Isaca

Exam Questions CISA

Isaca CISA

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 4)
Which of the following provides the MOST useful information for performing a business impact analysis (B1A)?

A. inventory of relevant business processes
B. Policies for business procurement
C. Documentation of application configurations
D. Results of business resumption planning efforts

Answer: A

NEW QUESTION 2
- (Exam Topic 4)
Which of the following is the GREATEST advantage of vulnerability scanning over penetration testing?

A. The testing produces a lower number of false positive results
B. Network bandwidth is utilized more efficiently
C. Custom-developed applications can be tested more accurately
D. The testing process can be automated to cover large groups of assets

Answer: D

NEW QUESTION 3
- (Exam Topic 4)
Afire alarm system has been installed in the computer room The MOST effective location for the fire alarm control panel would be inside the

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

Answer: D

NEW QUESTION 4
- (Exam Topic 4)
Which of the following should an IS auditor review when evaluating information systems governance for a large organization?

A. Approval processes for new system implementations
B. Procedures for adding a new user to the invoice processing system
C. Approval processes for updating the corporate website
D. Procedures for regression testing system changes

Answer: A

Explanation:
According to the ISACA CISA Study Manual, evaluating information systems governance for a large organization should include reviewing the approval processes for new system implementations, as well as reviewing the processes for system maintenance, system retirement, and system decommissioning.

NEW QUESTION 5
- (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 (ROIs)
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 (KPIs)

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 6
- (Exam Topic 4)
Which of the following is the BEST control to minimize the risk of unauthorized access to lost company-owned mobile devices?

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

Answer: A

NEW QUESTION 7
- (Exam Topic 4)
When planning an audit, it is acceptable for an IS auditor to rely on a third-party providers external audit report on service level management when the

A. scope and methodology meet audit requirements
B. service provider is independently certified and accredited
C. report confirms that service levels were not violated
D. report was released within the last 12 months

Answer: A

NEW QUESTION 8
- (Exam Topic 4)
When auditing an organization's software acquisition process the BEST way for an IS auditor to understand the software benefits to the organization would be to review the

A. feasibility study
B. business case
C. request for proposal (RFP)
D. alignment with IT strategy

Answer: B

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 the BEST indication to an IS auditor that management's post-implementation review was effective?

A. Lessons learned were documented and applied.
B. Business and IT stakeholders participated in the post-implementation review.
C. Post-implementation review is a formal phase in the system development life cycle (SDLC).
D. Internal audit follow-up was completed without any findings.

Answer: D

NEW QUESTION 10
- (Exam Topic 4)
Which of the following should be the FIRST step when planning an IS audit of a third-party service provider that monitors network activities?

A. Review the third party's monitoring logs and incident handling
B. Review the roles and responsibilities of the third-party provider
C. Evaluate the organization's third-party monitoring process
D. Determine if the organization has a secure connection to the provider

Answer: B

NEW QUESTION 11
- (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 13
- (Exam Topic 4)
Which of the following provides the MOST assurance of the integrity of a firewall log?

A. The log is reviewed on a monthly basis.
B. Authorized access is required to view the log.
C. The log cannot be modified.
D. The log is retained per policy.

Answer: C

NEW QUESTION 17
- (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 20
- (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 24
- (Exam Topic 4)
An organization has recently become aware of a pervasive chip-level security vulnerability that affects all of its processors. Which of the following is the BEST way to prevent this vulnerability from being exploited?

A. Implement security awareness training.
B. Install vendor patches
C. Review hardware vendor contracts.
D. Review security log incidents.

Answer: B

Explanation:
Vendor patches are updates released by hardware vendors that can fix security vulnerabilities, making it less likely that attackers will be able to exploit them. Additionally, hardware vendors may release patches for other security issues that have already been exploited, helping to protect the organization from future attacks. It is important for organizations to regularly review the available patches and install them as soon as possible in order to ensure their hardware and systems are secure.

NEW QUESTION 28
- (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 31
- (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 35
- (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 IT-related processes

Answer: B

NEW QUESTION 39
- (Exam Topic 4)
During a review, an IS auditor discovers that corporate users are able to access cloud-based applications and data any Internet-connected web browser. Which Of the following is the auditors BEST recommendation to prevent unauthorized access?

A. Implement an intrusion detection system (IDS),
B. Update security policies and procedures.
C. Implement multi-factor authentication.
D. Utilize strong anti-malware controls on all computing devices.

Answer: C

Explanation:
The best recommendation to prevent unauthorized access in this scenario is to implement multi-factor authentication (MFA). According to the ISACA CISA Study Manual, "MFA is a security technique that requires two or more independent credentials for user authentication. MFA can be used to provide additional security for cloud-based services and applications." Thus, implementing MFA would be an effective way to prevent unauthorized access and maintain a secure environment. Multi-factor authentication (MFA) is a security measure that requires users to provide two or more pieces of evidence to verify their identity before accessing cloud-based applications and data123. MFA can prevent unauthorized access by making it harder for attackers to compromise user credentials or bypass password protection

NEW QUESTION 44
- (Exam Topic 4)
Capacity management tools are PRIMARILY used to ensure that:

A. available resources are used efficiently and effectively
B. computer systems are used to their maximum capacity most of the time
C. concurrent use by a large number of users is enabled
D. proposed hardware acquisitions meet capacity requirements

Answer: A

NEW QUESTION 48
- (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 49
- (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 54
- (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 56
- (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 59
- (Exam Topic 4)
An organization has recently moved to an agile model for deploying custom code to its in-house accounting software system. When reviewing the procedures in place for production code deployment, which of the following is the MOST significant security concern to address?

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

Answer: A

NEW QUESTION 60
- (Exam Topic 4)
An organization has replaced all of the storage devices at its primary data center with new higher-capacity units The replaced devices have been installed at the disaster recovery site to replace older units An IS auditor s PRIMARY concern would be whether

A. the recovery site devices can handle the storage requirements
B. hardware maintenance contract is in place for both old and new storage devices
C. the procurement was in accordance with corporate policies and procedures
D. the relocation plan has been communicated to all concerned parties

Answer: A

NEW QUESTION 62
- (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 66
- (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 69
- (Exam Topic 4)
Which of the following is the PRIMARY reason for an IS audit manager to review the work performed by a senior IS auditor prior to presentation of a report?

A. To ensure the conclusions are adequately supported
B. To ensure adequate sampling methods were used during fieldwork
C. To ensure the work is properly documented and filed
D. To ensure the work is conducted according to industry standards

Answer: A

NEW QUESTION 72
- (Exam Topic 4)
Which of the following would be the BEST criteria for monitoring an IT vendor's service levels?

A. Service auditor's report
B. Performance metrics
C. Surprise visit to vendor
D. Interview with vendor

Answer: B

NEW QUESTION 74
- (Exam Topic 4)
An IS auditor is reviewing a data conversion project Which of the following is the auditor's BEST recommendation prior to go-live?

A. Review test procedures and scenarios
B. Conduct a mock conversion test
C. Establish a configuration baseline
D. Automate the test scripts

Answer: B

NEW QUESTION 77
- (Exam Topic 4)
What should an IS auditor do FIRST when a follow-up audit reveals some management action plans have not been initiated?

A. Confirm whether the identified risks are still valid.
B. Provide a report to the audit committee.
C. Escalate the lack of plan completion to executive management.
D. Request an additional action plan review to confirm the findings.

Answer: C

Explanation:
The first thing that an IS auditor should do when a follow-up audit reveals some management action plans have not been initiated is to escalate the lack of plan completion to executive management. This is because executive management is responsible for ensuring that necessary actions are taken to address identified risks and ensure the effectiveness of internal controls. The auditor should communicate the findings and the importance of timely action to mitigate the risks.
Reference: ISACA, CISA Exam Preparation Guide, pg.112.

NEW QUESTION 81
- (Exam Topic 4)
Which of the following would be MOST impacted if an IS auditor were to assist with the implementation of recommended control enhancements?

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

Answer: A

NEW QUESTION 84
- (Exam Topic 4)
Which of the following should be the PRIMARY role of an internal audit function in the management of identified business risks?

A. Establishing a risk appetite
B. Establishing a risk management framework
C. Validating enterprise risk management (ERM)
D. Operating the risk management framework

Answer: D

NEW QUESTION 87
- (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 89

- (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 90
- (Exam Topic 4)
An internal audit team is deciding whether to use an audit management application hosted by a third party in a different country.
What should be the MOST important consideration related to the uploading of payroll audit documentation in the hosted application?

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

Answer: C

NEW QUESTION 95
- (Exam Topic 4)
Which of the following information security requirements BE ST enables the tracking of organizational data in a bring your own device (BYOD) environment?

A. Employees must immediately report lost or stolen mobile devices containing organizational data
B. Employees must sign acknowledgment of the organization's mobile device acceptable use policy
C. Employees must enroll their personal devices in the organization's mobile device management program

Answer: C

NEW QUESTION 97
- (Exam Topic 4)
The operations team of an organization has reported an IS security attack Which of the following should be the FIRST step for the security incident response team?

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

Answer: C

NEW QUESTION 102
- (Exam Topic 4)
Which of the following can only be provided by asymmetric encryption?

A. Information privacy
B. 256-brt key length
C. Data availability
D. Nonrepudiation

Answer: D

NEW QUESTION 106
- (Exam Topic 4)
An organization is concerned with meeting new regulations for protecting data confidentiality and asks an IS auditor to evaluate their procedures for transporting data. Which of the
following would BEST support the organization's objectives?

A. Cryptographic hashes
B. Virtual local area network (VLAN)
C. Encryption
D. Dedicated lines

Answer: C

Explanation:
The best option to support the organization's objectives of protecting data confidentiality when transporting data is encryption. Encryption is a process of encoding data so that it cannot be accessed or read by unauthorized parties. Encryption can be used to secure data in transit, ensuring that confidential data remains confidential and protected from unauthorized access. According to the ISACA CISA Study Manual, "encryption is the most effective way to achieve data security."

NEW QUESTION 107
- (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 110
- (Exam Topic 4)
An IS auditor should look for which of the following to ensure the risk associated with scope creep has been mitigated during software development?

A. Source code version control
B. Project change management controls
C. Existence of an architecture review board
D. Configuration management

Answer: B

Explanation:
Based on the information provided, the IS auditor should look for B: Project change management controls to ensure the risk associated with scope creep has been mitigated during software development. Project change management controls ensure that any changes made to the project are properly documented, communicated, and approved by the appropriate personnel. This helps to ensure that changes to the project are tracked and managed and that the project remains within its originally defined scope. Additionally, project change management controls help to ensure that any changes made are in line with the organization's goals and objectives.

NEW QUESTION 113
- (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 117
- (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 119
- (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 124
- (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 127
- (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 132
- (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 136
- (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 137
- (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 138
- (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 143
- (Exam Topic 4)
A review of IT interface controls finds an organization does not have a process to identify and correct records that do not get transferred to the receiving system
Which of the following is the IS auditors BEST recommendation?

A. Enable automatic encryption decryption and electronic signing of data files
B. implement software to perform automatic reconciliations of data between systems
C. Have coders perform manual reconciliation of data between systems
D. Automate the transfer of data between systems as much as feasible

Answer: B

NEW QUESTION 144
- (Exam Topic 4)

When auditing the closing stages of a system development protect which of the following should be the MOST important consideration?

A. Control requirements
B. Rollback procedures
C. Functional requirements documentation
D. User acceptance lest (UAT) results

Answer: D

NEW QUESTION 147
- (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 152
- (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 157
- (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 162
- (Exam Topic 4)
Which of the following BEST addresses the availability of an online store?

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

Answer: C

NEW QUESTION 167
- (Exam Topic 4)
Which of the following is the MOST important consideration when evaluating the data retention policy for a global organization with regional offices in multiple countries?

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

Answer: D

NEW QUESTION 169
- (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 171
- (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 173
- (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 174
- (Exam Topic 4)
Demonstrated support from which of the following roles in an organization has the MOST influence over information security governance?

A. Chief information security officer (CISO)
B. Information security steering committee
C. Board of directors
D. Chief information officer (CIO)

Answer: C

NEW QUESTION 176
- (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 181
- (Exam Topic 4)
Which of the following is MOST important for an IS auditor to review when determining whether IT investments are providing value to tie business?

A. Return on investment (ROI)
B. Business strategy
C. Business cases
D. Total cost of ownership (TCO)

Answer: B

Explanation:
Business strategy is the most important for an IS auditor to review when determining whether IT investments are providing value to the business, because:

- Business strategy is a plan or vision that defines the goals, objectives, and direction of the business, and how it intends to achieve them1234.
- Business strategy is the basis for aligning and prioritizing IT investments with the business needs, expectations, and outcomes1234[].
- Business strategy is the source for identifying and measuring the benefits and value that IT investments deliver to the business, such as increased revenue, faster access to information, better customer service, or improved efficiency[1]2^ 3^ 4.
- Business strategy is the criterion for evaluating and communicating the performance and impact of IT investments on the business success[1]2^ 3^.

NEW QUESTION 185
- (Exam Topic 4)
When is it MOST important for an IS auditor to apply the concept of materiality in an audit?

A. When planning an audit engagement
B. When gathering information for the fieldwork
C. When a violation of a regulatory requirement has been identified
D. When evaluating representations from the auditee

Answer: C

NEW QUESTION 190
- (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 195
- (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 200
- (Exam Topic 4)
Which of the following concerns is MOST effectively addressed by implementing an IT framework for alignment between IT and business objectives?

A. Inaccurate business impact analysis (BIA)
B. Inadequate IT change management practices
C. Lack of a benchmark analysis
D. Inadequate IT portfolio management

Answer: D

Explanation:
Implementing an IT framework for alignment between IT and business objectives is an effective way to address inadequate IT portfolio management. This type of framework helps ensure that IT investments are aligned with the organization’s business objectives and that IT investments are tracked and managed in a way that maximizes the value of those investments. Additionally, the framework can provide a basis for evaluating the effectiveness of IT investments and making decisions about future investments.

NEW QUESTION 203
- (Exam Topic 4)
Audit frameworks cart assist the IS audit function by:

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

Answer: C

NEW QUESTION 208
- (Exam Topic 4)
Which of the following testing methods is MOST appropriate for assessing whether system integrity has been maintained after changes have been made?

A. Regression testing
B. Unit testing
C. Integration testing
D. Acceptance testing

Answer:

A

NEW QUESTION 213
- (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 215
- (Exam Topic 4)
Which of the following is the BEST methodology to use for estimating the complexity of developing a large business application?

A. Function point analysis
B. Work breakdown structure
C. Critical path analysts
D. Software cost estimation

Answer: A

NEW QUESTION 219
- (Exam Topic 4)
Which of the following is the BEST source of information to determine the required level of data protection on a file server?

A. Data classification policy and procedures
B. Access rights of similar file servers
C. Previous data breach incident reports
D. Acceptable use policy and privacy statements

Answer: A

NEW QUESTION 220
- (Exam Topic 4)
An IT governance body wants to determine whether IT service delivery is based on consistently effective processes. Which of the following is the BEST approach?

A. implement a control self-assessment (CSA)
B. Conduct a gap analysis
C. Develop a maturity model
D. Evaluate key performance indicators (KPIs)

Answer: D

NEW QUESTION 221
- (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 222
- (Exam Topic 4)
Which of the following is MOST important to consider when developing a service level agreement (SLAP)?

A. Description of the services from the viewpoint of the provider
B. Detailed identification of work to be completed
C. Provisions for regulatory requirements that impact the end users' businesses
D. Description of the services from the viewpoint of the client organization

Answer: D

NEW QUESTION 226
- (Exam Topic 4)
During a database management evaluation an IS auditor discovers that some accounts with database administrator (DBA) privileges have been assigned a default password with an unlimited number of failed login attempts Which of the following is the auditor's BEST course of action?

A. Identify accounts that have had excessive failed login attempts and request they be disabled
B. Request the IT manager to change administrator security parameters and update the finding

C. Document the finding and explain the risk of having administrator accounts with inappropriate security settings

Answer: C

NEW QUESTION 231
- (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 232
- (Exam Topic 4)
A bank has a combination of corporate customer accounts (higher monetary value) and small business accounts (lower monetary value) as part of online banking. Which of the following is the BEST sampling approach for an IS auditor to use for these accounts?

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

Answer: A

NEW QUESTION 235
- (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 236
- (Exam Topic 4)
Transaction records from a business database were inadvertently deleted, and system operators decided to restore from a snapshot copy. Which of the following provides assurance that the BEST transactions were recovered successfully?

A. Review transaction recovery logs to ensure no errors were recorded.
B. Recount the transaction records to ensure no records are missing.
C. Rerun the process on a backup machine to verify the results are the same.
D. Compare transaction values against external statements to verify accuracy.

Answer: B

Explanation:
Recounting the transaction records to ensure that no records are missing is the best method to provide assurance that the best transactions were recovered successfully. This is because it ensures that all of the records that were present in the database before the snapshot was taken have been restored successfully. Other methods such as reviewing transaction recovery logs, rerunning the process on a backup machine, or comparing transaction values against external statements are not as reliable as recounting the records, as they do not guarantee that all of the records have been restored correctly.

NEW QUESTION 240
- (Exam Topic 4)
Which of the following provides the MOST useful information regarding an organization's risk appetite and tolerance?

A. Gap analysis
B. Audit reports
C. Risk profile
D. Risk register

Answer: C

NEW QUESTION 242
- (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 243
- (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 244
- (Exam Topic 4)
An IS auditor is asked to review an organization's technology relationships, interfaces, and data. Which of the following enterprise architecture (EA) areas is MOST appropriate this review? (Choose Correct answer and give explanation from CISA Certification - Information Systems Auditor official book)

A. Reference architecture
B. Infrastructure architecture
C. Information security architecture
D. Application architecture

Answer: C

Explanation:
An IS auditor's review of an organization's technology relationships, interfaces, and data should focus on the organization's information security architecture. This includes analyzing the organization's security policies and procedures, as well as identifying and assessing the effectiveness of its security controls. The auditor should also review the organization's security framework to ensure that it is comprehensive and covers all areas of the enterprise architecture. Other areas such as reference architecture, infrastructure architecture, and application architecture should also be assessed, but should not be the primary focus of the review.

NEW QUESTION 246
- (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 248
- (Exam Topic 4)
In an IT organization where many responsibilities are shared which of the following is the BEST control for detecting unauthorized data changes'?

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

Answer: C

NEW QUESTION 249
- (Exam Topic 4)
Which of the following is the BEST method to delete sensitive information from storage media that will be reused?

A. Crypto-shredding
B. Multiple overwriting
C. Reformatting
D. Re-partitioning

Answer: B

Explanation:
Multiple overwriting involves writing over the data several times with different patterns, making it extremely difficult to recover the original data. This is considered the best method for securely wiping sensitive information from storage media that will be reused, as it ensures that the data is not recoverable and that the confidentiality of the information is protected.

Reference:
ISACA. (2021). 2021 CISA Review Manual, 27th Edition. ISACA. (Chapter 10, Information Systems Operations, Maintenance, and Service Management)

NEW QUESTION 252
- (Exam Topic 4)
When testing the accuracy of transaction data, which of the following situations BEST justifies the use of a smaller sample size?

A. The IS audit staff has a high level of experience.
B. It is expected that the population is error-free.
C. Proper segregation of duties is in place.
D. The data can be directly changed by users.

Answer: B

Explanation:
The best situation to justify the use of a smaller sample size when testing the accuracy of transaction data is when it is expected that the population is error-free. This is because if the data is assumed to be error-free, then a smaller sample size can be used to confirm the accuracy of the data. It is important to note, however, that this does not replace the need for proper segregation of duties and other controls to ensure accuracy and integrity of the data.

NEW QUESTION 253
- (Exam Topic 4)
What is the PRIMARY benefit of using one-time passwords?

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

Answer: A

NEW QUESTION 256
- (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 261
- (Exam Topic 4)
When reviewing the functionality of an intrusion detection system (IDS), the IS auditor should be MOST concerned if:

A. legitimate packets blocked by the system have increased
B. actual attacks have not been identified
C. detected events have increased false
D. positives have been reported

Answer: A

NEW QUESTION 265
- (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 270
- (Exam Topic 4)
Which of the following should be the GREATEST concern to an IS auditor reviewing an organization's method to transport sensitive data between offices?

A. The method relies exclusively on the use of asymmetric encryption algorithms.
B. The method relies exclusively on the use of 128-bit encryption.
C. The method relies exclusively on the use of digital signatures.
D. The method relies exclusively on the use of public key infrastructure (PKI).

Answer: D

Explanation:

When an IS auditor is reviewing an organization's method to transport sensitive data between offices, the greatest concern should be the use of a single method of protection, such as public key infrastructure (PKI), exclusively. While PKI is a useful and secure method of transmitting sensitive information, relying solely on this method can make the organization vulnerable to security threats if the system is compromised or if the encryption is broken. A comprehensive security program should include multiple layers of protection, such as firewalls, intrusion detection systems, and encryption, to ensure the confidentiality, integrity, and availability of sensitive information.
Reference:
ISACA. (2021). 2021 CISA Review Manual, 27th Edition. ISACA. (Chapter 3, Security Management Practices)

NEW QUESTION 271
- (Exam Topic 4)
Which of the following BEST enables an organization to improve the visibility of end-user computing (EUC) applications that support regulatory reporting?

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

Answer: C

NEW QUESTION 274
- (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 275
- (Exam Topic 4)
An IS auditor engaged in developing the annual internal audit plan learns that the chief information officer (CIO) has requested there be no IS audits in the upcoming year as more time is needed to address a large number of recommendations from the previous year. Which of the following should the auditor do FIRST

A. Escalate to audit management to discuss the audit plan
B. Notify the chief operating officer (COO) and discuss the audit plan risks
C. Exclude IS audits from the upcoming year's plan
D. Increase the number of IS audits in the clan

Answer: A

NEW QUESTION 276
- (Exam Topic 3)
Which of the following is the MOST efficient way to identify segregation of duties violations in a new system?

A. Review a report of security rights in the system.
B. Observe the performance of business processes.
C. Develop a process to identify authorization conflicts.
D. Examine recent system access rights violations.

Answer: B

NEW QUESTION 278
- (Exam Topic 3)

What should an IS auditor do FIRST upon discovering that a service provider did not notify its customers of a security breach?

A. Notify law enforcement of the finding.
B. Require the third party to notify customers.
C. The audit report with a significant finding.
D. Notify audit management of the finding.

Answer: C

NEW QUESTION 283
- (Exam Topic 3)
Management receives information indicating a high level of risk associated with potential flooding near the organization's data center within the next few years. As a result, a decision has been made to move data center operations to another facility on higher ground. Which approach has been adopted?

A. Risk avoidance
B. Risk transfer
C. Risk acceptance
D. Risk reduction

Answer: A

NEW QUESTION 285
- (Exam Topic 3)
Which of the following should be of GREATEST concern to an IS auditor reviewing a network printer disposal process?

A. Disposal policies and procedures are not consistently implemented
B. Evidence is not available to verify printer hard drives have been sanitized prior to disposal.
C. Business units are allowed to dispose printers directly to
D. Inoperable printers are stored in an unsecured area.

Answer: B

NEW QUESTION 289
- (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 292
- (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 297
- (Exam Topic 3)
Which of the following would be MOST effective to protect information assets in a data center from theft by a vendor?

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

Answer: A

NEW QUESTION 301
- (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 305
- (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 307
- (Exam Topic 3)
Which of the following should be of GREATEST concern for an IS auditor reviewing an organization's disaster recovery plan (DRP)?

A. The DRP has not been formally approved by senior management.
B. The DRP has not been distributed to end users.
C. The DRP has not been updated since an IT infrastructure upgrade.
D. The DRP contains recovery procedures for critical servers only.

Answer: C

NEW QUESTION 311
- (Exam Topic 3)
Which of the following would BEST ensure that a backup copy is available for restoration of mission critical data after a disaster"

A. Use an electronic vault for incremental backups
B. Deploy a fully automated backup maintenance system.
C. Periodically test backups stored in a remote location
D. Use both tape and disk backup systems

Answer: C

NEW QUESTION 314
- (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 319
- (Exam Topic 3)
If enabled within firewall rules, which of the following services would present the GREATEST risk?

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

Answer: D

NEW QUESTION 321
- (Exam Topic 3)
During a follow-up audit, an IS auditor finds that some critical recommendations have the IS auditor's BEST course of action?

A. Require the auditee to address the recommendations in full.
B. Adjust the annual risk assessment accordingly.
C. Evaluate senior management's acceptance of the risk.
D. Update the audit program based on management's acceptance of risk.

Answer: B

NEW QUESTION 325
- (Exam Topic 3)
Which of the following is the BEST way to ensure that an application is performing according to its specifications?

A. Unit testing
B. Pilot testing
C. System testing
D. Integration testing

Answer:

D

NEW QUESTION 327
- (Exam Topic 3)
Which of the following is a corrective control?

A. Separating equipment development testing and production
B. Verifying duplicate calculations in data processing
C. Reviewing user access rights for segregation
D. Executing emergency response plans

Answer: D

NEW QUESTION 330
- (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 331
- (Exam Topic 3)
Which of the following BEST describes an audit risk?

A. The company is being sued for false accusations.
B. The financial report may contain undetected material errors.
C. Employees have been misappropriating funds.
D. Key employees have not taken vacation for 2 years.

Answer: D

NEW QUESTION 336
- (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 340
- (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 344
- (Exam Topic 3)
Which of the following would be an appropriate role of internal audit in helping to establish an organization’s privacy program?

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

Answer: A

NEW QUESTION 346
- (Exam Topic 3)
Which of the following is MOST important for an IS auditor to determine during the detailed design phase of a system development project?

A. Program coding standards have been followed
B. Acceptance test criteria have been developed

C. Data conversion procedures have been establish.
D. The design has been approved by senior management.

Answer: B

NEW QUESTION 350
- (Exam Topic 3)
Which of the following is the BEST way to enforce the principle of least privilege on a server containing data with different security classifications?

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

Answer: C

NEW QUESTION 353
- (Exam Topic 3)
Which of the following BEST facilitates the legal process in the event of an incident?

A. Right to perform e-discovery
B. Advice from legal counsel
C. Preserving the chain of custody
D. Results of a root cause analysis

Answer: C

NEW QUESTION 355
- (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 358
- (Exam Topic 3)
A company has implemented an IT segregation of duties policy. In a role-based environment, which of the following roles may be assigned to an application developer?

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

Answer: B

NEW QUESTION 361
- (Exam Topic 3)
Which of the following should an IS auditor expect to see in a network vulnerability assessment?

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

Answer: A

NEW QUESTION 365
- (Exam Topic 3)
Which of the following should be the FRST step when developing a data toes prevention (DIP) solution for a large organization?

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

Answer: D

NEW QUESTION 369
- (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 373
- (Exam Topic 3)
Which of the following provides the BEST providence that outsourced provider services are being properly managed?

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

Answer: B

NEW QUESTION 374
- (Exam Topic 3)
An IS auditor finds that the process for removing access for terminated employees is not documented What is the MOST significant risk from this observation?

A. Procedures may not align with best practices
B. Human resources (HR) records may not match system access.
C. Unauthorized access cannot he identified.
D. Access rights may not be removed in a timely manner.

Answer: D

NEW QUESTION 376
- (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 379
- (Exam Topic 3)
Which of the following IT service management activities is MOST likely to help with identifying the root cause of repeated instances of network latency?

A. Change management
B. Problem management
C. incident management
D. Configuration management

Answer: C

NEW QUESTION 384
- (Exam Topic 3)
Which of the following application input controls would MOST likoly detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

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

Answer: C

NEW QUESTION 387
- (Exam Topic 3)
Which of the following is the BEST control lo mitigate attacks that redirect Internet traffic to an unauthorized website?

A. Utilize a network-based firewall.
B. Conduct regular user security awareness training.
C. Perform domain name system (DNS) server security hardening.
D. Enforce a strong password policy meeting complexity requirements.

Answer: C

NEW QUESTION 391
- (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 396
- (Exam Topic 3)
Which of the following is the BEST way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster?

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

Answer: B

NEW QUESTION 398
- (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 403
- (Exam Topic 2)
An IS audit learn is evaluating the documentation related to the most recent application user-access review performed by IT and business management It is determined that the user list was not system-generated. Which of the following should be the GREATEST concern?

A. Availability of the user list reviewed
B. Confidentiality of the user list reviewed
C. Source of the user list reviewed
D. Completeness of the user list reviewed

Answer: C

NEW QUESTION 406
- (Exam Topic 2)
Which of the following must be in place before an IS auditor initiates audit follow-up activities?

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

Answer: B

NEW QUESTION 407
- (Exam Topic 2)
The IS auditor has recommended that management test a new system before using it in production mode. The BEST approach for management in developing a test plan is to use processing parameters that are:

A. randomly selected by a test generator.
B. provided by the vendor of the application.
C. randomly selected by the user.
D. simulated by production entities and customers.

Answer: D

NEW QUESTION 410
- (Exam Topic 2)
Which of the following would lead an IS auditor to conclude that the evidence collected during a digital forensic investigation would not be admissible in court?

A. The person who collected the evidence is not qualified to represent the case.
B. The logs failed to identify the person handling the evidence.
C. The evidence was collected by the internal forensics team.
D. The evidence was not fully backed up using a cloud-based solution prior to the trial.

Answer: B

NEW QUESTION 412
- (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 417
- (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 422
- (Exam Topic 2)
An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

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

Answer: D

NEW QUESTION 425
- (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 430
- (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 435
- (Exam Topic 2)
An IS auditor is reviewing the release management process for an in-house software development solution. In which environment Is the software version MOST likely to be the same as production?

A. Staging
B. Testing
C. Integration
D. Development

Answer: B

NEW QUESTION 436
- (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 441
- (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 444
- (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 448
- (Exam Topic 2)
An organization is planning an acquisition and has engaged an IS auditor lo evaluate the IT governance framework of the target company. Which of the following would be MOST helpful In determining the effectiveness of the framework?

A. Sell-assessment reports of IT capability and maturity
B. IT performance benchmarking reports with competitors
C. Recent third-party IS audit reports
D. Current and previous internal IS audit reports

Answer: C

NEW QUESTION 451
- (Exam Topic 2)
Which of the following is MOST helpful for measuring benefits realization for a new system?

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

Answer: A

NEW QUESTION 455
- (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 456
- (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 460

- (Exam Topic 2)
Which of the following Is the BEST way to ensure payment transaction data is restricted to the appropriate users?

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

Answer: C

NEW QUESTION 464
- (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 465
- (Exam Topic 2)
Which of the following is the BEST reason for an organization to use clustering?

A. To decrease system response time
B. To Improve the recovery lime objective (RTO)
C. To facilitate faster backups
D. To improve system resiliency

Answer: B

NEW QUESTION 469
- (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 474
- (Exam Topic 2)
Which of the following is the BEST source of information for an IS auditor to use as a baseline to assess the adequacy of an organization's privacy policy?

A. Historical privacy breaches and related root causes
B. Globally accepted privacy best practices
C. Local privacy standards and regulations
D. Benchmark studies of similar organizations

Answer: C

NEW QUESTION 477
- (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 482
- (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 484
- (Exam Topic 2)
After the merger of two organizations, which of the following is the MOST important task for an IS auditor to perform?

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

Answer: A

NEW QUESTION 486
- (Exam Topic 2)
To enable the alignment of IT staff development plans with IT strategy, which of the following should be done FIRST?

A. Review IT staff job descriptions for alignment
B. Develop quarterly training for each IT staff member.
C. Identify required IT skill sets that support key business processes
D. Include strategic objectives m IT staff performance objectives

Answer: C

NEW QUESTION 490
- (Exam Topic 2)
An organization has assigned two now IS auditors to audit a now system implementation. One of the auditors has an IT-related degree, and one has a business degree. Which ol the following is MOST important to meet the IS audit standard for proficiency?

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

Answer: C

NEW QUESTION 494
- (Exam Topic 2)
Which of the following is MOST important to verify when determining the completeness of the vulnerability scanning process?

A. The organization's systems inventory is kept up to date.
B. Vulnerability scanning results are reported to the CISO.
C. The organization is using a cloud-hosted scanning tool for Identification of vulnerabilities
D. Access to the vulnerability scanning tool is periodically reviewed

Answer: B

NEW QUESTION 497
- (Exam Topic 2)
An internal audit department recently established a quality assurance (QA) program. Which of the following activities Is MOST important to include as part of the QA program requirements?

A. Long-term Internal audit resource planning
B. Ongoing monitoring of the audit activities
C. Analysis of user satisfaction reports from business lines
D. Feedback from Internal audit staff

Answer: C

NEW QUESTION 500
- (Exam Topic 2)
In a RAO model, which of the following roles must be assigned to only one individual?

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

Answer: D

NEW QUESTION 503
- (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 505
- (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 510
- (Exam Topic 2)
While auditing a small organization's data classification processes and procedures, an IS auditor noticed that data is often classified at the incorrect level. What is the MOST effective way for the organization to improve this situation?

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

Answer: D

NEW QUESTION 514
- (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 518
- (Exam Topic 2)
Which of the following provides the MOST assurance over the completeness and accuracy ol loan application processing with respect to the implementation ol a new system?

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

Answer: B

NEW QUESTION 520
- (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 525
- (Exam Topic 2)
Which of the following BEST protects an organization's proprietary code during a joint-development activity involving a third party?

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

Answer: D

NEW QUESTION 530
- (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 532
- (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 534
- (Exam Topic 2)
Which of the following weaknesses would have the GREATEST impact on the effective operation of a perimeter firewall?

A. Use of stateful firewalls with default configuration
B. Ad hoc monitoring of firewall activity
C. Misconfiguration of the firewall rules
D. Potential back doors to the firewall software

Answer: C

NEW QUESTION 535
- (Exam Topic 2)
Which of the following BEST enables the timely identification of risk exposure?

A. External audit review
B. Internal audit review
C. Control self-assessment (CSA)
D. Stress testing

Answer: C

NEW QUESTION 536
- (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 539
- (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 541
- (Exam Topic 2)
Which of the following are BEST suited for continuous auditing?

A. Low-value transactions
B. Real-lime transactions
C. Irregular transactions
D. Manual transactions

Answer: C

NEW QUESTION 544

- (Exam Topic 2)
Which of the following is the GREATEST security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system?

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

Answer: A

NEW QUESTION 548
- (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 550
- (Exam Topic 2)
Which of the following is MOST important for an IS auditor to verify when evaluating an organization's firewall?

A. Logs are being collected in a separate protected host
B. Automated alerts are being sent when a risk is detected
C. Insider attacks are being controlled
D. Access to configuration files Is restricted.

Answer: A

NEW QUESTION 555
- (Exam Topic 2)
Which of the following environments is BEST used for copying data and transformation into a compatible data warehouse formal?

A. Testing
B. Replication
C. Staging
D. Development

Answer: C

NEW QUESTION 556
- (Exam Topic 2)
Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor's BEST recommendation for a compensating control?

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

Answer: A

NEW QUESTION 559
- (Exam Topic 2)
Which of the following controls BEST ensures appropriate segregation of dudes within an accounts payable department?

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

Answer: D

NEW QUESTION 562
- (Exam Topic 2)
A third-party consultant is managing the replacement of an accounting system. Which of the following should be the IS auditor's GREATEST concern?

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

Answer: C

NEW QUESTION 566
- (Exam Topic 2)
Which of the following MUST be completed as part of the annual audit planning process?

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

Answer: C

NEW QUESTION 569
- (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 574
- (Exam Topic 2)
Which of the following should be of MOST concern to an IS auditor reviewing the public key infrastructure (PKI) for enterprise email?

A. The certificate revocation list has not been updated.
B. The PKI policy has not been updated within the last year.
C. The private key certificate has not been updated.
D. The certificate practice statement has not been published

Answer: A

NEW QUESTION 579
- (Exam Topic 2)
An IS auditor Is reviewing a recent security incident and is seeking information about me approval of a recent modification to a database system's security settings Where would the auditor MOST likely find this information?

A. System event correlation report
B. Database log
C. Change log
D. Security incident and event management (SIEM) report

Answer: C

NEW QUESTION 583
- (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 587
- (Exam Topic 2)
An organization with many desktop PCs is considering moving to a thin client architecture. Which of the following is the MAJOR advantage?

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

Answer: C

NEW QUESTION 591
- (Exam Topic 1)
An IS auditor finds that a key Internet-facing system is vulnerable to attack and that patches are not available. What should the auditor recommend be done FIRST?

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

Answer: D

NEW QUESTION 594
- (Exam Topic 1)
Which of the following is the GREATEST concern associated with a high number of IT policy exceptions approved by management?

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

Answer: B

NEW QUESTION 597
- (Exam Topic 1)
Which of the following is the PRIMARY advantage of parallel processing for a new system implementation?

A. Assurance that the new system meets functional requirements
B. More time for users to complete training for the new system
C. Significant cost savings over other system implemental or approaches
D. Assurance that the new system meets performance requirements

Answer: A

NEW QUESTION 599
- (Exam Topic 1)
Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system. What is the BEST control to ensure that data is accurately entered into the system?

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

Answer: A

NEW QUESTION 602
- (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 606
- (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 611
- (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 614
- (Exam Topic 1)
When auditing the security architecture of an online application, an IS auditor should FIRST review the:

A. firewall standards.

B. configuration of the firewall
C. firmware version of the firewall
D. location of the firewall within the network

Answer: D

NEW QUESTION 619
- (Exam Topic 1)
An incorrect version of source code was amended by a development team. This MOST likely indicates a weakness in:

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

Answer: C

NEW QUESTION 623
- (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 627
- (Exam Topic 1)
Which of the following is MOST important for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros?

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

Answer: D

NEW QUESTION 628
- (Exam Topic 1)
During a follow-up audit, an IS auditor learns that some key management personnel have been replaced since the original audit, and current management has decided not to implement some previously accepted recommendations. What is the auditor's BEST course of action?

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

Answer: B

NEW QUESTION 630
- (Exam Topic 1)
Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

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

Answer: D

NEW QUESTION 632
- (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 635

- (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 640
- (Exam Topic 1)
Which of the following is MOST important with regard to an application development acceptance test?

A. The programming team is involved in the testing process.
B. All data files are tested for valid information before conversion.
C. User management approves the test design before the test is started.
D. The quality assurance (QA) team is in charge of the testing process.

Answer: B

NEW QUESTION 645
- (Exam Topic 1)
Which of the following components of a risk assessment is MOST helpful to management in determining the level of risk mitigation to apply?

A. Risk identification
B. Risk classification
C. Control self-assessment (CSA)
D. Impact assessment

Answer: D

NEW QUESTION 650
- (Exam Topic 1)
Which of the following is the BEST control to mitigate the malware risk associated with an instant messaging (IM) system?

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

Answer: C

NEW QUESTION 652
- (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 656
- (Exam Topic 1)
The PRIMARY advantage of object-oriented technology is enhanced:

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

Answer: C

NEW QUESTION 659
- (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 662
- (Exam Topic 1)
Which of the following is the MOST important reason to implement version control for an end-user computing (EUC) application?

A. To ensure that older versions are availability for reference
B. To ensure that only the latest approved version of the application is used
C. To ensure compatibility different versions of the application
D. To ensure that only authorized users can access the application

Answer: B

NEW QUESTION 666
- (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 667
- (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 670
- (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 675
- (Exam Topic 1)
One benefit of return on investment (ROI) analysts in IT decision making is that it provides the:

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

Answer: D

NEW QUESTION 679
- (Exam Topic 1)
An organizations audit charier PRIMARILY:

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

Answer: A

NEW QUESTION 681
- (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 686
- (Exam Topic 1)
Which of the following is MOST important to include in forensic data collection and preservation procedures?

A. Assuring the physical security of devices
B. Preserving data integrity
C. Maintaining chain of custody
D. Determining tools to be used

Answer: B

NEW QUESTION 688
- (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 692
- (Exam Topic 1)
During the discussion of a draft audit report. IT management provided suitable evidence fiat 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. Re-perform the audit before changing the conclusion.
C. Change the conclusion based on evidence provided by IT management.
D. Add comments about the action taken by IT management in the report.

Answer: B

NEW QUESTION 693
- (Exam Topic 1)
Which of the following is the MOST effective way to maintain network integrity when using mobile devices?

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

Answer: A

NEW QUESTION 698
- (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 701
- (Exam Topic 1)
Which of the following tests would provide the BEST assurance that a health care organization is handling patient data appropriately?

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

Answer: B

NEW QUESTION 702
- (Exam Topic 1)
An IS auditor has been asked to assess the security of a recently migrated database system that contains personal and financial data for a bank's customers. Which of the following controls is MOST important for the auditor to confirm is in place?

A. The default configurations have been changed.

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

Answer: A

NEW QUESTION 704
- (Exam Topic 1)
Which of the following is the MOST important prerequisite for the protection of physical information assets in a data center?

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

Answer: B

NEW QUESTION 709
- (Exam Topic 1)
Which of the following is the BEST way to address segregation of duties issues in an organization with budget constraints?

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

Answer: D

NEW QUESTION 712
- (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 713
- (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 717
- (Exam Topic 1)
Which of the following is the BEST justification for deferring remediation testing until the next audit?

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

Answer: D

NEW QUESTION 718
- (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 721

- (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 723
- (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 725
- (Exam Topic 1)
When implementing Internet Protocol security (IPsec) architecture, the servers involved in application delivery:

A. communicate via Transport Layer Security (TLS),
B. block authorized users from unauthorized activities.
C. channel access only through the public-facing firewall.
D. channel access through authentication.

Answer: D

NEW QUESTION 729
- (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 734
- (Exam Topic 1)
A data breach has occurred due lo malware. Which of the following should be the FIRST course of action?

A. Notify the cyber insurance company.
B. Shut down the affected systems.
C. Quarantine the impacted systems.
D. Notify customers of the breach.

Answer: C

NEW QUESTION 737
- (Exam Topic 1)
An IS auditor is following up on prior period items and finds management did not address an audit finding. Which of the following should be the IS auditor's NEXT course of action?

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

Answer: D

NEW QUESTION 741
- (Exam Topic 1)
Which of the following is the MOST effective control for protecting the confidentiality and integrity of data stored unencrypted on virtual machines?

A. Monitor access to stored images and snapshots of virtual machines.
B. Restrict access to images and snapshots of virtual machines.
C. Limit creation of virtual machine images and snapshots.
D. Review logical access controls on virtual machines regularly.

Answer: A

NEW QUESTION 745
- (Exam Topic 1)
Cross-site scripting (XSS) attacks are BEST prevented through:

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

Answer: C

NEW QUESTION 748
- (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 753
- (Exam Topic 1)
Which of the following data would be used when performing a business impact analysis (BIA)?

A. Projected impact of current business on future business
B. Cost-benefit analysis of running the current business
C. Cost of regulatory compliance
D. Expected costs for recovering the business

Answer: A

NEW QUESTION 756
- (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 758
.....

Relate Links

100% Pass Your CISA Exam with Exambible Prep Materials

https://www.exambible.com/CISA-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/