Exam Questions CISA

Isaca CISA

https://www.2passeasy.com/dumps/CISA/

NEW QUESTION 1
- (Exam Topic 4)
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 action1?

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

Answer: C

NEW QUESTION 2
- (Exam Topic 4)
The use of access control lists (ACLs) is the MOST effective method to mitigate security risk for routers because they: (Identify Correct answer and related explanation/references from CISA Certification - Information Systems Auditor official Manual or book)

A. are recommended by security standards.
B. can limit Telnet and traffic from the open Internet.
C. act as fitters between the world and the network.
D. can detect cyberattacks.

Answer: B

Explanation:
The use of access control lists (ACLs) can limit Telnet and traffic from the open Internet, and they act as filters between the world and the network. This makes them effective in mitigating security risk for routers as they can restrict unauthorized access to the network and protect it from external threats.
Reference: CISA (Certified Information Systems Auditor) Official Study Guide, 7th Edition by ISACA.

NEW QUESTION 3
- (Exam Topic 4)
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.

Answer: D

NEW QUESTION 4
- (Exam Topic 4)
What should an IS auditor evaluate FIRST when reviewing an organization's response to new privacy legislation?

A. Implementation plan for restricting the collection of personal information
B. Privacy legislation in other countries that may contain similar requirements
C. Operational plan for achieving compliance with the legislation
D. Analysis of systems that contain privacy components

Answer: D

Explanation:
This is according to the ISACA's IS Auditing Guideline G14 on Privacy and Data Protection, which states that an IS auditor should first evaluate the organization's ability to identify and assess the systems that contain privacy components, and then review the adequacy of the operational plan for achieving compliance with the legislation.

NEW QUESTION 5
- (Exam Topic 4)
An IS auditor conducts a review of a third-party vendor's reporting of key performance indicators (KPIs) Which of the following findings should be of MOST concern to the auditor?

A. KPI data is not being analyzed
B. KPIs are not clearly defined
C. Some KPIs are not documented
D. KPIs have never been updated

Answer: B

NEW QUESTION 6
- (Exam Topic 4)
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 polices

Answer: D

NEW QUESTION 7
- (Exam Topic 4)
During the discussion of a draft audit report IT management provided suitable evidence that a process has been implemented for a control that had been concluded by the IS auditor as ineffective Which of the following is the auditor's BEST action?

A. Explain to IT management that the new control will be evaluated during follow-up
B. Add comments about the action taken by IT management in the report
C. Change the conclusion based on evidence provided by IT management
D. Re-perform the audit before changing the conclusion

Answer: D

NEW QUESTION 8
- (Exam Topic 4)
Which of the following is the BEST point in time to conduct a post-implementation review?

A. After a full processing cycle
B. Immediately after deployment
C. After the warranty period
D. Prior to the annual performance review

Answer: A

Explanation:
The best point in time to conduct a post-implementation review is after a full processing cycle. A post-implementation review is conducted to verify that the implemented system meets the original
requirements and that it is operating as intended. Therefore, it is important to wait until the system has gone through a full processing cycle, so that any errors or issues can be identified and addressed. This allows the organization to make sure that the system is stable and reliable before it is put into production.

NEW QUESTION 9
- (Exam Topic 4)
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

Answer: B

NEW QUESTION 10
- (Exam Topic 4)
Which of the following is MOST important to determine when conducting an audit Of an organization's data privacy practices?

A. Whether a disciplinary process is established for data privacy violations
B. Whether strong encryption algorithms are deployed for personal data protection
C. Whether privacy technologies are implemented for personal data protection
D. Whether the systems inventory containing personal data is maintained

Answer: D

Explanation:
The systems inventory containing personal data is a crucial element for auditing an organization’s data privacy practices. The systems inventory is a list of all the systems, applications, databases, and devices that collect, store, process, or transmit personal data within the organization12. The systems inventory helps the auditor to identify the scope, location, ownership, and classification of personal data, as well as the risks and controls associated with them12. The systems inventory also helps the auditor to verify compliance with data privacy laws, regulations, and internal policies that apply to different types of personal data

NEW QUESTION 10
- (Exam Topic 4)
When assessing whether an organization's IT performance measures are comparable to other organizations in the same industry, which of the following would be MOST helpful to review?

A. IT governance frameworks
B. Benchmarking surveys
C. Utilization reports
D. Balanced scorecard

Answer: B

Explanation:
Benchmarking surveys are used to compare an organization's IT performance measures to those of other organizations in the same industry. The surveys provide data on a variety of IT performance metrics, including system availability, system reliability, cost effectiveness, and customer satisfaction. This data can then be

used to assess whether an organization's IT performance measures are comparable to other organizations in the same industry.

NEW QUESTION 15
- (Exam Topic 4)
An IT balanced scorecard is PRIMARILY used for:

A. evaluating the IT project portfolio
B. measuring IT strategic performance
C. allocating IT budget and resources
D. monitoring risk in lT-related processes

Answer: B

NEW QUESTION 17
- (Exam Topic 4)
One advantage of monetary unit sampling is the fact that

A. results are stated m terms of the frequency of items in error
B. it can easily be applied manually when computer resources are not available
C. large-value population items are segregated and audited separately
D. it increases the likelihood of selecting material items from the population

Answer: D

NEW QUESTION 20
- (Exam Topic 4)
Which of the following provides the MOST reliable method of preventing unauthonzed logon?

A. issuing authentication tokens
B. Reinforcing current security policies
C. Limiting after-hours usage
D. Installing an automatic password generator

Answer: A

NEW QUESTION 23
- (Exam Topic 4)
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.

Answer: D

NEW QUESTION 28
- (Exam Topic 4)
Which of the following is the GREATEST risk if two users have concurrent access to the same database record?

A. Availability integrity
B. Data integrity
C. Entity integrity
D. Referential integrity

Answer: B

NEW QUESTION 31
- (Exam Topic 4)
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.

Answer: A

NEW QUESTION 32
- (Exam Topic 4)
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

Answer: A

NEW QUESTION 35
- (Exam Topic 4)
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

Answer: B

NEW QUESTION 39
- (Exam Topic 4)
Which of the following is the MOST important Issue for an IS auditor to consider with regard to Voice-over IP (VoIP) communications?

A. Continuity of service
B. Identity management
C. Homogeneity of the network
D. Nonrepudiation

Answer: C

NEW QUESTION 41
- (Exam Topic 4)
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

Answer: C

NEW QUESTION 45
- (Exam Topic 4)
Which of the following should be of GREATEST concern to an IS auditor who is assessing an organization's configuration and release management process?

A. The organization does not use an industry-recognized methodology
B. Changes and change approvals are not documented
C. All changes require middle and senior management approval
D. There is no centralized configuration management database (CMDB)

Answer: B

NEW QUESTION 50
- (Exam Topic 4)
Which of following is MOST important to determine when conducing a post-implementation review?

A. Whether the solution architecture compiles with IT standards
B. Whether success criteria have been achieved
C. Whether the project has been delivered within the approved budget
D. Whether lessons teamed have been documented

Answer: B

NEW QUESTION 53
- (Exam Topic 4)
Which of the following is the BEST recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage?

A. Require employees to waive privacy rights related to data on BYOD devices.
B. Require multi-factor authentication on BYOD devices,
C. Specify employee responsibilities for reporting lost or stolen BYOD devices.
D. Allow only registered BYOD devices to access the network.

Answer: B

NEW QUESTION 55
- (Exam Topic 4)
Which of the following is a method to prevent disclosure of classified documents printed on a shared printer?

A. Using passwords to allow authorized users to send documents to the printer
B. Requiring a key code to be entered on the printer to produce hard copy
C. Encrypting the data stream between the user's computer and the printer
D. Producing a header page with classification level for printed documents

Answer: B

Explanation:
The best way to prevent the disclosure of classified documents printed on a shared printer is to require a key code to be entered on the printer to produce hard copy. This key code should be known only by authorized personnel, and should be changed frequently to prevent unauthorized access. Other methods such as using passwords to allow authorized users to send documents to the printer, encrypting the data stream between the user's computer and the printer, and producing a header page with classification level for printed documents are also viable options, but requiring a key code to be entered on the printer is the most secure.

NEW QUESTION 59
- (Exam Topic 4)
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

Answer: C

NEW QUESTION 62
- (Exam Topic 4)
An organization has an acceptable use policy in place, but users do not formally acknowledge the policy. Which of the following is the MOST significant risk from this finding?

A. Lack of data for measuring compliance
B. Violation of industry standards
C. Noncompliance with documentation requirements
D. Lack of user accountability

Answer: D

Explanation:
Without formal acknowledgement of the acceptable use policy, users may not be aware of the policies and procedures that are in place and may not understand the consequences of their actions. This could lead to violations of the policy and the associated risks, such as data breaches, security violations, and financial losses.

NEW QUESTION 63
- (Exam Topic 4)
A company requires that all program change requests (PCRs) be approved and all modifications be automatically logged. Which of the following IS audit procedures will BEST determine whether unauthorized changes have been made to production programs?

A. Trace a sample of complete PCR forms to the log of all program changes
B. Use source code comparison software to determine whether any changes have been made to a sample of programs since the last audit date
C. Review a sample of PCRs for proper approval throughout the program change process
D. Trace a sample of program change from the log to completed PCR forms

Answer: D

NEW QUESTION 64
- (Exam Topic 4)
Email required for business purposes is being stored on employees' personal devices. Which of the following is an IS auditor's BEST recommendation?

A. Require employees to utilize passwords on personal devices
B. Prohibit employees from storing company email on personal devices
C. Ensure antivirus protection is installed on personal devices
D. Implement an email containerization solution on personal devices

Answer: D

NEW QUESTION 69
- (Exam Topic 4)
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

Answer: B

NEW QUESTION 73

- (Exam Topic 4)
Which of the following is MOST important to include in security awareness training?

A. How to respond to various types of suspicious activity
B. The importance of complex passwords
C. Descriptions of the organization's security infrastructure
D. Contact information for the organization's security team

Answer: A

Explanation:
This is according to the ISACA's IS Auditing Guideline G15 on Security Awareness Training, which states that security awareness training should include "an understanding of the types of suspicious activity and the appropriate response to them".

NEW QUESTION 74
- (Exam Topic 4)
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 lest for version control
C. Lack of awareness training for EUC users
D. Lack of defined criteria for EUC applications

Answer: D

NEW QUESTION 78
- (Exam Topic 4)
In which of the following system development life cycle (SDLC) phases would an IS auditor expect to find that controls have been incorporated into system specifications?

A. Implementation
B. Development
C. Feasibility
D. Design

Answer: D

NEW QUESTION 80
- (Exam Topic 4)
A bank wants to outsource a system to a cloud provider residing in another country. Which of the following would be the MOST appropriate IS audit recommendation?

A. Find an alternative provider in the bank's home country.
B. Ensure the provider's internal control system meets bank requirements.
C. Proceed as intended, as the provider has to observe all laws of the clients countries.
D. Ensure the provider has disaster recovery capability.

Answer: B

Explanation:
The most appropriate IS audit recommendation for a bank that wants to outsource a system to a cloud provider residing in another country is to ensure the provider's internal control system meets bank requirements. This is because the cloud provider will be handling the bank's data, so it is important to ensure that the provider has appropriate controls in place to protect the data and to ensure its integrity. Additionally, the provider should have policies and procedures in place to ensure the security and privacy of the data, as well as to ensure compliance with applicable laws and regulations. For more information, please refer to the ISACA CISA Study Guide section 4.13.2.2.

NEW QUESTION 81
- (Exam Topic 4)
With regard to resilience, which of the following is the GREATEST risk to an organization that has implemented a new critical system?

A. A business impact analysis (BIA) has not been performed
B. Business data is not sanitized in the development environment
C. There is no plan for monitoring system downtime
D. The process owner has not signed off on user acceptance testing (UAT)

Answer: A

NEW QUESTION 85
- (Exam Topic 4)
Which of the following is the BEST source of information for examining the classification of new data?

A. Input by data custodians
B. Security policy requirements
C. Risk assessment results
D. Current level of protection

Answer: C

NEW QUESTION 86
- (Exam Topic 4)
An IS auditor learns a server administration team regularly applies workarounds to address repeated failures of critical data processing services Which of the following would BEST enable the organization to resolve this issue?

A. Problem management
B. Incident management
C. Service level management
D. Change management

Answer: B

NEW QUESTION 88
- (Exam Topic 4)
Which of following areas is MOST important for an IS auditor to focus on when reviewing the maturity model for a technology organization?

A. Standard operating procedures
B. Service level agreements (SLAs)
C. Roles and responsibility matrix
D. Business resiliency

Answer: C

Explanation:
The most important area for an IS auditor to focus on when reviewing the maturity model for a technology organization is the roles and responsibility matrix. This matrix should clearly document the roles and responsibilities of each stakeholder within the organization, as this will help to ensure that the correct processes and procedures are being followed and that the appropriate controls are in place. Additionally, the roles and responsibility matrix should be regularly reviewed and updated to ensure that it is up-to-date and accurate.

NEW QUESTION 92
- (Exam Topic 4)
Which of the following should be of GREATEST concern to an IS auditor performing a review of information security controls?

A. The information security policy has not been approved by the chief audit executive (CAE).
B. The information security policy does not include mobile device provisions
C. The information security policy is not frequently reviewed
D. The information security policy has not been approved by the policy owner

Answer: D

NEW QUESTION 93
- (Exam Topic 4)
Which of the following should be an IS auditor's GREATEST concern when a data owner assigns an incorrect classification level to data?

A. Controls to adequately safeguard the data may not be applied.
B. Data may not be encrypted by the system administrator.
C. Competitors may be able to view the data.
D. Control costs may exceed the intrinsic value of the IT asset.

Answer: A

Explanation:
According to the ISACA CISA Study Manual (2020), "incorrectly classifying information or not implementing adequate controls to protect the information is a major risk" (p. 328). Therefore, the IS auditor's greatest concern should be that controls to adequately safeguard the data may not be applied.

NEW QUESTION 97
- (Exam Topic 4)
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

Answer: D

NEW QUESTION 99
- (Exam Topic 4)
Which of the following provides the BEST evidence that a third-party service provider's information security controls are effective?

A. An audit report of the controls by the service provider's external auditor
B. Documentation of the service provider's security configuration controls
C. An interview with the service provider's information security officer
D. A review of the service provider's policies and procedures

Answer: A

NEW QUESTION 104
- (Exam Topic 4)
Which of the following technologies has the SMALLEST maximum range for data transmission between devices?

A. Wi-Fi
B. Bluetooth
C. Long-term evolution (LTE)
D. Near-field communication (NFC)

Answer: D

NEW QUESTION 105
- (Exam Topic 4)
Which of the following is MOST important for an IS auditor to verify when reviewing the use of an outsourcer for disposal of storage media?

A. The vendor's process appropriately sanitizes the media before disposal
B. The contract includes issuance of a certificate of destruction by the vendor
C. The vendor has not experienced security incidents in the past.
D. The disposal transportation vehicle is fully secure

Answer: A

NEW QUESTION 110
- (Exam Topic 4)
Which of the following is the PRIMARY role of key performance indicators (KPIs) in supporting business process effectiveness?

A. To enable conclusions about me performance of the processes and target variances tor follow-up analysis
B. To analyze workflows in order to optimize business processes and eliminate tasks that do not provide value
C. To assess the functionality of a software deliverable based on business processes

Answer: A

NEW QUESTION 111
- (Exam Topic 4)
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

Answer: B

NEW QUESTION 115
- (Exam Topic 4)
Which of the following is the MOST important factor when an organization is developing information security policies and procedures?

A. Consultation with security staff
B. Inclusion of mission and objectives
C. Compliance with relevant regulations
D. Alignment with an information security framework

Answer: C

NEW QUESTION 116
- (Exam Topic 4)
Which of the following provides the BEST audit evidence that a firewall is configured in compliance with the organization's security policy?

A. Analyzing how the configuration changes are performed
B. Analyzing log files
C. Reviewing the rule base
D. Performing penetration testing

Answer: C

NEW QUESTION 120
- (Exam Topic 4)
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

Answer: A

NEW QUESTION 125
- (Exam Topic 4)
Which of the following indicates that an internal audit organization is structured to support the independence and clarity of the reporting process?

A. Auditors are responsible for performing operational duties or activities.
B. The internal audit manager reports functionally to a senior management official.
C. The internal audit manager has a reporting line to the audit committee.
D. Auditors are responsible for assessing and operating a system of internal controls.

Answer: B

Explanation:
where the internal audit manager reports functionally to a senior management official, is in accordance with the International Professional Practices Framework (IPPF) from the Institute of Internal Auditors (IIA), which states that internal audit functions should have a direct reporting line to the governing body or a senior management official in order to ensure objectivity and independence. This ensures that the internal audit function can provide accurate and unbiased information to senior management and the governing body.
Reference:
Institute of Internal Auditors. (2019). International Professional Practices Framework (IPPF). Institute of Internal Auditors. (Standards 2000.A2 and 2100.A1)

NEW QUESTION 129
- (Exam Topic 4)
An IS auditor reviewing the throat assessment for a data cantor 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.

Answer: B

NEW QUESTION 131
- (Exam Topic 4)
What is the BEST way to reduce the risk of inaccurate or misleading data proliferating through business intelligence systems?

A. Establish rules for converting data from one format to another
B. Implement data entry controls for new and existing applications
C. Implement a consistent database indexing strategy
D. Develop a metadata repository to store and access metadata

Answer: A

NEW QUESTION 134
- (Exam Topic 4)
Which of the following is an IS auditor's BEST recommendation to protect an organization from attacks when its file server needs to be accessible to external users?

A. Enforce a secure tunnel connection.
B. Enhance internal firewalls.
C. Set up a demilitarized zone (DMZ).
D. Implement a secure protocol.

Answer: C

Explanation:
A demilitarized zone (DMZ) is an isolated network segment that is used to protect an organization's internal network from external threats. It is the best recommendation to protect an organization from attacks when its file server needs to be accessible to external users, as it creates a secure boundary between the internal and external networks. The DMZ is typically configured with a high-level of security, allowing only authorized traffic to pass through.

NEW QUESTION 139
- (Exam Topic 4)
Which of the following is MOST important for an IS auditor to validate when auditing network device management?

A. Devices cannot be accessed through service accounts.
B. Backup policies include device configuration files.
C. All devices have current security patches assessed.
D. All devices are located within a protected network segment.

Answer: C

Explanation:
The most important factor for an IS auditor to validate when auditing network device management is C - that all devices have current security patches assessed. This is because security patches are essential for ensuring that devices are protected from the latest threats, and that any vulnerabilities are addressed quickly. While it is important to ensure that devices cannot be accessed through service accounts, have backup policies that include device configuration files, and are located within a protected network segment, these measures do not ensure that devices are protected from the latest threats.

NEW QUESTION 140

- (Exam Topic 4)
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.

Answer: A

NEW QUESTION 142
- (Exam Topic 4)
An auditee disagrees with a recommendation for corrective action that appears in the draft engagement report. Which of the following is the IS auditor's BEST course of action when preparing the final report?

A. Come to an agreement prior to issuing the final report.
B. Include the position supported by senior management in the final engagement report
C. Ensure the auditee's comments are included in the working papers
D. Exclude the disputed recommendation from the final engagement report

Answer: B

NEW QUESTION 144
- (Exam Topic 4)
Which of the following is the GREATEST benefit of adopting an international IT governance framework rather than establishing a new framework based on the actual situation of a specific organization1?

A. Readily available resources such as domains and risk and control methodologies
B. Comprehensive coverage of fundamental and critical risk and control areas for IT governance
C. Fewer resources expended on trial-and-error attempts to fine-tune implementation methodologies
D. Wide acceptance by different business and support units with IT governance objectives

Answer: D

NEW QUESTION 149
- (Exam Topic 4)
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

Answer: D

NEW QUESTION 154
- (Exam Topic 4)
An organization's IT risk assessment should include the identification of:

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

Answer: A

NEW QUESTION 155
- (Exam Topic 4)
Which of the following should be identified FIRST during the risk assessment process?

A. Vulnerability to threats
B. Existing controls
C. Information assets
D. Legal requirements

Answer: C

Explanation:
Based on the information provided, the first step in the risk assessment process should be to identify C: Information assets. Information assets are the most important component of the risk assessment process, as they are the basis for assessing the potential risks to the organization. Identifying information assets allows the auditor to assess the value and criticality of the assets and determine the level of risk associated with them. Once the information assets have been identified, the auditor can then move on to assess the vulnerability of the assets to threats, evaluate existing controls, and consider any relevant legal requirements.

NEW QUESTION 158
- (Exam Topic 4)
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

Answer: C

NEW QUESTION 160
- (Exam Topic 4)
Recovery facilities providing a redundant combination of Internet connections to the local communications loop is an example of which type of telecommunications continuity?

A. Voice recovery
B. Alternative routing
C. Long-haul network diversity
D. Last-mile circuit protection

Answer: D

NEW QUESTION 165
- (Exam Topic 4)
Which of the following should be of GREATEST concern to an IS auditor assessing the effectiveness of an organization's vulnerability scanning program''

A. Steps taken to address identified vulnerabilities are not formally documented
B. Results are not reported to individuals with authority to ensure resolution
C. Scans are performed less frequently than required by the organization's vulnerability scanning schedule
D. Results are not approved by senior management

Answer: B

NEW QUESTION 170
- (Exam Topic 4)
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.

Answer: D

NEW QUESTION 172
- (Exam Topic 4)
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

Answer: B

NEW QUESTION 174
- (Exam Topic 4)
Which of the following is MOST important during software license audits?

A. Judgmental sampling
B. Substantive testing
C. Compliance testing
D. Stop-or-go sampling

Answer: C

Explanation:
Compliance testing is the most important during software license audits. This is because compliance testing verifies that the organization is adhering to software licensing rules and regulations, and that the organization is using the software legally. Compliance testing ensures that the organization is not in violation of any software licenses, and that all software licenses are up to date and valid.
During software license audits, it is important to assess the compliance of an organization with its software license agreements. This includes verifying the number of licenses purchased, the terms of the agreements, and the actual use of the software. Compliance testing is the process of evaluating the organization's compliance with its software license agreements to determine if it is using the software within the terms of the license agreement.
Reference:
ISACA. (2021). 2021 CISA Review Manual, 27th Edition. ISACA. (Chapter 6, Software Acquisition, Development, and Maintenance)

NEW QUESTION 175
- (Exam Topic 4)

Which of the following is the PRIMARY purpose of obtaining a baseline image during an operating system audit?

A. To identify atypical running processes
B. To verify antivirus definitions
C. To identify local administrator account access
D. To verify the integrity of operating system backups

Answer: D

Explanation:
The primary purpose of obtaining a baseline image during an operating system audit is to verify the integrity of operating system backups. A baseline image provides a consistent and reliable reference for auditing and allows the auditor to determine if any changes have been made to the operating system since the baseline image was taken. This helps the auditor to detect any unauthorized changes that may have been made and to assess the impact of any changes on the system's security posture.

NEW QUESTION 176
- (Exam Topic 4)
Which of the following is MOST useful to an IS auditor performing a review of access controls for a document management system?

A. Policies and procedures for managing documents provided by department heads
B. A system-generated list of staff and their project assignment
C. roles, and responsibilities
D. Previous audit reports related to other departments' use of the same system
E. Information provided by the audit team lead an the authentication systems used by the department

Answer: B

Explanation:
A system-generated list of staff and their project assignments, roles, and responsibilities is the most useful to an IS auditor performing a review of access controls for a document management system (DMS). A DMS is a system used to create, store, manage, and track electronic documents and images of paper-based documents through software1. Access controls are the mechanisms that regulate who can access, modify, or delete documents in a DMS, and under what conditions2. A system-generated list of staff and their project assignments, roles, and responsibilities helps the IS auditor to verify the appropriateness, accuracy, and completeness of the access rights granted to different users or groups of users in the DMS, based on the principle of least privilege and the segregation of duties23.
Policies and procedures for managing documents provided by department heads (A) are not the most useful to an IS auditor performing a review of access controls for a DMS. Policies and procedures are the documents that define the rules, standards, and guidelines for managing documents in a DMS, such as the document lifecycle, retention, classification, security, etc1. Policies and procedures are important to establish the expectations and requirements for document management, but they do not provide sufficient evidence or assurance of the actual implementation and effectiveness of the access controls in the DMS.
Previous audit reports related to other departments' use of the same system © are not the most useful to an IS auditor performing a review of access controls for a DMS. Previous audit reports are the documents that summarize the findings, conclusions, and recommendations of previous audits conducted on the same or similar systems or processes4. Previous audit reports are useful to identify the common or recurring issues, risks, or gaps in the access controls of the DMS, as well as the best practices or lessons learned from other departments. However, previous audit reports do not reflect the current state or performance of the access controls in the DMS, and they may not be relevant or applicable to the specific department or scope of the current audit.
Information provided by the audit team lead on the authentication systems used by the department (D) are not the most useful to an IS auditor performing a review of access controls for a DMS. Authentication systems are the systems that verify the identity and credentials of the users who attempt to access the DMS, such as passwords, tokens, biometrics, etc2. Authentication systems are important to ensure the integrity and accountability of the users who access the DMS, but they do not provide sufficient information or assurance of the authorization and restriction of the users who access the DMS. Authorization and restriction are the aspects of access control that determine what actions or operations the users can perform on the documents in the DMS, such as read, write, edit, delete, etc2.

NEW QUESTION 180
- (Exam Topic 3)
What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

A. The contract does not contain a right-to-audit clause.
B. An operational level agreement (OLA) was not negotiated.
C. Several vendor deliverables missed the commitment date.
D. Software escrow was not negotiated.

Answer: D

NEW QUESTION 185
- (Exam Topic 3)
During an exit meeting, an IS auditor highlights that backup cycles are being missed due to operator error and that these exceptions are not being managed. Which of the following is the BEST way to help management understand the associated risk?

A. Explain the impact to disaster recovery.
B. Explain the impact to resource requirements.
C. Explain the impact to incident management.
D. Explain the impact to backup scheduling.

Answer: A

NEW QUESTION 186
- (Exam Topic 3)
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.

Answer: B

NEW QUESTION 190
- (Exam Topic 3)
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.

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 197
- (Exam Topic 3)
Which of the following should an IS auditor ensure is classified at the HIGHEST level of sensitivity?

A. Server room access history
B. Emergency change records
C. IT security incidents
D. Penetration test results

Answer: D

NEW QUESTION 199
- (Exam Topic 3)
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 lo 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.

Answer: B

NEW QUESTION 203
- (Exam Topic 3)
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.

Answer: C

NEW QUESTION 208
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 209
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 212
- (Exam Topic 3)
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 confidentialdata.
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.

Answer: B

NEW QUESTION 214
- (Exam Topic 3)
An IS auditor finds that capacity management for a key system is being performed by IT with no input from the business The auditor's PRIMARY concern would be:

A. failure to maximize the use of equipment
B. unanticipated increase in business s capacity needs.
C. cost of excessive data center storage capacity
D. impact to future business project funding.

Answer: B

NEW QUESTION 215
- (Exam Topic 3)
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.

Answer: D

NEW QUESTION 217
- (Exam Topic 3)
Which of the following should be the IS auditor's PRIMARY focus, when evaluating an organization's offsite storage facility?

A. Shared facilities
B. Adequacy of physical and environmental controls
C. Results of business continuity plan (BCP) test
D. Retention policy and period

Answer: B

NEW QUESTION 220
- (Exam Topic 3)
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.

Answer: D

NEW QUESTION 224
- (Exam Topic 3)
What should an IS auditor do FIRST when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective?

A. Determine the resources required to make the control effective.
B. Validate the overall effectiveness of the internal control.
C. Verify the impact of the control no longer being effective.
D. Ascertain the existence of other compensating controls.

Answer: D

NEW QUESTION 225
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 228
- (Exam Topic 3)
An organization is disposing of a system containing sensitive data and has deleted all files from the hard disk. An IS auditor should be concerned because:

A. deleted data cannot easily be retrieved.
B. deleting the files logically does not overwrite the files' physical data.
C. backup copies of files were not deleted as well.
D. deleting all files separately is not as efficient as formatting the hard disk.

Answer: B

NEW QUESTION 231
- (Exam Topic 3)
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 seventy 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

Answer: B

NEW QUESTION 234
- (Exam Topic 3)
During an IT general controls audit of a high-risk area where both internal and external audit teams are reviewing the same approach to optimize resources?

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

Answer: B

NEW QUESTION 236
- (Exam Topic 3)
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 identity as the associated risk?

A. The use of the cloud negatively impacting IT availably
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

Answer: C

NEW QUESTION 238
- (Exam Topic 3)
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 lo 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

Answer: A

NEW QUESTION 239
- (Exam Topic 3)
Which of the following presents the GREATEST challenge to the alignment of business and IT?

A. Lack of chief information officer (CIO) involvement in board meetings
B. Insufficient IT budget to execute new business projects

C. Lack of information security involvement in business strategy development
D. An IT steering committee chaired by the chief information officer (CIO)

Answer: C

NEW QUESTION 243
- (Exam Topic 3)
An IS auditor has completed the fieldwork phase of a network security review and is preparing the initial following findings should be ranked as the HIGHEST risk?

A. Network penetration tests are not performed
B. The network firewall policy has not been approved by the information security officer.
C. Network firewall rules have not been documented.
D. The network device inventory is incomplete.

Answer: A

NEW QUESTION 248
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 250
- (Exam Topic 3)
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.

Answer: A

NEW QUESTION 253
- (Exam Topic 3)
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 1o production

Answer: B

NEW QUESTION 255
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 260
- (Exam Topic 3)
Which of the following is MOST critical for the effective implementation of IT governance?

A. Strong risk management practices
B. Internal auditor commitment
C. Supportive corporate culture
D. Documented policies

Answer: C

NEW QUESTION 265
- (Exam Topic 3)

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.

Answer: C

NEW QUESTION 268
- (Exam Topic 2)
An IS auditor finds that an organization's data loss prevention (DLP) system is configured to use vendor default settings to identify violations. The auditor's MAIN concern should be that:

A. violation reports may not be reviewed in a timely manner.
B. a significant number of false positive violations may be reported.
C. violations may not be categorized according to the organization's risk profile.
D. violation reports may not be retained according to the organization's risk profile.

Answer: C

NEW QUESTION 272
- (Exam Topic 2)
An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?

A. Data with customer personal information
B. Data reported to the regulatory body
C. Data supporting financial statements
D. Data impacting business objectives

Answer: A

NEW QUESTION 274
- (Exam Topic 2)
An IS auditor concludes that an organization has a quality security policy. Which of the following is MOST important to determine next? The policy must be:

A. well understand by all employees.
B. based on industry standards.
C. developed by process owners.
D. updated frequently.

Answer: A

NEW QUESTION 279
- (Exam Topic 2)
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.

Answer: C

NEW QUESTION 280
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 283
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 285
- (Exam Topic 2)
IT disaster recovery time objectives (RTOs) should be based on the:

A. maximum tolerable loss of data.
B. nature of the outage
C. maximum tolerable downtime (MTD).
D. business-defined criticality of the systems.

Answer: D

NEW QUESTION 289
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of an organization's incident response program?

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

Answer: C

NEW QUESTION 293
- (Exam Topic 2)
Which of the following is a detective control?

A. Programmed edit checks for data entry
B. Backup procedures
C. Use of pass cards to gain access to physical facilities
D. Verification of hash totals

Answer: D

NEW QUESTION 296
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 300
- (Exam Topic 2)
Which of the following would BEST help lo support an auditors 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

Answer: D

NEW QUESTION 301
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 304
- (Exam Topic 2)
A now 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.

Answer: C

NEW QUESTION 307
- (Exam Topic 2)
In order to be useful, a key performance indicator (KPI) MUST

A. be approved by management.
B. be measurable in percentages.
C. be changed frequently to reflect organizational strategy.
D. have a target value.

Answer: C

NEW QUESTION 312
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 316
- (Exam Topic 2)
Which of the following is MOST important for an IS auditor to consider when performing the risk assessment poor 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

Answer: A

NEW QUESTION 317
- (Exam Topic 2)
An IS auditor is analyzing a sample of accesses recorded on the system log of an application. The auditor intends to launch an intensive investigation if one exception is found Which sampling method would be appropriate?

A. Discovery sampling
B. Judgmental sampling
C. Variable sampling
D. Stratified sampling

Answer: A

NEW QUESTION 320
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 322
- (Exam Topic 2)
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.

Answer: A

NEW QUESTION 323
- (Exam Topic 2)
What is the Most critical finding when reviewing an organization's information security management?

A. No dedicated security officer
B. No official charier for the information security management system
C. No periodic assessments to identify threats and vulnerabilities
D. No employee awareness training and education program

Answer: D

NEW QUESTION 326
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 328
- (Exam Topic 2)
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.

Answer: D

NEW QUESTION 332
- (Exam Topic 2)
Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?

A. Ensure that the facts presented in the report are correct
B. Communicate the recommendations lo senior management
C. Specify implementation dates for the recommendations.
D. Request input in determining corrective action.

Answer: A

NEW QUESTION 333
- (Exam Topic 2)
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. Purchase data cleansing tools from a reputable vendor.
C. Appoint data quality champions across the organization.
D. Implement business rules to reject invalid data.

Answer: D

NEW QUESTION 338
- (Exam Topic 2)
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.

Answer: C

NEW QUESTION 340
- (Exam Topic 2)
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.

Answer:

D

NEW QUESTION 344
- (Exam Topic 1)
Which of the following MOST effectively minimizes downtime during system conversions?

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

Answer: D

NEW QUESTION 347
- (Exam Topic 1)
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.

Answer: D

NEW QUESTION 351
- (Exam Topic 1)
During the implementation of an upgraded enterprise resource planning (ERP) system, which of the following is the MOST important consideration for a go-live decision?

A. Rollback strategy
B. Test cases
C. Post-implementation review objectives
D. Business case

Answer: D

NEW QUESTION 354
- (Exam Topic 1)
The PRIMARY benefit lo 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.

Answer: C

NEW QUESTION 356
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 359
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 360
- (Exam Topic 1)
What is the BEST control to address SQL injection vulnerabilities?

A. Unicode translation
B. Secure Sockets Layer (SSL) encryption

C. Input validation
D. Digital signatures

Answer: C

NEW QUESTION 365
- (Exam Topic 1)
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.

Answer: D

NEW QUESTION 368
- (Exam Topic 1)
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.

Answer: A

NEW QUESTION 370
- (Exam Topic 1)
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 v
C. industry benchmarks
D. Total number of hours budgeted to security
E. Total number of false positives

Answer: A

NEW QUESTION 372
- (Exam Topic 1)
Which of the following should be GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

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

Answer: C

NEW QUESTION 373
- (Exam Topic 1)
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.

Answer: B

NEW QUESTION 374
- (Exam Topic 1)
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.

Answer: D

NEW QUESTION 375

- (Exam Topic 1)
An organization has recently acquired and implemented intelligent-agent software for granting loans to customers. During the post-implementation review, which of the following is the MOST important procedure for the IS auditor to perform?

A. Review system and error logs to verify transaction accuracy.
B. Review input and output control reports to verify the accuracy of the system decisions.
C. Review signed approvals to ensure responsibilities for decisions of the system are well defined.
D. Review system documentation to ensure completeness.

Answer: B

NEW QUESTION 378
- (Exam Topic 1)
Which of the following should be done FIRST when planning a penetration test?

A. Execute nondisclosure agreements (NDAs).
B. Determine reporting requirements for vulnerabilities.
C. Define the testing scope.
D. Obtain management consent for the testing.

Answer: D

NEW QUESTION 383
- (Exam Topic 1)
To confirm integrity for a hashed message, the receiver should use:

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

Answer: A

NEW QUESTION 385
- (Exam Topic 1)
Which audit approach is MOST helpful in optimizing the use of IS audit resources?

A. Agile auditing
B. Continuous auditing
C. Outsourced auditing
D. Risk-based auditing

Answer: D

NEW QUESTION 388
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 390
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 392
- (Exam Topic 1)
When evaluating the design of controls related to network monitoring, which of the following is MOST important for an IS auditor to review?

A. Incident monitoring togs
B. The ISP service level agreement
C. Reports of network traffic analysis
D. Network topology diagrams

Answer: D

NEW QUESTION 393
- (Exam Topic 1)
Which of the following would BEST facilitate the successful implementation of an IT-related framework?

A. Aligning the framework to industry best practices
B. Establishing committees to support and oversee framework activities
C. Involving appropriate business representation within the framework
D. Documenting IT-related policies and procedures

Answer: C

NEW QUESTION 398
- (Exam Topic 1)
Which of the following is the BEST detective control for a job scheduling process involving data transmission?

A. Metrics denoting the volume of monthly job failures are reported and reviewed by senior management.
B. Jobs are scheduled to be completed daily and data is transmitted using a Secure File Transfer Protocol (SFTP).
C. Jobs are scheduled and a log of this activity is retained for subsequent review.
D. Job failure alerts are automatically generated and routed to support personnel.

Answer: D

NEW QUESTION 403
- (Exam Topic 1)
Which of the following should an IS auditor recommend as a PRIMARY area of focus when an organization decides to outsource technical support for its external customers?

A. Align service level agreements (SLAs) with current needs.
B. Monitor customer satisfaction with the change.
C. Minimize costs related to the third-party agreement.
D. Ensure right to audit is included within the contract.

Answer: A

NEW QUESTION 406
- (Exam Topic 1)
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.

Answer: B

NEW QUESTION 408
- (Exam Topic 1)
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.

Answer: D

NEW QUESTION 410
- (Exam Topic 1)
Which of the following would BEST demonstrate that an effective disaster recovery plan (DRP) is in place?

A. Frequent testing of backups
B. Annual walk-through testing
C. Periodic risk assessment
D. Full operational test

Answer: D

NEW QUESTION 412
- (Exam Topic 1)
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.

Answer: B

NEW QUESTION 413
- (Exam Topic 1)
Which of the following BEST ensures the quality and integrity of test procedures used in audit analytics?

A. Developing and communicating test procedure best practices to audit teams
B. Developing and implementing an audit data repository
C. Decentralizing procedures and Implementing periodic peer review
D. Centralizing procedures and implementing change control

Answer: D

NEW QUESTION 414
- (Exam Topic 1)
An online retailer is receiving customer complaints about receiving different items from what they ordered on the organization's website. The root cause has been traced to poor data quality. Despite efforts to clean erroneous data from the system, multiple data quality issues continue to occur. Which of the following recommendations would be the BEST way to reduce the likelihood of future occurrences?

A. Assign responsibility for improving data quality.
B. Invest in additional employee training for data entry.
C. Outsource data cleansing activities to reliable third parties.
D. Implement business rules to validate employee data entry.

Answer: D

NEW QUESTION 418
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 419
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 423
- (Exam Topic 1)
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.

Answer: A

NEW QUESTION 426
- (Exam Topic 1)
Coding standards provide which of the following?

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

Answer: D

NEW QUESTION 429
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 433
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 434
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 437
- (Exam Topic 1)
Due to limited storage capacity, an organization has decided to reduce the actual retention period for media containing completed low-value transactions. Which of the following is MOST important for the organization to ensure?

A. The policy includes a strong risk-based approach.
B. The retention period allows for review during the year-end audit.
C. The total transaction amount has no impact on financial reporting.
D. The retention period complies with data owner responsibilities.

Answer: D

NEW QUESTION 439
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 443
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISA Product From:

https://www.2passeasy.com/dumps/CISA/

Money Back Guarantee

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

* CISA Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year