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)
An IS auditor is reviewing the service agreement with a technology company that provides IT help desk services to the organization. Which of the following monthly performance metrics is the BEST indicator of service quality?

A. The total number of users requesting help desk services
B. The average call waiting time on each request
C. The percent of issues resolved by the first contact
D. The average turnaround time spent on each reported issue

Answer: C

NEW QUESTION 3
- (Exam Topic 4)
A vendor requires privileged access to a key business application. Which of the following is the BEST recommendation to reduce the risk of data leakage?

A. Implement real-time activity monitoring for privileged roles
B. Include the right-to-audit in the vendor contract
C. Perform a review of privileged roles and responsibilities
D. Require the vendor to implement job rotation for privileged roles

Answer: A

NEW QUESTION 4
- (Exam Topic 4)
An IS auditor finds a segregation of duties issue in an enterprise resource planning (ERP) system. Which of the following is the BEST way to prevent the misconfiguration from recurring?

A. Monitoring access rights on a regular basis
B. Referencing a standard user-access matrix
C. Granting user access using a role-based model
D. Correcting the segregation of duties conflicts

Answer: C

Explanation:
An effective way to prevent segregation of duties issues in an enterprise resource planning (ERP) system is to grant user access using a role-based model. This means that access to systems and applications is based on the role or job function of the user. This helps to enforce appropriate segregation of duties, so that critical tasks are not performed by the same individual, reducing the risk of fraud or other security breaches. A role-based model allows for the efficient and effective management of user access rights, helping to ensure that the system is properly configured and secured.
Reference:
ISACA. (2021). 2021 CISA Review Manual, 27th Edition. ISACA. (Chapter 7, Security Administration)

NEW QUESTION 5
- (Exam Topic 4)
Which of the following risk scenarios is BEST addressed by implementing policies and procedures related to full disk encryption?

A. Data leakage as a result of employees leaving to work for competitors
B. Noncompliance fines related to storage of regulated information
C. Unauthorized logical access to information through an application interface
D. Physical theft of media on which information is stored

Answer: D

NEW QUESTION 6
- (Exam Topic 4)
An IS auditor is reviewing the security of a web-based customer relationship management (CRM) system that is directly accessed by customers via the Internet, Which of the following should be a concern for the auditor?

A. The system is hosted on an external third-party service provider's servers.
B. The system is hosted in a hybrid-cloud platform managed by a service provider.
C. The system is hosted within a demilitarized zone (DMZ) of a corporate network.
D. The system is hosted within an internal segment of a corporate network.

Answer: D

Explanation:
A web-based CRM system that is directly accessed by customers via the Internet should be hosted in a secure and isolated environment to protect it from external threats and unauthorized access. A web-based CRM system should also be reliable, trusted, and backed up regularly1.
Hosting the system on an external third-party service provider's servers (A) or a hybrid-cloud platform managed by a service provider (B) may not be a concern for the auditor if the service provider has adequate security measures and service level agreements in place. The auditor should verify the security controls and contractual terms of the service provider before trusting them with the CRM data23.
Hosting the system within a demilitarized zone (DMZ) of a corporate network © is a common practice to provide an extra layer of security to the CRM system from untrusted networks, such as the Internet. A DMZ is a perimeter network that isolates the CRM system from the internal network and filters the incoming traffic from the external network using a security gateway4567.
Hosting the system within an internal segment of a corporate network (D) is a concern for the auditor because it exposes the CRM system and the internal network to potential attacks from the Internet. The CRM system should not be directly accessible from the Internet without a DMZ or a firewall to protect it. This could compromise the confidentiality, integrity, and availability of the CRM data and the internal network78.

NEW QUESTION 7
- (Exam Topic 4)
To mitigate the risk of exposing data through application programming interface (API) queries. which of the following design considerations is MOST important?

A. Data retention
B. Data minimization
C. Data quality
D. Data integrity

Answer: B

Explanation:
Data minimization is an important design consideration when mitigating the risk of exposing data through API queries. This involves limiting the amount of data returned from an API query to only the data that is required for the task at hand. This reduces the risk of exposing sensitive or confidential data, as well as reducing the risk of data overload. Additionally, data minimization helps to ensure that the API query is not overly complex, which can lead to performance issues.

NEW QUESTION 8
- (Exam Topic 4)
An organization has engaged a third party to implement an application to perform business-critical calculations. Which of the following is the MOST important process to help ensure the application provides accurate calculations?

A. Key performance indicator (KPI) monitoring
B. Change management
C. Configuration management
D. Quality assurance (QA)

Answer: A

NEW QUESTION 9
- (Exam Topic 4)
Which of the following is an IS auditor's BEST approach when prepanng to evaluate whether the IT strategy supports the organization's vision and mission?

A. Review strategic projects tor return on investments (ROls)
B. Solicit feedback from other departments to gauge the organization's maturity
C. Meet with senior management to understand business goals
D. Review the organization's key performance indicators (KPls)

Answer: C

Explanation:
The best approach for an IS auditor when preparing to evaluate whether the IT strategy supports the Organization's vision and mission is C. Meet with senior management to understand business goals. According to the ISACA Certified Information Systems Auditor (CISA) Study Guide [1], IS auditors should meet with senior management to understand the organization's vision and mission, and the related business goals, objectives and strategies. This will help the auditor to assess whether the proposed IT strategy is aligned with the organization's overall objectives, and whether the information systems are providing the expected returns. Additionally, the IS auditor should understand the organization's risk appetite and risk management approach, as these will affect the design and implementation of the IT strategy.

NEW QUESTION 10
- (Exam Topic 4)
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 slated 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.

Answer: C

NEW QUESTION 10
- (Exam Topic 4)
Which of the following is the PRIMARY advantage of using virtualization technology for corporate applications?

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

Answer: B

NEW QUESTION 13
- (Exam Topic 4)
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.

Answer: D

NEW QUESTION 18
- (Exam Topic 4)
Which of the following should be restricted from a network administrator's privileges in an adequately segregated IT environment?

A. Monitoring network traffic
B. Changing existing configurations for applications
C. Hardening network ports
D. Ensuring transmission protocols are functioning correctly

Answer: B

Explanation:
The network administrator should not have the privilege of changing existing configurations for applications in an adequately segregated IT environment. This is because changes to existing configurations can introduce vulnerabilities and cause unexpected behavior, which can lead to disruption of services or data loss. The network administrator should not have the ability to make such changes without the explicit authorization of the IT manager. Additionally, the network administrator should be monitored to ensure that any changes they make are in compliance with the organization's security policies and procedures. CISA Certification - Information Systems Auditor official site or book provides a comprehensive guide to best practices and security principles for the IT environment, which includes recommendations on how to restrict access to sensitive configuration changes.

NEW QUESTION 19
- (Exam Topic 4)
An organization implemented a cybersecurity policy last year Which of the following is the GREATE ST indicator that the policy may need to be revised"7 :

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

Answer: C

NEW QUESTION 20
- (Exam Topic 4)
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

Answer: B

NEW QUESTION 24
- (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 26
- (Exam Topic 4)
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 m 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

Answer: C

NEW QUESTION 27
- (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 31
- (Exam Topic 4)
When auditing the feasibility study of a system development project, the IS auditor should:

A. review qualifications of key members of the project team.
B. review the request for proposal (RFP) to ensure that it covers the scope of work.
C. review cost-benefit documentation for reasonableness.
D. ensure that vendor contracts are reviewed by legal counsel.

Answer: C

Explanation:
When auditing the feasibility study of a system development project, the IS auditor should review cost-benefit documentation for reasonableness. The feasibility study should include an assessment of the costs and benefits of the proposed system and a determination of whether the benefits of the project justify its costs. The IS auditor should review the cost-benefit analysis to ensure that it is reasonable and accurately reflects the costs and benefits of the proposed system.
Reference:
ISACA. (2021). 2021 CISA Review Manual, 27th Edition. ISACA. (Chapter 8, Systems Development, Acquisition, and Implementation)

NEW QUESTION 36
- (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 41
- (Exam Topic 4)
Which of the following should be done FIRST to minimize the risk of unstructured data?

A. Identify repositories of unstructured data.
B. Purchase tools to analyze unstructured data.
C. Implement strong encryption for unstructured data.
D. Implement user access controls to unstructured data.

Answer: A

Explanation:
Based on the information provided, the first step to minimize the risk of unstructured data should be to A: Identify repositories of unstructured data. Unstructured data can present a significant security risk if not managed properly, so it is important to identify where it is stored and who has access to it. Once the repositories of unstructured data have been identified, additional steps can be taken to protect it, such as implementing strong encryption and user access controls, and purchasing tools to analyze it.

NEW QUESTION 45
- (Exam Topic 4)
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

Answer: D

NEW QUESTION 48
- (Exam Topic 4)
An organization is planning to implement a work-from-home policy that allows users to work remotely as needed. Which of the following is the BEST solution for ensuring secure remote access to corporate resources?

A. Additional firewall rules
B. Multi-factor authentication
C. Virtual private network (VPN)
D. Virtual desktop

Answer: C

NEW QUESTION 51
- (Exam Topic 4)
Which of the following BEST protects evidence in a forensic investigation?

A. imaging the affected system
B. Powering down the affected system
C. Protecting the hardware of the affected system
D. Rebooting the affected system

Answer: A

Explanation:
This creates a duplicate copy of the data that can be used for examination, while preserving the original evidence in its original state. This helps to ensure that the data is not altered or corrupted during the examination process and the integrity of the evidence is maintained.

NEW QUESTION 54
- (Exam Topic 4)
The BEST way to prevent fraudulent payments is to implement segregation of duties between the vendor setup and:

A. payment processing.
B. payroll processing.
C. procurement.
D. product registration.

Answer: A

Explanation:
The best way to prevent fraudulent payments is to implement segregation of duties between the vendor setup and payment processing. Segregation of duties is an important control measure used to mitigate the risks associated with fraud and errors. By separating the processes of vendor setup and payment processing, it ensures that no single individual has control over both activities, and thereby reduces the risk of fraudulent payments. Additionally, other measures such as dual authorization and automated controls can be used to further reduce the risk.

NEW QUESTION 56
- (Exam Topic 4)
Which of the following should be of GREATEST concern to an IS auditor conducting an audit of an organization that recently experienced a ransomware attack?

A. Antivirus software was unable to prevent the attack even though it was properly updated
B. The most recent security patches were not tested prior to implementation
C. Backups were only performed within the local network
D. Employees were not trained on cybersecurity policies and procedures

Answer: C

NEW QUESTION 61
- (Exam Topic 4)
Which of the following is MOST important for an IS auditor to verify when evaluating an organization's data conversion and infrastructure migration plan?

A. Strategic: goals have been considered.
B. A rollback plan is included.
C. A code check review is included.
D. A migration steering committee has been formed.

Answer: B

NEW QUESTION 65
- (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 66
- (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 67
- (Exam Topic 4)
An IS department is evaluated monthly on its cost-revenue ratio user satisfaction rate, and computer downtime This is BEST zed as an application of.

A. risk framework
B. balanced scorecard
C. value chain analysis
D. control self-assessment (CSA)

Answer: B

NEW QUESTION 70
- (Exam Topic 4)
in a post-implantation Nation review of a recently purchased system it is MOST important for the iS auditor to determine whether the:

A. stakeholder expectations were identified
B. vendor product offered a viable solution.
C. user requirements were met.
D. test scenarios reflected operating activities.

Answer: C

NEW QUESTION 73
- (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 74
- (Exam Topic 4)
An organization that operates an e-commerce website wants to provide continuous service to its customers and is planning to invest in a hot site due to service criticality. Which of the following is the MOST important consideration when making this decision?

A. Maximum tolerable downtime (MTD)
B. Recovery time objective (RTO)
C. Recovery point objective (RPO)
D. Mean time to repair (MTTR)

Answer: A

Explanation:
The most important consideration when making a decision to invest in a hot site is the Maximum Tolerable Downtime (MTD). This is the maximum amount of time a system can be down before it affects the organization's operations or customer service. Other considerations, such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), are also important, but MTD is the most important factor when considering investing in a hot site.

NEW QUESTION 79

- (Exam Topic 4)
An IS auditor is reviewing a bank's service level agreement (SLA) with a third-party provider that hosts the bank's secondary data center, which of the following findings should be of GREATEST concern to the auditor?

A. The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan (ORP).
B. The SLA has not been reviewed in more than a year.
C. Backup data is hosted online only.
D. The recovery point objective (RPO) has a shorter duration than documented in the disaster recovery plan (DRP).

Answer: D

Explanation:
The recovery point objective (RPO) is the maximum amount of data that can be lost due to a system failure or disaster. If the SLA specifies a shorter RPO than the DRP, this could indicate a lack of adequate backup systems or procedures to ensure data integrity, which is of great concern to an IS auditor. Additionally, the IS auditor should also be sure to check that the SLA is up to date and that the RTO and RPO align with the DRP.

NEW QUESTION 82
- (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 85
- (Exam Topic 4)
An IS auditor is reviewing an organization's business continuity plan (BCP) following a change in organizational structure with significant impact to business processes. Which of the following findings should be the auditor's GREATEST concern?

A. Key business process end users did not participate in the business impact " analysis (BIA)
B. Copies of the BCP have not been distributed to new business unit end users sjnce the reorganization
C. A test plan for the BCP has not been completed during the last two years

Answer: C

NEW QUESTION 90
- (Exam Topic 4)
Which of the following is the MOST appropriate control to ensure integrity of online orders?

A. Data Encryption Standard (DES)
B. Digital signature
C. Public key encryption
D. Multi-factor authentication

Answer: C

NEW QUESTION 94
- (Exam Topic 4)
An IS auditor is evaluating the progress of a web-based customer service application development project. Which of the following would be MOST helpful for this evaluation?

A. Backlog consumption reports
B. Critical path analysis reports
C. Developer status reports
D. Change management logs

Answer: A

NEW QUESTION 98
- (Exam Topic 4)
Users are complaining that a newly released enterprise resource planning (ERP) system is functioning too slowly. Which of the following tests during the quality assurance (QA) phase would have identified this concern?

A. Stress
B. Regression
C. Interface
D. Integration

Answer: A

Explanation:
Stress testing is a type of QA testing that is designed to evaluate how a system responds to high load. This type of testing would have identified any performance issues with the ERP system, such as slow response times, before it was released. Other types of testing that may have identified this issue are load testing, performance testing, and volume testing.

NEW QUESTION 100
- (Exam Topic 4)
As part of business continuity planning, which of the following is MOST important to assess when conducting a business impact analysis (B1A)?

A. Risk appetite
B. Critical applications m the cloud
C. Completeness of critical asset inventory
D. Recovery scenarios

Answer: C

NEW QUESTION 105
- (Exam Topic 4)
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 off ne backups using software utilities
D. Reviewing and updating data restoration policies annually

Answer: B

NEW QUESTION 109
- (Exam Topic 4)
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

Answer: D

NEW QUESTION 112
- (Exam Topic 4)
An IS auditor is performing a follow-up audit for findings identified in an organization's user provisioning process
Which of the following is the MOST appropriate population to sample from when testing for remediation?

A. All users provisioned after the finding was originally identified
B. All users provisioned after management resolved the audit issue
C. All users provisioned after the final audit report was issued
D. All users who have followed user provisioning processes provided by management

Answer: C

NEW QUESTION 113
- (Exam Topic 4)
The BEST way to evaluate the effectiveness of a newly developed application is to:

A. perform a post-implementation review
B. analyze load testing results.
C. perform a secure code review.
D. review acceptance testing results.

Answer: D

Explanation:
Acceptance testing is the process of ensuring that a developed application meets the specified requirements and is fit for purpose. This type of testing is usually performed by the customer or users of the application, and is often used to determine if the application is ready for production. Reviewing the results of the acceptance testing is the best way to evaluate the effectiveness of a newly developed application.

NEW QUESTION 115
- (Exam Topic 4)
A senior auditor is reviewing work papers prepared by a junior auditor indicating that a finding was removed after the auditee said they corrected the problem.
Which of the following is the senior auditor s MOST appropriate course of action?

A. Ask the auditee to retest
B. Approve the work papers as written
C. Have the finding reinstated
D. Refer the issue to the audit director

Answer: A

NEW QUESTION 118
- (Exam Topic 4)
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.

Answer: A

NEW QUESTION 120
- (Exam Topic 4)
During which phase of the software development life cycle is it BEST to initiate the discussion of application controls?

A. Business case development phase when stakeholders are identified
B. Application design phase process functionalities are finalized
C. User acceptance testing (UAT) phase when test scenarios are designed
D. Application coding phase when algorithms are developed to solve business problems

Answer: B

Explanation:
The best time to initiate the discussion of application controls is during the Application Design phase, when the process functionalities are finalized. This is according to the ISACA CISA Study Manual, which states, "Application controls should be discussed during the design phase and implemented in the development of the system." (ISACA CISA Study Manual, 26th Edition, Section 4.2.2, Page 4.27)

NEW QUESTION 121
- (Exam Topic 4)
A checksum is classified as which type of control?

A. Detective control
B. Preventive control
C. Corrective control
D. Administrative control

Answer: A

NEW QUESTION 125
- (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 130
- (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 135
- (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 140
- (Exam Topic 4)
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

Answer: B

NEW QUESTION 145
- (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 146
- (Exam Topic 4)
Which of the following is the BEST way to help ensure new IT implementations align with enterprise architecture (EA) principles and requirements?

A. Document the security view as part of the EA
B. Consider stakeholder concerns when defining the EA
C. Perform mandatory post-implementation reviews of IT implementations
D. Conduct EA reviews as part of the change advisory board

Answer: B

NEW QUESTION 151
- (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 153
- (Exam Topic 4)
As part of the architecture of virtualized environments, in a bare metal or native visualization the hypervisor runs without:

A. a host operating system.
B. a guest operating system.
C. any applications on the guest operating system.
D. any applications on the host operating system.

Answer: D

Explanation:
This allows the hypervisor to take full control of the hardware and provide direct access to the underlying hardware, which allows for efficient use of resources and more direct control over the virtual environment. The CISA Study Manual recommends that organizations use best practices when setting up virtualized environments to ensure that the underlying hardware and software are configured correctly and securely.

NEW QUESTION 156
- (Exam Topic 4)
During a follow-up audit, an IS auditor finds that senior management has implemented a different remediation action plan than what was previously agreed upon. Which of the following is the auditor's BEST course of action?

A. Report the deviation by the control owner in the audit report.
B. Evaluate the implemented control to ensure it mitigates the risk to an acceptable level.
C. Cancel the follow-up audit and reschedule for the next audit period.
D. Request justification from management for not implementing the recommended control.

Answer: D

Explanation:

The auditor should understand the reason for the deviation and evaluate if the new control mitigates the risk to an acceptable level. If necessary, the auditor can report the deviation in the audit report and provide recommendations for improving the process in the future.

NEW QUESTION 158
- (Exam Topic 4)
Which of the following is the MOST efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care?

A. Infrastructure as a Service (laaS) provider
B. Software as a Service (SaaS) provider
C. Network segmentation
D. Dynamic localization

Answer: B

Explanation:
The most efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care is B. Software as a Service (SaaS) provider. SaaS providers offer cloud-based services that allow organizations to access applications, data, and infrastructure on demand, making it easier to access patient data no matter where the patient is located. Reference: ISACA CISA Study Manual, section 5.3.3.1.

NEW QUESTION 160
- (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 165
- (Exam Topic 4)
An IS auditor finds that while an organization's IT strategy is heavily focused on research and development, the majority of protects n the IT portfolio focus on operations and maintenance. Which of the Mowing is the BEST recommendation?

A. Align the IT strategy will 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.

Answer: A

NEW QUESTION 167
- (Exam Topic 4)
Which of the following is the PRIMARY reason to perform a risk assessment?

A. To determine the current risk profile
B. To ensure alignment with the business impact analysis (BIA)
C. To achieve compliance with regulatory requirements
D. To help allocate budget for risk mitigation controls

Answer: A

NEW QUESTION 172
- (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 177
- (Exam Topic 4)
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.

Answer: B

NEW QUESTION 178
- (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 179
- (Exam Topic 4)
The FIRST step in auditing a data communication system is to determine:

A. traffic volumes and response-time criteria
B. physical security for network equipment
C. the level of redundancy in the various communication paths
D. business use and types of messages to be transmitted

Answer: D

NEW QUESTION 183
- (Exam Topic 4)
A web proxy server for corporate connections to external resources reduces organizational risk by:

A. anonymizing users through changed IP addresses.
B. providing multi-factor authentication for additional security.
C. providing faster response than direct access.
D. load balancing traffic to optimize data pathways.

Answer: B

NEW QUESTION 185
- (Exam Topic 4)
Following a breach, what is the BEST source to determine the maximum amount of time before customers must be notified that their personal information may have been compromised?

A. Industry regulations
B. Industry standards
C. Incident response plan
D. Information security policy

Answer: C

NEW QUESTION 187
- (Exam Topic 4)
A database administrator (DBA) should be prevented from having end user responsibilities :

A. having end user responsibilities
B. accessing sensitive information
C. having access to production files
D. using an emergency user ID

Answer: A

NEW QUESTION 190
- (Exam Topic 4)
Which of the following should be of GREATEST concern to an |$ 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

Answer: C

NEW QUESTION 193
- (Exam Topic 4)
An organization is migrating its HR application to an Infrastructure as a Service (laaS) model in a private cloud. Who is PRIMARILY responsible for the security configurations of the deployed application's operating system?

A. The cloud provider's external auditor
B. The cloud provider
C. The operating system vendor

D. The organization

Answer: D

NEW QUESTION 195
- (Exam Topic 4)
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 m the IT strategic plan.

Answer: B

NEW QUESTION 199
- (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 200
- (Exam Topic 4)
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

Answer: A

NEW QUESTION 201
- (Exam Topic 4)
A computer forensic audit is MOST relevant in which of the following situations?

A. Inadequate controls in the IT environment
B. Mismatches in transaction data
C. Missing server patches
D. Data loss due to hacking of servers

Answer: D

NEW QUESTION 202
- (Exam Topic 4)
A characteristic of a digital signature is that it

A. is under control of the receiver
B. is unique to the message
C. is validated when data are changed
D. has a reproducible hashing algorithm

Answer: B

NEW QUESTION 207
- (Exam Topic 4)
An IS auditor notes that not all security tests were completed for an online sales system recently promoted to production. Which of the following is the auditor's BEST course of action?

A. Determine exposure to the business
B. Adjust future testing activities accordingly
C. Increase monitoring for security incidents
D. Hire a third party to perform security testing

Answer:

A

NEW QUESTION 211
- (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 215
- (Exam Topic 3)
Which of the following is MOST important when planning a network audit?

A. Determination of IP range in use
B. Analysis of traffic content
C. Isolation of rogue access points
D. Identification of existing nodes

Answer: D

NEW QUESTION 220
- (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 224
- (Exam Topic 3)
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 stat satisfied with their IT-related roles
D. Frequency of business process capability maturity assessments

Answer: B

NEW QUESTION 225
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 226
- (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 229
- (Exam Topic 3)
An organization has virtualized its server environment without making any other changes to the network or security infrastructure. Which of the following is the MOST significant risk?

A. Inability of the network intrusion detection system (IDS) to monitor virtual server-lo-server communications

B. Vulnerability in the virtualization platform affecting multiple hosts
C. Data center environmental controls not aligning with new configuration
D. System documentation not being updated to reflect changes in the environment

Answer: B

NEW QUESTION 233
- (Exam Topic 3)
A credit card company has decided to outsource the printing of customer statements It Is MOST important for the company to verify whether:

A. the provider has alternate service locations.
B. the contract includes compensation for deficient service levels.
C. the provider's information security controls are aligned with the company's.
D. the provider adheres to the company's data retention policies.

Answer: C

NEW QUESTION 238
- (Exam Topic 3)
Which of the following would MOST effectively help to reduce the number of repealed 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

Answer: C

NEW QUESTION 239
- (Exam Topic 3)
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.

Answer: A

NEW QUESTION 240
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 241
- (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 242
- (Exam Topic 3)
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. Using smart cards with one-time passwords
B. Periodically reviewing log files
C. Configuring the router as a firewall
D. Installing biometrics-based authentication

Answer: C

NEW QUESTION 246

- (Exam Topic 3)
Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

A. Restricting evidence access to professionally certified forensic investigators
B. Documenting evidence handling by personnel throughout the forensic investigation
C. Performing investigative procedures on the original hard drives rather than images of the hard drives
D. Engaging an independent third party to perform the forensic investigation

Answer: B

NEW QUESTION 250
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 254
- (Exam Topic 3)
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.

Answer: D

NEW QUESTION 256
- (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 260
- (Exam Topic 3)
Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

A. Inability to utilize the site when required
B. Inability to test the recovery plans onsite
C. Equipment compatibility issues at the site
D. Mismatched organizational security policies

Answer: B

NEW QUESTION 264
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 269
- (Exam Topic 3)
Which of the following is necessary for effective risk management in IT governance?

A. Local managers are solely responsible for risk evaluation.
B. IT risk management is separate from corporate risk management.
C. Risk management strategy is approved by the audit committee.
D. Risk evaluation is embedded in management processes.

Answer: D

NEW QUESTION 274
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 276
- (Exam Topic 3)
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.

Answer: C

NEW QUESTION 277
- (Exam Topic 3)
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.

Answer: D

NEW QUESTION 282
- (Exam Topic 3)
Which task should an IS auditor complete FIRST during the preliminary planning phase of a database security review?

A. Perform a business impact analysis (BIA).
B. Determine which databases will be in scope.
C. Identify the most critical database controls.
D. Evaluate the types of databases being used

Answer: B

NEW QUESTION 287
- (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 290
- (Exam Topic 3)
An audit has identified that business units have purchased cloud-based applications without IPs 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.

Answer: B

NEW QUESTION 292
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 293
- (Exam Topic 3)
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.

Answer: D

NEW QUESTION 295
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 297
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 300
- (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 302
- (Exam Topic 3)
An IS auditor is reviewing logical access controls for an organization's financial business application Which of the following findings should be of GREATEST concern to the auditor?

A. Users are not required to change their passwords on a regular basis
B. Management does not review application user activity logs
C. User accounts are shared between users
D. Password length is set to eight characters

Answer: C

NEW QUESTION 304
- (Exam Topic 3)
Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

A. Rotating backup copies of transaction files offsite
B. Using a database management system (DBMS) to dynamically back-out partially processed transactions
C. Maintaining system console logs in electronic formal
D. Ensuring bisynchronous capabilities on all transmission lines

Answer: D

NEW QUESTION 305
- (Exam Topic 3)
Which of the following would be of GREATEST concern when reviewing an organization's security information and event management (SIEM) solution?

A. SIEM reporting is customized.
B. SIEM configuration is reviewed annually
C. The SIEM is decentralized.
D. SIEM reporting is ad hoc.

Answer: C

NEW QUESTION 309
- (Exam Topic 3)
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 lenders from at least three different suppliers.

Answer: C

NEW QUESTION 313
- (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 316
- (Exam Topic 2)
During an exit interview, senior management disagrees with some of me facts presented m the draft audit report and wants them removed from the report. Which of the following would be the auditor's BEST course of action?

A. Revise the assessment based on senior management's objections.
B. Escalate the issue to audit management.
C. Finalize the draft audit report without changes.
D. Gather evidence to analyze senior management's objections

Answer: D

NEW QUESTION 319
- (Exam Topic 2)
The PRIMARY reason for an IS auditor to use data analytics techniques is to reduce which type of audit risk?

A. Technology risk
B. Detection risk
C. Control risk
D. Inherent risk

Answer: B

NEW QUESTION 321
- (Exam Topic 2)
Which of the following is an example of a preventative control in an accounts payable system?

A. The system only allows payments to vendors who are included In the system's master vendor list.
B. Backups of the system and its data are performed on a nightly basis and tested periodically.
C. The system produces daily payment summary reports that staff use to compare against invoice totals.
D. Policies and procedures are clearly communicated to all members of the accounts payable department

Answer: A

NEW QUESTION 324
- (Exam Topic 2)
Which of the following BEST demonstrates that IT strategy Is aligned with organizational goals and objectives?

A. IT strategies are communicated to all Business stakeholders
B. Organizational strategies are communicated to the chief information officer (CIO).
C. Business stakeholders are Involved In approving the IT strategy.
D. The chief information officer (CIO) is involved In approving the organizational strategies

Answer: C

NEW QUESTION 326
- (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 331
- (Exam Topic 2)
Which of the following activities would allow an IS auditor to maintain independence while facilitating a control sell-assessment (CSA)?

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

Answer: D

NEW QUESTION 335
- (Exam Topic 2)
In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

A. Discovery
B. Attacks
C. Planning
D. Reporting

Answer: A

NEW QUESTION 338
- (Exam Topic 2)
Which of the following is the BEST source of information tor an IS auditor to use when determining whether an organization's information security policy is adequate?

A. Information security program plans
B. Penetration test results
C. Risk assessment results
D. Industry benchmarks

Answer: C

NEW QUESTION 340
- (Exam Topic 2)
Providing security certification for a new system should include which of the following prior to the system's implementation?

A. End-user authorization to use the system in production
B. External audit sign-off on financial controls
C. Testing of the system within the production environment
D. An evaluation of the configuration management practices

Answer: A

NEW QUESTION 342
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 346
- (Exam Topic 2)
The GREATEST benefit of using a polo typing approach in software development is that it helps to:

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

Answer: C

NEW QUESTION 351
- (Exam Topic 2)
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.

Answer: D

NEW QUESTION 354
- (Exam Topic 2)
In data warehouse (DW) management, what is the BEST way to prevent data quality issues caused by changes from a source system?

A. Configure data quality alerts to check variances between the data warehouse and the source system
B. Require approval for changes in the extract/Transfer/load (ETL) process between the two systems
C. Include the data warehouse in the impact analysis (or any changes m the source system
D. Restrict access to changes in the extract/transfer/load (ETL) process between the two systems

Answer: B

NEW QUESTION 359
- (Exam Topic 2)
To develop meaningful recommendations 'or findings, which of the following is MOST important 'or an IS auditor to determine and understand?

A. Root cause
B. Responsible party
C. impact
D. Criteria

Answer: A

NEW QUESTION 361
- (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 363
- (Exam Topic 2)
An employee loses a mobile device resulting in loss of sensitive corporate data. Which o(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

Answer: A

NEW QUESTION 366
- (Exam Topic 2)
An IS auditor learns the organization has experienced several server failures in its distributed environment. Which of the following is the BEST recommendation to limit the potential impact of server failures in the future?

A. Redundant pathways
B. Clustering
C. Failover power
D. Parallel testing

Answer: B

NEW QUESTION 371
- (Exam Topic 2)
An IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer payments. The IS auditor should FIRST

A. document the exception in an audit report.

B. review security incident reports.
C. identify compensating controls.
D. notify the audit committee.

Answer: C

NEW QUESTION 374
- (Exam Topic 2)
Which of the following would MOST effectively ensure the integrity of data transmitted over a network?

A. Message encryption
B. Certificate authority (CA)
C. Steganography
D. Message digest

Answer: D

NEW QUESTION 375
- (Exam Topic 2)
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 protect 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

Answer: C

NEW QUESTION 376
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 379
- (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 380
- (Exam Topic 2)
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.

Answer: A

NEW QUESTION 385
- (Exam Topic 2)
Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization's incident management processes?

A. Service management standards are not followed.
B. Expected time to resolve incidents is not specified.
C. Metrics are not reported to senior management.
D. Prioritization criteria are not defined.

Answer: B

NEW QUESTION 388

- (Exam Topic 2)
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

Answer: A

NEW QUESTION 390
- (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 391
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 394
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 398
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 402
- (Exam Topic 2)
An IS auditor has been asked to audit the proposed acquisition of new computer hardware. The auditor’s PRIMARY concern Is that:

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

Answer: C

NEW QUESTION 404
- (Exam Topic 2)
Which of the following documents should specify roles and responsibilities within an IT audit organization?

A. Organizational chart
B. Audit charier
C. Engagement letter
D. Annual audit plan

Answer: A

NEW QUESTION 409
- (Exam Topic 2)
During an audit of a multinational bank's disposal process, an IS auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

A. Backup media are not reviewed before disposal.
B. Degaussing is used instead of physical shredding.
C. Backup media are disposed before the end of the retention period
D. Hardware is not destroyed by a certified vendor.

Answer: C

NEW QUESTION 411
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 414
- (Exam Topic 2)
Which of the following is the PRIMARY reason to follow a configuration management process to maintain application?

A. To optimize system resources
B. To follow system hardening standards
C. To optimize asset management workflows
D. To ensure proper change control

Answer: D

NEW QUESTION 418
- (Exam Topic 2)
Which of the following is the PRIMARY role of the IS auditor m 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

Answer: B

NEW QUESTION 423
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 424
- (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 429
- (Exam Topic 2)
The IS quality assurance (OA) group is responsible for:

A. ensuring that program changes adhere to established standards.
B. designing procedures to protect data against accidental disclosure.
C. ensuring that the output received from system processing is complete.
D. monitoring the execution of computer processing tasks.

Answer: A

NEW QUESTION 434
- (Exam Topic 2)
Upon completion of audit work, an IS auditor should:

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

Answer: B

NEW QUESTION 438
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 441
- (Exam Topic 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.

Answer: D

NEW QUESTION 444
- (Exam Topic 1)
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.

Answer: A

NEW QUESTION 445
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 448
- (Exam Topic 1)
A system development project is experiencing delays due to ongoing staff shortages. Which of the following strategies would provide the GREATEST assurance of system quality at implementation?

A. Implement overtime pay and bonuses for all development staff.
B. Utilize new system development tools to improve productivity.
C. Recruit IS staff to expedite system development.
D. Deliver only the core functionality on the initial target date.

Answer: C

NEW QUESTION 451
- (Exam Topic 1)
During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed. The auditor should FIRST

A. perform a business impact analysis (BIA).
B. issue an intermediate report to management.
C. evaluate the impact on current disaster recovery capability.
D. conduct additional compliance testing.

Answer: C

NEW QUESTION 456
- (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 457
- (Exam Topic 1)
Management has requested a post-implementation review of a newly implemented purchasing package to determine to what extent business requirements are being met. Which of the following is MOST likely to be assessed?

A. Purchasing guidelines and policies
B. Implementation methodology
C. Results of line processing
D. Test results

Answer: D

NEW QUESTION 459
- (Exam Topic 1)
Which of the following is a social engineering attack method?

A. An unauthorized person attempts to gam access to secure premises by following an authonzed person through a secure door.
B. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone.
C. A hacker walks around an office building using scanning tools to search for a wireless network to gain access.
D. An intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties.

Answer: B

NEW QUESTION 461
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 464
- (Exam Topic 1)
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.

Answer: C

NEW QUESTION 468
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 470

- (Exam Topic 1)
Secure code reviews as part of a continuous deployment program are which type of control?

A. Detective
B. Logical
C. Preventive
D. Corrective

Answer: C

NEW QUESTION 474
- (Exam Topic 1)
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.

Answer: D

NEW QUESTION 476
- (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 477
- (Exam Topic 1)
Which of the following is the MOST effective way for an organization to project against data loss?

A. Limit employee internet access.
B. Implement data classification procedures.
C. Review firewall logs for anomalies.
D. Conduct periodic security awareness training.

Answer: B

NEW QUESTION 479
- (Exam Topic 1)
Which of the following is MOST important to ensure when planning a black box penetration test?

A. The management of the client organization is aware of the testing.
B. The test results will be documented and communicated to management.
C. The environment and penetration test scope have been determined.
D. Diagrams of the organization's network architecture are available.

Answer: A

NEW QUESTION 483
- (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 487
- (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 492
- (Exam Topic 1)
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.

Answer: D

NEW QUESTION 497
- (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 498
- (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 502
- (Exam Topic 1)
Which of the following would be to MOST concern when determine if information assets are adequately safequately safeguarded during transport and disposal?

A. Lack of appropriate labelling
B. Lack of recent awareness training.
C. Lack of password protection
D. Lack of appropriate data classification

Answer: D

NEW QUESTION 505
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 506
- (Exam Topic 1)
Which of the following should be an IS auditor's GREATEST consideration when scheduling follow-up activities for agreed-upon management responses to remediate audit observations?

A. Business interruption due to remediation
B. IT budgeting constraints
C. Availability of responsible IT personnel
D. Risk rating of original findings

Answer: D

NEW QUESTION 507
- (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 512
- (Exam Topic 1)
A proper audit trail of changes to server start-up procedures would include evidence of:

A. subsystem structure.
B. program execution.
C. security control options.
D. operator overrides.

Answer: D

NEW QUESTION 513
- (Exam Topic 1)
An IS auditor discovers that validation controls m a web application have been moved from the server side into the browser to boost performance This would MOST likely increase the risk of a successful attack by.

A. phishing.
B. denial of service (DoS)
C. structured query language (SQL) injection
D. buffer overflow

Answer: D

NEW QUESTION 517
- (Exam Topic 1)
Which of the following strategies BEST optimizes data storage without compromising data retention practices?

A. Limiting the size of file attachments being sent via email
B. Automatically deleting emails older than one year
C. Moving emails to a virtual email vault after 30 days
D. Allowing employees to store large emails on flash drives

Answer: A

NEW QUESTION 521
- (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 524
- (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 528
- (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 532
- (Exam Topic 1)

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

Answer: C

NEW QUESTION 537
- (Exam Topic 1)
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.

Answer: D

NEW QUESTION 540
- (Exam Topic 1)
An IS auditor finds the log management system is overwhelmed with false positive alerts. The auditor's BEST recommendation would be to:

A. establish criteria for reviewing alerts.
B. recruit more monitoring personnel.
C. reduce the firewall rules.
D. fine tune the intrusion detection system (IDS).

Answer: D

NEW QUESTION 541
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 542
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 546
- (Exam Topic 1)
An IS auditor notes the transaction processing times in an order processing system have significantly increased after a major release. Which of the following should the IS auditor review FIRST?

A. Capacity management plan
B. Training plans
C. Database conversion results
D. Stress testing results

Answer: D

NEW QUESTION 551
- (Exam Topic 1)
Malicious program code was found in an application and corrected prior to release into production. After the release, the same issue was reported. Which of the following is the IS auditor's BEST recommendation?

A. Ensure corrected program code is compiled in a dedicated server.
B. Ensure change management reports are independently reviewed.
C. Ensure programmers cannot access code after the completion of program edits.
D. Ensure the business signs off on end-to-end user acceptance test (UAT) results.

Answer: A

NEW QUESTION 552
- (Exam Topic 1)
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.

Answer: D

NEW QUESTION 554
- (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 557
- (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 561
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 565
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 567
- (Exam Topic 1)
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.

Answer: B

NEW QUESTION 570
- (Exam Topic 1)
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.

Answer: A

NEW QUESTION 574
- (Exam Topic 1)
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).

Answer: C

NEW QUESTION 579
......