and assurance standards
- ● C. ISACA Audit Job Practice
- ○ D. IS audit and assurance guidelines

94. A conspicuous video surveillance system would be characterized as what type(s) of control?

- ● A. Detective and deterrent
- ○ B. Detective only
- ○ C. Deterrent only

○ D. Preventive and deterrent

95. Michael is developing an audit plan for an organization's data center operations. Which of the following will help Michael determine which controls require potentially more scrutiny than others?

○ A. Security incident log

○ B. Last year's data center audit results

● C. Risk assessment of the data center

○ D. Data center performance metrics

96. For the purposes of audit planning, can an auditor rely upon the audit client's risk assessment?

○ A. Yes, in all cases.

● B. Yes, if the risk assessment was performed by a qualified external entity.

○ C. No. The auditor must perform a risk assessment himself or herself.

○ D. No. The auditor does not require a risk

assessment to develop an audit plan.

97. Which of the following is the MOST effective method for an IS auditor to use in testing the program change management process?

● A. Trace from system-generated information to the change management documentation

○ B. Examine change management documentation for evidence of accuracy

○ C. Trace from the change management documentation to a system- generated audit trail

○ D. Examine change management documentation for evidence of completeness

98. When reviewing a network used for Internet communications, an IS auditor will FIRST examine the:

○ A. validity of password change occurrences.

○ B. architecture of the client-server application.

● C. network architecture and design.

○ D. firewall protection and proxy servers.

99. An insurance company is using public cloud computing for one of its critical applications to reduce costs. Which of the following would be of MOST concern to the IS auditor?

○ A. The inability to recover the service in a major technical failure scenario

● B. The data in the shared environment being accessed by other companies

○ C. The service provider not including investigative support for incidents

○ D. The long-term viability of the service if the provider goes out of business

100. When reviewing an implementation of a Voice-over Internet Protocol system over a corporate wide area network, an IS auditor should expect to find:

○ A. an integrated services digital network data link.

● B. traffic engineering.

○ C. wired equivalent privacy encryption of data.

○ D. analog phone terminals.

101. Which of the following is the PRIMARY purpose for conducting parallel testing?

○ A. To determine whether the system is cost-effective

○ B. To enable comprehensive unit and system testing

○ C. To highlight errors in the program interfaces with files

● D. To ensure the new system meets user requirements

102. Which of the following data validation edits is effective in detecting transposition and transcription errors?

○ A. Range check

● B. Check digit

○ C. Validity check

○ D. Duplicate check

103. User specifications for a software development project using the traditional (waterfall) system development life cycle methodology have not been met. An IS auditor looking for a cause should look in which of the following areas?

○ A. Quality assurance

○ B. Requirements

● C. Development

○ D. User training

104. To assist in testing an essential banking system being acquired, an organization has provided the vendor with sensitive data from its existing production system. An IS auditor's PRIMARY concern is that the data should be:

● A. sanitized.

○ B. complete.

○ C. representative.

○ D. current.

105. When conducting a review of business process reengineering, an IS auditor found that an important preventive control had been removed. In this case, the IS auditor should:

● A. inform management of the finding and determine whether management is willing to accept the potential material risk of not having that preventive control.

○ B. determine if a detective control has replaced the preventive control during the process, and if it has not, report the removal of the preventive control.

○ C. recommend that this and all control procedures that existed before the process was reengineered be included in the new process.

○ D. develop a continuous audit approach to monitor the effects of the removal of the preventive control.

106. Which of the following procedures should be implemented to help ensure the completeness of inbound transactions via electronic data interchange (EDI)?

○ A. Segment counts built into the transaction set trailer

○ B. A log of the number of messages received, periodically verified

with the transaction originator

○ C. An electronic audit trail for accountability and tracking

● D. Matching acknowledgment transactions received to the log of EDI messages sent

107. Which of the following weaknesses would be considered the MOST serious in enterprise resource planning software used by a financial organization?

● A. Access controls have not been reviewed.

○ B. Limited documentation is available.

○ C. Two-year-old backup tapes have not been replaced.

○ D. Database backups are performed once a day

108. When auditing the requirements phase of a software acquisition, an IS auditor should:

○ A. assess the reasonability of the project timetable.

○ B. assess the vendor’s proposed quality processes.

○ C. ensure that the best software package is acquired.

● D. review the completeness of the specifications.

109. An organization decides to purchase a software package instead of developing it. In such a case, the design and development phases of a traditional system development life cycle would be replaced with:

- A. selection and configuration phases
- B. feasibility and requirements phases
- C. implementation and testing phases
- D. nothing, as replacement is not required.

110. An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider MOST critical?

- A. The quality of the data is not monitored.
- B. The transfer protocol does not require authentication.
- C. Imported data is not disposed frequently.
- D. The transfer protocol is not encrypted.

111. When introducing thin client architecture, which of the following types of risk regarding servers is significantly increased?

- A. Integrity
- B. Concurrency
- C. Confidentiality

○ D. Availability

112. In a controlled application development environment, the MOST important segregation of duties should be between the person who implements changes into the production environment and the:

● • A. application programmer.

○ • B. quality assurance (QA) personnel.

○ • C. computer operator.

○ • D. systems programmer.

113. A small startup organization does not have the resources to implement segregation of duties. Which of the following is the MOST effective compensating control?

○ A. Rotation of log monitoring and analysis responsibilities

● B. Additional management reviews and reconciliations

○ C. Mandatory vacations

○ D. Third-party assessments

114. When planning an audit to assess application controls of a cloud-based system, it is MOST important for the IS auditor to understand the:

○ A. availability reports associated with the cloud-based system.

○ B. architecture and cloud environment of the system.

○ C. policies and procedures of the business area being audited.

● D. business process supported by the system.

115. Which of the following data would be used when performing a business impact analysis (BIA)?

● A. Projected impact of current business on future business

○ B. Expected costs for recovering the business

○ C. Cost of regulatory compliance

○ D. Cost-benefit analysis of running the current business

116. Which of the following is the BEST indicator of the effectiveness of an organization's incident response program?

- A. Number of successful penetration tests
- B. Percentage of protected business applications
- C. Number of security vulnerability patches
- D. Financial impact per security event

117. An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives.

Which of the following findings should be the IS auditor's GREATEST concern?

- A. Mobile devices are not encrypted.
- B. Users are not required to sign updated acceptable use agreements.
- C. The business continuity plan (BCP) was not updated.
- D. Users have not been trained on the new system.

118. Which of the following security measures will reduce the risk of propagation when a cyberattack occurs?

- A. Data loss prevention (DLP) system
- B. Perimeter firewall
- C. Network segmentation O Web application firewall
- D. Intrution Detection System (IDS)

119. An IS auditor notes that the previous year's disaster recovery test was not completed within the scheduled time frame due to insufficient hardware allocated by a third-party vendor. Which of the following provides the BEST evidence that adequate resources are now allocated to successfully recover the systems?

- A. Hardware change management policy
- B. An up-to-date RACI chart
- C. Vendor memo indicating problem correction

○ D. Service level agreement (SLA)

120. When implementing Internet Protocol security (IPsec) architecture, the servers involved in application delivery:

○ A. channel access only through the public-facing firewall.

○ B. channel access through authentication.

● C. communicate via Transport Layer Security (TLS).

○ D. block authorized users from unauthorized activities.

121. During audit fieldwork, an IS auditor learns that employees are allowed to connect their personal devices to company-owned computers. How can the auditor

BEST validate that appropriate security controls are in place to prevent data loss?

○ A. Verify the data loss prevention (DLP) tool is properly configured by the organization.

● B. Review compliance with data loss and applicable mobile device user acceptance policies.

○ C. Verify employees have received appropriate mobile device security awareness training.

○ D. Conduct a walk-through to view results of an employee plugging in a device to transfer confidential data.

122. Management has requested a post-implementation review of a newly implemented purchasing package to determine to what extent business requirements are being met. Which of the following is MOST likely to be assessed?

○ A. Implementation methodology

○ B. Test results

○ C. Purchasing guidelines and policies

● D. Results of live processing

123. Which of the following is an advantage of using agile software development methodology over the waterfall methodology?

○ A. Quicker end user acceptance

○ B. Clearly defined business expectations

● C. Quicker deliverables

○ D. Less funding required overa

124. In an online application, which of the following would provide the MOST information about the transaction audit trail?

○ A. File layouts

● B. Data architecture

○ C. System/process flowchart

○ D. Source code documentation

125. On a public-key cryptosystem when there is no previous knowledge between parties, which of the following will BEST help to prevent one person from using a fictitious key to impersonate someone else?

● A. Send a certificate that can be verified by a certification authority with the public key.

○ B. Encrypt the message containing the sender's public key, using the recipient's public key.

○ C. Send the public key to the recipient prior to establishing the connection.

○ D. Encrypt the message containing the sender's public key, using a private-key cryptosystem.

126. Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's business continuity plan (BCP)?

● A. The BCP has not been tested since it was first issued.

○ B. The BCP is not version-controlled.

○ C. The BCP's contact information needs to be updated.

○ D. The BCP has not been approved by senior management.

127. Which of the following would be MOST useful when analyzing computer performance?

- ○ A. Tuning of system software to optimize resource usage
- ● B. Operations report of user dissatisfaction with response time
- ○ C. Statistical metrics measuring capacity utilization
- ○ D. Report of off-peak utilization and response time

128. Which of the following is the GREATEST risk if two users have concurrent access to the same database record?

- ○ A. Entity integrity
- ○ B. Availability integrity
- ○ C. Referential integrity
- ● D. Data integrity

129. Which of the following is the MOST effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented?

- ● A. Ensure ownership is assigned.
- ○ B. Test corrective actions upon completion.
- ○ C. Ensure sufficient audit resources are allocated.
- ○ D. Communicate audit results organization-wide.

130. Which of the following issues associated with a data center's closed circuit television (CCTV) surveillance cameras should be of MOST concern to an IS auditor?

- ● A. CCTV recordings are not regularly reviewed.
- ○ B. CCTV records are deleted after one year.
- ○ C. CCTV footage is not recorded 24 x 7.
- ○ D. CCTV cameras are not installed in break rooms.

131. An IS auditor has been asked to audit the proposed acquisition of new computer hardware. The auditor's PRIMARY concern is that:

- ● A. a clear business case has been established.
- ○ B. the new hardware meets established security standards.
- ○ C. a full, visible audit trail will be included.
- ○ D. the implementation plan meets user requirements.

132. To confirm integrity for a hashed message, the receiver should use:

- ○ A. the same hashing algorithm as the sender's to create a binary image of the file.
- ○ B. a different hashing algorithm from the sender's to create a numerical representation of the file.
- ○ C. a different hashing algorithm from the sender's to create a binary image of the file.
- ● D. the same hashing algorithm as the sender's to create a numerical representation of the file.

133. An organization is implementing a new system that supports a month-end business process. Which of the following implementation strategies would be MOST efficient to decrease business downtime?

- ○ A. Cutover
- ○ B. Phased
- ○ C. Pilot
- ● D. Parallel

134. Which of the following should be the FIRST step in managing the impact of a recently discovered zero-day attack?

- ○ A. Estimating potential damage

- [x] B. Identifying vulnerable assets
- [ ] C. Evaluating the likelihood of attack
- [ ] D. Assessing the impact of vulnerabilities

135. Which of the following is the BEST way to ensure that an application is performing according to its specifications?

- [ ] A. Pilot testing
- [ ] B. System testing
- [x] C. Integration testing
- [ ] D. Unit testing

136. Which of the following would be MOST effective to protect information assets in a data center from theft by a vendor?

- [ ] A. Conceal data devices and information labels.
- [ ] B. Issue an access card to the vendor.
- [x] C. Monitor and restrict vendor activities.
- [ ] D. Restrict use of portable and wireless devices.

137. An employee loses a mobile device resulting in loss of sensitive corporate data. Which of the following would have BEST prevented data leakage?

- [x] A. Data encryption on the mobile device
- [ ] B. The triggering of remote data wipe capabilities
- [ ] C. Awareness training for mobile device users
- [ ] D. Complex password policy for mobile devices

138. During the evaluation of controls over a major application development project, the MOST effective use of an IS auditor's time would be to review and evaluate:

- [ ] A. cost-benefit analysis.

- B. acceptance testing.
- C. application test cases.
- D. project plans.

139. Upon completion of audit work, an IS auditor should:

- A. provide a report to the auditee stating the initial findings.
- B. provide a report to senior management prior to discussion with the auditee.
- C. distribute a summary of general findings to the members of the auditing team.
- D. review the working papers with the auditee.

140. During an IT general controls audit of a high-risk area where both internal and external audit teams are reviewing the same areas simultaneously, which of the following is the BEST approach to optimize resources?

- A. Leverage the work performed by external audit for the internal audit testing.
- B. Ensure both the internal and external auditors perform the work simultaneously.
- C. Roll forward the general controls audit to the subsequent audit year.
- D. Request that the external audit team leverage the internal audit work.

141. The GREATEST benefit of using a prototyping approach in software development is that it helps to:

- A. improve efficiency of quality assurance (QA) testing.
- B. conceptualize and clarify requirements.
- C. decrease the time allocated for user testing and review.
- D. minimize scope changes to the system.

142. After an employee termination, a network account was removed, but the application account remained active. To keep this issue from recurring, which of the following is the BEST recommendation?

- A. Integrate application accounts with network single sign-on.
- B. Perform periodic access reviews.
- C. Retrain system administration staff.

- ○ D. Leverage shared accounts for the application.

143. During an IT governance audit, an IS auditor notes that IT policies and procedures are not regularly reviewed and updated. The GREATEST concern to the IS auditor is that policies and procedures might not:

- ○ A. reflect current practices.
- ○ B. be subject to adequate quality assurance (QA).
- ○ C. include new systems and corresponding process changes.
- ● D. incorporate changes to relevant laws.

144. Management receives information indicating a high level of risk associated with potential flooding near the organization's data center with in the next few years. As a result, a decision has been made to move data center operations to another facility on higher ground. Which approach has been adopted?

- ○ A. Risk reduction
- ○ B. Risk acceptance
- ○ C. Risk transfer
- ● D. Risk avoidance

145. Which of the following is the PRIMARY role of the IS auditor in an organization's information classification process?

- ○ A. Securing information assets in accordance with the classification assigned
- ● B. Validating that assets are protected according to assigned classification
- ○ C. Ensuring classification levels align with regulatory guidelines
- ○ D. Defining classification levels for information assets within the organization

146. When evaluating whether the expected benefits of a project have been achieved, it is MOST important for an IS auditor to review:

- ○ A. the project schedule.
- ○ B. quality assurance (QA) results.

- ○ C. post-implementation issues.
- ● D. the business case

147. Which of the following is the MOST important reason for IS auditors to perform post-implementation reviews for critical IT projects?

- ○ A. To determine whether vendors should be paid for project deliverables
- ○ B. To provide the audit committee with an assessment of project team performance
- ○ C. To provide guidance on the financial return on investment (ROI) of projects
- ● D. To determine whether the organization's objectives were met as expected

148. Which of the following BEST indicates that an incident management process is effective?

- ○ A. Decreased number of calls to the help desk
- ○ B. Increased number of incidents reviewed by IT management
- ● C. Decreased time for incident resolution
- ○ D. Increased number of reported critical incidents

149. Which of the following MOST effectively minimizes downtime during system conversions?

- ○ A. Phased approach
- ● B. Parallel run
- ○ C. Direct cutover
- ○ D. Pilot study

150. Which of the following would be MOST useful to an IS auditor assessing the effectiveness of IT resource planning?

- ○ A. Budget execution status
- ● B. A capacity analysis of IT operations
- ○ C. A succession plan for key IT personnel
- ○ D. A list of new applications to be implemented