

Isaca.CISA.vMay-2024.by.Tom.312q

Number: CISA
Passing Score: 800
Time Limit: 120
File Version: 31.0

Exam Code: CISA
Exam Name: Certified Information Systems Auditor



Exam A

QUESTION 1

An IS auditor notes that several employees are spending an excessive amount of time using social media sites for personal reasons. Which of the following should the auditor recommend be performed FIRST?

- A. Implement a process to actively monitor postings on social networking sites.
- B. Adjust budget for network usage to include social media usage.
- C. Use data loss prevention (DLP) tools on endpoints.
- D. implement policies addressing acceptable usage of social media during working hours.

Correct Answer: D

Section:

QUESTION 2

Which of the following fire suppression systems needs to be combined with an automatic switch to shut down the electricity supply in the event of activation?

- A. Carbon dioxide
- B. FM-200
- C. Dry pipe
- D. Halon

Correct Answer: C

Section:



QUESTION 3

An IT balanced scorecard is the MOST effective means of monitoring:

- A. governance of enterprise IT.
- B. control effectiveness.
- C. return on investment (ROI).
- D. change management effectiveness.

Correct Answer: A

Section:

QUESTION 4

When reviewing an organization's information security policies, an IS auditor should verify that the policies have been defined PRIMARILY on the basis of:

- A. a risk management process.
- B. an information security framework.
- C. past information security incidents.
- D. industry best practices.

Correct Answer: B

Section:

QUESTION 5

Which of the following would be an IS auditor's GREATEST concern when reviewing the early stages of a software development project?

- A. The lack of technical documentation to support the program code
- B. The lack of completion of all requirements at the end of each sprint
- C. The lack of acceptance criteria behind user requirements.
- D. The lack of a detailed unit and system test plan

Correct Answer: C

Section:

QUESTION 6

Which of the following is the BEST data integrity check?

- A. Counting the transactions processed per day
- B. Performing a sequence check
- C. Tracing data back to the point of origin
- D. Preparing and running test data

Correct Answer: C

Section:

QUESTION 7

Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system. What is the BEST control to ensure that data is accurately entered into the system?

- A. Reconciliation of total amounts by project
- B. Validity checks, preventing entry of character data
- C. Reasonableness checks for each cost type
- D. Display back of project detail after entry

Correct Answer: A

Section:

QUESTION 8

An incorrect version of source code was amended by a development team. This MOST likely indicates a weakness in:

- A. incident management.
- B. quality assurance (QA).
- C. change management.
- D. project management.

Correct Answer: C

Section:

QUESTION 9



An organizations audit charter PRIMARILY:

- A. describes the auditors' authority to conduct audits.
- B. defines the auditors' code of conduct.
- C. formally records the annual and quarterly audit plans.
- D. documents the audit process and reporting standards.

Correct Answer: A

Section:

QUESTION 10

The decision to accept an IT control risk related to data quality should be the responsibility of the:

- A. information security team.
- B. IS audit manager.
- C. chief information officer (CIO).
- D. business owner.

Correct Answer: D

Section:

QUESTION 11

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. Cost-benefit analysis of running the current business
- C. Cost of regulatory compliance
- D. Expected costs for recovering the business

Correct Answer: A

Section:

QUESTION 12

Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organization's information security policy?

- A. Alignment with the IT tactical plan
- B. IT steering committee minutes
- C. Compliance with industry best practice
- D. Business objectives

Correct Answer: D

Section:

QUESTION 13

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. application test cases.



- B. acceptance testing.
- C. cost-benefit analysis.
- D. project plans.

Correct Answer: A

Section:

QUESTION 14

An IS auditor finds that firewalls are outdated and not supported by vendors. Which of the following should be the auditor's NEXT course of action?

- A. Report the mitigating controls.
- B. Report the security posture of the organization.
- C. Determine the value of the firewall.
- D. Determine the risk of not replacing the firewall.

Correct Answer: D

Section:

QUESTION 15

Which of the following would MOST likely impair the independence of the IS auditor when performing a post-implementation review of an application system?

- A. The IS auditor provided consulting advice concerning application system best practices.
- B. The IS auditor participated as a member of the application system project team, but did not have operational responsibilities.
- C. The IS auditor designed an embedded audit module exclusively for auditing the application system.
- D. The IS auditor implemented a specific control during the development of the application system.

Correct Answer: D

Section:

QUESTION 16

An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

- A. Obtain error codes indicating failed data feeds.
- B. Appoint data quality champions across the organization.
- C. Purchase data cleansing tools from a reputable vendor.
- D. Implement business rules to reject invalid data.

Correct Answer: D

Section:

QUESTION 17

An IS auditor suspects an organization's computer may have been used to commit a crime. Which of the following is the auditor's BEST course of action?

- A. Examine the computer to search for evidence supporting the suspicions.
- B. Advise management of the crime after the investigation.
- C. Contact the incident response team to conduct an investigation.
- D. Notify local law enforcement of the potential crime before further investigation.

Correct Answer: C

Section:

QUESTION 18

Which of the following access rights presents the GREATEST risk when granted to a new member of the system development staff?

- A. Write access to production program libraries
- B. Write access to development data libraries
- C. Execute access to production program libraries
- D. Execute access to development program libraries

Correct Answer: A

Section:

QUESTION 19

An IS auditor is conducting a post-implementation review of an enterprise resource planning (ERP) system. End users indicated concerns with the accuracy of critical automatic calculations made by the system. The auditor's FIRST course of action should be to:

- A. review recent changes to the system.
- B. verify completeness of user acceptance testing (UAT).
- C. verify results to determine validity of user concerns.
- D. review initial business requirements.

Correct Answer: C

Section:



QUESTION 20

Which of the following provides the MOST reliable audit evidence on the validity of transactions in a financial application?

- A. Walk-through reviews
- B. Substantive testing
- C. Compliance testing
- D. Design documentation reviews

Correct Answer: B

Section:

QUESTION 21

During an incident management audit, an IS auditor finds that several similar incidents were logged during the audit period. Which of the following is the auditor's MOST important course of action?

- A. Document the finding and present it to management.
- B. Determine if a root cause analysis was conducted.
- C. Confirm the resolution time of the incidents.
- D. Validate whether all incidents have been actioned.

Correct Answer: B

Section:

QUESTION 22

During an external review, an IS auditor observes an inconsistent approach in classifying system criticality within the organization. Which of the following should be recommended as the PRIMARY factor to determine system criticality?

- A. Key performance indicators (KPIs)
- B. Maximum allowable downtime (MAD)
- C. Recovery point objective (RPO)
- D. Mean time to restore (MTTR)

Correct Answer: B

Section:

QUESTION 23

An IS auditor discovers an option in a database that allows the administrator to directly modify any table. This option is necessary to overcome bugs in the software, but is rarely used. Changes to tables are automatically logged. The IS auditor's FIRST action should be to:

- A. recommend that the option to directly modify the database be removed immediately.
- B. recommend that the system require two persons to be involved in modifying the database.
- C. determine whether the log of changes to the tables is backed up.
- D. determine whether the audit trail is secured and reviewed.

Correct Answer: D

Section:

QUESTION 24

An IS auditor finds that a key Internet-facing system is vulnerable to attack and that patches are not available. What should the auditor recommend be done FIRST?

- A. Implement a new system that can be patched.
- B. Implement additional firewalls to protect the system.
- C. Decommission the server.
- D. Evaluate the associated risk.

Correct Answer: D

Section:

QUESTION 25

IS management has recently disabled certain referential integrity controls in the database management system (DBMS) software to provide users increased query performance. Which of the following controls will MOST effectively compensate for the lack of referential integrity?

- A. More frequent data backups
- B. Periodic table link checks
- C. Concurrent access controls
- D. Performance monitoring tools

Correct Answer: B

Section:



QUESTION 26

A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

- A. Periodically reviewing log files
- B. Configuring the router as a firewall
- C. Using smart cards with one-time passwords
- D. Installing biometrics-based authentication

Correct Answer: B

Section:

QUESTION 27

The PRIMARY advantage of object-oriented technology is enhanced:

- A. efficiency due to the re-use of elements of logic.
- B. management of sequential program execution for data access.
- C. grouping of objects into methods for data access.
- D. management of a restricted variety of data types for a data object.

Correct Answer: C

Section:

QUESTION 28

From an IS auditor's perspective, which of the following would be the GREATEST risk associated with an incomplete inventory of deployed software in an organization?

- A. Inability to close unused ports on critical servers
- B. Inability to identify unused licenses within the organization
- C. Inability to deploy updated security patches
- D. Inability to determine the cost of deployed software

Correct Answer: C

Section:

QUESTION 29

Which of the following BEST minimizes performance degradation of servers used to authenticate users of an e-commerce website?

- A. Configure a single server as a primary authentication server and a second server as a secondary authentication server.
- B. Configure each authentication server as belonging to a cluster of authentication servers.
- C. Configure each authentication server and ensure that each disk of its RAID is attached to the primary controller.
- D. Configure each authentication server and ensure that the disks of each server form part of a duplex.

Correct Answer: B

Section:

QUESTION 30

During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be MOST concerned with the:

- A. allocation of resources during an emergency.
- B. frequency of system testing.
- C. differences in IS policies and procedures.
- D. maintenance of hardware and software compatibility.

Correct Answer: D

Section:

QUESTION 31

Which of the following attack techniques will succeed because of an inherent security weakness in an Internet firewall?

- A. Phishing
- B. Using a dictionary attack of encrypted passwords
- C. Intercepting packets and viewing passwords
- D. Flooding the site with an excessive number of packets

Correct Answer: D

Section:

QUESTION 32

Which of the following is an executive management concern that could be addressed by the implementation of a security metrics dashboard?

- A. Effectiveness of the security program
- B. Security incidents vs. industry benchmarks
- C. Total number of hours budgeted to security
- D. Total number of false positives



Correct Answer: A

Section:

QUESTION 33

One benefit of return on investment (ROI) analysts in IT decision making is that it provides the:

- A. basis for allocating indirect costs.
- B. cost of replacing equipment.
- C. estimated cost of ownership.
- D. basis for allocating financial resources.

Correct Answer: D

Section:

QUESTION 34

Which of the following is an audit reviewer's PRIMARY role with regard to evidence?

- A. Ensuring unauthorized individuals do not tamper with evidence after it has been captured
- B. Ensuring evidence is sufficient to support audit conclusions
- C. Ensuring appropriate statistical sampling methods were used

D. Ensuring evidence is labeled to show it was obtained from an approved source

Correct Answer: B

Section:

QUESTION 35

Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

- A. Identifying relevant roles for an enterprise IT governance framework
- B. Making decisions regarding risk response and monitoring of residual risk
- C. Verifying that legal, regulatory, and contractual requirements are being met
- D. Providing independent and objective feedback to facilitate improvement of IT processes

Correct Answer: D

Section:

QUESTION 36

Which of the following is MOST important for an effective control self-assessment (CSA) program?

- A. Determining the scope of the assessment
- B. Performing detailed test procedures
- C. Evaluating changes to the risk environment
- D. Understanding the business process

Correct Answer: D

Section:

QUESTION 37

What should be the PRIMARY basis for selecting which IS audits to perform in the coming year?

- A. Senior management's request
- B. Prior year's audit findings
- C. Organizational risk assessment
- D. Previous audit coverage and scope

Correct Answer: C

Section:

QUESTION 38

Which of the following is the MOST important prerequisite for the protection of physical information assets in a data center?

- A. Segregation of duties between staff ordering and staff receiving information assets
- B. Complete and accurate list of information assets that have been deployed
- C. Availability and testing of onsite backup generators
- D. Knowledge of the IT staff regarding data protection requirements

Correct Answer: B



Section:

QUESTION 39

Which of the following should be the MOST important consideration when conducting a review of IT portfolio management?

- A. Assignment of responsibility for each project to an IT team member
- B. Adherence to best practice and industry approved methodologies
- C. Controls to minimize risk and maximize value for the IT portfolio
- D. Frequency of meetings where the business discusses the IT portfolio

Correct Answer: D

Section:

QUESTION 40

Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

- A. Audit cycle defined in the audit plan
- B. Complexity of management's action plans
- C. Recommendation from executive management
- D. Residual risk from the findings of previous audits

Correct Answer: D

Section:

QUESTION 41

Which of the following is the BEST control to prevent the transfer of files to external parties through instant messaging (IM) applications?

- A. File level encryption
- B. File Transfer Protocol (FTP)
- C. Instant messaging policy
- D. Application level firewalls

Correct Answer: D

Section:

QUESTION 42

Which of the following is the BEST control to mitigate the malware risk associated with an instant messaging (IM) system?

- A. Blocking attachments in IM
- B. Blocking external IM traffic
- C. Allowing only corporate IM solutions
- D. Encrypting IM traffic

Correct Answer: C

Section:

QUESTION 43



Which of the following should be an IS auditor's PRIMARY focus when developing a risk-based IS audit program?

- A. Portfolio management
- B. Business plans
- C. Business processes
- D. IT strategic plans

Correct Answer: D

Section:

QUESTION 44

Cross-site scripting (XSS) attacks are BEST prevented through:

- A. application firewall policy settings.
- B. a three-tier web architecture.
- C. secure coding practices.
- D. use of common industry frameworks.

Correct Answer: C

Section:

QUESTION 45

When determining whether a project in the design phase will meet organizational objectives, what is BEST to compare against the business case?

- A. Implementation plan
- B. Project budget provisions
- C. Requirements analysis
- D. Project plan

Correct Answer: C

Section:

QUESTION 46

An organization has outsourced its data processing function to a service provider. Which of the following would BEST determine whether the service provider continues to meet the organization's objectives?

- A. Assessment of the personnel training processes of the provider
- B. Adequacy of the service provider's insurance
- C. Review of performance against service level agreements (SLAs)
- D. Periodic audits of controls by an independent auditor

Correct Answer: D

Section:

QUESTION 47

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

- A. communicate via Transport Layer Security (TLS),



- B. block authorized users from unauthorized activities.
- C. channel access only through the public-facing firewall.
- D. channel access through authentication.

Correct Answer: D

Section:

QUESTION 48

Coding standards provide which of the following?

- A. Program documentation
- B. Access control tables
- C. Data flow diagrams
- D. Field naming conventions

Correct Answer: D

Section:

QUESTION 49

Prior to a follow-up engagement, an IS auditor learns that management has decided to accept a level of residual risk related to an audit finding without remediation. The IS auditor is concerned about management's decision. Which of the following should be the IS auditor's NEXT course of action?

- A. Accept management's decision and continue the follow-up.
- B. Report the issue to IS audit management.
- C. Report the disagreement to the board.
- D. Present the issue to executive management.



Correct Answer: B

Section:

QUESTION 50

The PRIMARY benefit to using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system:

- A. is more effective at suppressing flames.
- B. allows more time to abort release of the suppressant.
- C. has a decreased risk of leakage.
- D. disperses dry chemical suppressants exclusively.

Correct Answer: C

Section:

QUESTION 51

Which of the following is MOST important with regard to an application development acceptance test?

- A. The programming team is involved in the testing process.
- B. All data files are tested for valid information before conversion.
- C. User management approves the test design before the test is started.

D. The quality assurance (QA) team is in charge of the testing process.

Correct Answer: B

Section:

QUESTION 52

An organization's enterprise architecture (EA) department decides to change a legacy system's components while maintaining its original functionality. Which of the following is MOST important for an IS auditor to understand when reviewing this decision?

- A. The current business capabilities delivered by the legacy system
- B. The proposed network topology to be used by the redesigned system
- C. The data flows between the components to be used by the redesigned system
- D. The database entity relationships within the legacy system

Correct Answer: A

Section:

QUESTION 53

An IS auditor is evaluating an organization's IT strategy and plans. Which of the following would be of GREATEST concern?

- A. There is not a defined IT security policy.
- B. The business strategy meeting minutes are not distributed.
- C. IT is not engaged in business strategic planning.
- D. There is inadequate documentation of IT strategic planning.

Correct Answer: C

Section:



QUESTION 54

When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor's BEST recommendation is to place an intrusion detection system (IDS) between the firewall and:

- A. the Internet.
- B. the demilitarized zone (DMZ).
- C. the organization's web server.
- D. the organization's network.

Correct Answer: D

Section:

QUESTION 55

An IS auditor is reviewing an organization's information asset management process. Which of the following would be of GREATEST concern to the auditor?

- A. The process does not require specifying the physical locations of assets.
- B. Process ownership has not been established.
- C. The process does not include asset review.
- D. Identification of asset value is not included in the process.

Correct Answer: B

Section:

QUESTION 56

An IS audit reveals that an organization is not proactively addressing known vulnerabilities. Which of the following should the IS auditor recommend the organization do FIRST?

- A. Verify the disaster recovery plan (DRP) has been tested.
- B. Ensure the intrusion prevention system (IPS) is effective.
- C. Assess the security risks to the business.
- D. Confirm the incident response team understands the issue.

Correct Answer: C

Section:

QUESTION 57

Which of the following is the BEST way to address segregation of duties issues in an organization with budget constraints?

- A. Rotate job duties periodically.
- B. Perform an independent audit.
- C. Hire temporary staff.
- D. Implement compensating controls.

Correct Answer: D

Section:

QUESTION 58

An organization's security policy mandates that all new employees must receive appropriate security awareness training. Which of the following metrics would BEST assure compliance with this policy?

- A. Percentage of new hires that have completed the training.
- B. Number of new hires who have violated enterprise security policies.
- C. Number of reported incidents by new hires.
- D. Percentage of new hires who report incidents

Correct Answer: C

Section:

QUESTION 59

An IS auditor is following up on prior period items and finds management did not address an audit finding. Which of the following should be the IS auditor's NEXT course of action?

- A. Note the exception in a new report as the item was not addressed by management.
- B. Recommend alternative solutions to address the repeat finding.
- C. Conduct a risk assessment of the repeat finding.
- D. Interview management to determine why the finding was not addressed.

Correct Answer: D

Section:



QUESTION 60

Which of the following tests would provide the BEST assurance that a health care organization is handling patient data appropriately?

- A. Compliance with action plans resulting from recent audits
- B. Compliance with local laws and regulations
- C. Compliance with industry standards and best practice
- D. Compliance with the organization's policies and procedures

Correct Answer: B

Section:

QUESTION 61

An organization allows employees to retain confidential data on personal mobile devices. Which of the following is the BEST recommendation to mitigate the risk of data leakage from lost or stolen devices?

- A. Require employees to attend security awareness training.
- B. Password protect critical data files.
- C. Configure to auto-wipe after multiple failed access attempts.
- D. Enable device auto-lock function.

Correct Answer: C

Section:

QUESTION 62

Which of the following demonstrates the use of data analytics for a loan origination process?

- A. Evaluating whether loan records are included in the batch file and are validated by the servicing system
- B. Comparing a population of loans input in the origination system to loans booked on the servicing system
- C. Validating whether reconciliations between the two systems are performed and discrepancies are investigated
- D. Reviewing error handling controls to notify appropriate personnel in the event of a transmission failure

Correct Answer: B

Section:

QUESTION 63

Which of the following BEST indicates the effectiveness of an organization's risk management program?

- A. Inherent risk is eliminated.
- B. Residual risk is minimized.
- C. Control risk is minimized.
- D. Overall risk is quantified.

Correct Answer: B

Section:

QUESTION 64

An IS auditor has been asked to assess the security of a recently migrated database system that contains personal and financial data for a bank's customers. Which of the following controls is MOST important for the auditor to confirm is in place?

- A. The default configurations have been changed.
- B. All tables in the database are normalized.
- C. The service port used by the database server has been changed.
- D. The default administration account is used after changing the account password.

Correct Answer: A

Section:

QUESTION 65

Which of the following is the BEST justification for deferring remediation testing until the next audit?

- A. The auditor who conducted the audit and agreed with the timeline has left the organization.
- B. Management's planned actions are sufficient given the relative importance of the observations.
- C. Auditee management has accepted all observations reported by the auditor.
- D. The audit environment has changed significantly.

Correct Answer: D

Section:

QUESTION 66

What is BEST for an IS auditor to review when assessing the effectiveness of changes recently made to processes and tools related to an organization's business continuity plan (BCP)?

- A. Full test results
- B. Completed test plans
- C. Updated inventory of systems
- D. Change management processes



Correct Answer: A

Section:

QUESTION 67

During a follow-up audit, an IS auditor learns that some key management personnel have been replaced since the original audit, and current management has decided not to implement some previously accepted recommendations. What is the auditor's BEST course of action?

- A. Notify the chair of the audit committee.
- B. Notify the audit manager.
- C. Retest the control.
- D. Close the audit finding.

Correct Answer: B

Section:

QUESTION 68

Which of the following is the BEST compensating control when segregation of duties is lacking in a small IS department?

- A. Background checks

- B. User awareness training
- C. Transaction log review
- D. Mandatory holidays

Correct Answer: C

Section:

QUESTION 69

Which of the following would BEST determine whether a post-implementation review (PIR) performed by the project management office (PMO) was effective?

- A. Lessons learned were implemented.
- B. Management approved the PIR report.
- C. The review was performed by an external provider.
- D. Project outcomes have been realized.

Correct Answer: D

Section:

QUESTION 70

Which of the following is MOST important for an IS auditor to examine when reviewing an organization's privacy policy?

- A. Whether there is explicit permission from regulators to collect personal data
- B. The organization's legitimate purpose for collecting personal data
- C. Whether sharing of personal information with third-party service providers is prohibited
- D. The encryption mechanism selected by the organization for protecting personal data



Correct Answer: B

Section:

QUESTION 71

Which of the following is the GREATEST concern associated with a high number of IT policy exceptions approved by management?

- A. The exceptions are likely to continue indefinitely.
- B. The exceptions may result in noncompliance.
- C. The exceptions may elevate the level of operational risk.
- D. The exceptions may negatively impact process efficiency.

Correct Answer: B

Section:

QUESTION 72

During a new system implementation, an IS auditor has been assigned to review risk management at each milestone. The auditor finds that several risks to project benefits have not been addressed. Who should be accountable for managing these risks?

- A. Enterprise risk manager
- B. Project sponsor
- C. Information security officer

D. Project manager

Correct Answer: D

Section:

QUESTION 73

Which of the following will be the MOST effective method to verify that a service vendor keeps control levels as required by the client?

- A. Conduct periodic on-site assessments using agreed-upon criteria.
- B. Periodically review the service level agreement (SLA) with the vendor.
- C. Conduct an unannounced vulnerability assessment of vendor's IT systems.
- D. Obtain evidence of the vendor's control self-assessment (CSA).

Correct Answer: C

Section:

QUESTION 74

While executing follow-up activities, an IS auditor is concerned that management has implemented corrective actions that are different from those originally discussed and agreed with the audit function. In order to resolve the situation, the

IS auditor's BEST course of action would be to:

- A. re-prioritize the original issue as high risk and escalate to senior management.
- B. schedule a follow-up audit in the next audit cycle.
- C. postpone follow-up activities and escalate the alternative controls to senior audit management.
- D. determine whether the alternative controls sufficiently mitigate the risk.

The logo for Vdumps.com, featuring a stylized orange 'V' followed by the word 'dumps' in a grey, lowercase, sans-serif font.

Correct Answer: D

Section:

QUESTION 75

During an ongoing audit, management requests a briefing on the findings to date. Which of the following is the IS auditor's BEST course of action?

- A. Review working papers with the auditee.
- B. Request the auditee provide management responses.
- C. Request management wait until a final report is ready for discussion.
- D. Present observations for discussion only.

Correct Answer: D

Section:

QUESTION 76

Which of the following is the PRIMARY concern when negotiating a contract for a hot site?

- A. Availability of the site in the event of multiple disaster declarations
- B. Coordination with the site staff in the event of multiple disaster declarations
- C. Reciprocal agreements with other organizations
- D. Complete testing of the recovery plan

Correct Answer: A

Section:

QUESTION 77

Which of the following is MOST important for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros?

- A. Encryption of the spreadsheet
- B. Version history
- C. Formulas within macros
- D. Reconciliation of key calculations

Correct Answer: D

Section:

QUESTION 78

Which of the following is the BEST recommendation to prevent fraudulent electronic funds transfers by accounts payable employees?

- A. Periodic vendor reviews
- B. Dual control
- C. Independent reconciliation
- D. Re-keying of monetary amounts
- E. Engage an external security incident response expert for incident handling.

Correct Answer: B

Section:



QUESTION 79

A new regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditor's BEST recommendation to facilitate compliance with the regulation?

- A. Include the requirement in the incident management response plan.
- B. Establish key performance indicators (KPIs) for timely identification of security incidents.
- C. Enhance the alert functionality of the intrusion detection system (IDS).
- D. Engage an external security incident response expert for incident handling.

Correct Answer: A

Section:

QUESTION 80

An IS auditor has found that an organization is unable to add new servers on demand in a costefficient manner. Which of the following is the auditor's BEST recommendation?

- A. Increase the capacity of existing systems.
- B. Upgrade hardware to newer technology.
- C. Hire temporary contract workers for the IT function.
- D. Build a virtual environment.

Correct Answer: D

Section:

QUESTION 81

An IS auditor who was instrumental in designing an application is called upon to review the application. The auditor should:

- A. refuse the assignment to avoid conflict of interest.
- B. use the knowledge of the application to carry out the audit.
- C. inform audit management of the earlier involvement.
- D. modify the scope of the audit.

Correct Answer: C

Section:

QUESTION 82

Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

- A. Independent reconciliation
- B. Re-keying of wire dollar amounts
- C. Two-factor authentication control
- D. System-enforced dual control

Correct Answer: D

Section:

QUESTION 83

In a small IT web development company where developers must have write access to production, the BEST recommendation of an IS auditor would be to:

- A. hire another person to perform migration to production.
- B. implement continuous monitoring controls.
- C. remove production access from the developers.
- D. perform a user access review for the development team

Correct Answer: C

Section:

QUESTION 84

Which of the following is the PRIMARY reason for an IS auditor to conduct post-implementation reviews?

- A. To determine whether project objectives in the business case have been achieved
- B. To ensure key stakeholder sign-off has been obtained
- C. To align project objectives with business needs
- D. To document lessons learned to improve future project delivery

Correct Answer: A

Section:

QUESTION 85



In a 24/7 processing environment, a database contains several privileged application accounts with passwords set to never expire. Which of the following recommendations would BEST address the risk with minimal disruption to the business?

- A. Modify applications to no longer require direct access to the database.
- B. Introduce database access monitoring into the environment
- C. Modify the access management policy to make allowances for application accounts.
- D. Schedule downtime to implement password changes.

Correct Answer: B

Section:

QUESTION 86

Management is concerned about sensitive information being intentionally or unintentionally emailed as attachments outside the organization by employees. What is the MOST important task before implementing any associated email controls?

- A. Require all employees to sign nondisclosure agreements (NDAs).
- B. Develop an acceptable use policy for end-user computing (EUC).
- C. Develop an information classification scheme.
- D. Provide notification to employees about possible email monitoring.

Correct Answer: A

Section:

QUESTION 87

An IS auditor will be testing accounts payable controls by performing data analytics on the entire population of transactions. Which of the following is MOST important for the auditor to confirm when sourcing the population data?

- A. The data is taken directly from the system.
- B. There is no privacy information in the data.
- C. The data can be obtained in a timely manner.
- D. The data analysis tools have been recently updated.

Correct Answer: A

Section:

QUESTION 88

Which of the following is MOST important to ensure when developing an effective security awareness program?

- A. Training personnel are information security professionals.
- B. Phishing exercises are conducted post-training.
- C. Security threat scenarios are included in the program content.
- D. Outcome metrics for the program are established.

Correct Answer: D

Section:

QUESTION 89

Which of the following is the BEST source of information for assessing the effectiveness of IT process monitoring?

- A. Real-time audit software
- B. Performance data
- C. Quality assurance (QA) reviews
- D. Participative management techniques

Correct Answer: A

Section:

QUESTION 90

Which of the following is the MOST effective way to maintain network integrity when using mobile devices?

- A. Implement network access control.
- B. Implement outbound firewall rules.
- C. Perform network reviews.
- D. Review access control lists.

Correct Answer: A

Section:

QUESTION 91

An IS auditor wants to determine who has oversight of staff performing a specific task and is referencing the organization's RACI chart. Which of the following roles within the chart would provide this information?

- A. Consulted
- B. Informed
- C. Responsible
- D. Accountable

Correct Answer: D

Section:

QUESTION 92

Which of the following is MOST important for an IS auditor to consider when performing the risk assessment prior to an audit engagement?

- A. The design of controls
- B. Industry standards and best practices
- C. The results of the previous audit
- D. The amount of time since the previous audit

Correct Answer: A

Section:

QUESTION 93

An IS auditor is reviewing the release management process for an in-house software development solution. In which environment is the software version MOST likely to be the same as production?

- A. Staging



- B. Testing
- C. Integration
- D. Development

Correct Answer: B

Section:

QUESTION 94

An IS auditor should ensure that an application's audit trail:

- A. has adequate security.
- B. logs all database records.
- C. Is accessible online
- D. does not impact operational efficiency

Correct Answer: D

Section:

QUESTION 95

Which of the following business continuity activities prioritizes the recovery of critical functions?

- A. Business continuity plan (BCP) testing
- B. Business impact analysis (BIA)
- C. Disaster recovery plan (DRP) testing
- D. Risk assessment

Correct Answer: B

Section:

QUESTION 96

Capacity management enables organizations to:

- A. forecast technology trends
- B. establish the capacity of network communication links
- C. identify the extent to which components need to be upgraded
- D. determine business transaction volumes.

Correct Answer: D

Section:

QUESTION 97

A manager identifies active privileged accounts belonging to staff who have left the organization. Which of the following is the threat actor in this scenario?

- A. Terminated staff
- B. Unauthorized access
- C. Deleted log data



D. Hacktivists

Correct Answer: A

Section:

QUESTION 98

The due date of an audit project is approaching, and the audit manager has determined that only 60% of the audit has been completed. Which of the following should the audit manager do FIRST?

- A. Determine where delays have occurred
- B. Assign additional resources to supplement the audit
- C. Escalate to the audit committee
- D. Extend the audit deadline

Correct Answer: A

Section:

QUESTION 99

The BEST way to determine whether programmers have permission to alter data in the production environment is by reviewing:

- A. the access control system's log settings.
- B. how the latest system changes were implemented.
- C. the access control system's configuration.
- D. the access rights that have been granted.

Correct Answer: D

Section:



QUESTION 100

Which of the following is the GREATEST risk associated with storing customer data on a web server?

- A. Data availability
- B. Data confidentiality
- C. Data integrity
- D. Data redundancy

Correct Answer: B

Section:

QUESTION 101

When auditing the alignment of IT to the business strategy, it is MOST Important for the IS auditor to:

- A. compare the organization's strategic plan against industry best practice.
- B. interview senior managers for their opinion of the IT function.
- C. ensure an IT steering committee is appointed to monitor new IT projects.
- D. evaluate deliverables of new IT initiatives against planned business services.

Correct Answer: D

Section:

QUESTION 102

Which of the following is the BEST audit procedure to determine whether a firewall is configured in compliance with the organization's security policy?

- A. Reviewing the parameter settings
- B. Reviewing the system log
- C. Interviewing the firewall administrator
- D. Reviewing the actual procedures

Correct Answer: D

Section:

QUESTION 103

Which of the following is the GREATEST security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system?

- A. Data from the source and target system may be intercepted.
- B. Data from the source and target system may have different data formats.
- C. Records past their retention period may not be migrated to the new system.
- D. System performance may be impacted by the migration

Correct Answer: A

Section:

QUESTION 104

An IS auditor is conducting a review of a data center. Which of the following observations could indicate an access control issue?

- A. Security cameras deployed outside main entrance
- B. Antistatic mats deployed at the computer room entrance
- C. Muddy footprints directly inside the emergency exit
- D. Fencing around facility is two meters high

Correct Answer: C

Section:

QUESTION 105

The waterfall life cycle model of software development is BEST suited for which of the following situations?

- A. The protect requirements are well understood.
- B. The project is subject to time pressures.
- C. The project intends to apply an object-oriented design approach.
- D. The project will involve the use of new technology.

Correct Answer: C

Section:

QUESTION 106



Which of the following is the BEST way to ensure payment transaction data is restricted to the appropriate users?

- A. Implementing two-factor authentication
- B. Restricting access to transactions using network security software
- C. implementing role-based access at the application level
- D. Using a single menu for sensitive application transactions

Correct Answer: C

Section:

QUESTION 107

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

Correct Answer: C

Section:

QUESTION 108

An IS auditor is reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit. What should the auditor consider the MOST significant concern?

- A. Attack vectors are evolving for industrial control systems.
- B. There is a greater risk of system exploitation.
- C. Disaster recovery plans (DRPs) are not in place.
- D. Technical specifications are not documented.

Correct Answer: C

Section:

QUESTION 109

The PRIMARY focus of a post-implementation review is to verify that:

- A. enterprise architecture (EA) has been complied with.
- B. user requirements have been met.
- C. acceptance testing has been properly executed.
- D. user access controls have been adequately designed.

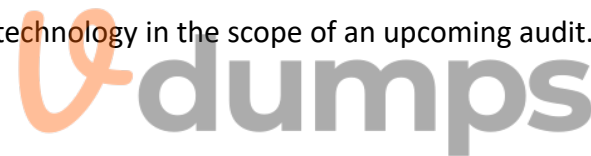
Correct Answer: B

Section:

QUESTION 110

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. include new systems and corresponding process changes.
- C. incorporate changes to relevant laws.
- D. be subject to adequate quality assurance (QA).

Correct Answer: D

Section:

QUESTION 111

Which of the following is the BEST way for an organization to mitigate the risk associated with thirdparty application performance?

- A. Ensure the third party allocates adequate resources to meet requirements.
- B. Use analytics within the internal audit function
- C. Conduct a capacity planning exercise
- D. Utilize performance monitoring tools to verify service level agreements (SLAs)

Correct Answer: D

Section:

QUESTION 112

An organization with many desktop PCs is considering moving to a thin client architecture. Which of the following is the MAJOR advantage?

- A. The security of the desktop PC is enhanced.
- B. Administrative security can be provided for the client.
- C. Desktop application software will never have to be upgraded.
- D. System administration can be better managed



Correct Answer: C

Section:

QUESTION 113

An IS auditor is reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents. Which of the following observations should be of MOST concern to the auditor?

- A. Training was not provided to the department that handles intellectual property and patents
- B. Logging and monitoring for content filtering is not enabled.
- C. Employees can share files with users outside the company through collaboration tools.
- D. The collaboration tool is hosted and can only be accessed via an Internet browser

Correct Answer: B

Section:

QUESTION 114

Which of the following types of firewalls provide the GREATEST degree of control against hacker intrusion?

- A. Circuit gateway
- B. Application level gateway
- C. Packet filtering router
- D. Screening router

Correct Answer: B

Section:

QUESTION 115

An IS auditor is evaluating the risk associated with moving from one database management system (DBMS) to another. Which of the following would be MOST helpful to ensure the integrity of the system throughout the change?

- A. Preserving the same data classifications
- B. Preserving the same data inputs
- C. Preserving the same data structure
- D. Preserving the same data interfaces

Correct Answer: C

Section:

QUESTION 116

Which of the following provides the MOST assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system?

- A. Comparing code between old and new systems
- B. Running historical transactions through the new system
- C. Reviewing quality assurance (QA) procedures
- D. Loading balance and transaction data to the new system

Correct Answer: B

Section:



QUESTION 117

Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

- A. The job scheduler application has not been designed to display pop-up error messages.
- B. Access to the job scheduler application has not been restricted to a maximum of two staff members
- C. Operations shift turnover logs are not utilized to coordinate and control the processing environment
- D. Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor

Correct Answer: D

Section:

QUESTION 118

The performance, risks, and capabilities of an IT infrastructure are BEST measured using a:

- A. risk management review
- B. control self-assessment (CSA).
- C. service level agreement (SLA).
- D. balanced scorecard.

Correct Answer: B

Section:

QUESTION 119

Which of the following would BEST help to support an auditor's conclusion about the effectiveness of an implemented data classification program?

- A. Purchase of information management tools
- B. Business use cases and scenarios
- C. Access rights provisioned according to scheme
- D. Detailed data classification scheme

Correct Answer: D

Section:

QUESTION 120

Which of the following is the MAIN purpose of an information security management system?

- A. To identify and eliminate the root causes of information security incidents
- B. To enhance the impact of reports used to monitor information security incidents
- C. To keep information security policies and procedures up-to-date
- D. To reduce the frequency and impact of information security incidents

Correct Answer: D

Section:

QUESTION 121

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

Correct Answer: B

Section:

QUESTION 122

Which of the following is MOST important to consider when scheduling follow-up audits?

- A. The efforts required for independent verification with new auditors
- B. The impact if corrective actions are not taken
- C. The amount of time the auditee has agreed to spend with auditors
- D. Controls and detection risks related to the observations

Correct Answer: B

Section:

QUESTION 123

An information systems security officer's PRIMARY responsibility for business process applications is to:

- A. authorize secured emergency access
- B. approve the organization's security policy
- C. ensure access rules agree with policies
- D. create role-based rules for each business process

Correct Answer: D

Section:

QUESTION 124

During a follow-up audit, it was found that a complex security vulnerability of low risk was not resolved within the agreed-upon timeframe. IT has stated that the system with the identified vulnerability is being replaced and is expected to be fully functional in two months. Which of the following is the BEST course of action?

- A. Require documentation that the finding will be addressed within the new system
- B. Schedule a meeting to discuss the issue with senior management
- C. Perform an ad hoc audit to determine if the vulnerability has been exploited
- D. Recommend the finding be resolved prior to implementing the new system

Correct Answer: C

Section:

QUESTION 125

An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

- A. There is a reconciliation process between the spreadsheet and the finance system
- B. A separate copy of the spreadsheet is routinely backed up
- C. The spreadsheet is locked down to avoid inadvertent changes
- D. Access to the spreadsheet is given only to those who require access



Correct Answer: D

Section:

QUESTION 126

A project team has decided to switch to an agile approach to develop a replacement for an existing business application. Which of the following should an IS auditor do FIRST to ensure the effectiveness of the project audit?

- A. Compare the agile process with previous methodology.
- B. Identify and assess existing agile process control
- C. Understand the specific agile methodology that will be followed.
- D. Interview business process owners to compile a list of business requirements

Correct Answer: C

Section:

QUESTION 127

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. architecture and cloud environment of the system.
- B. business process supported by the system.

- C. policies and procedures of the business area being audited.
- D. availability reports associated with the cloud-based system.

Correct Answer: B

Section:

QUESTION 128

Which of the following concerns is BEST addressed by securing production source libraries?

- A. Programs are not approved before production source libraries are updated.
- B. Production source and object libraries may not be synchronized.
- C. Changes are applied to the wrong version of production source libraries.
- D. Unauthorized changes can be moved into production.

Correct Answer: D

Section:

QUESTION 129

During the planning stage of a compliance audit, an IS auditor discovers that a bank's inventory of compliance requirements does not include recent regulatory changes related to managing data risk. What should the auditor do FIRST?

- A. Ask management why the regulatory changes have not been included.
- B. Discuss potential regulatory issues with the legal department.
- C. Report the missing regulatory updates to the chief information officer (CIO).
- D. Exclude recent regulatory changes from the audit scope.



Correct Answer: A

Section:

QUESTION 130

Which of the following activities would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA)?

- A. Implementing the remediation plan
- B. Partially completing the CSA
- C. Developing the remediation plan
- D. Developing the CSA questionnaire

Correct Answer: D

Section:

QUESTION 131

Which of the following would be an appropriate role of internal audit in helping to establish an organization's privacy program?

- A. Analyzing risks posed by new regulations
- B. Designing controls to protect personal data
- C. Defining roles within the organization related to privacy
- D. Developing procedures to monitor the use of personal data

Correct Answer: A

Section:

QUESTION 132

Which of the following occurs during the issues management process for a system development project?

- A. Contingency planning
- B. Configuration management
- C. Help desk management
- D. Impact assessment

Correct Answer: D

Section:

QUESTION 133

Which of the following findings from an IT governance review should be of GREATEST concern?

- A. The IT budget is not monitored
- B. All IT services are provided by third parties.
- C. IT value analysis has not been completed.
- D. IT supports two different operating systems.

Correct Answer: C

Section:

QUESTION 134

A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon. The MOST effective plan of action would be to:

- A. evaluate replacement systems and performance monitoring software.
- B. restrict functionality of system monitoring software to security-related events.
- C. re-install the system and performance monitoring software.
- D. use analytical tools to produce exception reports from the system and performance monitoring software.

Correct Answer: B

Section:

QUESTION 135

An organization that has suffered a cyber attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

- A. An imaging process was used to obtain a copy of the data from each computer.
- B. The legal department has not been engaged.
- C. The chain of custody has not been documented.
- D. Audit was only involved during extraction of the information.

Correct Answer: C

Section:



QUESTION 136

An IS auditor performs a follow-up audit and learns the approach taken by the auditee to fix the findings differs from the agreed-upon approach confirmed during the last audit. Which of the following should be the auditor's NEXT course of action?

- A. Evaluate the appropriateness of the remedial action taken.
- B. Conduct a risk analysis incorporating the change.
- C. Report results of the follow-up to the audit committee.
- D. Inform senior management of the change in approach.

Correct Answer: A

Section:

QUESTION 137

Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at test?

- A. Short key length
- B. Random key generation
- C. Use of symmetric encryption
- D. Use of asymmetric encryption

Correct Answer: A

Section:

QUESTION 138

Which of the following metrics would BEST measure the agility of an organization's IT function?

- A. Average number of learning and training hours per IT staff member
- B. Frequency of security assessments against the most recent standards and guidelines
- C. Average time to turn strategic IT objectives into an agreed upon and approved initiative
- D. Percentage of staff with sufficient IT-related skills for the competency required of their roles

Correct Answer: C

Section:

QUESTION 139

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

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

Correct Answer: A

Section:

QUESTION 140

Which of the following should an IS auditor review FIRST when planning a customer data privacy audit?



- A. Legal and compliance requirements
- B. Customer agreements
- C. Data classification
- D. Organizational policies and procedures

Correct Answer: D

Section:

QUESTION 141

Which of the following provides IS audit professionals with the BEST source of direction for performing audit functions?

- A. Audit charter
- B. IT steering committee
- C. Information security policy
- D. Audit best practices

Correct Answer: A

Section:

QUESTION 142

A third-party consultant is managing the replacement of an accounting system. Which of the following should be the IS auditor's GREATEST concern?

- A. Data migration is not part of the contracted activities.
- B. The replacement is occurring near year-end reporting
- C. The user department will manage access rights.
- D. Testing was performed by the third-party consultant



Correct Answer: C

Section:

QUESTION 143

Which of the following MUST be completed as part of the annual audit planning process?

- A. Business impact analysis (BIA)
- B. Fieldwork
- C. Risk assessment
- D. Risk control matrix

Correct Answer: C

Section:

QUESTION 144

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

- A. System/process flowchart
- B. File layouts

- C. Data architecture
- D. Source code documentation

Correct Answer: A

Section:

QUESTION 145

In an environment that automatically reports all program changes, which of the following is the MOST efficient way to detect unauthorized changes to production programs?

- A. Reviewing the last compile date of production programs
- B. Manually comparing code in production programs to controlled copies
- C. Periodically running and reviewing test data against production programs
- D. Verifying user management approval of modifications

Correct Answer: A

Section:

QUESTION 146

Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor's BEST recommendation for a compensating control?

- A. Require written authorization for all payment transactions
- B. Restrict payment authorization to senior staff members.
- C. Reconcile payment transactions with invoices.
- D. Review payment transaction history

Correct Answer: A

Section:

QUESTION 147

Which of the following BEST protects an organization's proprietary code during a joint-development activity involving a third party?

- A. Statement of work (SOW)
- B. Nondisclosure agreement (NDA)
- C. Service level agreement (SLA)
- D. Privacy agreement

Correct Answer: D

Section:

QUESTION 148

An organization has assigned two new IS auditors to audit a new system implementation. One of the auditors has an IT-related degree, and one has a business degree. Which of the following is MOST important to meet the IS audit standard for proficiency?

- A. The standard is met as long as one member has a globally recognized audit certification.
- B. Technical co-sourcing must be used to help the new staff.
- C. Team member assignments must be based on individual competencies.
- D. The standard is met as long as a supervisor reviews the new auditors' work.



Correct Answer: C

Section:

QUESTION 149

Which of the following is the MOST important activity in the data classification process?

- A. Labeling the data appropriately
- B. Identifying risk associated with the data
- C. Determining accountability of data owners
- D. Determining the adequacy of privacy controls

Correct Answer: A

Section:

QUESTION 150

Which of the following represents the HIGHEST level of maturity of an information security program?

- A. A training program is in place to promote information security awareness.
- B. A framework is in place to measure risks and track effectiveness.
- C. Information security policies and procedures are established.
- D. The program meets regulatory and compliance requirements.

Correct Answer: A

Section:

QUESTION 151

Which of the following findings should be of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simulation test administered for staff members?

- A. Staff members who failed the test did not receive follow-up education
- B. Test results were not communicated to staff members.
- C. Staff members were not notified about the test beforehand.
- D. Security awareness training was not provided prior to the test.

Correct Answer: D

Section:

QUESTION 152

Which of the following is the MOST important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

- A. Availability of IS audit resources
- B. Remediation dates included in management responses
- C. Peak activity periods for the business
- D. Complexity of business processes identified in the audit

Correct Answer: C

Section:



QUESTION 153

When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor's BEST recommendation is to place an intrusion detection system (IDS) between the firewall and:

- A. the organization's web server.
- B. the demilitarized zone (DMZ).
- C. the organization's network.
- D. the Internet

Correct Answer: C

Section:

QUESTION 154

Which of the following is the MOST important reason to classify a disaster recovery plan (DRP) as confidential?

- A. Ensure compliance with the data classification policy.
- B. Protect the plan from unauthorized alteration.
- C. Comply with business continuity best practice.
- D. Reduce the risk of data leakage that could lead to an attack.

Correct Answer: D

Section:

QUESTION 155

A new regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditors BEST recommendation to facilitate compliance with the regulation?

- A. Establish key performance indicators (KPIs) for timely identification of security incidents.
- B. Engage an external security incident response expert for incident handling.
- C. Enhance the alert functionality of the intrusion detection system (IDS).
- D. Include the requirement in the incident management response plan.

Correct Answer: C

Section:

QUESTION 156

After the merger of two organizations, which of the following is the MOST important task for an IS auditor to perform?

- A. Verifying that access privileges have been reviewed
- B. Investigating access rights for expiration dates
- C. Updating the continuity plan for critical resources
- D. Updating the security policy

Correct Answer: A

Section:

QUESTION 157

An IS auditor is reviewing an organization's primary router access control list. Which of the following should result in a finding?

- A. There are conflicting permit and deny rules for the IT group.
- B. The network security group can change network address translation (NAT).
- C. Individual permissions are overriding group permissions.
- D. There is only one rule per group with access privileges.

Correct Answer: C

Section:

QUESTION 158

While auditing a small organization's data classification processes and procedures, an IS auditor noticed that data is often classified at the incorrect level. What is the MOST effective way for the organization to improve this situation?

- A. Use automatic document classification based on content.
- B. Have IT security staff conduct targeted training for data owners.
- C. Publish the data classification policy on the corporate web portal.
- D. Conduct awareness presentations and seminars for information classification policies.

Correct Answer: D

Section:

QUESTION 159

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

Correct Answer: C

Section:

QUESTION 160

Which of the following must be in place before an IS auditor initiates audit follow-up activities?

- A. Available resources for the activities included in the action plan
- B. A management response in the final report with a committed implementation date
- C. A heat map with the gaps and recommendations displayed in terms of risk
- D. Supporting evidence for the gaps and recommendations mentioned in the audit report

Correct Answer: B

Section:

QUESTION 161

Which of the following is the MOST appropriate and effective fire suppression method for an unstaffed computer room?

- A. Water sprinkler
- B. Fire extinguishers
- C. Carbon dioxide (CO2)
- D. Dry pipe

Correct Answer: C

Section:

QUESTION 162

In a RAO model, which of the following roles must be assigned to only one individual?

- A. Responsible
- B. Informed
- C. Consulted
- D. Accountable

Correct Answer: D

Section:

QUESTION 163

Which of the following should an IS auditor consider FIRST when evaluating firewall rules?

- A. The organization's security policy
- B. The number of remote nodes
- C. The firewalls' default settings
- D. The physical location of the firewalls

Correct Answer: A

Section:

QUESTION 164

Which of the following is MOST helpful for measuring benefits realization for a new system?

- A. Function point analysis
- B. Balanced scorecard review
- C. Post-implementation review
- D. Business impact analysis (BIA)

Correct Answer: A

Section:

Explanation:

Topic 3, Exam Pool C

QUESTION 165

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 cameras are not installed in break rooms
- C. CCTV records are deleted after one year.
- D. CCTV footage is not recorded 24 x 7.

Correct Answer: A

Section:

QUESTION 166

Which of the following is the BEST way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster?

- A. Prepare detailed plans for each business function.
- B. Involve staff at all levels in periodic paper walk-through exercises.
- C. Regularly update business impact assessments.
- D. Make senior managers responsible for their plan sections.

Correct Answer: B

Section:

QUESTION 167

Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

- A. Limit check
- B. Parity check
- C. Reasonableness check
- D. Validity check



Correct Answer: C

Section:

QUESTION 168

Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organization's information security policy?

- A. IT steering committee minutes
- B. Business objectives
- C. Alignment with the IT tactical plan
- D. Compliance with industry best practice

Correct Answer: B

Section:

QUESTION 169

An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in-house. Which of the following findings should be the IS auditor's GREATEST concern?

- A. The cost of outsourcing is lower than in-house development.
- B. The vendor development team is located overseas.

- C. A training plan for business users has not been developed.
- D. The data model is not clearly documented.

Correct Answer: D

Section:

QUESTION 170

Which of the following provides the BEST providence that outsourced provider services are being properly managed?

- A. The service level agreement (SLA) includes penalties for non-performance.
- B. Adequate action is taken for noncompliance with the service level agreement (SLA).
- C. The vendor provides historical data to demonstrate its performance.
- D. Internal performance standards align with corporate strategy.

Correct Answer: B

Section:

QUESTION 171

A company has implemented an IT segregation of duties policy. In a role-based environment, which of the following roles may be assigned to an application developer?

- A. IT operator
- B. System administration
- C. Emergency support
- D. Database administration

Correct Answer: B

Section:

QUESTION 172

The PRIMARY role of a control self-assessment (CSA) facilitator is to:

- A. conduct interviews to gain background information.
- B. focus the team on internal controls.
- C. report on the internal control weaknesses.
- D. provide solutions for control weaknesses.

Correct Answer: B

Section:

QUESTION 173

Which of the following is the PRIMARY advantage of using visualization technology for corporate applications?

- A. Improved disaster recovery
- B. Better utilization of resources
- C. Stronger data security
- D. Increased application performance



Correct Answer: A

Section:

QUESTION 174

A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items to the inventory system. Which control would have BEST prevented this type of fraud in a retail environment?

- A. Separate authorization for input of transactions
- B. Statistical sampling of adjustment transactions
- C. Unscheduled audits of lost stock lines
- D. An edit check for the validity of the inventory transaction

Correct Answer: A

Section:

QUESTION 175

An organization allows its employees to use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

- A. Installing security software on the devices
- B. Partitioning the work environment from personal space on devices
- C. Preventing users from adding applications
- D. Restricting the use of devices for personal purposes during working hours

Correct Answer: B

Section:



QUESTION 176

Which of the following would provide an IS auditor with the GREATEST assurance that data disposal controls support business strategic objectives?

- A. Media recycling policy
- B. Media sanitization policy
- C. Media labeling policy
- D. Media shredding policy

Correct Answer: A

Section:

QUESTION 177

An IS auditor has been asked to advise on measures to improve IT governance within the organization. Which of the following is the BEST recommendation?

- A. Implement key performance indicators (KPIs)
- B. Implement annual third-party audits.
- C. Benchmark organizational performance against industry peers.
- D. Require executive management to draft IT strategy

Correct Answer: A

Section:

QUESTION 178

An IS auditor reviewing the threat assessment for a data center would be MOST concerned if:

- A. some of the identified threats are unlikely to occur.
- B. all identified threats relate to external entities.
- C. the exercise was completed by local management.
- D. neighboring organizations operations have been included.

Correct Answer: C

Section:

QUESTION 179

Which of the following features of a library control software package would protect against unauthorized updating of source code?

- A. Required approvals at each life cycle step
- B. Date and time stamping of source and object code
- C. Access controls for source libraries
- D. Release-to-release comparison of source code

Correct Answer: B

Section:

QUESTION 180

What is the BEST method to determine if IT resource spending is aligned with planned project spending?

- A. Earned value analysis (EVA)
- B. Return on investment (ROI) analysis
- C. Gantt chart
- D. Critical path analysis

Correct Answer: A

Section:

QUESTION 181

An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

- A. Increasing the frequency of risk-based IS audits for each business entity
- B. Developing a risk-based plan considering each entity's business processes
- C. Conducting an audit of newly introduced IT policies and procedures
- D. Revising IS audit plans to focus on IT changes introduced after the split

Correct Answer: D

Section:

QUESTION 182

An audit has identified that business units have purchased cloud-based applications without IP support. What is the GREATEST risk associated with this situation?

- A. The applications are not included in business continuity plans (BCFs)
- B. The applications may not reasonably protect data.
- C. The application purchases did not follow procurement policy.
- D. The applications could be modified without advanced notice.

Correct Answer: B

Section:

QUESTION 183

Which of the following would BEST enable an organization to address the security risks associated with a recently implemented bring your own device (BYOD) strategy?

- A. Mobile device tracking program
- B. Mobile device upgrade program
- C. Mobile device testing program
- D. Mobile device awareness program

Correct Answer: D

Section:

QUESTION 184

Which of the following is MOST important to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition?

- A. Role-based access control policies
- B. Types of data that can be uploaded to the platform
- C. Processes for on-boarding and off-boarding users to the platform
- D. Processes for reviewing administrator activity



Correct Answer: B

Section:

QUESTION 185

An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor's BEST recommendation for the organization?

- A. Analyze a new application that moots the current re
- B. Perform an analysis to determine the business risk
- C. Bring the escrow version up to date.
- D. Develop a maintenance plan to support the application using the existing code

Correct Answer: C

Section:

QUESTION 186

In response to an audit finding regarding a payroll application, management implemented a new automated control. Which of the following would be MOST helpful to the IS auditor when evaluating the effectiveness of the new control?

- A. Approved test scripts and results prior to implementation

- B. Written procedures defining processes and controls
- C. Approved project scope document
- D. A review of tabletop exercise results

Correct Answer: B

Section:

QUESTION 187

What would be an IS auditor's BEST recommendation upon finding that a third-party IT service provider hosts the organization's human resources (HR) system in a foreign country?

- A. Perform background verification checks.
- B. Review third-party audit reports.
- C. Implement change management review.
- D. Conduct a privacy impact analysis.

Correct Answer: D

Section:

QUESTION 188

Which of the following is the BEST way to enforce the principle of least privilege on a server containing data with different security classifications?

- A. Limiting access to the data files based on frequency of use
- B. Obtaining formal agreement by users to comply with the data classification policy
- C. Applying access controls determined by the data owner
- D. Using scripted access control lists to prevent unauthorized access to the server



Correct Answer: C

Section:

QUESTION 189

Management receives information indicating a high level of risk associated with potential flooding near the organization's data center within 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 avoidance
- B. Risk transfer
- C. Risk acceptance
- D. Risk reduction

Correct Answer: A

Section:

QUESTION 190

Which of the following is the BEST control to mitigate attacks that redirect Internet traffic to an unauthorized website?

- A. Utilize a network-based firewall.
- B. Conduct regular user security awareness training.
- C. Perform domain name system (DNS) server security hardening.

D. Enforce a strong password policy meeting complexity requirements.

Correct Answer: C

Section:

QUESTION 191

An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported. The auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

- A. Verify all patches have been applied to the software system's outdated version
- B. Close all unused ports on the outdated software system.
- C. Segregate the outdated software system from the main network.
- D. Monitor network traffic attempting to reach the outdated software system.

Correct Answer: D

Section:

QUESTION 192

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

- A. Apply single sign-on for access control
- B. Implement segregation of duties.
- C. Enforce an internal data access policy.
- D. Enforce the use of digital signatures.

Correct Answer: C

Section:

QUESTION 193

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

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

Correct Answer: A

Section:

QUESTION 194

An IS auditor discovers that an IT organization serving several business units assigns equal priority to all initiatives, creating a risk of delays in securing project funding. Which of the following would be MOST helpful in matching demand for projects and services with available resources in a way that supports business objectives?

- A. Project management
- B. Risk assessment results
- C. IT governance framework
- D. Portfolio management



Correct Answer: A

Section:

QUESTION 195

An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

- A. Loss of application support
- B. Lack of system integrity
- C. Outdated system documentation
- D. Developer access to production

Correct Answer: B

Section:

QUESTION 196

What is the PRIMARY purpose of documenting audit objectives when preparing for an engagement?

- A. To address the overall risk associated with the activity under review
- B. To identify areas with relatively high probability of material problems
- C. To help ensure maximum use of audit resources during the engagement
- D. To help prioritize and schedule auditee meetings

Correct Answer: B

Section:



QUESTION 197

Which of the following should be the FIRST step in the incident response process for a suspected breach?

- A. Inform potentially affected customers of the security breach
- B. Notify business management of the security breach.
- C. Research the validity of the alerted breach
- D. Engage a third party to independently evaluate the alerted breach.

Correct Answer: C

Section:

QUESTION 198

An IS auditor plans to review all access attempts to a video-monitored and proximity card-controlled communications room. Which of the following would be MOST useful to the auditor?

- A. Manual sign-in and sign-out log
- B. System electronic log
- C. Alarm system with CCTV
- D. Security incident log

Correct Answer: A

Section:

Explanation:

<https://www.slideshare.net/desmond.devendran/chap5-2007-cisa-review-course>

QUESTION 199

Which of the following should be the FIRST step when developing a data loss prevention (DLP) solution for a large organization?

- A. Identify approved data workflows across the enterprise.
- B. Conduct a threat analysis against sensitive data usage.
- C. Create the DLP policies and templates
- D. Conduct a data inventory and classification exercise

Correct Answer: D

Section:

QUESTION 200

An IS auditor reviewing security incident processes realizes incidents are resolved and closed, but root causes are not investigated. Which of the following should be the MAJOR concern with this situation?

- A. Abuses by employees have not been reported.
- B. Lessons learned have not been properly documented
- C. vulnerabilities have not been properly addressed
- D. Security incident policies are out of date.

Correct Answer: C

Section:



QUESTION 201

Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

- A. Review of program documentation
- B. Use of test transactions
- C. Interviews with knowledgeable users
- D. Review of source code

Correct Answer: B

Section:

QUESTION 202

A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement.

- A. A formal request for proposal (RFP) process
- B. Business case development procedures
- C. An information asset acquisition policy
- D. Asset life cycle management.

Correct Answer: D

Section:

QUESTION 203

An IS auditor follows up on a recent security incident and finds the incident response was not adequate. Which of the following findings should be considered MOST critical?

- A. The security weakness facilitating the attack was not identified.
- B. The attack was not automatically blocked by the intrusion detection system (IDS).
- C. The attack could not be traced back to the originating person.
- D. Appropriate response documentation was not maintained.

Correct Answer: A

Section:

QUESTION 204

A review of Internet security disclosed that users have individual user accounts with Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only the corporate network is used. The organization should FIRST:

- A. use a proxy server to filter out Internet sites that should not be accessed.
- B. keep a manual log of Internet access.
- C. monitor remote access activities.
- D. include a statement in its security policy about Internet use.

Correct Answer: D

Section:

QUESTION 205

Which of the following would BEST detect that a distributed denial of service (DDoS) attack is occurring?

- A. Customer service complaints
- B. Automated monitoring of logs
- C. Server crashes
- D. Penetration testing

Correct Answer: A

Section:

QUESTION 206

Which of the following is MOST important when implementing a data classification program?

- A. Understanding the data classification levels
- B. Formalizing data ownership
- C. Developing a privacy policy
- D. Planning for secure storage capacity

Correct Answer: B

Section:

QUESTION 207

Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable department?

- A. Restricting program functionality according to user security profiles
- B. Restricting access to update programs to accounts payable staff only
- C. Including the creators user ID as a field in every transaction record created
- D. Ensuring that audit trails exist for transactions

Correct Answer: A

Section:

QUESTION 208

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

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

Correct Answer: B

Section:

QUESTION 209

Which of the following types of environmental equipment will MOST likely be deployed below the floor tiles of a data center?

- A. Temperature sensors
- B. Humidity sensors
- C. Water sensors
- D. Air pressure sensors

Correct Answer: C

Section:

QUESTION 210

Which of the following would an IS auditor recommend as the MOST effective preventive control to reduce the risk of data leakage?

- A. Ensure that paper documents are disposed securely.
- B. Implement an intrusion detection system (IDS).
- C. Verify that application logs capture any changes made.
- D. Validate that all data files contain digital watermarks

Correct Answer: D

Section:

QUESTION 211

An IS auditor assessing the controls within a newly implemented call center would first

- A. gather information from the customers regarding response times and quality of service.
- B. review the manual and automated controls in the call center.



- C. test the technical infrastructure at the call center.
- D. evaluate the operational risk associated with the call center.

Correct Answer: D

Section:

QUESTION 212

An audit identified that a computer system is not assigning sequential purchase order numbers to order requests. The IS auditor is conducting an audit follow-up to determine if management has reserved this finding. Which of two following is the MOST reliable follow-up procedure?

- A. Review the documentation of recent changes to implement sequential order numbering.
- B. Inquire with management if the system has been configured and tested to generate sequential order numbers.
- C. Inspect the system settings and transaction logs to determine if sequential order numbers are generated.
- D. Examine a sample of system generated purchase orders obtained from management

Correct Answer: C

Section:

QUESTION 213

When reviewing a data classification scheme, it is MOST important for an IS auditor to determine if.

- A. each information asset is to a assigned to a different classification.
- B. the security criteria are clearly documented for each classification
- C. Senior IT managers are identified as information owner.
- D. the information owner is required to approve access to the asset



Correct Answer: B

Section:

QUESTION 214

Which of the following would be the MOST useful metric for management to consider when reviewing a project portfolio?

- A. Cost of projects divided by total IT cost
- B. Expected return divided by total project cost
- C. Net present value (NPV) of the portfolio
- D. Total cost of each project

Correct Answer: C

Section:

QUESTION 215

An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

- A. Improve the change management process
- B. Establish security metrics.
- C. Perform a penetration test
- D. Perform a configuration review

Correct Answer: D

Section:

QUESTION 216

Which of the following should an IS auditor expect to see in a network vulnerability assessment?

- A. Misconfiguration and missing updates
- B. Malicious software and spyware
- C. Zero-day vulnerabilities
- D. Security design flaws

Correct Answer: A

Section:

QUESTION 217

An IS auditor is reviewing the installation of a new server. The IS auditor's PRIMARY objective is to ensure that

- A. security parameters are set in accordance with the manufacturer's standards.
- B. a detailed business case was formally approved prior to the purchase.
- C. security parameters are set in accordance with the organization's policies.
- D. the procurement project invited bidders from at least three different suppliers.

Correct Answer: C

Section:

QUESTION 218

What is the PRIMARY benefit of an audit approach which requires reported findings to be issued together with related action plans, owners, and target dates?

- A. it facilitates easier audit follow-up
- B. it enforces action plan consensus between auditors and auditees
- C. it establishes accountability for the action plans
- D. it helps to ensure factual accuracy of findings

Correct Answer: C

Section:

QUESTION 219

During the planning phase of a data loss prevention (DLP) audit, management expresses a concern about mobile computing. Which of the following should the IS auditor identify as the associated risk?

- A. The use of the cloud negatively impacting IT availability
- B. Increased need for user awareness training
- C. Increased vulnerability due to anytime, anywhere accessibility
- D. Lack of governance and oversight for IT infrastructure and applications

Correct Answer: C

Section:



QUESTION 220

Which of the following would be an appropriate role of internal audit in helping to establish an organization's privacy program?

- A. Analyzing risks posed by new regulations
- B. Developing procedures to monitor the use of personal data
- C. Defining roles within the organization related to privacy
- D. Designing controls to protect personal data

Correct Answer: A

Section:

QUESTION 221

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

- A. The BCP's contact information needs to be updated
- B. The BCP is not version controlled.
- C. The BCP has not been approved by senior management.
- D. The BCP has not been tested since it was first issued.

Correct Answer: D

Section:

QUESTION 222

A post-implementation review was conducted by issuing a survey to users. Which of the following should be of GREATEST concern to an IS auditor?

- A. The survey results were not presented in detail to management.
- B. The survey questions did not address the scope of the business case.
- C. The survey form template did not allow additional feedback to be provided.
- D. The survey was issued to employees a month after implementation.

Correct Answer: B

Section:

QUESTION 223

Which of the following is the BEST reason to implement a data retention policy?

- A. To limit the liability associated with storing and protecting information
- B. To document business objectives for processing data within the organization
- C. To assign responsibility and ownership for data protection outside IT
- D. To establish a recovery point objective (RPO) for (toaster recovery procedures

Correct Answer: A

Section:

QUESTION 224

Which of the following would MOST effectively help to reduce the number of repeated incidents in an organization?

- A. Testing incident response plans with a wide range of scenarios
- B. Prioritizing incidents after impact assessment.
- C. Linking incidents to problem management activities
- D. Training incident management teams on current incident trends

Correct Answer: C

Section:

QUESTION 225

Which of the following is the MOST significant risk that IS auditors are required to consider for each engagement?

- A. Process and resource inefficiencies
- B. Irregularities and illegal acts
- C. Noncompliance with organizational policies
- D. Misalignment with business objectives

Correct Answer: D

Section:

QUESTION 226

An externally facing system containing sensitive data is configured such that users have either read- only or administrator rights. Most users of the system have administrator access. Which of the following is the GREATEST risk associated with this situation?

- A. Users can export application logs.
- B. Users can view sensitive data.
- C. Users can make unauthorized changes.
- D. Users can install open-licensed software.



Correct Answer: C

Section:

QUESTION 227

During an audit of an organization's risk management practices, an IS auditor finds several documented IT risk acceptances have not been renewed in a timely manner after the assigned expiration date. When assessing the severity of this finding, which mitigating factor would MOST significantly minimize the associated impact?

- A. There are documented compensating controls over the business processes.
- B. The risk acceptances were previously reviewed and approved by appropriate senior management
- C. The business environment has not significantly changed since the risk acceptances were approved.
- D. The risk acceptances with issues reflect a small percentage of the total population

Correct Answer: B

Section:

QUESTION 228

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 sufficient audit resources are allocated,

- B. Communicate audit results organization-wide.
- C. Ensure ownership is assigned.
- D. Test corrective actions upon completion.

Correct Answer: C

Section:

QUESTION 229

Which of the following is the BEST metric to measure the alignment of IT and business strategy?

- A. Level of stakeholder satisfaction with the scope of planned IT projects
- B. Percentage of enterprise risk assessments that include IT-related risk
- C. Percentage of staff satisfied with their IT-related roles
- D. Frequency of business process capability maturity assessments

Correct Answer: B

Section:

QUESTION 230

Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks?

- A. The end-to-end process is understood and documented.
- B. Roles and responsibilities are defined for the business processes in scope.
- C. A benchmarking exercise of industry peers who use RPA has been completed.
- D. A request for proposal (RFP) has been issued to qualified vendors.



Correct Answer: B

Section:

QUESTION 231

Which of the following should be performed FIRST before key performance indicators (KPIs) can be implemented?

- A. Analysis of industry benchmarks
- B. Identification of organizational goals
- C. Analysis of quantitative benefits
- D. Implementation of a balanced scorecard

Correct Answer: B

Section:

QUESTION 232

During audit framework, an IS auditor teams 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. Conduct a walk-through to view results of an employee plugging in a device to transfer confidential data.
- B. Review compliance with data loss and applicable mobile device user acceptance policies.
- C. Verify the data loss prevention (DLP) tool is properly configured by the organization.

D. Verify employees have received appropriate mobile device security awareness training.

Correct Answer: B

Section:

QUESTION 233

If enabled within firewall rules, which of the following services would present the GREATEST risk?

- A. Simple mail transfer protocol (SMTP)
- B. Simple object access protocol (SOAP)
- C. Hypertext transfer protocol (HTTP)
- D. File transfer protocol (FTP)

Correct Answer: D

Section:

QUESTION 234

Which of the following is the BEST way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC)?

- A. Have an independent party review the source calculations
- B. Execute copies of EUC programs out of a secure library
- C. Implement complex password controls
- D. Verify EUC results through manual calculations

Correct Answer: B

Section:

QUESTION 235

Which of the following BEST enables the effectiveness of an agile project for the rapid development of a new software application?

- A. Project segments are established.
- B. The work is separated into phases.
- C. The work is separated into sprints.
- D. Project milestones are created.

Correct Answer: D

Section:

QUESTION 236

Which of the following is the MOST effective way to identify exfiltration of sensitive data by a malicious insider?

- A. Implement data loss prevention (DLP) software
- B. Review perimeter firewall logs
- C. Provide ongoing information security awareness training
- D. Establish behavioral analytics monitoring

Correct Answer: A



Section:

QUESTION 237

An IS auditor identifies that a legacy application to be decommissioned in three months cannot meet the security requirements established by the current policy. What is the BEST way (or the auditor to address this issue?

- A. Recommend the application be patched to meet requirements.
- B. Inform the IT director of the policy noncompliance.
- C. Verify management has approved a policy exception to accept the risk.
- D. Take no action since the application will be decommissioned in three months.

Correct Answer: C

Section:

QUESTION 238

An IS auditor reviewing the threat assessment for a data center would be MOST concerned if:

- A. some of the identified threats are unlikely to occur.
- B. all identified threats relate to external entities.
- C. the exercise was completed by local management.
- D. neighboring organizations' operations have been included.

Correct Answer: C

Section:

QUESTION 239

Which of the following is the BEST indication of effective IT investment management?

- A. IT investments are implemented and monitored following a system development life cycle (SDLC)
- B. IT investments are mapped to specific business objectives
- C. Key performance indicators (KPIs) are defined for each business requiring IT Investment
- D. The IT Investment budget is significantly below industry benchmarks

Correct Answer: B

Section:

QUESTION 240

Which of the following is the MOST important responsibility of user departments associated with program changes?

- A. Providing unit test data
- B. Analyzing change requests
- C. Updating documentation to reflect latest changes
- D. Approving changes before implementation

Correct Answer: A

Section:

QUESTION 241



Audit frameworks can assist the IS audit function by:

- A. defining the authority and responsibility of the IS audit function.
- B. providing details on how to execute the audit program.
- C. providing direction and information regarding the performance of audits.
- D. outlining the specific steps needed to complete audits

Correct Answer: C

Section:

QUESTION 242

Which of the following would be the BEST process for continuous auditing to a large financial institution?

- A. Testing encryption standards on the disaster recovery system
- B. Validating access controls for real-time data systems
- C. Performing parallel testing between systems
- D. Validating performance of help desk metrics

Correct Answer: B

Section:

QUESTION 243

Which of the following methods will BEST reduce the risk associated with the transition to a new system using technologies that are not compatible with the old system?

- A. Parallel changeover
- B. Modular changeover
- C. Phased operation
- D. Pilot operation

Correct Answer: A

Section:

QUESTION 244

An internal audit team is deciding whether to use an audit management application hosted by a third party in a different country. What should be the MOST important consideration related to the uploading of payroll audit documentation in the hosted application?

- A. Financial regulations affecting the organization
- B. Data center physical access controls where the application is hosted
- C. Privacy regulations affecting the organization
- D. Per-unit cost charged by the hosting services provider for storage

Correct Answer: C

Section:

QUESTION 245

Which of the following findings should be of GREATEST concern to an IS auditor assessing the risk associated with end-user computing (EUC) in an organization?



- A. Insufficient processes to track ownership of each EUC application?
- B. Insufficient processes to test for version control
- C. Lack of awareness training for EUC users
- D. Lack of defined criteria for EUC applications

Correct Answer: D

Section:

QUESTION 246

What would be an IS auditor's BEST course of action when an auditee is unable to close all audit recommendations by the time of the follow-up audit?

- A. Ensure the open issues are retained in the audit results.
- B. Terminate the follow-up because open issues are not resolved
- C. Recommend compensating controls for open issues.
- D. Evaluate the residual risk due to open issues.

Correct Answer: D

Section:

QUESTION 247

Which of the following is the BEST way to sanitize a hard disk for reuse to ensure the organization's information cannot be accessed?

- A. Re-partitioning
- B. Degaussing
- C. Formatting
- D. Data wiping

Correct Answer: D

Section:

QUESTION 248

An IS auditor is evaluating the access controls for a shared customer relationship management (CRM) system. Which of the following would be the GREATEST concern?

- A. Single sign-on is not enabled
- B. Audit logging is not enabled
- C. Security baseline is not consistently applied
- D. Complex passwords are not required

Correct Answer: B

Section:

QUESTION 249

An IS auditor concludes that logging and monitoring mechanisms within an organization are ineffective because critical servers are not included within the central log repository. Which of the following audit procedures would have MOST likely identified this exception?

- A. Inspecting a sample of alerts generated from the central log repository
- B. Comparing a list of all servers from the directory server against a list of all servers present in the central log repository



- C. Inspecting a sample of alert settings configured in the central log repository
- D. Comparing all servers included in the current central log repository with the listing used for the prior-year audit

Correct Answer: B

Section:

QUESTION 250

A financial group recently implemented new technologies and processes, Which type of IS audit would provide the GREATEST level of assurance that the department's objectives have been met?

- A. Performance audit
- B. Integrated audit
- C. Cyber audit
- D. Financial audit

Correct Answer: B

Section:

QUESTION 251

Which of the following areas is MOST likely to be overlooked when implementing a new data classification process?

- A. End-user computing (EUC) systems
- B. Email attachments
- C. Data sent to vendors
- D. New system applications

Correct Answer: B

Section:

QUESTION 252

An IS auditor is renewing the deployment of a new automated system Which of the following findings presents the MOST significant risk?

- A. The new system has resulted in layoffs of key experienced personnel.
- B. Users have not been trained on the new system.
- C. Data from the legacy system is not migrated correctly to the new system.
- D. The new system is not platform agnostic

Correct Answer: C

Section:

QUESTION 253

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

- A. Less funding required overall
- B. Quicker deliverables
- C. Quicker end user acceptance
- D. Clearly defined business expectations



Correct Answer: B

Section:

QUESTION 254

Which of the following is the BEST control to minimize the risk of unauthorized access to lost company-owned mobile devices?

- A. Password/PIN protection
- B. Device tracking software
- C. Device encryption
- D. Periodic backup

Correct Answer: A

Section:

QUESTION 255

Which of the following is the BEST approach for determining the overall IT risk appetite of an organization when business units use different methods for managing IT risks?

- A. Average the business units' IT risk levels
- B. Identify the highest-rated IT risk level among the business units
- C. Prioritize the organization's IT risk scenarios
- D. Establish a global IT risk scoring criteria

Correct Answer: C

Section:

QUESTION 256

Which of the following should be of GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

- A. The change management process was not formally documented
- B. Backups of the old system and data are not available online
- C. Unauthorized data modifications occurred during conversion,
- D. Data conversion was performed using manual processes

Correct Answer: C

Section:

QUESTION 257

An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported. The auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

- A. Verify all patches have been applied to the software system's outdated version.
- B. Close all unused ports on the outdated software system.
- C. Monitor network traffic attempting to reach the outdated software system.
- D. Segregate the outdated software system from the main network.

Correct Answer: C

Section:



QUESTION 258

An IS auditor finds that while an organization's IT strategy is heavily focused on research and development, the majority of projects in the IT portfolio focus on operations and maintenance. Which of the following is the BEST recommendation?

- A. Align the IT strategy with business objectives
- B. Review priorities in the IT portfolio
- C. Change the IT strategy to focus on operational excellence.
- D. Align the IT portfolio with the IT strategy.

Correct Answer: A

Section:

QUESTION 259

Which of the following is the BEST performance indicator for the effectiveness of an incident management program?

- A. Average time between incidents
- B. Incident alert meantime
- C. Number of incidents reported
- D. Incident resolution meantime

Correct Answer: D

Section:

QUESTION 260

Which of the following is the BEST way to verify the effectiveness of a data restoration process?

- A. Performing periodic reviews of physical access to backup media
- B. Performing periodic complete data restorations
- C. Validating offline backups using software utilities
- D. Reviewing and updating data restoration policies annually

Correct Answer: B

Section:

QUESTION 261

In which phase of the internal audit process is contact established with the individuals responsible for the business processes in scope for review?

- A. Planning phase
- B. Execution phase
- C. Follow-up phase
- D. Selection phase

Correct Answer: A

Section:

QUESTION 262

A bank has a combination of corporate customer accounts (higher monetary value) and small business accounts (lower monetary value) as part of online banking. Which of the following is the BEST sampling approach for an



IS auditor to use for these accounts?

- A. Difference estimation sampling
- B. Stratified mean per unit sampling
- C. Customer unit sampling
- D. Unstratified mean per unit sampling

Correct Answer: A

Section:

QUESTION 263

Which of the following should be the FIRST step to successfully implement a corporate data classification program?

- A. Approve a data classification policy.
- B. Select a data loss prevention (DLP) product.
- C. Confirm that adequate resources are available for the project.
- D. Check for the required regulatory requirements.

Correct Answer: D

Section:

QUESTION 264

A CFO has requested an audit of IT capacity management due to a series of finance system slowdowns during month-end reporting. What would be MOST important to consider before including this audit in the program?

- A. Whether system delays result in more frequent use of manual processing
- B. Whether the system's performance poses a significant risk to the organization
- C. Whether stakeholders are committed to assisting with the audit
- D. Whether internal auditors have the required skills to perform the audit

Correct Answer: B

Section:

QUESTION 265

The use of which of the following is an inherent risk in the application container infrastructure?

- A. Shared registries
- B. Host operating system
- C. Shared data
- D. Shared kernel

Correct Answer: B

Section:

QUESTION 266

A data center's physical access log system captures each visitor's identification document numbers along with the visitor's photo. Which of the following sampling methods would be MOST useful to an IS auditor conducting compliance testing for the effectiveness of the system?

- A. Quota sampling
- B. Haphazard sampling
- C. Attribute sampling
- D. Variable sampling

Correct Answer: D

Section:

QUESTION 267

Which of the following is the MOST appropriate indicator of change management effectiveness?

- A. Time lag between changes to the configuration and the update of records
- B. Number of system software changes
- C. Time lag between changes and updates of documentation materials
- D. Number of incidents resulting from changes

Correct Answer: D

Section:

QUESTION 268

An organization has recently moved to an agile model for deploying custom code to its in-house accounting software system. When reviewing the procedures in place for production code deployment, which of the following is the MOST significant security concern to address?

- A. Software vulnerability scanning is done on an ad hoc basis.
- B. Change control does not include testing and approval from quality assurance (QA).
- C. Production code deployment is not automated.
- D. Current DevSecOps processes have not been independently verified.



Correct Answer: A

Section:

QUESTION 269

Which of the following provides a new IS auditor with the MOST useful information to evaluate overall IT performance?

- A. IT value analysis
- B. Prior audit reports
- C. IT balanced scorecard
- D. Vulnerability assessment report

Correct Answer: C

Section:

QUESTION 270

A disaster recovery plan (DRP) should include steps for:

- A. assessing and quantifying risk.
- B. negotiating contracts with disaster planning consultants.

- C. identifying application control requirements.
- D. obtaining replacement supplies.

Correct Answer: A

Section:

QUESTION 271

Which of the following is the BEST indication that there are potential problems within an organization's IT service desk function?

- A. Undocumented operating procedures
- B. Lack of segregation of duties
- C. An excessive backlog of user requests
- D. Lack of key performance indicators (KPIs)

Correct Answer: C

Section:

QUESTION 272

While evaluating the data classification process of an organization, an IS auditor's PRIMARY focus should be on whether:

- A. data classifications are automated.
- B. a data dictionary is maintained.
- C. data retention requirements are clearly defined.
- D. data is correctly classified.

Correct Answer: D

Section:

QUESTION 273

An IS auditor is preparing a plan for audits to be carried out over a specified period. Which of the following activities should the IS auditor perform FIRST?

- A. Allocate audit resources.
- B. Prioritize risks.
- C. Review prior audit reports.
- D. Determine the audit universe.

Correct Answer: B

Section:

QUESTION 274

When assessing the overall effectiveness of an organization's disaster recovery planning process, which of the following is MOST important for the IS auditor to verify?

- A. Management contracts with a third party for warm site services.
- B. Management schedules an annual tabletop exercise.
- C. Management documents and distributes a copy of the plan to all personnel.
- D. Management reviews and updates the plan annually or as changes occur.



Correct Answer: D

Section:

QUESTION 275

In the development of a new financial application, the IS auditor's FIRST involvement should be in the:

- A. control design.
- B. feasibility study.
- C. application design.
- D. system test.

Correct Answer: A

Section:

QUESTION 276

What is the MOST effective way to detect installation of unauthorized software packages by employees?

- A. Regular scanning of hard drives
- B. Communicating the policy to employees
- C. Logging of activity on the network
- D. Maintaining current antivirus software

Correct Answer: A

Section:

QUESTION 277

The PRIMARY benefit of automating application testing is to:

- A. provide test consistency.
- B. provide more flexibility.
- C. replace all manual test processes.
- D. reduce the time to review code.

Correct Answer: D

Section:

QUESTION 278

Which of the following BEST addresses the availability of an online store?

- A. RAID level 5 storage devices
- B. Online backups
- C. A mirrored site at another location
- D. Clustered architecture

Correct Answer: C

Section:



QUESTION 279

Which of the following is the BEST way to prevent social engineering incidents?

- A. Maintain an onboarding and annual security awareness program.
- B. Ensure user workstations are running the most recent version of antivirus software.
- C. Include security responsibilities in job descriptions and require signed acknowledgment.
- D. Enforce strict email security gateway controls

Correct Answer: A

Section:

QUESTION 280

The PRIMARY purpose of a configuration management system is to:

- A. track software updates.
- B. define baselines for software.
- C. support the release procedure.
- D. standardize change approval.

Correct Answer: B

Section:

QUESTION 281

Which of the following is the MOST important consideration when evaluating the data retention policy for a global organization with regional offices in multiple countries?

- A. The policy aligns with corporate policies and practices.
- B. The policy aligns with global best practices.
- C. The policy aligns with business goals and objectives.
- D. The policy aligns with local laws and regulations.

Correct Answer: D

Section:

QUESTION 282

Which of the following BEST enables alignment of IT with business objectives?

- A. Benchmarking against peer organizations
- B. Developing key performance indicators (KPIs)
- C. Completing an IT risk assessment
- D. Leveraging an IT governance framework

Correct Answer: D

Section:

QUESTION 283

Which of the following are used in a firewall to protect the entity's internal resources?

- A. Remote access servers
- B. Secure Sockets Layers (SSLs)
- C. Internet Protocol (IP) address restrictions
- D. Failover services

Correct Answer: C

Section:

QUESTION 284

Which of the following would be MOST impacted if an IS auditor were to assist with the implementation of recommended control enhancements?

- A. Independence
- B. Integrity
- C. Materiality
- D. Accountability

Correct Answer: A

Section:

QUESTION 285

Controls related to authorized modifications to production programs are BEST tested by:

- A. tracing modifications from the original request for change forward to the executable program.
- B. tracing modifications from the executable program back to the original request for change.
- C. testing only the authorizations to implement the new program.
- D. reviewing only the actual lines of source code changed in the program.



Correct Answer: A

Section:

QUESTION 286

Which of the following is a PRIMARY responsibility of an IT steering committee?

- A. Prioritizing IT projects in accordance with business requirements
- B. Reviewing periodic IT risk assessments
- C. Validating and monitoring the skill sets of IT department staff
- D. Establishing IT budgets for the business

Correct Answer: A

Section:

QUESTION 287

Which of the following is MOST important to define within a disaster recovery plan (DRP)?

- A. Business continuity plan (BCP)
- B. Test results for backup data restoration
- C. A comprehensive list of disaster recovery scenarios and priorities

D. Roles and responsibilities for recovery team members

Correct Answer: D

Section:

QUESTION 288

Management has learned the implementation of a new IT system will not be completed on time and has requested an audit. Which of the following audit findings should be of GREATEST concern?

- A. The actual start times of some activities were later than originally scheduled.
- B. Tasks defined on the critical path do not have resources allocated.
- C. The project manager lacks formal certification.
- D. Milestones have not been defined for all project products.

Correct Answer: D

Section:

QUESTION 289

Which of the following is MOST effective for controlling visitor access to a data center?

- A. Visitors are escorted by an authorized employee
- B. Pre-approval of entry requests
- C. Visitors sign in at the front desk upon arrival
- D. Closed-circuit television (CCTV) is used to monitor the facilities

Correct Answer: A

Section:



QUESTION 290

Which of the following BEST enables an organization to improve the visibility of end-user computing (EUC) applications that support regulatory reporting?

- A. EUC inventory
- B. EUC availability controls
- C. EUC access control matrix
- D. EUC tests of operational effectiveness

Correct Answer: C

Section:

QUESTION 291

In an IT organization where many responsibilities are shared which of the following is the BEST control for detecting unauthorized data changes'?

- A. Users are required to periodically rotate responsibilities
- B. Segregation of duties conflicts are periodically reviewed
- C. Data changes are independently reviewed by another group
- D. Data changes are logged in an outside application

Correct Answer: C

Section:

QUESTION 292

Which of the following is the BEST testing approach to facilitate rapid identification of application interface errors?

- A. Integration testing
- B. Regression testing
- C. Automated testing
- D. User acceptance testing (UAT)

Correct Answer: C

Section:

QUESTION 293

An IS auditor is assigned to review the IS department's quality procedures. Upon contacting the IS manager, the auditor finds that there is an informal unwritten set of standards. Which of the following should be the auditor's NEXT action?

- A. Make recommendations to IS management as to appropriate quality standards
- B. Postpone the audit until IS management implements written standards
- C. Document and test compliance with the informal standards
- D. Finalize the audit and report the finding

Correct Answer: C

Section:

QUESTION 294

Which of the following analytical methods would be MOST useful when trying to identify groups with similar behavior or characteristics in a large population?

- A. Deviation detection
- B. Cluster sampling
- C. Random sampling
- D. Classification

Correct Answer: A

Section:

QUESTION 295

When reviewing a project to replace multiple manual data entry systems with an artificial intelligence (AI) system, the IS auditor should be MOST concerned with the impact AI will have on

- A. employee retention
- B. enterprise architecture (EA)
- C. future task updates
- D. task capacity output

Correct Answer: B

Section:



QUESTION 296

After delivering an audit report, the audit manager discovers that evidence was overlooked during the audit. This evidence indicates that a procedural control may have failed and could contradict a conclusion of the audit. Which of the following risks is MOST affected by this oversight?

- A. Inherent
- B. Operational
- C. Audit
- D. Financial

Correct Answer: A

Section:

QUESTION 297

An IS auditor observes that a business-critical application does not currently have any level of fault tolerance. Which of the following is the GREATEST concern with this situation?

- A. Degradation of services
- B. Limited tolerance for damage
- C. Decreased mean time between failures (MTBF)
- D. Single point of failure

Correct Answer: D

Section:

QUESTION 298

An IS auditor requests direct access to data required to perform audit procedures instead of asking management to provide the data. Which of the following is the PRIMARY advantage of this approach?

- A. Audit transparency
- B. Data confidentiality
- C. Professionalism
- D. Audit efficiency

Correct Answer: A

Section:

QUESTION 299

A new system development project is running late against a critical implementation deadline. Which of the following is the MOST important activity?

- A. Document last-minute enhancements
- B. Perform a pre-implementation audit
- C. Perform user acceptance testing (UAT)
- D. Ensure that code has been reviewed

Correct Answer: A

Section:

QUESTION 300

Which of the following findings should be of GREATEST concern to an IS auditor reviewing an organization's newly implemented online security awareness program?

- A. Only new employees are required to attend the program
- B. Metrics have not been established to assess training results
- C. Employees do not receive immediate notification of results
- D. The timing for program updates has not been determined

Correct Answer: B

Section:

QUESTION 301

Which of the following should be of GREATEST concern to an IS auditor when auditing an organization's IT strategy development process?

- A. The IT strategy was developed before the business plan
- B. A business impact analysis (BIA) was not performed to support the IT strategy
- C. The IT strategy was developed based on the current IT capability
- D. Information security was not included as a key objective in the IT strategic plan.

Correct Answer: B

Section:

QUESTION 302

An organization implemented a cybersecurity policy last year. Which of the following is the GREATEST indicator that the policy may need to be revised?

- A. A significant increase in authorized connections to third parties
- B. A significant increase in cybersecurity audit findings
- C. A significant increase in approved exceptions
- D. A significant increase in external attack attempts



Correct Answer: C

Section:

QUESTION 303

The operations team of an organization has reported an IS security attack. Which of the following should be the FIRST step for the security incident response team?

- A. Report results to management
- B. Document lessons learned
- C. Perform a damage assessment
- D. Prioritize resources for corrective action

Correct Answer: C

Section:

QUESTION 304

An IS auditor is reviewing the perimeter security design of a network. Which of the following provides the GREATEST assurance outgoing Internet traffic is controlled?

- A. Intrusion detection system (IDS)
- B. Security information and event management (SIEM) system

- C. Stateful firewall
- D. Load balancer

Correct Answer: C

Section:

QUESTION 305

Backup procedures for an organization's critical data are considered to be which type of control?

- A. Directive
- B. Corrective
- C. Detective
- D. Compensating

Correct Answer: B

Section:

QUESTION 306

What is the PRIMARY benefit of using one-time passwords?

- A. An intercepted password cannot be reused
- B. Security for applications can be automated
- C. Users do not have to memorize complex passwords
- D. Users cannot be locked out of an account

Correct Answer: A

Section:

QUESTION 307

Which of the following should an organization do to anticipate the effects of a disaster?

- A. Define recovery point objectives (RPO)
- B. Simulate a disaster recovery
- C. Develop a business impact analysis (BIA)
- D. Analyze capability maturity model gaps

Correct Answer: C

Section:

QUESTION 308

A fire alarm system has been installed in the computer room. The MOST effective location for the fire alarm control panel would be inside the

- A. computer room closest to the uninterruptible power supply (UPS) module
- B. computer room closest to the server computers
- C. system administrators office
- D. booth used by the building security personnel



Correct Answer: D

Section:

QUESTION 309

Which of the following methods BEST enforces data leakage prevention in a multi-tenant cloud environment?

- A. Monitoring tools are configured to alert in case of downtime
- B. A comprehensive security review is performed every quarter.
- C. Data for different tenants is segregated by database schema
- D. Tenants are required to implement data classification policies

Correct Answer: D

Section:

QUESTION 310

Which of the following is the BEST way to minimize sampling risk?

- A. Use a larger sample size
- B. Perform statistical sampling
- C. Perform judgmental sampling
- D. Enhance audit testing procedures

Correct Answer: B

Section:

QUESTION 311

An organization has implemented a distributed security administration system to replace the previous centralized one. Which of the following presents the GREATEST potential concern?

- A. Security procedures may be inadequate to support the change
- B. A distributed security system is inherently a weak security system
- C. End-user acceptance of the new system may be difficult to obtain
- D. The new system will require additional resources

Correct Answer: A

Section:

QUESTION 312

An organization's IT risk assessment should include the identification of:

- A. vulnerabilities
- B. compensating controls
- C. business needs
- D. business process owners

Correct Answer: A

Section:

