Isaca

Exam Questions CISA

Isaca CISA

NEW QUESTION 1
- (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: A

Explanation:
The most efficient way to identify segregation of duties violations in a new system is to review a report of security rights in the system. Segregation of duties is a control principle that aims to prevent or detect errors, fraud, or abuse by ensuring that no single individual has the ability to perform incompatible or conflicting functions or activities within a system or process. A report of security rights in the system can provide a comprehensive and accurate overview of the roles, responsibilities, and access levels assigned to different users or groups in the system, and can help to identify any potential segregation of duties violations or risks. The other options are not as efficient as reviewing a report of security rights in the system, because they either rely on observation or testing rather than analysis, or they focus on existing rather than potential violations. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2

NEW QUESTION 2
- (Topic 3)
Which of the following should be performed FIRST before key performance indicators (KPIs) can be implemented?

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

Answer: B

Explanation:
The first thing that should be performed before key performance indicators (KPIs) can be implemented is the identification of organizational goals. This is because KPIs are measurable values that demonstrate how effectively an organization is achieving its key business objectives4. Therefore, it is necessary that the organization defines its goals clearly and aligns them with its vision, mission, and strategy. By identifying its goals, the organization can then determine what KPIs are relevant and meaningful to measure its progress and performance . References: 4: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.3: Benefits Realization, page 77 : CISA Online Review Course, Module 2: Governance and Management of IT, Lesson 2.3: Benefits Realization : ISACA Journal Volume 1, 2020, Article: How to Measure Anything in IT Governance

NEW QUESTION 3
- (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

Explanation:
The auditor’s primary concern when capacity management for a key system is being performed by IT with no input from the business would be an unanticipated increase in business’s capacity needs. This could result in performance degradation, service disruption or customer dissatisfaction if IT is not able to provide sufficient capacity to meet the business demand. Failure to maximize the use of equipment, cost of excessive data center storage capacity or impact to future business project funding are secondary concerns that relate to resource optimization or budget allocation, but not to service
delivery or customer satisfaction. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 374

NEW QUESTION 4
- (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

Explanation:
An appropriate role of internal audit in helping to establish an organization’s privacy program is analyzing risks posed by new regulations. A privacy program is a set of policies, procedures, and controls that aim to protect the personal data of individuals from unauthorized or unlawful collection, use, disclosure, or disposal. A privacy program should comply with the applicable laws and regulations that govern the privacy rights and obligations of individuals and organizations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). New regulations may introduce new requirements or changes that affect the organization’s privacy program and expose it to potential compliance risks or penalties. Therefore, internal audit can help to establish an organization’s privacy program by analyzing the risks posed by new regulations and providing assurance, advice, or recommendations on how to address them1. The other options are less appropriate or incorrect because:
? B. Developing procedures to monitor the use of personal data is not an appropriate role of internal audit in helping to establish an organization’s privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization’s privacy program,

as it would compromise its independence and objectivity. Internal audit should provide assurance on the effectiveness and efficiency of the organization's privacy program, but not create or execute it2.
? C. Defining roles within the organization related to privacy is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a governance or strategic role. Internal audit should not be involved in setting or approving the organization's privacy strategy, objectives, or policies, as it would compromise its independence and objectivity. Internal audit should provide assurance on the alignment and compliance of the organization's privacy program with its strategy, objectives, and policies, but not define or approve them2.
? D. Designing controls to protect personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the adequacy and effectiveness of the organization's privacy program, but not design or implement it2. References: ISACA Introduces New Audit Programs for Business Continuity/Disaster …, Best Practices for Privacy Audits - ISACA, ISACA Produces New Audit and Assurance Programs for Data Privacy and …

NEW QUESTION 5
- (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

Explanation:
The best way to ensure that a backup copy is available for restoration of mission critical data after a disaster is to periodically test backups stored in a remote location. Testing backups is essential to verify that the backup copies are valid, complete, and recoverable. Testing backups also helps to identify any issues or errors that may affect the backup process or the restoration of data. Storing backups in a remote location is important to protect the backup copies from physical damage, theft, or unauthorized access that may occur at the primary site. Using an electronic vault for incremental backups, deploying a fully automated backup maintenance system, or using both tape and disk backup systems are not sufficient to ensure that a backup copy is available for restoration of mission critical data after a disaster, as they do not address the need for testing backups or storing them in a remote location. References: Backup and Recovery of Data: The Essential Guide | Veritas, The Truth About Data Backup for Mission-Critical Environments - DATAVERSITY.

NEW QUESTION 6
- (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: C

Explanation:
Segregation of duties (SOD) is a core internal control and an essential component of an effective risk management strategy. SOD emphasizes sharing the responsibilities of key business processes by distributing the discrete functions of these processes to multiple people and departments, helping to reduce the risk of possible errors and fraud1.
SOD is especially important in IT security, where granting excessive system access to one person or group can lead to harmful consequences, such as data breaches, identity theft, or bypassing security controls2. SOD breaks IT-related tasks into four separate function categories: authorization, custody, recordkeeping, and reconciliation1. Ideally, no one person or department holds responsibility in multiple categories.
In a role-based environment, where access privileges are granted based on predefined roles, it is important to ensure that the roles are designed and assigned in a way that supports SOD. For example, the person who develops an application should not also be the one who tests it, deploys it, or maintains it.
Therefore, an application developer should not be assigned the roles of IT operator, system administration, or database administration, as these roles may conflict with their development role and create opportunities for misuse or abuse of the system. The only role that may be assigned to an application developer without violating SOD is emergency support, which is a temporary role that allows the developer to access the system in case of a critical issue that requires immediate resolution3. However, even this role should be granted with caution and monitored closely to ensure compliance with SOD policies. References:
? ISACA, CISA Review Manual, 27th Edition, 2019, page 2824
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 1066692
? Hyperproof Blog, Segregation of Duties: What it is and Why it's Important1
? Advisera Blog, Segregation of duties in your ISMS according to ISO 27001A.6.1.23

NEW QUESTION 7
- (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

Explanation:
The approach adopted by management in this scenario is risk
avoidance. Risk avoidance is the elimination of a risk by discontinuing or not undertaking an activity that poses a threat to the organization3. By moving data center operations to another facility on higher ground, management is avoiding the potential flooding risk that could disrupt or damage the data center. Risk transfer, risk acceptance and risk reduction are other possible approaches for dealing with risks, but they do not apply in this case. References:
? CISA Review Manual, 27th Edition, page 641

? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 8
- (Topic 3)
When reviewing a data classification scheme, it is MOST important for an IS auditor to determine if.

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

Answer: B

Explanation:
When reviewing a data classification scheme, it is most important for an IS auditor to determine if the security criteria are clearly documented for each classification. This will help the IS auditor to evaluate if the data classification scheme is consistent, comprehensive, and aligned with the organizational objectives and regulatory requirements. The security criteria should define the level of confidentiality, integrity, and availability for each data classification, as well as the corresponding controls such as access control, rights management, and cryptographic protection1. The other options are less important or incorrect because:
? A. Each information asset is not necessarily assigned to a different classification. Data classification schemes usually have a limited number of categories, such as “Sensitive,” “Confidential,” and “Public,” and multiple information assets can belong to the same category2.
? C. Senior IT managers are not necessarily identified as information owners. Information owners are typically the business units or functions that create, use, or maintain the information assets, and they may or may not be senior IT managers3.
? D. The information owner is not required to approve access to the asset. The information owner is responsible for defining the access requirements and rules for the asset, but the actual approval of access requests may be delegated to other roles, such as data custodians or administrators3. References: Simplify and Contextualize Your Data Classification Efforts - ISACA, 3.7: Establish and Maintain a Data Classification Scheme, Data Classification and Practices - NIST, CISA Exam Content Outline | CISA Certification | ISACA

NEW QUESTION 9
- (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

Explanation:
The most significant risk from this observation is that access rights may not be removed in a timely manner. If the process for removing access for terminated employees is not documented, there is no clear guidance or accountability for who, how, when, and what actions should be taken to revoke the access rights of the employees who leave the organization. This could result in delays, inconsistencies, or omissions in removing access rights, which could allow terminated employees to retain unauthorized access to the organization’s systems and data. This could compromise the security, confidentiality, integrity, and availability of the information assets. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 10
- (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

Explanation:
The associated risk of mobile computing that an IS auditor should identify during the planning phase of a data loss prevention (DLP) audit is increased vulnerability due to anytime, anywhere accessibility. Mobile computing refers to the use of portable devices, such as laptops, tablets, smartphones, or wearable devices, that can access data and applications over wireless networks from any location6. Mobile computing enables greater flexibility, productivity, and convenience for users, but also poses significant security challenges for organizations. One of these challenges is increased vulnerability due to anytime, anywhere accessibility. This means that mobile devices are exposed to a higher risk of loss, theft, damage, or unauthorized access than stationary devices7. If mobile devices contain or access sensitive data without proper protection, such as encryption or authentication, they could result in data leakage or breach in case of compromise8. Therefore, an IS auditor should identify this risk as part of a DLP audit. The other options are less relevant or incorrect because:
? A. The use of cloud negatively impacting IT availability is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more related to cloud computing than mobile computing. Cloud computing refers to the delivery of computing services, such as data storage or processing, over the Internet from remote servers. Cloud computing may enable or support mobile computing by providing access to data and applications from any device or location, but it does not necessarily imply mobile computing. The use of cloud may negatively impact IT availability if there are disruptions or outages in the cloud service provider’s network or infrastructure, but this is not a direct
consequence of mobile computing.
? B. Increased need for user awareness training is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a control or mitigation measure than a risk. User awareness training refers to educating users about security policies, procedures, and best practices for using mobile devices and protecting data. User awareness training may help to reduce the risk of data loss or breach due to mobile computing by increasing user knowledge and responsibility, but it does not eliminate or prevent the risk.
? D. Lack of governance and oversight for IT infrastructure and applications is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a general or organizational risk than a specific or technical risk. Governance and oversight refer to the establishment and implementation of policies, standards, and procedures for managing IT resources and aligning them with business objectives. Lack of

governance and oversight for IT infrastructure and applications may affect the security and performance of mobile devices and data, but it is not a direct or inherent result of mobile computing. References: Mobile Computing - ISACA, Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous - ISACA, Data Loss Prevention—Next Steps - ISACA, [Cloud Computing - ISACA], [Cloud Computing Risk Assessment - ISACA], [User Awareness Training - ISACA], [Governance and Oversight - ISACA]

NEW QUESTION 10
- (Topic 3)
In response to an audit finding regarding a payroll application, management implemented a new automated control. Which of the following would be MOST helpful to the IS auditor when evaluating the effectiveness of the new control?

A. Approved test scripts and results prior to implementation
B. Written procedures defining processes and controls
C. Approved project scope document
D. A review of tabletop exercise results

Answer: B

Explanation:
The best way to evaluate the effectiveness of a new automated control is to review the written procedures that define the processes and controls. This will help the IS auditor to understand the objectives, scope, roles, responsibilities, and expected outcomes of the control. The written procedures will also provide a basis for testing the control and verifying its compliance with the audit finding recommendations. References:
? ISACA Frameworks: Blueprints for Success
? CISA Review Manual (Digital Version)

NEW QUESTION 13
- (Topic 3)
A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items lo the inventory system. Which control would have BEST prevented this type of fraud in a retail environment?

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

Answer: A

Explanation:
Separate authorization for input of transactions. This control would have best prevented this type of fraud in a retail environment by ensuring that the warehouse employee who handles the inventory items does not have the authority to enter adjustments to the inventory system. This would create a segregation of duties that would reduce the risk of collusion and concealment of theft.
The other options are not as effective as option A in preventing this type of fraud. Option B, statistical sampling of adjustment transactions, is a detective control that may help identify fraudulent transactions after they have occurred, but it does not prevent them from happening in the first place. Option C, unscheduled audits of lost stock lines, is also a detective control that may reveal discrepancies between the physical and recorded inventory, but it does not address the root cause of the fraud. Option D, an edit check for the validity of the inventory transaction, is a preventive control that may help verify the accuracy and completeness of the transaction data, but it does not prevent unauthorized or fraudulent adjustments.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Different Types of Inventory Fraud and How to Prevent Them1
? 6 Ways to Prevent Inventory Fraud in Your Business2

NEW QUESTION 17
- (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

Explanation:
The type of risk associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration is detection risk. Detection risk is the risk that the auditor’s procedures will not detect a material misstatement or error that exists in an assertion or a control. Detection risk can be affected by factors such as the nature, timing, and extent of the audit procedures, the quality and sufficiency of the audit evidence, and the auditor’s professional judgment and competence. Detection risk can be reduced by applying appropriate audit techniques, such as sampling, testing, observation, inquiry, and analysis. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 18
- (Topic 3)
An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor's BEST recommendation for the organization?

A. Analyze a new application that moots the current re
B. Perform an analysis to determine the business risk

C. Bring the escrow version up to date.
D. Develop a maintenance plan to support the application using the existing code

Answer: C

Explanation:
This means that the organization should obtain the source code from the escrow agent and compare it with the current version of the application that they are using. The organization should then identify and apply any changes or updates that are missing or different in the escrow version, so that it matches the current version. This way, the organization can ensure that they have a complete and accurate copy of the source code that reflects their current needs and requirements.
Bringing the escrow version up to date can help the organization to avoid or reduce the risks and costs associated with using an outdated or incompatible version of the source code. For example, an older version of the source code may have bugs, errors, or vulnerabilities that could affect the functionality, security, or performance of the application.
An older version of the source code may also lack some features, enhancements, or integrations that could improve the usability, efficiency, or value of the application. An older version of the source code may also not comply with some standards, regulations, or contracts that could affect the quality, reliability, or legality of the application1.
The other options are not as good as bringing the escrow version up to date for the organization. Option A, analyzing a new application that meets the current requirements, is a possible option but it may be more time-consuming, expensive, and risky than updating the existing application. The organization may have to go through a complex and lengthy process of selecting, acquiring, implementing, testing, and migrating to a new application, which could disrupt their operations and performance. The organization may also have to deal with compatibility, interoperability, or data quality issues when switching to a new application2. Option B, performing an analysis to determine the business risk, is a necessary step but not a recommendation for the organization. The organization should already be aware of the business risk of using an application whose vendor has gone out of business and whose escrow has an older version of the source code. The organization should focus on finding and implementing a solution to mitigate or eliminate this risk3. Option D, developing a maintenance plan to support the application using the existing code, is not a feasible option because it assumes that the organization has access to the existing code. However, this is not the case because the vendor has gone out of business and the escrow has an older version of the source code. The organization cannot support or maintain an application without having a complete and accurate copy of its source code. References:
? How Important Is Source Code Escrow - ISACA1
? The What and Why of Source Code Escrow2
? Unlocking Source Code In Escrow 2023: A Guide To Secure Software3

NEW QUESTION 21
- (Topic 3)
An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported the auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

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

Answer: C

Explanation:
The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the main network. An unsupported software system may have unpatched vulnerabilities that could be exploited by attackers to compromise the system or access sensitive data. By isolating the system from the rest of the network, the organization can limit the exposure and impact of a potential breach. Verifying all patches have been applied to the outdated software system, closing all unused ports on the outdated software system and monitoring network traffic attempting to reach the outdated software system are also good practices, but they do not address the root cause of the risk, which is the lack of vendor support and updates.
References:
? CISA Review Manual, 27th Edition, page 2951
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 22
- (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

Explanation:
The most critical finding for an IS auditor following up on a recent security incident is that the security weakness facilitating the attack was not identified. This finding indicates that the root cause of the incident was not analyzed, and the vulnerability that allowed the attack to succeed was not remediated. This means that the organization is still exposed to the same or similar attacks in the future, and its security posture has not improved. Identifying and addressing the security weakness is a key step in the incident response process, as it helps to prevent recurrence, mitigate impact, and improve resilience.
The other findings are not as critical as the failure to identify the security weakness, but they are still important issues that should be addressed by the organization. The attack was not automatically blocked by the intrusion detection system (IDS) is a finding that suggests that the IDS was not configured properly, or that it did not have the latest signatures or rules to detect and prevent the attack. The attack could not be traced back to the originating person is a finding that implies that the organization did not have sufficient logging, monitoring, or forensic capabilities to identify and attribute the attacker. Appropriate response documentation was not maintained is a finding that indicates that the organization did not follow a consistent and formal incident response procedure, or that it did not document its actions, decisions, and lessons learned from the incident.
References:
? ISACA CISA Review Manual 27th Edition (2019), page 254
? Incident Response Process - ISACA1
? Incident Response: How to Identify and Fix Security Weaknesses

NEW QUESTION 27
- (Topic 3)
What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

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

Answer: D

Explanation:
The greatest concern for an IS auditor reviewing contracts for licensed software that executes a critical business process is that software escrow was not negotiated. Software escrow is an arrangement where a third-party holds a copy of the source code and documentation of a licensed software in a secure location. The software escrow agreement specifies the conditions under which the licensee can access the escrowed materials, such as in case of bankruptcy, termination, or breach of contract by the licensor. Software escrow is important for ensuring the continuity and availability of a critical business process that depends on a licensed software. Without software escrow, the licensee may face significant risks and challenges in maintaining, modifying, or recovering the software in case of any disruption or dispute with the licensor. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 32
- (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: C

Explanation:
The best course of action for an IS auditor who finds that some critical recommendations have not been implemented is to evaluate senior management’s acceptance of the risk. The IS auditor should understand the reasons why the recommendations have not been implemented and the implications for the organization’s risk exposure. The IS auditor should also verify that senior management has formally acknowledged and accepted the residual risk and has documented the rationale and justification for their decision. The IS auditor should communicate the findings and the risk acceptance to the audit committee and other relevant stakeholders. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 37
- (Topic 3)
An audit identified that a computer system is not assigning sequential purchase order numbers to order requests. The IS auditor is conducting an audit follow-up to determine if management has reserved this finding. Which of two following is the MOST reliable follow- up procedure?

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

Answer: C

Explanation:
The most reliable follow-up procedure to determine if management has resolved the finding of non-sequential purchase order numbers is to inspect the system settings and transaction logs to determine if sequential order numbers are generated. This will provide direct evidence of the system’s functionality and compliance with the audit recommendation. The other options are less reliable because they rely on indirect evidence or information obtained from management, which may not be accurate or complete. References: CISA Review Manual (Digital Version), Standards, Guidelines, Tools and Techniques

NEW QUESTION 40
- (Topic 3)
During an exit meeting, an IS auditor highlights that backup cycles are being missed due to operator error and that these exceptions are not being managed. Which of the following is the BEST way to help management understand the associated risk?

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

Answer: A

Explanation:
The best way to help management understand the associated risk of missing backup cycles due to operator error and lack of exception management is to explain the impact to disaster recovery. Disaster recovery is the process of restoring normal operations and functions after a disruptive event, such as a natural disaster, a cyberattack, or a hardware failure. Backup cycles are essential for disaster recovery, because they ensure that the organization has copies of its critical data and systems that can be restored in case of data loss or corruption. If backup cycles are missed due to operator error, and these exceptions are not managed, the organization may not have the latest or complete backups available for disaster recovery, which can result in prolonged downtime, reduced productivity, lost revenue, reputational damage, and legal or regulatory penalties. The other options are not as effective as explaining the impact to disaster recovery, because they either do not address the risk of data loss or corruption, or they focus on operational or technical aspects rather than business outcomes. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.1

NEW QUESTION 41
- (Topic 3)
An IS auditor assessing the controls within a newly implemented call center would First

A. gather information from the customers regarding response times and quality of service.
B. review the manual and automated controls in the call center.
C. test the technical infrastructure at the call center.
D. evaluate the operational risk associated with the call center.

Answer: D

Explanation:
The first step in assessing the controls within a newly implemented call center is to evaluate the operational risk associated with the call center. This will help the IS auditor to identify the potential threats, vulnerabilities, and impacts that could affect the call center's objectives, performance, and availability. The evaluation of operational risk will also provide a basis for determining the scope, objectives, and approach of the audit. The other options are possible audit procedures, but they are not the first step in the audit process. References: ISACA Frameworks: Blueprints for Success, CISA Review Manual (Digital Version)

NEW QUESTION 45
- (Topic 3)
An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in- house. Which of the following findings should be the IS auditor's GREATEST concern?

A. The cost of outsourcing is lower than in-house development.
B. The vendor development team is located overseas.
C. A training plan for business users has not been developed.
D. The data model is not clearly documented.

Answer: D

Explanation:
The finding that should be the IS auditor's greatest concern is that the data model is not clearly documented. A data model is a representation of the structure, relationships, and constraints of the data used by an application. It is a vital component of the software development process, as it helps to ensure the accuracy, consistency, and quality of the data1. A clear and comprehensive documentation of the data model is essential for the maintenance and support of the application, as it facilitates the understanding, modification, and troubleshooting of the data and the application logic2.
If the organization plans to bring the support and future maintenance of the application back in-house, it will need to have access to the data model documentation from the vendor. Without it, the organization may face difficulties in transferring the knowledge and skills from the vendor to the in-house team, as well as in adapting and enhancing the application to meet changing business needs and requirements3. The lack of data model documentation may also increase the risk of errors, inconsistencies, and inefficiencies in the data and the application performance2.
The other findings are not as concerning as the lack of data model documentation, because they do not directly affect the quality and maintainability of the application. The cost of outsourcing is lower than in-house development is a benefit rather than a risk for the organization, as it implies that outsourcing has helped to save time and money for the organization4. The vendor development team is located overseas is a common practice in outsourcing, and it does not necessarily imply a lower quality or a higher risk of the application. However, it may pose some challenges in terms of communication, coordination, and cultural differences, which can be managed by establishing clear expectations, roles, and responsibilities, as well as using effective tools and methods for communication and collaboration5. A training plan for business users has not been developed is a gap that should be addressed by the organization before deploying the application, as it may affect the user acceptance and satisfaction of the application. However, it does not directly impact the quality or maintainability of the application itself. References:
? What is Data Modeling? Definition & Types | Informatica1
? Data Modeling Best Practices: Documentation | erwin2
? Data Model Documentation - an overview | ScienceDirect Topics3
? Outsourcing App Development Pros and Cons – Droids On Roids4
? 8 Risks of Software Development Outsourcing & Their Solutions - Acropolium5
? Software Training Plan: How to Create One for Your Business - Elinext

NEW QUESTION 48
- (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: A

Explanation:
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 data analytics findings. Data analytics is a technique that uses software tools and statistical methods to analyze large volumes of data and identify patterns, anomalies, errors or inconsistencies. Data analytics can help to compare the source and target data sets, validate the data quality and integrity, and detect any data loss or corruption during the migration process. The other options are not as effective, because audit trails only record the actions performed on the data, acceptance testing results only verify the functionality of the new system, and rollback plans only provide contingency measures in case of migration failure. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.6

NEW QUESTION 49
- (Topic 3)
Which of the following is the BEST metric to measure the alignment of IT and business strategy?

A. Level of stakeholder satisfaction with the scope of planned IT projects
B. Percentage of enterprise risk assessments that include IT-related risk

C. Percentage of stat satisfied with their IT-related roles
D. Frequency of business process capability maturity assessments

Answer: B

Explanation:
The best metric to measure the alignment of IT and business strategy is the percentage of enterprise risk assessments that include IT-related risk. This metric indicates how well the organization identifies and manages the IT risks that could affect its strategic objectives and performance. A high percentage of enterprise risk assessments that include IT-related risk shows that the organization considers IT as an integral part of its business strategy and aligns its IT resources and capabilities with its business needs and goals. References: : CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.2: IT Strategy, page 67 : CISA Online Review Course, Module 2: Governance and Management of IT, Lesson 2.2: IT Strategy

NEW QUESTION 50
- (Topic 3)
An IS auditor has been asked to advise on measures to improve IT governance within the organization. Which at the following is the BEST recommendation?

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

Answer: A

Explanation:
The best recommendation for improving IT governance within the organization is to implement key performance indicators (KPIs). KPIs are measurable values that show how effectively the organization is achieving its key business objectives. KPIs can help the organization to monitor and evaluate the performance, efficiency, and alignment of its IT processes and resources with its business goals and strategies1.
The other options are not as effective as implementing KPIs for improving IT governance. Option B, implementing annual third-party audits, is a good practice but may not be sufficient or timely to identify and address the issues or gaps in IT governance. Option C, benchmarking organizational performance against industry peers, is a useful technique but may not reflect the specific needs and expectations of the organization's stakeholders. Option D, requiring executive management to draft IT strategy, is a necessary step but not enough to ensure that IT governance is implemented and monitored throughout the organization.

NEW QUESTION 51
- (Topic 3)
A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement.

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

Answer: D

Explanation:
Asset life cycle management is a technique of asset management where facility managers maximize the usable life of assets through planning, purchasing, using, maintaining, and disposing of assets1. The main aim of asset life cycle management is to reduce costs and increase productivity by optimizing the performance, reliability, and lifespan of assets2. Asset life cycle management can help prevent the situation of having unused applications by ensuring that the applications are aligned with the business needs, objectives, and strategies, and that they are regularly reviewed, updated, or retired as necessary3.
The other options are not as effective as asset life cycle management for preventing unused applications. A formal request for proposal (RFP) process is a method of soliciting bids from potential vendors or suppliers for a project or service. A RFP process can help select the best application for a specific requirement, but it does not ensure that the application will be used or maintained throughout its lifecycle. Business case development procedures are a set of steps that involve defining the problem, analyzing the alternatives, and proposing a solution for a project or initiative. Business case development procedures can help justify the need and value of an application, but they do not guarantee that the application will be utilized or supported after its implementation. An information asset acquisition policy is a document that outlines the rules and standards for acquiring information assets such as applications. An information asset acquisition policy can help ensure that the applications are acquired in a consistent and compliant manner, but it does not address how the applications will be managed or disposed of after their acquisition.

NEW QUESTION 53
- (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

Explanation:
The best way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster is to involve staff at all levels in periodic paper walk-through exercises. This means that the BCPs are tested and validated by the people who will execute them in a real situation, and any gaps, errors, or inconsistencies can be identified and corrected. Paper walk-through exercises are also a good way to raise awareness and train staff on their roles and responsibilities in a BCP scenario, as well as to evaluate the feasibility and effectiveness of the recovery strategies1.
The other options are not the best ways to ensure that BCPs will work effectively, because they do not involve testing or validating the plans. Preparing detailed plans for each business function is important, but it does not guarantee that the plans are realistic, practical, or aligned with the overall business objectives and priorities2. Regularly updating business impact assessments is also essential, but it does not ensure that the BCPs are aligned with the current business environment and risks2. Making senior managers responsible for their plan sections is a good way to assign accountability and authority, but it does not ensure that the plan sections are coordinated and integrated with each other2.
References:

? Best Practice Guide: Business Continuity Planning (BCP)3
? Best Practices for Creating a Business Continuity Plan1
? Business Continuity Plan Best Practices

NEW QUESTION 54
- (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

Explanation:
The primary objective of value delivery in reference to IT governance is to optimize investments. Value delivery is one of the five focus areas of IT governance that aims to ensure that IT delivers expected benefits to stakeholders and enables business value creation. Value delivery involves aligning IT investments with business objectives and strategies, managing IT performance and benefits realization, optimizing IT costs and risks, and enhancing IT innovation and agility. Value delivery helps to maximize the return on investment (ROI) and value for money (VFM) of IT resources and capabilities. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 56
- (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

Explanation:
The greatest risk associated with having most users with administrator access to an externally facing system containing sensitive data is that users can make unauthorized changes to the system or the data, which could compromise the integrity, confidentiality, and availability of the system and the data. Users can export application logs, view sensitive data, and install open-licensed software are also risks, but they are not as severe as unauthorized changes. References: ISACA CISA Review Manual 27th Edition Chapter 4

NEW QUESTION 61
- (Topic 3)
Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable department?

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

Answer: D

Explanation:
Segregation of duties (SoD) is a key internal control that aims to prevent fraud and errors by ensuring that no single individual can perform incompatible or conflicting tasks within a business process. SoD reduces the risk of unauthorized or improper transactions, manipulation of data, or misappropriation of assets.
In the accounts payable department, SoD involves separating the following functions: invoice processing, payment authorization, payment execution, and reconciliation. For example, the person who approves an invoice should not be the same person who issues the payment or reconciles the bank statement.
One of the best ways to ensure appropriate SoD within the accounts payable department is to restrict program functionality according to user security profiles. This means that each user of the accounts payable system should have a unique login and password, and should only have access to the functions that are relevant to their role and responsibilities. For instance, an invoice processor should not be able to approve payments or modify vendor records. This way, the system can enforce SoD and prevent unauthorized or fraudulent activities.
The other options are not as effective as restricting program functionality according to user security profiles. Restricting access to update programs to accounts payable staff only is a general access control measure, but it does not address the SoD issue within the accounts payable department. Including the creator’s user ID as a field in every transaction record created is a useful audit trail feature, but it does not prevent users from performing incompatible functions. Ensuring that audit trails exist for transactions is a detective control that can help identify and investigate any irregularities, but it does not prevent them from occurring in the first place.

NEW QUESTION 64
- (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

Explanation:

The greatest concern for an IS auditor reviewing an organization's disaster recovery plan (DRP) is that the DRP has not been updated since an IT infrastructure upgrade. This could render the DRP obsolete or ineffective, as it may not reflect the current configuration, dependencies or recovery requirements of the IT systems. The IS auditor should ensure that the DRP is reviewed and updated regularly to align with any changes in the IT environment. The DRP has not been formally approved by senior management is a concern for an IS auditor reviewing an organization's DRP, but it is not as critical as ensuring that the DRP is up to date and valid. The DRP has not been distributed to end users or the DRP contains recovery procedures for critical servers only are issues that relate to the communication or scope of the DRP, but not to its validity or effectiveness. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 389

NEW QUESTION 66
- (Topic 2)
Due to a recent business divestiture, an organization has limited IT resources to deliver critical projects Reviewing the IT staffing plan against which of the following would BEST guide IT management when estimating resource requirements for future projects?

A. Human resources (HR) sourcing strategy
B. Records of actual time spent on projects
C. Peer organization staffing benchmarks
D. Budgeted forecast for the next financial year

Answer: B

Explanation:
The best source of information for IT management to estimate resource requirements for future projects is the records of actual time spent on projects. This data can provide a realistic and reliable basis for forecasting future resource needs based on historical trends and patterns. The records of actual time spent on projects can also help IT management to identify any gaps or inefficiencies in resource allocation and utilization. The human resources (HR) sourcing strategy is not a good source of information for estimating resource requirements for future projects, as it may not reflect the actual demand and availability of IT resources. The peer organization staffing benchmarks are not a good source of information for estimating resource requirements for future projects, as they may not account for the specific characteristics and needs of each organization. The budgeted forecast for the next financial year is not a good source of information for estimating resource requirements for future projects, as it may not be based on accurate or realistic assumptions. References:
? CISA Review Manual, 27th Edition, pages 465-4661
? CISA Review Questions, Answers & Explanations Database, Question ID: 263

NEW QUESTION 67
- (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

Explanation:
Analyzing risks posed by new regulations is an appropriate role of internal audit in helping to establish an organization's privacy program. An internal auditor can provide assurance and advisory services on the compliance and effectiveness of the privacy program, as well as identify and assess the potential risks and impacts of new or changing privacy regulations. The other options are not appropriate roles of internal audit, but rather the responsibilities of the management, the information security officer, or the privacy officer. References:
? CISA Review Manual (Digital Version), Chapter 7, Section 7.4.21
? CISA Review Questions, Answers & Explanations Database, Question ID 216

NEW QUESTION 72
- (Topic 2)
The PRIMARY reason for an IS auditor to use data analytics techniques is to reduce which type of audit risk?

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

Answer: B

Explanation:
The primary reason for an IS auditor to use data analytics techniques is to reduce detection risk. Detection risk is the risk that an IS auditor will fail to detect material errors or irregularities in the information systems environment. By using data analytics techniques, such as data extraction, analysis, visualization, and reporting, an IS auditor can enhance the audit scope, coverage, efficiency, and effectiveness. Data analytics techniques can help an IS auditor to identify anomalies, patterns, trends, correlations, and outliers in large volumes of data that may indicate potential issues or risks. Technology risk, control risk, and inherent risk are types of audit risk that are not directly affected by the
use of data analytics techniques by an IS auditor. References: [ISACA Journal Article: Data Analytics for Auditors]

NEW QUESTION 76
- (Topic 2)
The PRIMARY focus of a post-implementation review is to verify that:

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

Answer: B

Explanation:
The primary focus of a post-implementation review is to verify that user requirements have been met. User requirements are specifications that define what users need or expect from a system or service, such as functionality, usability, reliability, etc. User requirements are usually gathered and documented at the beginning of a project, and used as a basis for designing, developing, testing, and implementing a system or service. A post-implementation review is an evaluation that assesses whether a system or service meets its objectives and delivers its expected benefits after it has been implemented. The primary focus of a post-implementation review is to verify that user requirements have been met, as this can indicate whether the system or service satisfies the user needs and expectations, provides value and quality to the users, and supports the user goals and tasks. Enterprise architecture (EA) has been complied with is a possible focus of a post- implementation review, but it is not the primary one. EA is a framework that defines how an organization's business processes, information systems, and technology infrastructure are aligned and integrated to support its vision and strategy. EA has been complied with, as this can indicate whether the system or service fits with the organization's current and future state, and follows the organization's standards and principles. Acceptance testing has been properly executed is a possible focus of a post-implementation review, but it is not the primary one. Acceptance testing is a process that verifies whether a system or service meets the user requirements and expectations before it is accepted by the users or stakeholders. Acceptance testing has been properly executed, as this can indicate whether the system or service has been tested and validated by the users or stakeholders, and whether any issues or defects have been identified and resolved. User access controls have been adequately designed is a possible focus of a post-implementation review, but it is not the primary one. User access controls are mechanisms that ensure that only authorized users can access or use a system or service, and prevent unauthorized access or use. User access controls have been adequately designed, as this can indicate whether the system or service has appropriate security and privacy measures in place, and whether any risks or threats have been mitigated.

NEW QUESTION 79
- (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

Explanation:
The best source of information for an IS auditor to use as a baseline to assess the adequacy of an organization's privacy policy is the local privacy standards and regulations. Privacy standards and regulations are legal requirements that specify how personal data should be collected, processed, stored, shared, and disposed of by organizations. By using local privacy standards and regulations as a baseline, the IS auditor can ensure that the organization's privacy policy complies with the applicable laws and protects the rights and interests of data subjects. Historical privacy breaches and related root causes, globally accepted privacy best practices, and benchmark studies of similar organizations are useful sources of information for improving an organization's privacy policy, but they are not as authoritative and relevant as local privacy standards and regulations. References: CISA Review Manual (Digital Version): Chapter 2 - Governance and Management of Information Technology

NEW QUESTION 84
- (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: B

Explanation:
Ongoing monitoring of the audit activities is the most important activity to include as part of the quality assurance (QA) program requirements for an internal audit department. An IS auditor should perform regular reviews and evaluations of the audit processes, methods, standards, and outcomes to ensure that they comply with the QA program objectives and criteria. This will help to maintain and improve the quality and consistency of the audit services and deliverables. The other options are less important activities to include as part of the QA program requirements, as they may involve long-term resource planning, user satisfaction reports, or feedback from internal audit staff. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.61
? CISA Review Questions, Answers & Explanations Database, Question ID 224

NEW QUESTION 87
- (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: B

Explanation:
This is the most effective way for the organization to improve its data classification processes and procedures, because data owners are the ones who are responsible for assigning the appropriate level of classification to the data they create, collect, or manage. Data owners should be aware of the data classification policy, the criteria for each level of classification, and the implications of misclassification. IT security staff can provide tailored training for data owners based on their roles, functions, and types of data they handle.
The other options are not as effective as having IT security staff conduct targeted training for data owners:
? Use automatic document classification based on content. This is a possible option, but it may not be feasible or accurate for a small organization. Automatic document classification is a process that uses artificial intelligence or machine learning to analyze the content of a document and assign a class label based on predefined rules or models. However, this process may require a lot of resources, expertise, and maintenance, and it may not capture all the nuances and context

of the data. The IS auditor should also verify the reliability and validity of the automatic document classification system.
? Publish the data classification policy on the corporate web portal. This is a good practice, but it is not enough to improve the data classification situation. Publishing the data classification policy on the corporate web portal can increase the visibility and accessibility of the policy, but it does not ensure that data owners will read, understand, and follow it. The IS auditor should also monitor and enforce the compliance with the policy.
? Conduct awareness presentations and seminars for information classification policies. This is a useful measure, but it is not the most effective one. Conducting awareness presentations and seminars can raise the general awareness and knowledge of information classification policies among all employees, but it may not address the specific needs and challenges of data owners. The IS auditor should also provide more in-depth and practical training for data owners.

NEW QUESTION 91
- (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

Explanation:
When auditing the alignment of IT to the business strategy, it is most important for the IS auditor to evaluate deliverables of new IT initiatives against planned business services. This can help the IS auditor to assess whether the IT initiatives are meeting the business needs and expectations, delivering value and benefits, and supporting the business objectives and goals. Comparing the organization’s strategic plan against industry best practice is a possible technique for auditing the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as industry best practice may not be applicable or relevant to the specific context or situation of the organization. Interviewing senior managers for their opinion of the IT function is a possible technique for auditing the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as senior managers’ opinions may be subjective or biased, and may not reflect the actual performance or outcomes of the IT function. Ensuring an IT steering committee is appointed to monitor new IT projects is a possible control for ensuring the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as an IT steering committee may not be effective or efficient in monitoring new IT projects, and may not have sufficient authority or influence over the IT function.

NEW QUESTION 94
- (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

Explanation:
The best way to prevent accepting bad data from a third-party service provider is to implement business rules to reject invalid data. Business rules are logical statements that define the data quality requirements and standards for the organization. By implementing business rules, the organization can ensure that only data that meets the predefined criteria is accepted into the enterprise data warehouse. Obtaining error codes indicating failed data feeds, purchasing data cleansing tools from a reputable vendor, and appointing data quality champions across the organization are useful measures to improve data quality, but they do not prevent accepting bad data in the first place. References:
ISACA Journal Article: Data Quality Management

NEW QUESTION 96
- (Topic 2)
Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm tor potential software vulnerabilities?

A. Guest operating systems are updated monthly
B. The hypervisor is updated quarterly.
C. A variety of guest operating systems operate on one virtual server
D. Antivirus software has been implemented on the guest operating system only.

Answer: D

Explanation:
Antivirus software has been implemented on the guest operating system only is the observation that an IS auditor would consider the greatest risk when conducting an audit of a virtual server farm for potential software vulnerabilities. A virtual server farm is a collection of servers that run multiple virtual machines (VMs) on a single physical host using a software layer called a hypervisor. A guest operating system is the operating system installed on each VM. Antivirus software is a software program that detects and removes malicious software from a computer system. If antivirus software has been implemented on the guest operating system only, it means that the hypervisor and the host operating system are not protected from malware attacks, which could compromise the security and availability of all VMs running on the same host. Therefore, antivirus software should be implemented on both the guest and host operating systems as well as on the hypervisor. References: CISA Review Manual, 27th Edition, page 378

NEW QUESTION 100
- (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

Explanation:
Access to the spreadsheet is given only to those who require access is the most important control for maintaining the security of data in the spreadsheet. An IS auditor should ensure that the principle of least privilege is applied to limit the access to sensitive financial data and prevent unauthorized disclosure, modification, or deletion. The other options are less important controls that may enhance the accuracy, availability, or integrity of data in the spreadsheet, but not its security.
References:
? CISA Review Manual (Digital Version), Chapter 6, Section 6.31
? CISA Review Questions, Answers & Explanations Database, Question ID 210

NEW QUESTION 105
- (Topic 2)
Which of the following findings from an IT governance review should be of GREATEST concern?

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

Answer: C

Explanation:
IT value analysis has not been completed is a finding from an IT governance review that should be of greatest concern. IT value analysis is a process of measuring and demonstrating the contribution of IT to the organization's goals and objectives. An IS auditor should be concerned about the lack of IT value analysis, as it may indicate that the IT investments and resources are not aligned with the business needs and expectations, or that the IT performance and outcomes are not monitored and evaluated. The other options are less critical findings that may not have a significant impact on the IT governance. References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.11
? CISA Review Questions, Answers & Explanations Database, Question ID 218

NEW QUESTION 110
- (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: C

Explanation:
This is the most helpful method for measuring benefits realization for a new system, because it involves evaluating the actual outcomes and impacts of the system after it has been implemented and used for a certain period of time. A post-implementation review can compare the actual benefits with the expected benefits that were defined in the business case or the benefits realization plan, and identify any gaps, issues, or opportunities for improvement. A post-implementation review can also assess the effectiveness, efficiency, and satisfaction of the system's users, stakeholders, and customers, and provide feedback and recommendations for future enhancements or changes.
The other options are not as helpful as post-implementation review for measuring benefits realization for a new system:
? Function point analysis. This is a technique that measures the size and complexity
of a software system based on the number and types of functions it provides. Function point analysis can help estimate the cost, effort, and time required to develop, maintain, or enhance a software system, but it does not measure the actual benefits or value that the system delivers to the organization or its users.
? Balanced scorecard review. This is a strategic management tool that measures the
performance of an organization or a business unit based on four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard review can help align the organization's vision, mission, and goals with its activities and outcomes, but it does not measure the specific benefits or impacts of a new system.
? Business impact analysis (BIA). This is a process that identifies and evaluates the potential effects of a disruption or disaster on the organization's critical business functions and processes. A BIA can help determine the recovery priorities, objectives, and strategies for the organization in case of an emergency, but it does not measure the benefits or value of a new system.

NEW QUESTION 111
- (Topic 2)
Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS audit has been asked to conduct a control assessment. the auditor's BEST course of action would be to determine if:

A. the patches were updated.
B. The logs were monitored.
C. The network traffic was being monitored.
D. The domain controller was classified for high availability.

Answer: B

Explanation:
The auditor's best course of action after a security breach in which a hacker exploited a well-known vulnerability in the domain controller is to determine if the logs were monitored. Log monitoring is an essential control for detecting and responding to security incidents, especially when known vulnerabilities exist in the system. The auditor should assess if the logs were properly configured, collected, reviewed, analyzed, and acted upon by the responsible parties. Updating patches, monitoring network traffic, and classifying domain controllers for high availability are also important controls, but they are not directly related to the detection and response of the security breach. References:
? CISA Review Manual (Digital Version), page 301
? CISA Questions, Answers & Explanations Database, question ID 3340

NEW QUESTION 115
- (Topic 2)
A new system is being developed by a vendor for a consumer service organization. The vendor will provide its proprietary software once system development is completed Which of the following is the MOST important requirement to include In the vendor contract to ensure continuity?

A. Continuous 24/7 support must be available.
B. The vendor must have a documented disaster recovery plan (DRP) in place.
C. Source code for the software must be placed in escrow.
D. The vendor must train the organization's staff to manage the new software

Answer: C

Explanation:
Source code for the software must be placed in escrow is the most important requirement to include in the vendor contract to ensure continuity. Source code is the original code of a software program that can be modified or enhanced by programmers. Placing source code in escrow means depositing it with a trusted third party who can release it to the customer under certain conditions, such as vendor bankruptcy, breach of contract, or failure to provide support. This can help to ensure continuity of the software product and its maintenance in case of vendor unavailability or dispute. The other options are less important requirements to include in the vendor contract, as they may involve support availability, disaster recovery plan, or staff training. References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.51
? CISA Review Questions, Answers & Explanations Database, Question ID 228

NEW QUESTION 116
- (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

Explanation:
Control self-assessment (CSA) is a technique that enables business managers and staff to assess and improve the effectiveness of their own controls and risk management processes. CSA can best enable the timely identification of risk exposure, as it allows for continuous monitoring and reporting of risks by those who are closest to the business processes and activities. External audit review, internal audit review, and stress testing are also useful methods for identifying risk exposure, but they are not as timely as CSA, as they are performed periodically or on demand by external or internal parties who may not have as much insight into the business operations and environment. References:
ISACA CISA Review Manual 27th Edition, page 95.

NEW QUESTION 118
- (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: C

Explanation:
Determining accountability of data owners is the most important activity in the data classification process. Data classification is a process that assigns categories or labels to data based on their value, sensitivity, criticality and risk to the organization. Data classification helps to determine the appropriate level of protection, access and retention for data. Determining accountability of data owners is an activity that identifies and assigns roles and responsibilities for data classification, protection and management to individuals or functions within the organization. Data owners are individuals or functions who have authority and responsibility for defining, classifying, protecting and managing data throughout their lifecycle. Determining accountability of data owners is essential for ensuring that data are classified correctly and consistently, and that data classification policies and procedures are followed and enforced. The other options are not as important as option C, as they are dependent on or derived from the accountability of data owners. Labeling the data appropriately is an activity that applies the categories or labels assigned by data owners to data based on their classification criteria. Identifying risk associated with the data is an activity that assesses the potential impact and likelihood of loss, disclosure, modification or destruction of data based on their classification level. Determining the adequacy of privacy controls is an activity that evaluates whether the controls implemented to protect personal or sensitive data are sufficient and effective based on their classification level.
References: CISA Review Manual (Digital Version) , Chapter 5: Protection of Information Assets, Section 5.3: Data Classification.

NEW QUESTION 121
- (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

Explanation:
The best way to determine whether programmers have permission to alter data in the production environment is by reviewing the access rights that have been granted. Access rights are permissions or privileges that define what actions or operations a user can perform on an information system or resource. By reviewing the access rights that have been granted to programmers, an IS auditor can verify whether they have been authorized to modify data in the production

environment, which is where live data and applications are stored and executed. The access control system's log settings are parameters that define what events or activities are recorded by the access control system, which is a system that enforces the access rights and policies of an information system or resource. The access control system's log settings are not the best way to determine whether programmers have permission to alter data in the production environment, as they do not indicate what permissions or privileges have been granted to programmers. How the latest system changes were implemented is a process that describes how software updates or modifications are deployed to the production environment. How the latest system changes were implemented is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers. The access control system's configuration is a set of rules or parameters that define how the access control system operates and functions. The access control system's configuration is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers.

NEW QUESTION 122
- (Topic 2)
Which of the following business continuity activities prioritizes the recovery of critical functions?

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

Answer: B

Explanation:
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects or consequences of disruptions or disasters on an organization's critical business functions or processes. A BIA can help prioritize the recovery of critical functions by assessing their importance and urgency for the organization's operations, objectives, and stakeholders, and determining their recovery time objectives (RTOs), which are the maximum acceptable time for restoring a function after a disruption. A business continuity plan (BCP) testing is a process that verifies and validates the effectiveness and readiness of a BCP, which is a document that outlines the strategies and procedures for ensuring the continuity of critical business functions in the event of a disruption or disaster. A BCP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are recovered according to the BCP. A disaster recovery plan (DRP) testing is a process that verifies and validates the effectiveness and readiness of a DRP, which is a document that outlines the technical and operational steps for restoring the IT systems and infrastructure that support critical business functions in the event of a disruption or disaster. A DRP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are supported by the IT systems and infrastructure according to the DRP. A risk assessment is a process that identifies and analyzes the potential threats and vulnerabilities that could affect an organization's critical business functions or processes. A risk assessment does not prioritize the recovery of critical functions, but rather estimates their likelihood and impact of being disrupted by various risk scenarios.

NEW QUESTION 124
- (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

Explanation:
The observation that should be of most concern to the auditor when reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents is that employees can share files with users outside the company through collaboration tools. Collaboration tools are software or hardware devices that enable users to communicate, cooperate, and coordinate with each other on a common task or project. Collaboration tools can facilitate information sharing and knowledge exchange among users, but they can also pose security risks if not properly controlled or managed. Employees can share files with users outside the company through collaboration tools, as this can compromise the security and confidentiality of intellectual property and patents, which are valuable and sensitive assets of the organization. Employees may share files with unauthorized or untrusted users who may misuse or disclose the intellectual property and patents, either intentionally or unintentionally. This can cause harm or damage to the organization, such as loss of competitive advantage, reputation, revenue, or legal rights. Training was not provided to the department that handles intellectual property and patents is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Training is an activity that educates and instructs users on how to use collaboration tools effectively and securely,
such as how to access, share, store, and protect information using collaboration tools. Training was not provided to the department that handles intellectual property and patents, as this can affect the awareness and competence of users on collaboration tools, and increase the likelihood of errors or mistakes that may compromise the security or quality of information. However, this observation may not be directly related to collaboration tools, as it may apply to any information system or resource used by the department. Logging and monitoring for content filtering is not enabled is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Logging and monitoring are processes that record and analyze the events or activities that occur on an information system or network, such as user actions, system operations, data changes, errors, alerts, etc. Content filtering is a technique that blocks or allows access to certain types of information based on predefined criteria or rules, such as keywords, categories, sources, etc. Logging and monitoring for content filtering is not enabled, as this can affect the auditability, accountability, and visibility of collaboration tools, and prevent detection or investigation of security incidents or violations related to information sharing using collaboration tools. However, this observation may not be specific to collaboration tools, as it may affect any information system or network that uses content filtering. The collaboration tool is hosted and can only be accessed via an Internet browser is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. A hosted collaboration tool is a type of cloud-based service that provides collaboration functionality over the Internet without requiring installation or maintenance on local devices. An Internet browser is a software application that enables users to access and interact with web-based content or services. The collaboration tool is hosted and can only be accessed via an Internet browser, as this can affect the availability and reliability of collaboration tools, and introduce security or privacy risks for information sharing using collaboration tools. However, this observation may not be unique to collaboration tools, as it may apply to any cloud-based service that uses an Internet browser.

NEW QUESTION 125
- (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

Explanation:
The best way for an organization to mitigate the risk associated with third- party application performance is to utilize performance monitoring tools to verify service level agreements (SLAs). Performance monitoring tools are software or hardware devices that measure and report the performance of an application or system, such as speed, availability, reliability, etc. Performance monitoring tools can help mitigate the risk associated with third-party application performance, by allowing the organization to verify whether the third-party provider is meeting the SLAs, which are contracts or agreements that define the expected level and quality of service for an application or system. Performance monitoring tools can also help identify and resolve any performance issues or problems that may arise from the third-party application. Ensuring the third party allocates adequate resources to meet requirements is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be feasible or effective depending on the availability, cost, and suitability of the resources. Using analytics within the internal audit function is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be timely or relevant depending on the frequency, scope, and quality of the analytics. Conducting a capacity planning exercise is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be accurate or reliable depending on the assumptions, methods, and data used for the capacity planning.

NEW QUESTION 127
- (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

Explanation:
The first thing that the audit manager should do when faced with a situation where only 60% of the audit has been completed and the due date is approaching is to determine where delays have occurred. This can help the audit manager to identify and analyze the root causes of the delays, such as unexpected issues, scope changes, resource constraints, communication problems, etc., and evaluate their impact on the audit objectives, scope, quality, and timeline. Based on this analysis, the audit manager can then decide on the best course of action to address the delays and complete the audit successfully. Assigning additional resources to supplement the audit is a possible option for resolving delays in an audit project, but it is not the first thing that the audit manager should do, as it may not be feasible or effective depending on the availability, cost, and suitability of the additional resources. Escalating to the audit committee is a possible option for communicating delays in an audit project and seeking guidance or support from senior management, but it is not the first thing that the audit manager should do, as it may not be necessary or appropriate depending on the severity and urgency of the delays. Extending the audit deadline is a possible option for accommodating delays in an audit project and ensuring sufficient time for completing the audit tasks and activities, but it is not the first thing that the audit manager should do, as it may not be possible or desirable depending on the contractual obligations, stakeholder expectations, and regulatory requirements.

NEW QUESTION 128
- (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

Explanation:
The most appropriate and effective fire suppression method for an un-staffed computer room is carbon dioxide (CO2). Carbon dioxide is a gaseous clean agent that extinguishes fire by displacing oxygen and reducing the combustion process. Carbon dioxide is suitable for un-staffed computer rooms because it does not leave any residue, damage, or corrosion on the electronic equipment, and it does not require water or other chemicals that could harm the environment or human health. However, carbon dioxide can pose a risk of asphyxiation to any person who may enter the computer room during or after the discharge, so proper safety precautions and warning signs should be in place.
The other options are not as appropriate or effective as carbon dioxide for an un-staffed computer room:
? Water sprinkler. This is a common fire suppression method that uses water to cool down and extinguish fire. However, water sprinkler is not suitable for un-staffed computer rooms because it can cause severe damage to the electronic equipment, such as short circuits, corrosion, or data loss. Water sprinkler can also create a risk of electric shock to any person who may enter the computer room during or after the discharge.
? Fire extinguishers. These are portable devices that contain a pressurized agent that can be sprayed on a fire to put it out. However, fire extinguishers are not effective for un-staffed computer rooms because they require manual operation by a trained person who can identify the type and location of the fire, and use the appropriate extinguisher. Fire extinguishers can also cause damage to the electronic equipment if they contain water or chemical agents.
? Dry pipe. This is a type of sprinkler system that uses pressurized air or nitrogen in the pipes instead of water until a fire is detected. When a fire is detected, the air or nitrogen is released and water flows into the pipes and sprinklers. However, dry pipe is not ideal for un-staffed computer rooms because it still uses water as the extinguishing agent, which can damage the electronic equipment as mentioned above. Dry pipe also has a slower response time than wet pipe sprinkler systems, which can allow the fire to spread more quickly.

NEW QUESTION 131
- (Topic 2)
Which of the following provides the MOST assurance over the completeness and accuracy ol loan application processing with respect to the implementation of a new system?

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

Answer: B

Explanation:
The most assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system can be obtained by running historical transactions through the new system. Historical transactions are transactions that have been processed and recorded by the old system in the past. Running historical transactions through the new system can provide the most assurance over the completeness and accuracy of loan application processing, by comparing the results and outputs of the new system with those of the old system, and verifying whether they match or differ. This can help identify and resolve any errors or issues that may arise from the new system, such as data conversion, functionality, compatibility, etc. Comparing code between old and new systems is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. Code is a set of instructions or commands that define how a system operates or functions. Comparing code between old and new systems can provide some assurance over the completeness and accuracy of loan application processing, by checking whether the logic, algorithms, or functions of the new system are consistent or equivalent with those of the old system. However, this may not be sufficient or reliable, as code may not reflect the actual performance or outcomes of the system, and may not detect any errors or issues that may occur at the data or user level. Reviewing quality assurance (QA) procedures is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. QA procedures are steps or activities that ensure that a system meets its quality standards and requirements, such as testing, verification, validation, etc. Reviewing QA procedures can provide some assurance over the completeness and accuracy of loan application processing, by evaluating whether the new system has been properly tested and verified before implementation. However, this may not be adequate or accurate, as QA procedures may not cover all aspects or scenarios of loan application processing, and may not reveal any errors or issues that may arise after implementation. Loading balance and transaction data to the new system is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. Balance and transaction data are data that reflect the status and history of loan applications in a system, such as amounts, dates, payments, etc. Loading balance and transaction data to the new system can provide some assurance over the completeness and accuracy of loan application processing, by transferring data from the old system to the new system and ensuring that they are consistent and correct. However, this may not be enough or valid, as balance and transaction data may not represent all aspects or features of loan application processing, and may not indicate any errors or issues that may arise

NEW QUESTION 134
- (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

Explanation:
Discovery sampling is an appropriate sampling method for an IS auditor who intends to launch an intensive investigation if one exception is found. Discovery sampling is a type of attribute sampling that determines the sample size based on an acceptable risk of not finding at least one occurrence of an attribute when a given rate of occurrence exists in a population. Discovery sampling can be used by an IS auditor who wants to detect fraud or errors that have a low probability but high impact on an audit objective. The other options are not appropriate sampling methods for this purpose, as they may involve judgmental sampling, variable sampling, or stratified sampling. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.31
? CISA Review Questions, Answers & Explanations Database, Question ID 230

NEW QUESTION 139
- (Topic 2)
An information systems security officer's PRIMARY responsibility for business process applications is to:

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

Answer: C

Explanation:
Ensuring access rules agree with policies is an information systems security officer’s primary responsibility for business process applications. An information systems security officer should verify that the access controls implemented for the business process applications are consistent with the organization’s security policy and objectives. The other options are not the primary responsibility of an information systems security officer, but rather the tasks of an application owner, a senior management, or a business analyst. References:
? CISA Review Manual (Digital Version), Chapter 7, Section 7.3.11
? CISA Review Questions, Answers & Explanations Database, Question ID 208

NEW QUESTION 142
- (Topic 2)
Which of the following would BEST manage the risk of changes in requirements after the analysis phase of a business application development project?

A. Expected deliverables meeting project deadlines
B. Sign-off from the IT team
C. Ongoing participation by relevant stakeholders
D. Quality assurance (OA) review

Answer: B

NEW QUESTION 145
- (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

Explanation:
Clustering is a technique that allows multiple servers to work together as a single system, providing high availability, load balancing, and fault tolerance. Clustering can limit the potential impact of server failures in a distributed environment, as it can automatically switch the workload to another server in the cluster if one server fails, without interrupting the service. Redundant pathways, failover power, and parallel testing are also useful for improving the reliability and availability of servers, but they do not directly address the issue of server failures.

NEW QUESTION 146
- (Topic 2)
Which of the following findings should be of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simu-lation test administered for staff members?

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

Answer: A

Explanation:
The IS auditor should be most concerned about the lack of follow-up education for staff members who failed the phishing simulation test. Phishing simulation tests are designed to assess the level of awareness and susceptibility of staff members to phishing attacks, and to provide feedback and training to improve their security behavior. If staff members who failed the test do not receive follow-up education, they will not learn from their mistakes and may continue to fall victim to real phishing attacks, which could compromise the security of the organization.
The other options are less concerning for the IS auditor:
? Test results were not communicated to staff members. This is not ideal, as staff members should receive feedback on their performance and learn from the test results. However, this does not necessarily mean that they did not receive any training or education on how to avoid phishing attacks.
? Staff members were not notified about the test beforehand. This is a common practice for phishing simulation tests, as it mimics the real-world scenario where staff members do not know when they will receive a phishing email. The purpose of the test is to measure their spontaneous reaction and awareness, not their preparedness or compliance.
? Security awareness training was not provided prior to the test. This is not a major concern, as the test can serve as a baseline measurement of the current level of awareness and susceptibility of staff members, and as a starting point for providing tailored training and education based on the test results.

NEW QUESTION 150
- (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

Explanation:
The system only allows payments to vendors who are included in the system’s master vendor list is an example of a preventative control in an accounts payable system. A preventative control is a control that aims to prevent errors or irregularities from occurring in the first place. By restricting payments to vendors who are authorized and verified in the master vendor list, the system prevents unauthorized or fraudulent payments from being made. The other options are examples of other types of controls, such as backup (recovery), reconciliation (detective), and communication (directive) controls.
References: CISA Review Manual, 27th Edition, page 223

NEW QUESTION 155
- (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: D

Explanation:
he design of an incident management process should include prioritization criteria to ensure that incidents are handled according to their impact and urgency. Without prioritization criteria, the organization may not be able to allocate resources effectively and respond to incidents in a timely manner. Expected time to resolve incidents, service management standards, and metrics reporting are important aspects of incident management, but they are not as critical as prioritization criteria for the design of the process. References: ISACA Journal Article: Incident Management: A Practical Approach

NEW QUESTION 156
- (Topic 2)
The performance, risks, and capabilities of an IT infrastructure are BEST measured using a:

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

Answer: C

Explanation:
A service level agreement (SLA) is a contract between a service provider and a customer that defines the expected level of performance, risks, and capabilities of an IT infrastructure. An IS auditor can use an SLA to measure how well the IT infrastructure meets the business needs and objectives, as well as to identify any gaps or issues that need to be addressed. The other options are not directly related to measuring the performance, risks, and capabilities of an IT infrastructure.
References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.2.11
? CISA Review Questions, Answers & Explanations Database, Question ID 203

NEW QUESTION 157
- (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

Explanation:
Root cause is the most important thing for an IS auditor to determine and understand to develop meaningful recommendations for findings. A root cause is the underlying factor or condition that leads to a problem or issue. A finding is a statement that describes a problem or issue identified during an audit. A recommendation is a suggestion or advice that aims to address or resolve a finding. To develop meaningful recommendations for findings, an IS auditor should determine and understand the root cause of each finding, as this can help to identify the most effective and appropriate actions to prevent or correct the problem or issue. The other options are not as important as determining and understanding the root cause, as they do not directly address or resolve the finding. References: CISA Review Manual, 27th Edition, page 434

NEW QUESTION 162
- (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 163
- (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

Explanation:
The most important task for an IS auditor to perform after the merger of two organizations is to verify that access privileges have been reviewed. Access privileges are the permissions granted to users, groups, or roles to access, modify, or manage IT resources, such as systems, applications, data, or networks. After a merger, the IS auditor should ensure that the access privileges of both organizations are aligned with the new business objectives, policies, and processes, and that there are no conflicts, overlaps, or gaps in the access rights. The IS auditor should also verify that the access privileges are based on the principle of least privilege, which means that users are granted only the minimum level of access required to perform their tasks.
The other options are not as important as verifying that access privileges have been reviewed:
? Investigating access rights for expiration dates is a useful task, but it is not the most important one. Expiration dates are the dates when access rights are automatically revoked or suspended after a certain period of time or after a specific event. The IS auditor should check that the expiration dates are set appropriately and enforced consistently, but this is not as critical as reviewing the access privileges themselves.
? Updating the continuity plan for critical resources is a necessary task, but it is not the most urgent one. A continuity plan is a document that outlines the procedures and actions to be taken in the event of a disruption or disaster that affects the availability of IT resources. The IS auditor should update the continuity plan to reflect the changes and dependencies introduced by the merger, but this can be done after verifying that the access privileges are secure and compliant.
? Updating the security policy is an essential task, but it is not the most immediate one. A security policy is a document that defines the rules and guidelines for securing IT resources and protecting information assets. The IS auditor should update the security policy to incorporate the best practices and standards of both organizations, and to address any new risks or threats posed by the merger, but this can be done after verifying that the access privileges are aligned with the policy.

NEW QUESTION 166
- (Topic 2)
During the implementation of a new system, an IS auditor must assess whether certain automated calculations comply with the regulatory requirements Which of the following is the BEST way to obtain this assurance?

A. Review sign-off documentation
B. Review the source code related to the calculation
C. Re-perform the calculation with audit software
D. Inspect user acceptance lest (UAT) results

Answer: C

Explanation:
The best way to obtain assurance that certain automated calculations comply with the regulatory requirements is to re-perform the calculation with audit software. This will allow the auditor to independently verify the accuracy and validity of the calculation and compare it with the expected results. Reviewing sign-off documentation, source code, or user acceptance test results may not provide sufficient evidence or assurance that the calculation is correct and compliant.
References:
? CISA Review Manual (Digital Version), page 325
? CISA Questions, Answers & Explanations Database, question ID 3335

NEW QUESTION 171
- (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

Explanation:
The best way to ensure payment transaction data is restricted to the appropriate users is implementing role-based access at the application level. Role-based access is a method of access control that assigns permissions or privileges to users based on their roles or functions within an organization or system. Role-based access can help ensure that payment transaction data is restricted to the appropriate users, by allowing only authorized users who have a legitimate need or purpose to access or use the payment transaction data, and preventing unauthorized or unnecessary access or use by other users. Implementing two-factor authentication is a possible way to enhance the security and verification of user identities, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not define what permissions or privileges users have on the payment transaction data. Restricting access to transactions using network security software is a possible way to protect the network communication and transmission of payment transaction data, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not specify what actions or operations users can perform on the payment transaction data. Using a single menu for sensitive application transactions is a possible way to simplify the user interface and navigation of payment transaction data, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not limit what users can access or use the payment transaction data.

NEW QUESTION 172
- (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

Explanation:
The IS auditor’s primary concern when auditing the proposed acquisition of new computer hardware is that a clear business case has been established. A business case is a document that justifies the need, feasibility, and benefits of a proposed project or investment. A clear business case can help to ensure that the acquisition of new computer hardware is aligned with the organization’s goals, objectives, and requirements, and that it provides value for money and return on investment. The other options are not as important as establishing a clear business case, as they do not address the rationale or justification for acquiring new computer hardware. References: CISA Review Manual, 27th Edition, page 467

NEW QUESTION 177
- (Topic 2)
Which of the following will MOST likely compromise the control provided By a digital signature created using RSA encryption?

A. Reversing the hash function using the digest
B. Altering the plaintext message
C. Deciphering the receiver's public key
D. Obtaining the sender's private key

Answer: D

Explanation:
A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document, by using a hash function and an asymmetric encryption algorithm. A hash function is a mathematical function that transforms any input data into a fixed-length output value called a digest, which is unique for each input. An asymmetric encryption algorithm uses two keys: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret by the owner. To create a digital signature, the sender first applies a hash function to the plaintext message to generate a digest. Then, the sender encrypts the digest with their private key to produce the digital signature. To verify the digital signature, the receiver decrypts the digital signature with the sender’s public key to obtain the digest. Then, the receiver applies the same hash function to the plaintext message to generate another digest. If the two digests match, it means that the message has not been altered and that it came from the sender. The security of a digital signature depends on the secrecy of the sender’s private key. If an attacker obtains the sender’s private key, they can create fake digital signatures for any message they want, thus compromising the control provided by the digital signature. Reversing the hash function using the digest is not possible, as hash functions are designed to be one-way functions that cannot be inverted. Altering the plaintext message will result in a different digest after applying the hash function, which will not match with the decrypted digest from the digital signature, thus invalidating the digital signature. Deciphering the receiver’s public key is not relevant, as public keys are meant to be publicly

available and do not affect the security of digital signatures.

NEW QUESTION 181
- (Topic 2)
Which of the following BEST demonstrates that IT strategy Is aligned with organizational goals and objectives?

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

Answer: C

Explanation:
Business stakeholders being involved in approving the IT strategy best demonstrates that IT strategy is aligned with organizational goals and objectives. IT strategy is a plan that defines how IT resources and capabilities will support and enable the achievement of business goals and objectives. Business stakeholders are the individuals or groups who have an interest or influence in the organization's activities and outcomes. By involving business stakeholders in approving the IT strategy, the organization can ensure that the IT strategy reflects and supports the business needs, expectations, and priorities. The other options do not necessarily indicate that IT strategy is aligned with organizational goals and objectives, as they do not involve the participation or feedback of business stakeholders. References: CISA Review Manual, 27th Edition, page 97

NEW QUESTION 186
- (Topic 2)
Which of the following is the MOST important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

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

Answer: B

Explanation:
The most important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings is the remediation dates included in management responses. The IS auditor should ensure that the follow-up activities are aligned with the agreed-upon action plans and deadlines that management has committed to in response to the audit findings. The follow-up activities should verify that management has implemented the corrective actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.
The other options are less important factors for establishing timeframes for follow-up activities:
? Availability of IS audit resources. This is a practical factor that may affect the scheduling and execution of follow-up activities, but it should not override the priority and urgency of verifying management's corrective actions.
? Peak activity periods for the business. This is a factor that may affect the availability and cooperation of auditees during follow-up activities, but it should not delay or postpone the verification of management's corrective actions beyond reasonable limits.
? Complexity of business processes identified in the audit. This is a factor that may affect the scope and depth of follow-up activities, but it should not affect the timeframe for verifying management's corrective actions.

NEW QUESTION 190
- (Topic 2)
Which of the following would provide the MOST important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program?

A. Findings from prior audits
B. Results of a risk assessment
C. An inventory of personal devices to be connected to the corporate network
D. Policies including BYOD acceptable user statements

Answer: D

Explanation:
The most important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program is policies including BYOD acceptable user statements. Policies are documents that define the organization's objectives, requirements, expectations, and responsibilities regarding a specific topic or area. BYOD policies should include acceptable user statements that specify what types of personal devices are allowed to connect to the corporate network, what security measures must be implemented on those devices, what data can be accessed or stored on those devices, what actions must be taken in case of device loss or theft, and what consequences will apply for non-compliance. Policies including BYOD acceptable user statements can provide an IS auditor with a clear understanding of the scope, criteria, and objectives of the BYOD program audit. Findings from prior audits, results of a risk assessment, and an inventory of personal devices to be connected to the corporate network are also useful inputs for planning a BYOD program audit, but they are not as important as policies including BYOD acceptable user statements. References: ISACA CISA Review Manual 27th Edition, page 381.

NEW QUESTION 194
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

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

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