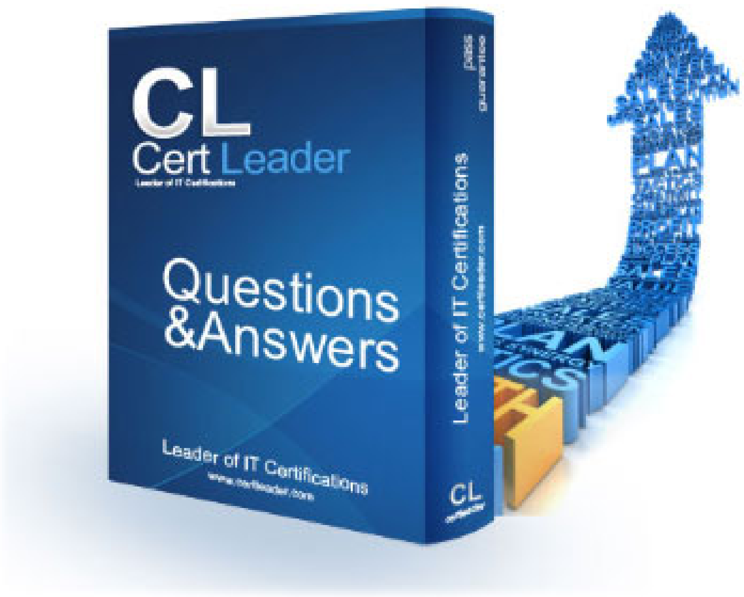
CISA Dumps

Isaca CISA

https://www.certleader.com/CISA-dumps.html



NEW QUESTION 1
- (Exam Topic 4)
Which type of device sits on the perimeter of a corporate of home network, where it obtains a public IP address and then generates private IP addresses internally?

A. Switch
B. Intrusion prevention system (IPS)
C. Gateway
D. Router

Answer: D

NEW QUESTION 2
- (Exam Topic 4)
Which of the following is an example of a preventive control for physical access?

A. Keeping log entries for all visitors to the building
B. Implementing a fingerprint-based access control system for the building
C. Installing closed-circuit television (CCTV) cameras for all ingress and egress points
D. Implementing a centralized logging server to record instances of staff logging into workstations

Answer: B

Explanation:
A fingerprint-based access control system is an example of a preventive control for physical access, as it requires authentication of the user's identity before granting access to the building. Other preventive controls for physical access include using locks and keys, using biometric systems, and using CCTV cameras.

NEW QUESTION 3
- (Exam Topic 4)
When assessing the overall effectiveness of an organization's disaster recovery planning process, which of the following is MOST important for the IS auditor to verify?

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

Answer: D

NEW QUESTION 4
- (Exam Topic 4)
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 5
- (Exam Topic 4)
When assessing a proposed project for the two-way replication of a customer database with a remote call center, the IS auditor should ensure that:

A. database conflicts are managed during replication.
B. end users are trained in the replication process.
C. the source database is backed up on both sites.
D. user rights are identical on both databases.

Answer: A

Explanation:
When assessing a proposed project for the two-way replication of a customer database with a remote call center, the IS auditor should ensure that database conflicts are managed during replication. This should include verifying that the replication process is designed to reconcile any discrepancies between the databases, such as conflicting data or duplicate records. Additionally, the IS auditor should review the security and access controls in place to ensure that the replications are performed securely and only authorized users have access to the replicated data.

NEW QUESTION 6
- (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 7
- (Exam Topic 4)
An IS auditor conducts a review of a third-party vendor's reporting of key performance indicators (KPIs) Which of the following findings should be of MOST concern to the auditor?

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

Answer: B

NEW QUESTION 8
- (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 9
- (Exam Topic 4)
Which of the following BEST enables alignment of IT with business objectives?

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

Answer: D

NEW QUESTION 10
- (Exam Topic 4)
Backup procedures for an organization's critical data are considered to be which type of control?

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

Answer: B

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

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

Answer: D

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

NEW QUESTION 15
- (Exam Topic 4)
An organization has implemented a distributed security administration system to replace the previous centralized one. Which of the following presents the GREATEST potential concern?

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

Answer: A

NEW QUESTION 16
- (Exam Topic 4)
Which of the following provides an IS auditor assurance that the interface between a point-of-sale (POS) system and the general ledger is transferring sales data completely and accurately?

A. Electronic copies of customer sales receipts are maintained.
B. Monthly bank statements are reconciled without exception.
C. Nightly batch processing has been replaced with real-time processing.
D. The data transferred over the POS interface is encrypted.

Answer: A

Explanation:
Electronic copies of customer sales receipts are records that show the details of each sales transaction, such as the date, time, amount, item, and payment method12. Electronic copies of customer sales receipts can provide an IS auditor assurance that the interface between a point-of-sale (POS) system and the general ledger is transferring sales data completely and accurately, because:

- Electronic copies of customer sales receipts can be used to verify and reconcile the sales data that is captured by the POS system and posted to the general ledger12.
- Electronic copies of customer sales receipts can be used to detect and correct any errors, discrepancies, or frauds that may occur during the data transfer process12.
- Electronic copies of customer sales receipts can be used to comply with accounting standards, tax regulations, and audit requirements12.

NEW QUESTION 18
- (Exam Topic 4)
Which of the following is the MOST effective control to mitigate against the risk of inappropriate activity by employees?

A. User activity monitoring
B. Two-factor authentication
C. Network segmentation
D. Access recertification

Answer: A

Explanation:
The most effective control to mitigate against the risk of inappropriate activity by employees is A. User activity monitoring. User activity monitoring (UAM) is a control that can be used to identify and monitor any suspicious or inappropriate user activity, such as unauthorized access or data manipulation. UAM can also be used to detect insider threats and detect any malicious activity that could lead to security breaches. Reference: ISACA CISA Study Manual, section 3.3.3.3.

NEW QUESTION 22
- (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 24
- (Exam Topic 4)
Which of the following is MOST effective for controlling visitor access to a data center?

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

Answer: A

NEW QUESTION 26
- (Exam Topic 4)
Which of the following provides the BEST assurance of data integrity after file transfers?

A. Check digits
B. Monetary unit sampling
C. Hash values
D. Reasonableness check

Answer: C

NEW QUESTION 30
- (Exam Topic 4)
Management has learned the implementation of a new IT system will not be completed on time and has requested an audit. Which of the following audit findings should be of GREATEST concern?

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

Answer: D

NEW QUESTION 34
- (Exam Topic 4)
Which of the following should be an IS auditor's PRIMARY focus when evaluating the response process for cyber crimes?

A. Communication with law enforcement
B. Notification to regulators
C. Root cause analysis
D. Evidence collection

Answer: D

Explanation:
According to the ISACA CISA Study Guide, the primary focus of an IS auditor when evaluating the response process for cyber crimes should be evidence collection. This is because the investigation and resolution of cyber incidents rely heavily on the evidence that is collected and analyzed. For more information, please refer to the ISACA CISA Study Guide section 4.13.2.2.

NEW QUESTION 38
- (Exam Topic 4)
A disaster recovery plan (DRP) should include steps for:

A. assessing and quantifying risk.
B. negotiating contracts with disaster planning consultants.
C. identifying application control requirements.
D. obtaining replacement supplies.

Answer: A

NEW QUESTION 43
- (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 48
- (Exam Topic 4)
Which of the following would be the BEST process for continuous auditing to a large financial Institution?

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

Answer: B

NEW QUESTION 49
- (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 51
- (Exam Topic 4)

Which of the following is the BEST recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage?

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

Answer: B

NEW QUESTION 56
- (Exam Topic 4)
An IS auditor is concerned that unauthorized access to a highly sensitive data center might be gained by piggybacking or tailgating. Which of the following is the BEST recommendation? (Choose Correct answer and give explanation from CISA Certification - Information Systems Auditor official book)

A. Biometrics
B. Procedures for escorting visitors
C. Airlock entrance
D. Intruder alarms

Answer: B

Explanation:
Piggybacking and tailgating are two common methods of unauthorized access, whereby an individual follows an authorized user into a secure area without going through the necessary security checks. To prevent this, organizations should have procedures in place for escorting visitors and monitoring their movements while they are in the data center. This will ensure that unauthorized users cannot gain access to the sensitive data center.

NEW QUESTION 61
- (Exam Topic 4)
Which of the following BEST protects evidence in a forensic investigation?

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

Answer: A

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

NEW QUESTION 64
- (Exam Topic 4)
An organization is shifting to a remote workforce In preparation the IT department is performing stress and capacity testing of remote access infrastructure and systems What type of control is being implemented?

A. Directive
B. Detective
C. Preventive
D. Compensating

Answer: C

NEW QUESTION 69
- (Exam Topic 4)
Email required for business purposes is being stored on employees' personal devices. Which of the following is an IS auditor's BEST recommendation?

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

Answer: D

NEW QUESTION 74
- (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 77
- (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 80
- (Exam Topic 4)
In which of the following system development life cycle (SDLC) phases would an IS auditor expect to find that controls have been incorporated into system specifications?

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

Answer: D

NEW QUESTION 81
- (Exam Topic 4)
A bank wants to outsource a system to a cloud provider residing in another country. Which of the following would be the MOST appropriate IS audit recommendation?

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

Answer: B

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

NEW QUESTION 83
- (Exam Topic 4)
Which of following areas is MOST important for an IS auditor to focus on when reviewing the maturity model for a technology organization?

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

Answer: C

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

NEW QUESTION 86
- (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 89
- (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 90
- (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 93
- (Exam Topic 4)
An IS auditor evaluating the change management process must select a sample from the change log. What is the BEST way tor the auditor to confirm the change log is complete?

A. Interview change management personnel about completeness.
B. Take an item from the log and trace it back to the system.
C. Obtain management attestation of completeness.
D. Take the last change from the system and trace it back to the log.

Answer: D

Explanation:
Taking the last change from the system and tracing it back to the log is the best way for the auditor to confirm the change log is complete, because:

- It verifies that the most recent change made to the system is recorded and documented in the change log, which implies that the change log is up to date and accurate12.
- It tests the effectiveness of the change management process and controls that ensure that all changes made to the system are authorized, approved, tested, implemented, and monitored123.
- It provides evidence of the traceability and accountability of the change management process and personnel, which can help the auditor identify any gaps, errors, or risks in the process123.

NEW QUESTION 94
- (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 96
- (Exam Topic 4)
Which of the following is the MOST effective method of destroying sensitive data stored on electronic media?

A. Degaussing
B. Random character overwrite
C. Physical destruction
D. Low-level formatting

Answer: B

NEW QUESTION 101
- (Exam Topic 4)
An IS auditor is evaluating the progress of a web-based customer service application development project. Which of the following would be MOST helpful for this evaluation?

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

Answer: A

NEW QUESTION 104
- (Exam Topic 4)
Which of the following should be the FIRST step to successfully implement a corporate data classification program?

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

Answer: D

NEW QUESTION 108
- (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 109
- (Exam Topic 4)
Which of the following would BEST help to ensure that an incident receives attention from appropriate personnel in a timely manner?

A. Completing the incident management log
B. Broadcasting an emergency message
C. Requiring a dedicated incident response team
D. Implementing incident escalation procedures

Answer: D

NEW QUESTION 113
- (Exam Topic 4)
In the development of a new financial application, the IS auditor's FIRST involvement should be in the:

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

Answer: A

NEW QUESTION 117
- (Exam Topic 4)
A data center's physical access log system captures each visitor's identification document numbers along with the visitor's photo. Which of the following sampling methods would be MOST useful to an IS auditor conducting compliance testing for the effectiveness of the system?

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

Answer: D

NEW QUESTION 120
- (Exam Topic 4)
Which of the following provides the BEST audit evidence that a firewall is configured in compliance with the organization's security policy?

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

Answer: C

NEW QUESTION 122
- (Exam Topic 4)
During a routine internal software licensing review, an IS auditor discovers instances where employees shared license keys to critical pieces of business software. Which of the following would be the auditor's BEST course of action?

A. Recommend the utilization of software licensing monitoring tools

B. Recommend the purchase of additional software license keys
C. Validate user need for shared software licenses
D. Verify whether the licensing agreement allows shared use

Answer: D

NEW QUESTION 124
- (Exam Topic 4)
A new system development project is running late against a critical implementation deadline Which of the following is the MOST important activity?

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

Answer: A

NEW QUESTION 127
- (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 131
- (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 133
- (Exam Topic 4)
What is the BEST way to reduce the risk of inaccurate or misleading data proliferating through business intelligence systems?

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

Answer: A

NEW QUESTION 138
- (Exam Topic 4)
When classifying information it is MOST important to align the classification to:

A. business risk
B. security policy
C. data retention requirements
D. industry standards

Answer: A

NEW QUESTION 139
- (Exam Topic 4)
An IS auditor is analyzing a sample of accounts payable transactions for a specific vendor and identifies one transaction with a value five times as high as the average transaction. Which of the following should the auditor do NEXT?

A. Report the variance immediately to the audit committee
B. Request an explanation of the variance from the auditee
C. Increase the sample size to 100% of the population
D. Exclude the transaction from the sample population

Answer: B

NEW QUESTION 144
- (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 147
- (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 148
- (Exam Topic 4)
During a follow-up audit, an IS auditor finds that senior management has implemented a different remediation action plan than what was previously agreed upon. Which of the following is the auditor's BEST course of action?

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

Answer: D

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

NEW QUESTION 150
- (Exam Topic 4)
Which of the following is the MOST efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care?

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

Answer: B

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

NEW QUESTION 151
- (Exam Topic 4)
Which of the following is a PRIMARY responsibility of an IT steering committee?

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

Answer: A

NEW QUESTION 155
- (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 156

- (Exam Topic 4)
Which of the following is MOST important to define within a disaster recovery plan (DRP)?

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

Answer: D

NEW QUESTION 161
- (Exam Topic 4)
Which of the following should be identified FIRST during the risk assessment process?

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

Answer: C

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

NEW QUESTION 165
- (Exam Topic 4)
Which of the following should be of GREATEST concern to an IS auditor when auditing an organization's IT strategy development process?

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

Answer: B

NEW QUESTION 169
- (Exam Topic 4)
Which of the following is the BEST indication of effective IT investment management?

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

Answer: B

NEW QUESTION 170
- (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 171
- (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 173
- (Exam Topic 4)
An organization has shifted from a bottom-up approach to a top-down approach in the development of IT policies. This should result in:

A. greater consistency across the organization.
B. a synthesis of existing operational policies.
C. a more comprehensive risk assessment plan.
D. greater adherence to best practices.

Answer: A

Explanation:
A top-down approach to the development of IT policies typically involves setting goals at the top and then developing policies to meet those goals. This type of approach results in greater consistency across the organization, as all policies are developed in alignment with the overall goals. Additionally, this approach may result in greater adherence to best practices, as the policies are developed with the organization's long-term goals in mind. It may also result in a synthesis of existing operational policies, as the goals set at the top are used to develop a unified IT policy. Finally, it may also result in a more comprehensive risk assessment plan, as all policies must be evaluated for their potential risks to the organization.

NEW QUESTION 175
- (Exam Topic 4)
An IS auditor notes that not all security tests were completed for an online sales system recently promoted to production. Which of the following is the auditor's BEST course of action?

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

Answer: A

NEW QUESTION 179
- (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 180
- (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 181
- (Exam Topic 3)
Which of the following would be the MOST useful metric for management to consider when reviewing a project portfolio?

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

Answer: C

NEW QUESTION 182
- (Exam Topic 3)
An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider MOST critical?

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

Answer: A

NEW QUESTION 185
- (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 188
- (Exam Topic 3)
During audit framework. an IS auditor teams that employees are allowed to connect their personal devices to company-owned computers. How can the auditor BEST validate that appropriate security controls are in place to prevent data loss?

A. Conduct a walk-through to view results of an employee plugging in a device to transfer confidentialdata.
B. Review compliance with data loss and applicable mobile device user acceptance policies.
C. Verify the data loss prevention (DLP) tool is properly configured by the organization.
D. Verify employees have received appropriate mobile device security awareness training.

Answer: B

NEW QUESTION 190
- (Exam Topic 3)
An IS auditor finds that capacity management for a key system is being performed by IT with no input from the business The auditor's PRIMARY concern would be:

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

Answer: B

NEW QUESTION 193
- (Exam Topic 3)
When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system. It is MOST effective for an IS auditor to review;

A. data analytics findings.
B. audit trails
C. acceptance lasting results
D. rollback plans

Answer: B

NEW QUESTION 196
- (Exam Topic 3)
Which of the following is the BEST evidence that an organization's IT strategy is aligned lo its business objectives?

A. The IT strategy is modified in response to organizational change.
B. The IT strategy is approved by executive management.
C. The IT strategy is based on IT operational best practices.
D. The IT strategy has significant impact on the business strategy

Answer: A

NEW QUESTION 199
- (Exam Topic 3)
Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

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

Answer: B

NEW QUESTION 201
- (Exam Topic 3)
Which of the following backup schemes is the BEST option when storage media is limited?

A. Real-time backup
B. Virtual backup
C. Differential backup

D. Full backup

Answer: C

NEW QUESTION 202
- (Exam Topic 3)
Which of the following would be MOST useful when analyzing computer performance?

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

Answer: B

NEW QUESTION 203
- (Exam Topic 3)
Which of the following is MOST important when implementing a data classification program?

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

Answer: B

NEW QUESTION 206
- (Exam Topic 3)
Which of the following features of a library control software package would protect against unauthorized updating of source code?

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

Answer: B

NEW QUESTION 208
- (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 210
- (Exam Topic 3)
During the planning phase of a data loss prevention (DLP) audit, management expresses a concern about mobile computing. Which of the following should the IS auditor identity as the associated risk?

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

Answer: C

NEW QUESTION 215
- (Exam Topic 3)
What Is the BEST method to determine if IT resource spending is aligned with planned project spending?

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

Answer: A

NEW QUESTION 220
- (Exam Topic 3)
The PRIMARY objective of value delivery in reference to IT governance is to:

A. promote best practices
B. increase efficiency.
C. optimize investments.
D. ensure compliance.

Answer: C

NEW QUESTION 222
- (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 225
- (Exam Topic 3)
An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

A. Loss of application support
B. Lack of system integrity
C. Outdated system documentation
D. Developer access 1o production

Answer: B

NEW QUESTION 226
- (Exam Topic 3)
During a security audit, an IS auditor is tasked with reviewing log entries obtained from an enterprise intrusion prevention system (IPS). Which type of risk would be associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration?

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

Answer: B

NEW QUESTION 228
- (Exam Topic 3)
Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA> to automate routine business tasks?

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

Answer: B

NEW QUESTION 229
- (Exam Topic 3)
Which of the following would be of GREATEST concern when reviewing an organization's security information and event management (SIEM) solution?

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

Answer: C

NEW QUESTION 231
- (Exam Topic 2)
When auditing the alignment of IT to the business strategy, it is MOST Important for the IS auditor to:

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

Answer: D

NEW QUESTION 236
- (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 239
- (Exam Topic 2)
When testing the adequacy of tape backup procedures, which step BEST verifies that regularly scheduled Backups are timely and run to completion?

A. Observing the execution of a daily backup run
B. Evaluating the backup policies and procedures
C. Interviewing key personnel evolved In the backup process
D. Reviewing a sample of system-generated backup logs

Answer: A

NEW QUESTION 244
- (Exam Topic 2)
During an IT governance audit, an IS auditor notes that IT policies and procedures are not regularly reviewed and updated. The GREATEST concern to the IS auditor is that policies and procedures might not:

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

Answer: D

NEW QUESTION 245
- (Exam Topic 2)
The waterfall life cycle model of software development is BEST suited for which of the following situations?

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

Answer: C

NEW QUESTION 246
- (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 251
- (Exam Topic 2)
During the planning stage of a compliance audit, an IS auditor discovers that a bank's inventory of compliance requirements does not include recent regulatory changes related to managing data risk. What should the auditor do FIRST?

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

Answer: A

NEW QUESTION 253
- (Exam Topic 2)
Which of the following activities provides an IS auditor with the MOST insight regarding potential single person dependencies that might exist within the organization?

A. Reviewing vacation patterns
B. Reviewing user activity logs
C. Interviewing senior IT management
D. Mapping IT processes to roles

Answer: D

NEW QUESTION 258
- (Exam Topic 2)
Which of the following is the BEST way for an organization to mitigate the risk associated with third-party application performance?

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

Answer: D

NEW QUESTION 263
- (Exam Topic 2)
Which of the following would be an appropriate rote of internal audit in helping to establish an organization's privacy program?

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

Answer: A

NEW QUESTION 264
- (Exam Topic 2)
The GREATEST benefit of using a polo typing approach in software development is that it helps to:

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

Answer: C

NEW QUESTION 266
- (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 271
- (Exam Topic 2)
An IS auditor is reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents. Which of the following observations should be of MOST concern to the auditor?

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

Answer: B

NEW QUESTION 273
- (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 276
- (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 279
- (Exam Topic 2)
What is the MAIN reason to use incremental backups?

A. To improve key availability metrics
B. To reduce costs associates with backups
C. To increase backup resiliency and redundancy
D. To minimize the backup time and resources

Answer: D

NEW QUESTION 280
- (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 281
- (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 285
- (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 290
- (Exam Topic 2)
An IS auditor performs a follow-up audit and learns the approach taken by the auditee to fix the findings differs from the agreed-upon approach confirmed during the last audit. Which of the following should be the auditor's NEXT course of action?

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

Answer: A

NEW QUESTION 291
- (Exam Topic 2)
Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization's incident management processes?

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

Answer: B

NEW QUESTION 295

- (Exam Topic 2)
A manager Identifies active privileged accounts belonging to staff who have left the organization. Which of the following is the threat actor In this scenario?

A. Terminated staff
B. Unauthorized access
C. Deleted log data
D. Hacktivists

Answer: A

NEW QUESTION 298
- (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 302
- (Exam Topic 2)
Which of the following is the MOST appropriate and effective fire suppression method for an unstaffed computer room?

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

Answer: C

NEW QUESTION 307
- (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 312
- (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 314
- (Exam Topic 2)
An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

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

Answer: D

NEW QUESTION 317
- (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 322
- (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 326
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of signature-based intrusion detection systems (lDS)?

A. An increase in the number of identified false positives
B. An increase in the number of detected Incidents not previously identified
C. An increase in the number of unfamiliar sources of intruders
D. An increase in the number of internally reported critical incidents

Answer: B

NEW QUESTION 331
- (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 334
- (Exam Topic 2)
The IS quality assurance (OA) group is responsible for:

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

Answer: A

NEW QUESTION 336
- (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 340
- (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 344
- (Exam Topic 1)
Which of the following is the BEST compensating control when segregation of duties is lacking in a small IS department?

A. Background checks
B. User awareness training

C. Transaction log review
D. Mandatory holidays

Answer: C

NEW QUESTION 346
- (Exam Topic 1)
During the implementation of an upgraded enterprise resource planning (ERP) system, which of the following is the MOST important consideration for a go-live decision?

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

Answer: D

NEW QUESTION 347
- (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 349
- (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 352
- (Exam Topic 1)
Which of the following is MOST important for an effective control self-assessment (CSA) program?

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

Answer: D

NEW QUESTION 355
- (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 360
- (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 365

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

A. Unicode translation
B. Secure Sockets Layer (SSL) encryption
C. Input validation
D. Digital signatures

Answer: C

NEW QUESTION 369
- (Exam Topic 1)
Which of the following would be a result of utilizing a top-down maturity model process?

A. A means of benchmarking the effectiveness of similar processes with peers
B. A means of comparing the effectiveness of other processes within the enterprise
C. Identification of older, more established processes to ensure timely review
D. Identification of processes with the most improvement opportunities

Answer: D

NEW QUESTION 370
- (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 371
- (Exam Topic 1)
Which of the following is the BEST method to safeguard data on an organization's laptop computers?

A. Disabled USB ports
B. Full disk encryption
C. Biometric access control
D. Two-factor authentication

Answer: C

NEW QUESTION 372
- (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 374
- (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 378
- (Exam Topic 1)
Which of the following documents would be MOST useful in detecting a weakness in segregation of duties?

A. System flowchart
B. Data flow diagram
C. Process flowchart
D. Entity-relationship diagram

Answer: C

NEW QUESTION 381
- (Exam Topic 1)
An organization has recently acquired and implemented intelligent-agent software for granting loans to customers. During the post-implementation review, which of the following is the MOST important procedure for the IS auditor to perform?

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

Answer: B

NEW QUESTION 383
- (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 384
- (Exam Topic 1)
Which of the following is the BEST way to determine whether a test of a disaster recovery plan (DRP) was successful?

A. Analyze whether predetermined test objectives were met.
B. Perform testing at the backup data center.
C. Evaluate participation by key personnel.
D. Test offsite backup files.

Answer: A

NEW QUESTION 389
- (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 392
- (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 397
- (Exam Topic 1)
During a new system implementation, an IS auditor has been assigned to review risk management at each
milestone. The auditor finds that several risks to project benefits have not been addressed. Who should be accountable for managing these risks?

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

Answer: D

NEW QUESTION 402
- (Exam Topic 1)
Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

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

Answer: D

NEW QUESTION 403
- (Exam Topic 1)
When reviewing an organization's information security policies, an IS auditor should verify that the policies have been defined PRIMARILY on the basis of:

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

Answer: B

NEW QUESTION 404
- (Exam Topic 1)
Which of the following would be an IS auditor's GREATEST concern when reviewing the early stages of a software development project?

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

Answer: C

NEW QUESTION 407
- (Exam Topic 1)
What should be the PRIMARY basis for selecting which IS audits to perform in the coming year?

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

Answer: C

NEW QUESTION 410
- (Exam Topic 1)
In a small IT web development company where developers must have write access to production, the BEST recommendation of an IS auditor would be to:

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

Answer: C

NEW QUESTION 415
- (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 416
- (Exam Topic 1)
Which of the following is the BEST data integrity check?

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

Answer: C

NEW QUESTION 418
- (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 420
- (Exam Topic 1)
In a 24/7 processing environment, a database contains several privileged application accounts with passwords set to never expire. Which of the following recommendations would BEST address the risk with minimal disruption to the business?

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

Answer: B

NEW QUESTION 424
- (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 428
......