Exam Questions CISA

Isaca CISA

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

NEW QUESTION 1
- (Topic 3)
Which of the following is MOST important for an IS auditor to look for in a project feasibility study?

A. An assessment of whether requirements will be fully met
B. An assessment indicating security controls will operate effectively
C. An assessment of whether the expected benefits can be achieved
D. An assessment indicating the benefits will exceed the implement

Answer: C

Explanation:
The most important thing for an IS auditor to look for in a project feasibility study is an assessment of whether the expected benefits can be achieved. A project feasibility study is a preliminary analysis that evaluates the viability and suitability of a proposed project based on various criteria, such as technical, economic, legal, operational, and social factors. The expected benefits are the positive outcomes and value that the project aims to deliver to the organization and its stakeholders. The IS auditor should verify whether the project feasibility study has clearly defined and quantified the expected benefits, and whether it has assessed the likelihood and feasibility of achieving them within the project scope, budget, schedule, and quality parameters. The other options are also important for an IS auditor to look for in a project feasibility study, but not as important as an assessment of whether the expected benefits can be achieved, because they either focus on specific aspects of the project rather than the overall value proposition, or they assume that the project will be implemented rather than evaluating its viability. References:
CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.1

NEW QUESTION 2
- (Topic 3)
Which of the following would an IS auditor recommend as the MOST effective preventive control to reduce the risk of data leakage?

A. Ensure that paper documents arc disposed security.
B. Implement an intrusion detection system (IDS).
C. Verify that application logs capture any changes made.
D. Validate that all data files contain digital watermarks

Answer: D

Explanation:
Digital watermarks are hidden marks or codes that can be embedded into digital files, such as images, videos, audio, or documents. They can be used to identify the source, owner, or authorized user of the data, as well as to track any unauthorized copying or distribution of the data. Digital watermarks can help prevent data leakage by deterring potential leakers from sharing sensitive data or by providing evidence of data leakage if it occurs.
The other options are not as effective as digital watermarks in preventing data leakage. Ensuring that paper documents are disposed securely can reduce the risk of physical data leakage, but it does not address the digital data leakage that is more prevalent in today's environment. Implementing an intrusion detection system (IDS) can help detect and respond to cyberattacks that may cause data leakage, but it does not prevent data leakage from insiders or authorized users who have legitimate access to the data. Verifying that application logs capture any changes made can help audit and investigate data leakage incidents, but it does not prevent them from happening in the first place.
References:
? What is Data Leakage?
? What is Digital Watermarking?

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

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

Answer: B

Explanation:
The IS auditor's primary focus when evaluating an organization's offsite storage facility should be the adequacy of physical and environmental controls. Physical and environmental controls are essential to protect the offsite storage facility from unauthorized access, theft, fire, water damage, pests or other hazards that could compromise the integrity and availability of backup media. Shared facilities is something that the IS auditor should consider when evaluating the offsite storage facility, but it is not the primary focus. Results of business continuity plan (BCP) test or retention policy and period are things that the IS auditor should review when evaluating the organization's BCP or backup strategy, not the offsite storage facility itself. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 388

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)
An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

A. Increasing the frequency of risk-based IS audits for each business entity
B. Developing a risk-based plan considering each entity's business processes
C. Conducting an audit of newly introduced IT policies and procedures
D. Revising IS audit plans to focus on IT changes introduced after the split

Answer: B

Explanation:
Developing a risk-based plan considering each entity's business processes would best help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan. A risk-based plan is a plan that prioritizes the audit activities based on the level of risk associated with each area or process. A risk-based plan can help to allocate the audit resources more efficiently and effectively, and provide more assurance and value to the stakeholders1. By considering each entity's business processes, the IS audit can identify and assess the specific risks and controls that affect the IT environment of each entity, and tailor the audit objectives, scope, and procedures accordingly. This can help to address the unique needs and expectations of each entity, and ensure that the IS audit covers the key risk areas that are relevant and significant to each entity's operations, performance, and compliance2.
The other options are not as effective as developing a risk-based plan considering each entity's business processes in ensuring that IS audit still covers key risk areas within the IT environment as part of its annual plan. Option A, increasing the frequency of risk-based IS audits for each business entity, is not a feasible or efficient solution, as it may increase the audit costs and workload, and create duplication or overlap of audit efforts. Option C, conducting an audit of newly introduced IT policies and procedures, is a limited and narrow approach, as it may not cover all the aspects or dimensions of the IT environment that may have changed or been affected by the split. Option D, revising IS audit plans to focus on IT changes introduced after the split, is a reactive and short-term approach, as it may not reflect the current or future state of the IT environment or the business objectives of each entity.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Risk-Based Audit Planning: A Guide for Internal Audit1
? Risk-Based Audit Approach: Definition & Example

NEW QUESTION 7
- (Topic 3)
An organization is disposing of a system containing sensitive data and has deleted all files from the hard disk. An IS auditor should be concerned because:

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

Answer: B

Explanation:
An IS auditor should be concerned because deleting the files logically does not overwrite the files' physical data. Deleting a file from a hard disk only removes the reference or pointer to the file from the file system, but does not erase the actual data stored on the disk sectors. The deleted data can still be recovered using special tools or techniques until it is overwritten by new data. This poses a risk of data leakage, theft, or misuse if the hard disk falls into the wrong hands. To securely dispose of a system containing sensitive data, the hard disk should be wiped or sanitized using methods that overwrite or destroy the physical data beyond recovery. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 8
- (Topic 3)
The PRIMARY benefit of information asset classification is that it:

A. prevents loss of assets.
B. helps to align organizational objectives.
C. facilitates budgeting accuracy.
D. enables risk management decisions.

Answer: D

Explanation:
The primary benefit of information asset classification is that it enables risk management decisions. Information asset classification helps to identify the value, sensitivity and criticality of information assets, and to determine the appropriate level of protection and controls required for them. This facilitates risk assessment and risk treatment processes, and ensures that information assets are aligned with business objectives and regulatory requirements. Preventing loss of assets, helping to align organizational objectives or facilitating budgeting accuracy are secondary benefits of information asset classification, but not the main purpose. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 300

NEW QUESTION 9
- (Topic 3)
An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's BEST recommendation should be to:

A. reclassify the data to a lower level of confidentiality
B. require the business owner to conduct regular access reviews.
C. implement a strong password schema for users.
D. recommend corrective actions to be taken by the security administrator.

Answer: B

Explanation:
The best recommendation for an IS auditor who finds that one employee has unauthorized access to confidential data is to require the business owner to conduct regular access reviews. Access reviews are periodic assessments of user access rights and permissions to ensure that they are appropriate, necessary, and aligned with the business needs and objectives. Access reviews help to identify and remediate any unauthorized, excessive, or obsolete access that could pose a security risk or violate compliance requirements. The business owner is responsible for defining and approving the access requirements for their data and ensuring that they are enforced and monitored. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

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 10
- (Topic 3)
Which of the following is MOST critical for the effective implementation of IT governance?

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

Answer: C

Explanation:
The most critical factor for the effective implementation of IT governance is a supportive corporate culture. A supportive corporate culture is one that fosters

collaboration, communication and commitment among all stakeholders involved in IT governance processes. A supportive corporate culture also promotes a shared vision, values and goals for IT governance across the organization. Strong risk management practices, internal auditor commitment or documented policies are important elements for IT governance implementation, but they are not sufficient without a supportive corporate culture. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 41

NEW QUESTION 15
- (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 20
- (Topic 3)
Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

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

Answer: B

Explanation:
The best way to ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure is to use a database management system (DBMS) to dynamically back-out partially processed transactions. A DBMS is a software system that manages the creation, manipulation, retrieval, and security of data stored in a database. A DBMS can provide features such as transaction management, concurrency control, recovery management, and integrity management. A DBMS can dynamically back-out partially processed transactions by using mechanisms such as rollback segments, undo logs, or write-ahead logs. These mechanisms allow the DBMS to restore the database to a consistent state before the failure occurred.
References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 21
- (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 22
- (Topic 3)
Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA> to automate routine business tasks?

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

Answer: A

Explanation:
The most important thing for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks is that the end-to-end process is understood and documented. This is because RPA involves the use of software robots or digital workers to mimic human actions and execute predefined rules and workflows. Therefore, it is essential that the IS auditor verifies that the organization has a clear and accurate understanding of the current state of the process, the desired state of the process, the inputs and outputs, the exceptions and errors, the roles and responsibilities, and the performance measures12. Without a proper documentation of the end-to-end process, the organization may face challenges in designing, developing, testing, deploying, and monitoring the RPA solution3. References:
1: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support, page 211 2: CISA Online Review Course, Module 4: Information Systems Operations and Business
Resilience, Lesson 4.2: IT Service Delivery and Support 3: ISACA Journal Volume 5, 2019, Article: Robotic Process Automation: Benefits, Risks and Controls

NEW QUESTION 23
- (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 28
- (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 29
- (Topic 3)
Which of the following presents the GREATEST challenge to the alignment of business and IT?

A. Lack of chief information officer (CIO) involvement in board meetings
B. Insufficient IT budget to execute new business projects
C. Lack of information security involvement in business strategy development
D. An IT steering committee chaired by the chief information officer (CIO)

Answer: A

Explanation:
The greatest challenge to the alignment of business and IT is the lack of chief information officer (CIO) involvement in board meetings. The CIO is the senior executive responsible for overseeing the IT strategy, governance, and operations of the organization, and ensuring that they support the business objectives and needs. The CIO should be involved in board meetings to communicate the value and contribution of IT to the organization, to align the IT vision and direction with the business strategy and priorities, and to advocate for the IT resources and investments required to achieve the desired outcomes. The lack of CIO involvement in board meetings can result in a disconnect between business and IT, a loss of trust and confidence in IT, and missed
opportunities for innovation and value creation. The other options are not as challenging as the lack of CIO involvement in board meetings, because they either do not affect the strategic alignment of business and IT, or they can be addressed by other means such as collaboration, negotiation, or escalation. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

NEW QUESTION 32
- (Topic 3)
Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

A. Review of program documentation
B. Use of test transactions
C. Interviews with knowledgeable users
D. Review of source code

Answer: B

Explanation:
The most conclusive audit procedure for evaluating the effectiveness of an e- commerce application system’s edit routine is to use test transactions. A test transaction is a simulated input that is processed by the system to verify its output and performance1. By using test transactions, an auditor can directly observe how the edit routine checks the validity, accuracy, and completeness of data entered by users, and how it handles incorrect or invalid data. A test transaction can also help measure the efficiency, reliability, and security of the edit routine, as well as identify any errors or weaknesses in the system.
The other options are not as conclusive as using test transactions, as they rely on indirect or secondary sources of information. Reviewing program documentation is an audit procedure that involves examining the written description of the system’s design, specifications, and functionality2. However, program documentation may not reflect the actual implementation or operation of the system, and it may not reveal any discrepancies or defects in the edit routine. Interviews with knowledgeable users is an audit procedure that involves asking questions to the people who use or manage the system3. However, interviews with knowledgeable users may not provide sufficient or objective evidence of the edit routine’s effectiveness, and they may be influenced by personal opinions or
biases. Reviewing source code is an audit procedure that involves analyzing the programming language and logic of the system4. However, reviewing source code may not be feasible or practical for complex or large systems, and it may not demonstrate how the edit routine performs in real scenarios.

NEW QUESTION 33
- (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 38
- (Topic 3)
Which of the following is the BEST way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC)?

A. Have an independent party review the source calculations
B. Execute copies of EUC programs out of a secure library
C. implement complex password controls
D. Verify EUC results through manual calculations

Answer: B

Explanation:
The best way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC) is to execute copies of EUC programs out of a secure library. This will ensure that the original EUC programs are protected from unauthorized changes and that the copies are run in a controlled environment. A secure library is a repository of EUC programs that have been tested, validated, and approved by the appropriate authority. Executing copies of EUC programs out of a secure library can also help with version control, backup, and recovery of EUC programs. Having an independent party review

the source calculations, implementing complex password controls, and verifying EUC results through manual calculations are not as effective as executing copies of EUC programs out of a secure library, as they do not prevent or detect unintentional modifications of complex calculations in EUC. References:
End-User Computing (EUC) Risks: A Comprehensive Guide, End User Computing (EUC) Risk Management

NEW QUESTION 43
- (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)
Which of the following would be MOST useful when analyzing computer performance?

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

Answer: A

Explanation:
Computer performance is the measure of how well a computer system can execute tasks and applications within a given time frame. Computer performance can be affected by various factors, such as hardware specifications, software configuration, network conditions, and user behavior. To analyze computer performance, it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.
The other options are not as useful as statistical metrics when analyzing computer performance. An operations report of user dissatisfaction with response time is a subjective measure that may not reflect the actual performance of the system. Tuning of system software to optimize resource usage is a corrective action that can improve performance, but it is not a method of analysis. A report of off-peak utilization and response time is a limited snapshot that may not capture the peak performance or the average performance of the system.
References:
? What is Computer Performance?
? How to Measure Computer Performance

NEW QUESTION 50
- (Topic 3)
An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider MOST critical?

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

Answer: A

Explanation:
The most critical finding that the IS auditor should consider when reviewing processes for importing market price data from external data providers is that the quality of the data is not monitored. This is because market price data is essential for financial transactions, risk management, valuation and reporting, and any

errors or inaccuracies in the data can have significant impact on the organization's performance, reputation and compliance. The IS auditor should ensure that the organization has established quality criteria and controls for the imported data, such as validity, completeness, timeliness, consistency and accuracy, and that the data is regularly checked and verified against these criteria. The other findings are also important, but not as critical as data quality. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

NEW QUESTION 51
- (Topic 3)
Which of the following is MOST important when planning a network audit?

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

Answer: D

Explanation:
The most important factor when planning a network audit is to identify the existing nodes on the network. Nodes are devices or systems that are connected to the network and can communicate with each other. Nodes can include servers, workstations, routers, switches, firewalls, printers, scanners, cameras, etc. Identifying the existing nodes on the network will help the auditor to determine the scope, objectives, and methodology of the audit. It will also help the auditor to assess the network topology, architecture, performance, security, and compliance. 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 58
- (Topic 2)
Which of the following is the MOST important reason to classify a disaster recovery plan (DRP) as confidential?

A. Ensure compliance with the data classification policy.
B. Protect the plan from unauthorized alteration.
C. Comply with business continuity best practice.
D. Reduce the risk of data leakage that could lead to an attack.

Answer: D

Explanation:
The most important reason to classify a disaster recovery plan (DRP) as confidential is to reduce the risk of data leakage that could lead to an attack. A DRP contains sensitive information about the organization's IT infrastructure, systems, processes, and procedures for recovering from a disaster. If this information falls into the wrong hands, it could be exploited by malicious actors to launch targeted attacks, sabotage recovery efforts, or extort ransom. Therefore, a DRP should be protected from unauthorized access, disclosure, modification, or destruction.
The other options are not as important as reducing the risk of data leakage that could lead to an attack:
? Ensuring compliance with the data classification policy is a good practice, but it is not a sufficient reason to classify a DRP as confidential. The data classification policy should reflect the level of risk and impact associated with each type of data, and a DRP should be classified as confidential based on its potential harm if compromised.
? Protecting the plan from unauthorized alteration is a valid concern, but it is not a primary reason to classify a DRP as confidential. A DRP should be protected from unauthorized alteration by implementing access controls, audit trails, version control, and change management processes. Classifying a DRP as confidential may deter some unauthorized alterations, but it does not prevent them.
? Complying with business continuity best practice is a desirable goal, but it is not a compelling reason to classify a DRP as confidential. Business continuity best practice may recommend classifying a DRP as confidential, but it does not mandate it. The decision to classify a DRP as confidential should be based on a risk assessment and a cost-benefit analysis.

NEW QUESTION 59
- (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 64
- (Topic 2)
An IS auditor is conducting a review of a data center. Which of the following observations could indicate an access control Issue?

A. Security cameras deployed outside main entrance
B. Antistatic mats deployed at the computer room entrance
C. Muddy footprints directly inside the emergency exit
D. Fencing around facility is two meters high

Answer: C

Explanation:
An IS auditor is conducting a review of a data center. An observation that could indicate an access control issue is muddy footprints directly inside the emergency exit. Access control is a process that ensures that only authorized entities or individuals can access or use an information system or resource, and prevents unauthorized access or use. Access control can be implemented using various methods or mechanisms, such as physical, logical, administrative, etc. Muddy footprints directly inside the emergency exit could indicate an access control issue, as they could suggest that someone has entered the data center through the emergency exit without proper authorization or authentication, and potentially compromised the security or integrity of the data center. Security cameras deployed outside main entrance is not an observation that could indicate an access control issue, but rather a control that could enhance access control, as security cameras are devices that capture and record video footage of the surroundings, and can help monitor and deter unauthorized access or activity. Antistatic mats deployed at the computer room entrance is not an observation that could indicate an access control issue, but rather a control that could prevent static electricity damage, as antistatic mats are devices that dissipate or reduce static charges from people or objects, and can help protect electronic equipment from electrostatic discharge (ESD). Fencing around facility is two meters high is not an observation that could indicate an access control issue, but rather a control that could improve physical security, as fencing is a barrier that encloses or surrounds an area, and can help prevent unauthorized entry or intrusion.

NEW QUESTION 65
- (Topic 2)
An IS auditor is reviewing an organization's primary router access control list. Which of the following should result in a finding?

A. There are conflicting permit and deny rules for the IT group.
B. The network security group can change network address translation (NAT).
C. Individual permissions are overriding group permissions.
D. There is only one rule per group with access privileges.

Answer: C

Explanation:
This should result in a finding because it violates the best practice of setting rules for groups rather than users. According to one of the web search results1, using group permissions instead of individual permissions can simplify the management and maintenance of ACLs, reduce the risk of human errors, and ensure consistency and compliance. Individual permissions can create conflicts, confusion, and security gaps in the ACLs. Therefore, the IS auditor should report this as a finding and recommend using group permissions instead.

NEW QUESTION 67
- (Topic 2)
An organization has recently implemented a Voice-over IP (VoIP) communication system. Which ot the following should be the IS auditor's PRIMARY concern?

A. A single point of failure for both voice and data communications
B. Inability to use virtual private networks (VPNs) for internal traffic
C. Lack of integration of voice and data communications
D. Voice quality degradation due to packet toss

Answer: A

Explanation:
The IS auditor’s primary concern when an organization has recently implemented a Voice-over IP (VoIP) communication system is a single point of failure for both voice and data communications. VoIP is a technology that allows voice communication over IP networks such as the internet. VoIP can offer benefits such as lower costs, higher flexibility, and better integration with other applications. However, VoIP also introduces risks such as dependency on network availability, performance, and security. If both voice and data communications share the same network infrastructure and devices, then a single point of failure can affect both services simultaneously and cause significant disruption to business operations. Therefore, the IS auditor should evaluate the availability and redundancy of the network components and devices that support VoIP communication. The other options are not as critical as a single point of failure for both voice and data communications, as they do not pose a direct threat to business continuity. References: CISA Review Manual, 27th Edition, page 385

NEW QUESTION 70
- (Topic 2)
Which of the following is the BEST indicator of the effectiveness of an organization's incident response program?

A. Number of successful penetration tests

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

Answer: C

Explanation:
The best indicator of the effectiveness of an organization's incident response program is the financial impact per security event. This metric measures the direct and indirect costs associated with security incidents, such as loss of revenue, reputation damage, legal fees, recovery expenses, and fines. By reducing the financial impact per security event, the organization can demonstrate that its incident response program is effective in mitigating the consequences of security breaches and restoring normal operations as quickly as possible. Number of successful penetration tests, percentage of protected business applications, and number of security vulnerability patches are indicators of the security posture of the organization, but they do not reflect the effectiveness of the incident response program. References: ISACA Journal Article: Measuring Incident Response Effectiveness

NEW QUESTION 75
- (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 79
- (Topic 2)
Due to limited storage capacity, an organization has decided to reduce the actual retention period for media containing completed low-value transactions. Which of the following is MOST important for the organization to ensure?

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

Answer: C

Explanation:
The most important factor for the organization to ensure when reducing the retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for defining the retention and disposal requirements for the data under their custody, based on business, legal, regulatory, and contractual obligations. The policy should reflect the data owner's decisions and obtain their approval. The policy should also include a risk-based approach, but this is not as important as complying with data owner responsibilities. The retention period should allow for review during the year-end audit, but this may not be necessary for low-value transactions that have minimal impact on financial reporting. The total transaction amount may have some impact on financial reporting, but this is not a direct consequence of reducing the retention period. References:
? CISA Review Manual, 27th Edition, pages 414-4151
? CISA Review Questions, Answers & Explanations Database, Question ID: 255

NEW QUESTION 81
- (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 82
- (Topic 2)
Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?

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

Answer: A

Explanation:
Ensuring that the facts presented in the report are correct is the most important thing for an IS auditor to do during an exit meeting with an auditee. An IS auditor should confirm that the audit findings and observations are accurate, complete, and supported by sufficient evidence, as well as that the auditee understands and agrees with them. This will help to avoid any misunderstandings or disputes later on, as well as to enhance the credibility and quality of the audit report. The other options are less important things for an IS auditor to do during an exit meeting, as they may involve communicating the recommendations to senior management, specifying implementation dates for the recommendations, or requesting input in determining corrective action. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.21
? CISA Review Questions, Answers & Explanations Database, Question ID 222

NEW QUESTION 87
- (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 88
- (Topic 2)
An IS auditor Is reviewing a recent security incident and is seeking information about me approval of a recent modification to a database system's security settings Where would the auditor MOST likely find this information?

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

Answer: C

Explanation:
A change log is a record of all changes made to a system or application, including the date, time, description, and approval of each change. A change log can help an IS auditor to trace the source and authorization of a modification to a system’s security settings. A system event correlation report is a tool that analyzes data from multiple sources to identify patterns and anomalies that indicate potential security incidents. A database log is a record of all transactions and activities performed on a database, such as queries, updates, and backups. A security incident and event management (SIEM) report is a tool that collects, analyzes, and reports on data from various sources to detect and respond to security incidents.

NEW QUESTION 90
- (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 91
- (Topic 2)
Which of the following is MOST important for an IS auditor to verify when evaluating an organization's firewall?

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

Answer: A

Explanation:
A firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A firewall can help protect an organization's network and information systems from unauthorized or malicious access, by filtering or blocking unwanted or harmful packets. The most important thing for an IS auditor to verify when evaluating an organization's firewall is that the logs are being collected in a separate protected host. Logs are records of events or activities that occur on a system or network, such as connections, requests, responses, errors, and alerts. Logs can provide valuable information for auditing, monitoring, troubleshooting, and investigating security incidents. However, logs can also be tampered with, deleted, or corrupted by attackers or insiders who want to hide their tracks or evidence of their actions. Therefore, it is essential that logs are stored in a separate host that is isolated and secured from the network and the firewall itself, to prevent unauthorized access or modification of the logs. Automated alerts are being sent when a risk is detected is a good practice for enhancing the security and efficiency of a firewall, but it is not the most important thing for an IS auditor to verify, as alerts may not always be accurate, timely, or actionable. Insider attacks are being controlled is a desirable outcome for a firewall, but it is not the most important thing for an IS auditor to verify, as insider attacks may involve other factors or methods that bypass or compromise the firewall, such as social engineering, credential theft, or physical access. Access to configuration files is restricted is a critical control for ensuring the security and integrity of a firewall, but it is not the most important thing for an IS auditor to verify, as configuration files may not reflect the actual state or performance of the firewall.

NEW QUESTION 94
- (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 97
- (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 98
- (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 100
- (Topic 2)
During a follow-up audit, it was found that a complex security vulnerability of low risk was not resolved within the agreed-upon timeframe. IT has stated that the system with the identified vulnerability is being replaced and is expected to be fully functional in two months Which of the following is the BEST course of action?

A. Require documentation that the finding will be addressed within the new system
B. Schedule a meeting to discuss the issue with senior management
C. Perform an ad hoc audit to determine if the vulnerability has been exploited
D. Recommend the finding be resolved prior to implementing the new system

Answer: A

Explanation:
Requiring documentation that the finding will be addressed within the new system is the best course of action for a follow-up audit. An IS auditor should obtain evidence that the complex security vulnerability of low risk will be resolved in the new system and that there is a reasonable timeline for its implementation. The other options are not appropriate courses of action, as they may be too costly, time-consuming, or impractical for a low-risk finding. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31
? CISA Review Questions, Answers & Explanations Database, Question ID 209

NEW QUESTION 102
- (Topic 2)
Which of the following is a social engineering attack method?

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

Answer: A

Explanation:
Social engineering is a technique that exploits human weaknesses, such as trust, curiosity, or greed, to obtain information or access from a target. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone is an example of a social engineering attack method, as it involves manipulating the employee into divulging sensitive information that can be used to compromise the network or system. A hacker walks around an office building using scanning tools to search for a wireless network to gain access, an intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties, and an unauthorized person attempts to gain access to secure premises by following an authorized person through a secure door are not examples of social engineering attack methods, as they do not involve human interaction or deception. References: [ISACA CISA Review Manual 27th Edition], page 361.

NEW QUESTION 104
- (Topic 2)
Which of the following is the GREATEST risk associated with storing customer data on a web server?

A. Data availability
B. Data confidentiality
C. Data integrity
D. Data redundancy

Answer: B

Explanation:
The greatest risk associated with storing customer data on a web server is data confidentiality. Data confidentiality is the property that ensures that data are accessible only to authorized entities or individuals, and protected from unauthorized disclosure or exposure. Storing customer data on a web server poses a high risk to data confidentiality, as web servers are exposed to the internet and may be vulnerable to various types of attacks or breaches that can compromise the security and privacy of customer data, such as hacking, phishing, malware, denial of service (DoS), etc. Customer data may contain sensitive or personal information that can cause harm or damage to customers or the organization if disclosed or exposed, such as identity theft, fraud, reputation loss, legal liability, etc. Data availability is the property that ensures that data are accessible and usable by authorized entities or individuals when needed. Data availability is a risk associated with storing customer data on a web server, as web servers may experience failures or disruptions that can affect the accessibility and usability of customer data, such as hardware faults, network issues, power outages, etc. However, data availability is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data integrity is the property that ensures that data are accurate and consistent, and protected from unauthorized modification or corruption. Data integrity is a risk associated with storing customer data on a web server, as web servers may be subject to attacks or errors that can affect the accuracy and consistency of customer data, such as injection attacks, tampering, replication issues, etc. However, data integrity is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data redundancy is the condition of having duplicate or unnecessary data in a database or system. Data redundancy is not a risk associated with storing customer data on a web server, but rather a result of poor database design or management.

NEW QUESTION 105
- (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 106
- (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 109
- (Topic 2)
An IS auditor concludes that an organization has a quality security policy. Which of the following is MOST important to determine next? The policy must be:

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

Answer: A

Explanation:
The most important thing to determine next after concluding that an organization has a quality security policy is whether the policy is well understood by all employees. A security policy is a document that defines the objectives, scope, roles, responsibilities, and rules for information security within an organization. A quality security policy is one that is clear, concise, consistent, comprehensive, and aligned with business goals and requirements. However, a quality security policy is useless if it is not well understood by all employees who are expected to comply with it. Therefore, the IS auditor should assess the level of awareness and understanding of the security policy among employees and identify any gaps or issues that need to be addressed. The other options are not as important as ensuring that the security policy is well understood by all employees, as they do not directly affect the implementation and effectiveness of the security policy.
References: CISA Review Manual, 27th Edition, page 317

NEW QUESTION 114
- (Topic 2)
In an online application which of the following would provide the MOST information about the transaction audit trail?

A. File layouts
B. Data architecture
C. System/process flowchart
D. Source code documentation

Answer: C

Explanation:
The most information about the transaction audit trail in an online application can be obtained by reviewing the system/process flowchart. A system/process flowchart is a diagram that illustrates the sequence of steps, activities, or events that occur within or affect a system or process. A system/process flowchart can provide the most information about the transaction audit trail in an online application, by showing how transactions are initiated, processed, recorded, and completed, and identifying the inputs, outputs, controls, and dependencies involved in each transaction. File layouts are specifications that define how data are structured or organized on a file or database. File layouts can provide some information about the transaction audit trail in an online application, by showing what

data elements are stored or retrieved for each transaction, but they do not provide information about how transactions are executed or tracked. Data architecture is a framework that defines how data are collected, stored, managed, and used within an organization or system. Data architecture can provide some information about the transaction audit trail in an online application, by showing what data sources, models, standards, and policies are used for each transaction, but they do not provide information about how transactions are performed or monitored. Source code documentation is a description or explanation of the source code of a software program or application. Source code documentation can provide some information about the transaction audit trail in an online application, by showing what logic, algorithms, or functions are used for each transaction, but they do not provide information about how transactions are handled or audited.

NEW QUESTION 118
- (Topic 2)
A third-party consultant is managing the replacement of an accounting system. Which of the following should be the IS auditor's GREATEST concern?

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

Answer: C

Explanation:
The greatest concern for an IS auditor in this scenario is that the user department will manage access rights to the new accounting system. This could pose a significant risk of unauthorized access, segregation of duties violations, data tampering and fraud. The IS auditor should ensure that access rights are defined, approved and monitored by an independent function, such as IT security or internal audit. The other options are not as concerning as option C, as they can be mitigated by other controls or procedures. Data migration is an important part of the system replacement project, but it can be performed by another party or verified by the IS auditor. The timing of the replacement near year-end reporting is a challenge, but it can be managed by proper planning, testing and contingency plans. Testing performed by the third-party consultant is acceptable, as long as it is reviewed and validated by the IS auditor or another independent party.
References: CISA Review Manual (Digital Version) 1, Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.4: System Implementation.

NEW QUESTION 119
- (Topic 2)
An employee loses a mobile device resulting in loss of sensitive corporate data. Which o(the following would have BEST prevented data leakage?

A. Data encryption on the mobile device
B. Complex password policy for mobile devices
C. The triggering of remote data wipe capabilities
D. Awareness training for mobile device users

Answer: A

Explanation:
The best way to prevent data leakage from a lost mobile device is data encryption on the mobile device. Data encryption is a technique that transforms data into an unreadable format using a secret key or algorithm. Data encryption protects data from unauthorized access or disclosure in case of loss or theft of a mobile device. Complex password policy for mobile devices, triggering of remote data wipe capabilities, and awareness training for mobile device users are useful measures to enhance data security on mobile devices, but they do not prevent data leakage as effectively as data encryption. A complex password policy can be bypassed by brute force attacks or password cracking tools. Remote data wipe capabilities depend on network connectivity and device power availability. Awareness training for mobile device users can reduce human errors or negligence, but it cannot guarantee compliance or behavior change. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION 122
- (Topic 2)
Which of the following is the PRIMARY reason to follow a configuration management process to maintain application?

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

Answer: D

Explanation:
Following a configuration management process to maintain applications is the primary reason for ensuring proper change control. Configuration management is a process of identifying, documenting, controlling, and verifying the configuration items and their interrelationships within an IT system or environment. Following a configuration management process can help to ensure that any changes to the applications are authorized, tested, documented, and tracked throughout their lifecycle. This will help to prevent unauthorized or improper changes that could affect the functionality, performance, or security of the applications. The other options are not the primary reasons for following a configuration management process, but rather possible benefits or outcomes of doing so. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
? CISA Review Questions, Answers & Explanations Database, Question ID 225

NEW QUESTION 127
- (Topic 2)
What is the MAIN reason to use incremental backups?

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

Answer: D

Explanation:
Incremental backups are backups that only copy the data that has changed since the last backup, whether it was a full or incremental backup. The main reason to use incremental backups is to minimize the backup time and resources, as they require less storage space and network bandwidth than full backups. Incremental backups can also improve key availability metrics, such as recovery point objective (RPO) and recovery time objective (RTO), but that is not their primary purpose. Reducing costs associated with backups and increasing backup resiliency and redundancy are possible benefits of incremental backups, but they depend on other factors, such as the backup frequency, retention policy, and media type. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION 132
- (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 135
- (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 139
- (Topic 2)
An IS auditor is reviewing the release management process for an in-house software development solution. In which environment Is the software version MOST likely to be the same as production?

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

Answer: A

Explanation:
A staging environment is a replica of the production environment that is used to test and verify software before deploying it to production. A staging environment is most likely to have the same software version as production, as it mimics the real-world conditions and configurations that will be encountered in production. A testing environment is a separate environment that is used to perform various types of testing on software, such as functional testing, performance testing, security testing, etc. A testing environment may not have the same software version as production, as it may undergo frequent changes or updates based on testing results or feedback. An integration environment is a separate environment that is used to combine and test software components or modules from different developers or sources, to ensure that they work together as expected. An integration environment may not have the same software version as production, as it may involve

different versions or branches of software from different sources. A development environment is a separate environment that is used by developers to create and modify software code. A development environment may not have the same software version as production, as it may contain unfinished or untested code that has not been released yet.

NEW QUESTION 140
- (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 144
- (Topic 2)
Which of the following controls BEST ensures appropriate segregation of dudes within an accounts payable department?

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

Answer: D

Explanation:
Restricting program functionality according to user security profiles is the best control for ensuring appropriate segregation of duties within an accounts payable department. An IS auditor should verify that the access rights and permissions of the accounts payable staff are based on their roles and responsibilities, and that they are not able to perform incompatible or conflicting functions such as creating, approving, or paying invoices. This will help to prevent fraud, errors, or abuse of authority within the accounts payable process. The other options are less effective controls for ensuring segregation of duties, as they may involve audit trails, access restrictions, or user identification. References:
? CISA Review Manual (Digital Version), Chapter 6, Section 6.31
? CISA Review Questions, Answers & Explanations Database, Question ID 223

NEW QUESTION 148
- (Topic 2)
For an organization that has plans to implement web-based trading, it would be MOST important for an IS auditor to verify the organization's information security plan includes:

A. attributes for system passwords.
B. security training prior to implementation.
C. security requirements for the new application.
D. the firewall configuration for the web server.

Answer: C

Explanation:
For an organization that has plans to implement web-based trading, it would be most important for an IS auditor to verify that the organization’s information security plan includes security requirements for the new application. Security requirements are statements that define what security features and functions are needed to protect the confidentiality, integrity, and availability of the web-based trading application and its data. Security requirements should be identified and documented during the planning phase of the application development life cycle, before any design or coding activities take place. Attributes for system passwords, security training prior to implementation, and firewall configuration for the web server are also important aspects of information security, but they are not as essential as security requirements for ensuring that the web-based trading application meets its security objectives.

NEW QUESTION 152
- (Topic 2)
Which of the following should an IS auditor consider FIRST when evaluating firewall rules?

A. The organization's security policy
B. The number of remote nodes
C. The firewalls' default settings
D. The physical location of the firewalls

Answer: A

Explanation:
This should be the first thing that an IS auditor considers when evaluating firewall rules, because it defines the objectives, standards, and guidelines for securing the organization’s network and information assets. The firewall rules should be aligned with the organization’s security policy, and reflect the level of risk and protection required for each type of network traffic, system, or data. The IS auditor should compare the firewall rules with the security policy, and identify any discrepancies, gaps, or conflicts that could compromise the security or performance of the network.
The other options are not as important as the organization’s security policy when evaluating firewall rules:
? The number of remote nodes. This is a factor that may affect the complexity and scalability of the firewall rules, but it is not a primary consideration for the IS auditor. Remote nodes are devices or systems that connect to the network from outside locations, such as teleworkers, mobile users, or branch offices. The IS auditor should ensure that the firewall rules provide adequate security and access control for remote nodes, but this depends on the organization’s security policy and business needs.
? The firewalls’ default settings. These are the predefined configurations that come with the firewall devices or software, and that determine how they handle network traffic by default. The IS auditor should review the firewalls’ default settings, and verify that they are appropriate and secure for the organization’s network environment. However, the firewalls’ default settings may not match the organization’s security policy or specific requirements, and may need to be customized or

overridden by firewall rules.
? The physical location of the firewalls. This is a factor that may affect the placement and design of the firewall rules, but it is not a critical consideration for the IS auditor. The physical location of the firewalls refers to where they are installed or deployed in relation to the network topology, such as at the network perimeter, between network segments, or on individual hosts. The IS auditor should ensure that the firewall rules are consistent and coordinated across different locations, but this depends on the organization's security policy and network architecture.

NEW QUESTION 153
- (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 158
- (Topic 2)
The IS auditor has recommended that management test a new system before using it in production mode. The BEST approach for management in developing a test plan is to use processing parameters that are:

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

Answer: D

Explanation:
The best approach for management in developing a test plan is to use processing parameters that are simulated by production entities and customers. This is because using realistic data and scenarios can help to evaluate the functionality, performance, reliability, and security of the new system under actual operating conditions and expectations. Using processing parameters that are randomly selected by a test generator, provided by the vendor of the application, or randomly selected by the user may not be sufficient or representative of the production environment and may not reveal all the potential issues or defects of the new system. References: [ISACA CISA Review Manual 27th Edition], page 266.

NEW QUESTION 162
- (Topic 2)
An IS auditor is reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit. What should the auditor consider the MOST significant concern?

A. Attack vectors are evolving for industrial control systems.
B. There is a greater risk of system exploitation.
C. Disaster recovery plans (DRPs) are not in place.
D. Technical specifications are not documented.

Answer: B

Explanation:
The most significant concern for an IS auditor when reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit is that there is a greater risk of system exploitation. System exploitation is an attack that occurs when an unauthorized entity or individual takes advantage of a vulnerability or weakness in a system to compromise its security or functionality. System exploitation can cause harm or damage to the system or its users, such as data loss, corruption, theft, manipulation, denial of service (DoS), etc. An ICS that uses older unsupported technology poses a high risk of system exploitation, as older technology may have known or unknown vulnerabilities or defects that have not been patched or fixed by the vendor or manufacturer, and unsupported technology may not receive any updates or support from the vendor or manufacturer in case of issues or incidents. Attack vectors are evolving for industrial control systems is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. Attack vectors are methods or pathways that attackers use to gain access to or attack a system. Attack vectors are evolving for industrial control systems, as attackers are developing new techniques or tools to target ICSs that are increasingly connected and complex. However, this concern may not be specific to older unsupported technology, as it may affect any ICS regardless of its technology level. Disaster recovery plans (DRPs) are not in place is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. DRPs are documents that outline the technical and operational steps for restoring the IT systems and infrastructure that support critical functions or processes in the event of a disruption or disaster. DRPs are not in place, as they may affect the availability and continuity of the ICS and its functions or processes in case of a failure or incident. However, this concern may not be related to older unsupported technology, as it may apply to any ICS regardless of its technology level. Technical specifications are not documented is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. Technical specifications are documents that describe the technical characteristics or requirements of a system or component, such as functionality, performance, design, etc. Technical specifications are not documented, as they may affect the understanding, maintenance, and improvement of the ICS and its components. However, this concern may not be associated with older unsupported technology, as it may affect any ICS regardless of its technology level.

NEW QUESTION 163
- (Topic 2)
In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

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

Answer: A

Explanation:
Penetration testing is a method of evaluating the security of a system or network by simulating an attack from a malicious source. Penetration testing typically consists of four phases: planning, discovery, attacks, and reporting. In the discovery phase, penetration testers gather information about the target system or network, such as host detection, domain name system (DNS) interrogation, port scanning, service identification, operating system fingerprinting, vulnerability scanning, etc. This information can help to identify potential entry points, weaknesses, or vulnerabilities that can be exploited in the subsequent attack phase. Host detection and DNS interrogation are techniques that can be used in the discovery phase to determine the active hosts and their IP addresses and hostnames on the target network. References: [ISACA CISA Review Manual 27th Edition], page 368.

NEW QUESTION 168
- (Topic 2)
Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at test?

A. Short key length
B. Random key generation
C. Use of symmetric encryption
D. Use of asymmetric encryption

Answer: A

Explanation:
The condition that would be of most concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at rest is short key length. A brute force attack is a method of breaking encryption by trying all possible combinations of keys until finding the correct one. The shorter the key length, the easier it is for an attacker to guess or crack the encryption. Random key generation, use of symmetric encryption, and use of asymmetric encryption are not conditions that would increase the risk of a successful brute force attack. In fact, random key generation can enhance security by preventing predictable patterns in key selection. Symmetric encryption and asymmetric encryption are different types of encryption that have their own advantages and disadvantages, but neither is inherently more vulnerable to brute force attacks than the other. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION 173
- (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 176
- (Topic 2)
Which of the following are BEST suited for continuous auditing?

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

Answer: B

Explanation:
Continuous auditing is a method of performing audit-related activities on a real-time or near real-time basis. Continuous auditing is best suited for real-time transactions, such as online banking, e-commerce, or electronic funds transfer, that require immediate verification and assurance. Low-value transactions are not necessarily suitable for continuous auditing, as they may not pose significant risks or require frequent monitoring. Irregular transactions are not suitable for continuous auditing, as they may not occur frequently or consistently enough to justify the use of continuous auditing techniques. Manual transactions are not

suitable for continuous auditing, as they may not be captured or processed by automated systems that enable continuous auditing. References:
? CISA Review Manual, 27th Edition, pages 307-3081
? CISA Review Questions, Answers & Explanations Database, Question ID: 253

NEW QUESTION 178
- (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 182
- (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 185
- (Topic 2)
Which of the following is the BEST source of information tor an IS auditor to use when determining whether an organization's information security policy is adequate?

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

Answer: C

Explanation:
The best source of information for an IS auditor to use when determining whether an organization's information security policy is adequate is the risk assessment results. The risk assessment results provide the auditor with an overview of the organization's risk profile, including the identification, analysis, and evaluation of the risks that affect the confidentiality, integrity, and availability of the information assets. The auditor can use the risk assessment results to compare the organization's information security policy with the risk appetite, risk tolerance, and risk treatment strategies of the organization. The auditor can also use the risk assessment results to evaluate if the information security policy is aligned with the organization's objectives, requirements, and regulations.
Some of the web sources that support this answer are:
? Performance Measurement Guide for Information Security
? ISO 27001 Annex A.5 - Information Security Policies
? [CISA Certified Information Systems Auditor – Question0551]

NEW QUESTION 189
- (Topic 2)
An organization that has suffered a cyber-attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

A. An imaging process was used to obtain a copy of the data from each computer.

B. The legal department has not been engaged.
C. The chain of custody has not been documented.
D. Audit was only involved during extraction of the Information

Answer: C

Explanation:
The chain of custody has not been documented is a finding that should be of greatest concern for an IS auditor reviewing a forensic analysis process of an organization that has suffered a cyber attack. The chain of custody is a record of who handled, accessed, or modified the evidence during a forensic investigation. Documenting the chain of custody is essential to preserve the integrity, authenticity, and admissibility of the evidence in a court of law. The other options are less concerning findings that may not affect the validity or reliability of the forensic analysis process. References:
? CISA Review Manual (Digital Version), Chapter 7, Section 7.51
? CISA Review Questions, Answers & Explanations Database, Question ID 220

NEW QUESTION 193
- (Topic 2)
Which of the following metrics would BEST measure the agility of an organization's IT function?

A. Average number of learning and training hours per IT staff member
B. Frequency of security assessments against the most recent standards and guidelines
C. Average time to turn strategic IT objectives into an agreed upon and approved initiative
D. Percentage of staff with sufficient IT-related skills for the competency required of their roles

Answer: C

Explanation:
The metric that would best measure the agility of an organization’s IT function is average time to turn strategic IT objectives into an agreed upon and approved initiative. IT agility is the ability of an IT function to respond quickly and effectively to changing business needs and opportunities. By measuring how fast an IT function can translate strategic IT objectives into actionable initiatives, such as projects or programs, an organization can assess how well its IT function can align with and support its business strategy. Average number of learning and training hours per IT staff member, frequency of security assessments against the most recent standards and guidelines, and percentage of staff with sufficient IT-related skills for the competency required of their roles are metrics that may indicate other aspects of IT performance, such as capability development, security maturity, and skills gap analysis, but they do not directly measure IT agility. References:
ISACA Journal Article: Measuring IT Agility

NEW QUESTION 197
- (Topic 2)
Which of the following should an IS auditor consider the MOST significant risk associated with a new health records system that replaces a legacy system?

A. Staff were not involved in the procurement process, creating user resistance to the new system.
B. Data is not converted correctly, resulting in inaccurate patient records.
C. The deployment project experienced significant overruns, exceeding budget projections.
D. The new system has capacity issues, leading to slow response times for users.

Answer: B

Explanation:
The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection. Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as
significant as data not being converted correctly. References: [ISACA CISA Review Manual 27th Edition], page 281.

NEW QUESTION 202
- (Topic 1)
Which of the following is the MOST effective control to mitigate unintentional misuse of authorized access?

A. Annual sign-off of acceptable use policy
B. Regular monitoring of user access logs
C. Security awareness training
D. Formalized disciplinary action

Answer: C

Explanation:
The most effective control to mitigate unintentional misuse of authorized access is security awareness training. This is because security awareness training can educate users on the proper use of their access rights, the potential consequences of misuse, and the best practices to protect the confidentiality, integrity, and availability of information systems. Security awareness training can also help users recognize and avoid common threats such as phishing, malware, and social engineering.
Annual sign-off of acceptable use policy, regular monitoring of user access logs, and formalized disciplinary action are not the most effective controls to mitigate unintentional misuse of authorized access. These controls may help deter or detect intentional misuse, but they do not address the root cause of unintentional misuse, which is often a lack of knowledge or awareness of security policies and procedures.

NEW QUESTION 207
- (Topic 1)
Which of the following MOST effectively minimizes downtime during system conversions?

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

Answer: D

Explanation:
The most effective way to minimize downtime during system conversions is to use a parallel run. A parallel run is a method of system conversion where both the old and new systems operate simultaneously for a period of time until the new system is verified to be functioning correctly. This reduces the risk of errors, data loss, or system failure during conversion and allows for a smooth transition from one system to another. References: CISA Review Manual, 27th Edition, page 467

NEW QUESTION 208
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

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

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