Exam Questions CISA

Isaca CISA

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

NEW QUESTION 1
- (Topic 3)
What should an IS auditor do FIRST when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective?

A. Determine the resources required to make the control effective.
B. Validate the overall effectiveness of the internal control.
C. Verify the impact of the control no longer being effective.
D. Ascertain the existence of other compensating controls.

Answer: D

Explanation:
The first thing that an IS auditor should do when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective is to ascertain the existence of other compensating controls. Compensating controls are alternative controls that provide reasonable assurance of achieving the same objective as the original control. The IS auditor should verify whether there are any compensating controls in place that can mitigate the risk of the key control being ineffective, and evaluate their adequacy and effectiveness. The other options are not the first steps, because they either require more information about the compensating controls, or they are actions to be taken after identifying and assessing the compensating controls. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.3

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

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

Answer: B

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

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

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

Answer: B

Explanation:
The greatest concern for an IS auditor reviewing a network printer disposal process is that evidence is not available to verify printer hard drives have been sanitized prior to disposal. This can expose sensitive data to unauthorized parties and cause data breaches. Disposal policies and procedures not being consistently implemented or business units being allowed to dispose printers directly to vendors are compliance issues, but not as critical as data protection. Inoperable printers being stored in an unsecured area is a physical security issue, but not as severe as data leakage. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 387

NEW QUESTION 4
- (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 5
- (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 6
- (Topic 3)
An IS auditor finds that capacity management for a key system is being performed by IT with no input from the business The auditor's PRIMARY concern would be:

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

Answer: B

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

NEW QUESTION 7
- (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 8
- (Topic 3)
Management receives information indicating a high level of risk associated with potential flooding near the organization's data center within the next few years. As a result, a decision has been made to move data center operations to another facility on higher ground. Which approach has been adopted?

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

Answer: A

Explanation:
The approach adopted by management in this scenario is risk
avoidance. Risk avoidance is the elimination of a risk by discontinuing or not undertaking an activity that poses a threat to the organization3. By moving data center operations to another facility on higher ground, management is avoiding the potential flooding risk that could disrupt or damage the data center. Risk transfer, risk acceptance and risk reduction are other possible approaches for dealing with risks, but they do not apply in this case. References:
? CISA Review Manual, 27th Edition, page 641
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 9

- (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 10
- (Topic 3)
What Is the BEST method to determine if IT resource spending is aligned with planned project spending?

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

Answer: A

Explanation:
The best method to determine if IT resource spending is aligned with planned project spending is earned value analysis (EVA). EVA is a technique that compares the actual cost, schedule, and scope of a project with the planned or budgeted values. EVA can help to measure the project progress and performance, and identify any variances or deviations from the baseline plan1.
EVA uses three basic values to calculate the project status: planned value (PV), earned value (EV), and actual cost (AC). PV is the amount of work that was expected to be completed by a certain date, according to the project plan. EV is the amount of work that was actually completed by that date, measured in terms of the budgeted cost. AC is the amount of money that was actually spent to complete the work by that date1.
By comparing these values, EVA can determine if the project is on track, ahead, or behind schedule and budget. EVA can also calculate various indicators, such as cost variance (CV), schedule variance (SV), cost performance index (CPI), and schedule performance index (SPI), to quantify the magnitude and direction of the variances. EVA can also forecast the future performance and completion of the project, based on the current trends and assumptions1.
The other options are not as effective as EVA in determining if IT resource spending is aligned with planned project spending. Option B, return on investment (ROI) analysis, is a technique that evaluates the profitability or efficiency of an investment, by comparing the benefits or revenues with the costs. ROI analysis can help to justify or prioritize a project, but it does not measure the actual progress or performance of the project against the plan2. Option C, Gantt chart, is a tool that displays the tasks, durations, dependencies, and milestones of a project in a graphical format. Gantt chart can help to plan and monitor a project schedule, but it does not show the actual cost or scope of the project3. Option D, critical path analysis, is a technique that identifies the longest sequence of tasks or activities that must be completed on time for the project to finish on schedule. Critical path analysis can help to optimize and control a project schedule, but it does not account for the actual cost or scope of the project4.
References:
? Earned Value Analysis & Management (EVA/EVM) – Definition & Formulae1
? Return on Investment (ROI) Formula2
? What Is a Gantt Chart?3
? Critical Path Method for Project Management

NEW QUESTION 10
- (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 11
- (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 12
- (Topic 3)
A post-implementation review was conducted by issuing a survey to users. Which of the following should be of GREATEST concern to an IS auditor?

A. The survey results were not presented in detail lo management.
B. The survey questions did not address the scope of the business case.
C. The survey form template did not allow additional feedback to be provided.
D. The survey was issued to employees a month after implementation.

Answer: B

Explanation:
The greatest concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users is that the survey questions did not address the scope of the business case. A post-implementation review is a process of evaluating the outcomes and benefits of a project after it has been completed and implemented. A post-implementation review can help to assess whether the project met its objectives, delivered its expected value, and satisfied its stakeholders1. A survey is a method of collecting feedback and opinions from users or other stakeholders about their experience and satisfaction with the project. A survey can help to measure the user acceptance, usability, and functionality of the project deliverables2. A business case is a document that justifies the need for a project based on its expected benefits, costs, risks, and alternatives. A business case defines the scope, objectives, and requirements of the project and provides a basis for its approval and initiation3. Therefore, an IS auditor should be concerned if the survey questions did not address the scope of the business case, as it may indicate that the post-implementation review was not comprehensive, relevant, or aligned with the project goals. The other options are less concerning or incorrect because:
? A. The survey results were not presented in detail to management is not a great
concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a communication or reporting issue than an audit issue. While presenting the survey results in detail to management may help to inform them about the project performance and outcomes, it does not affect the validity or quality of the post-implementation review itself.
? C. The survey form template did not allow additional feedback to be provided is not
a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a design or format issue than an audit issue. While allowing additional feedback to be provided may help to capture more insights or suggestions from users, it does not affect the validity or quality of the post-implementation review itself.
? D. The survey was issued to employees a month after implementation is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a timing or scheduling issue than an audit issue. While issuing the survey to employees sooner after implementation may help to collect more accurate and timely feedback from users, it does not affect the validity or quality of the post-implementation review
itself. References: Post Implementation Review - ISACA, Survey - ISACA, Business Case - ISACA

NEW QUESTION 13
- (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 18
- (Topic 3)
What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

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

Answer: D

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

NEW QUESTION 19
- (Topic 3)
An IS auditor is reviewing the installation of a new server. The IS auditor's PRIMARY objective is to ensure that

A. security parameters are set in accordance with the manufacturer s standards.
B. a detailed business case was formally approved prior to the purchase.
C. security parameters are set in accordance with the organization's policies.
D. the procurement project invited lenders from at least three different suppliers.

Answer: C

Explanation:
The primary objective of an IS auditor when reviewing the installation of a new server is to ensure that security parameters are set in accordance with the organization’s policies. Security parameters are settings or options that control the security level and behavior of the server, such as authentication methods, encryption algorithms, access rights, audit logs, firewall rules, or password policies7. The organization’s policies are documents that define the security goals, requirements, standards, and guidelines for the organization’s information systems. An IS auditor should verify that security parameters are set in accordance with the organization’s policies to ensure that the new server complies with the organization’s security expectations and regulations. The other options are less important or incorrect because:
? A. Security parameters should not be set in accordance with the manufacturer’s standards alone, as they may not reflect the organization’s specific security needs and environment. The manufacturer’s standards are general recommendations or best practices for configuring the server’s security parameters based on common scenarios and threats. An IS auditor should compare the manufacturer’s standards with the organization’s policies and identify any gaps or conflicts that need to be resolved.
? B. A detailed business case should have been formally approved prior to the purchase of a new server rather than during its installation. A business case is a document that justifies the need for a new server based on its expected benefits, costs, risks, and alternatives. A business case should be approved by senior management before initiating a project to acquire a new server.
? D. The procurement project should have invited tenders from at least three different suppliers before purchasing a new server rather than during its installation. A tender is a formal offer or proposal to provide a product or service at a specified price and quality. Inviting tenders from multiple suppliers helps to ensure a fair and competitive procurement process that can result in the best value for money and quality for the organization. References: Server Security - ISACA, [Information Security Policy - ISACA], [Server Hardening - ISACA], [Business Case- ISACA], [Tender - ISACA], [Procurement Management - ISACA]

NEW QUESTION 20
- (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 24
- (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 29
- (Topic 3)
Which of the following would be of GREATEST concern when reviewing an organization's security information and event management (SIEM) solution?

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

Answer: C

Explanation:
The greatest concern that the IS auditor should have when reviewing an organization's security information and event management (SIEM) solution is that the SIEM is decentralized. This is because a decentralized SIEM can pose challenges for collecting, correlating, analyzing and reporting on security events and incidents from multiple sources and locations. A decentralized SIEM can also increase the complexity and cost of maintaining and updating the SIEM components, as well as the risk of inconsistent or incomplete security monitoring and response. The IS auditor should recommend that the organization adopts a centralized or hybrid SIEM architecture that can provide a holistic and integrated view of the security posture and activities across the organization. The other findings are not as concerning as a decentralized SIEM, because they can be addressed by implementing best practices and standards for SIEM reporting and configuration.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION 32
- (Topic 3)
When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system. It is MOST effective for an IS auditor to review;

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

Answer: A

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

NEW QUESTION 37
- (Topic 3)
Which of the following would BEST help to ensure that potential security issues are considered by the development team as part of incremental changes to agile-developed software?

A. Assign the security risk analysis to a specially trained member of the project management office.
B. Deploy changes in a controlled environment and observe for security defects.
C. Include a mandatory step to analyze the security impact when making changes.
D. Mandate that the change analyses are documented in a standard format.

Answer: C

Explanation:
The best way to ensure that potential security issues are considered by the development team as part of incremental changes to agile-developed software is to include a mandatory step to analyze the security impact when making changes. This will help to identify and mitigate any security risks or vulnerabilities that may arise from the changes, and to ensure that the software meets the security requirements and standards. The other options are not as effective, because they either delegate the security analysis to someone outside the development team, rely on post-deployment testing, or focus on documentation rather than analysis.
References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.5

NEW QUESTION 41
- (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 43
- (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 45
- (Topic 3)
Which of the following should be of GREATEST concern for an IS auditor reviewing an organization's disaster recovery plan (DRP)?

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

Answer: C

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

NEW QUESTION 47
- (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 50
- (Topic 2)
In a RAO model, which of the following roles must be assigned to only one individual?

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

Answer: D

Explanation:
In a RAO model, which stands for Responsible, Accountable, Consulted, and Informed, the accountable role must be assigned to only one individual. The accountable role is the person who has the ultimate authority and responsibility for the outcome of the project or task, and who approves or rejects the work done by the responsible role. The accountable role cannot be delegated or shared, as it is essential to have a clear and single point of accountability for each project or task.
The other roles can be assigned to more than one individual:
? Responsible. This is the person who does the work or performs the task. There can be multiple responsible roles for different aspects or phases of a project or task, as long as they are coordinated and supervised by the accountable role.
? Informed. This is the person who needs to be notified or updated about the progress or results of the project or task. There can be multiple informed roles who have an interest or stake in the project or task, but who do not need to be consulted or involved in the decision-making process.
? Consulted. This is the person who provides input, feedback, or advice on the project or task. There can be multiple consulted roles who have expertise or experience relevant to the project or task, but who do not have the authority or responsibility to approve or reject the work done by the responsible role.

NEW QUESTION 52
- (Topic 2)
What is the Most critical finding when reviewing an organization's information security management?

A. No dedicated security officer
B. No official charier for the information security management system
C. No periodic assessments to identify threats and vulnerabilities
D. No employee awareness training and education program

Answer: C

Explanation:
The most critical finding when reviewing an organization's information security management is no periodic assessments to identify threats and vulnerabilities. Periodic assessments are essential for ensuring that the organization's information security policies, procedures, standards, and controls are aligned with the current and emerging risks and threats that may affect its information assets. Without periodic assessments, the organization may not be aware of its actual security posture, gaps, or weaknesses, and may not be able to take appropriate measures to mitigate or prevent potential security incidents. No dedicated security officer, no official charter for the information security management system, and no employee awareness training and education program are also findings that may indicate some deficiencies in the organization's information security management, but they are not as critical as no periodic assessments to identify threats and vulnerabilities. References: ISACA CISA Review Manual 27th Edition, page 343.

NEW QUESTION 57
- (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 59
- (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 64
- (Topic 2)
When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor's BEST recommendation is to place an intrusion detection system (IDS) between the firewall and:

A. the organization's web server.
B. the demilitarized zone (DMZ).
C. the organization's network.
D. the Internet

Answer: D

Explanation:
The best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet. An IDS is a device or software that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. By placing an IDS between the firewall and the Internet, the IS auditor can enhance the security of the network perimeter and detect any attack attempts that the firewall was unable to recognize.
The other options are not as effective as placing an IDS between the firewall and the Internet:
? Placing an IDS between the firewall and the organization's web server would not
protect the web server from external attacks that bypass the firewall. The web server should be placed in a demilitarized zone (DMZ), which is a separate network segment that isolates public-facing servers from the internal network.
? Placing an IDS between the firewall and the demilitarized zone (DMZ) would not protect the DMZ from external attacks that bypass the firewall. The DMZ should be protected by two firewalls, one facing the Internet and one facing the internal network, with an IDS monitoring both sides of each firewall.
? Placing an IDS between the firewall and the organization's network would not protect the organization's network from external attacks that bypass the firewall. The organization's network should be protected by a firewall that blocks unauthorized traffic from entering or leaving the network, with an IDS monitoring both sides of the firewall.

NEW QUESTION 67
- (Topic 2)
An organization has assigned two now IS auditors to audit a now system implementation. One of the auditors has an IT-related degree, and one has a business degree. Which ol the following is MOST important to meet the IS audit standard for proficiency?

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

Answer: C

Explanation:
Team member assignments based on individual competencies is the most important factor to meet the IS audit standard for proficiency. Proficiency is the ability to apply knowledge, skills and experience to perform audit tasks effectively and efficiently. The IS audit standard for proficiency requires that IS auditors must possess the knowledge, skills and discipline to perform audit tasks in accordance with applicable standards, guidelines and procedures. Team member assignments based on individual competencies is a way to ensure that each IS auditor is assigned to audit tasks that match their level of
proficiency, and that the audit team as a whole has sufficient and appropriate proficiency to conduct the audit. The other options are not as important as option C, as they do not ensure that the IS auditors have the required proficiency to perform audit tasks. Having a globally recognized audit certification is a way to demonstrate proficiency in IS auditing, but it does not guarantee that the IS auditor has the specific knowledge, skills and experience needed for a particular audit task or system. Technical co-sourcing is a way to supplement the proficiency of the IS audit team by hiring external experts or consultants to perform certain audit tasks or functions, but it does not replace the need for internal IS auditors to have adequate proficiency. Having a supervisor review the new auditors' work is a way to ensure quality and accuracy of the audit work, but it does not ensure that the new auditors have the necessary proficiency to perform audit tasks independently or competently. References: CISA Review Manual (Digital Version) , Chapter 1: Information Systems Auditing Process, Section 1.4: Audit Skills and Competencies.

NEW QUESTION 68
- (Topic 2)
Which of the following is the GREATEST security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system?

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

Answer: A

Explanation:
The greatest security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system is data from the source and target system may be intercepted. Data interception is an attack that occurs when an unauthorized entity or individual captures or accesses data that are being transmitted or stored on an information system or network. Data interception can compromise the confidentiality and integrity of data, and cause harm or damage to data owners or users. Data migration from a legacy HR system to a cloud-based system involves transferring data from one system or location to another system or location over a network connection. This poses a high risk of data interception, as data may be exposed or vulnerable during transit or storage on unsecured or untrusted networks or systems. Data from the source and target system may have different data formats is a possible challenge associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. Data formats are specifications that define how data are structured or encoded on an information system or network. Data formats may vary depending on different systems or platforms. Data migration may require converting data from one format to another format to ensure compatibility and interoperability between systems. Records past their retention period may not be migrated to the new system is a possible outcome associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. Retention period is a duration that defines how long data should be kept or stored on an information system or network before being deleted or destroyed. Retention period may depend on various factors such as legal requirements, business needs, storage capacity, etc. Data migration may involve deleting or destroying data that are past their retention period to reduce the volume or complexity of data to be transferred or to comply with regulations or policies. System performance may be impacted by the migration is a possible impact associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. System performance is a measure of how well an information system or network functions or operates, such as speed, reliability, availability, etc. System performance may be affected by data migration, as data migration may consume significant resources or bandwidth, cause interruptions or delays, or introduce errors or inconsistencies.

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 71
- (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 72

- (Topic 2)
Which of the following is the BEST audit procedure to determine whether a firewall is configured in compliance with the organization's security policy?

A. Reviewing the parameter settings
B. Reviewing the system log
C. Interviewing the firewall administrator
D. Reviewing the actual procedures

Answer: A

Explanation:
The best audit procedure to determine whether a firewall is configured in compliance with the organization’s security policy is reviewing the parameter settings. Parameter settings are values or options that define how a firewall operates and functions, such as rules, filters, ports, protocols, etc. By reviewing the parameter settings of a firewall, an IS auditor can verify whether they match with the organization’s security policy, which is a document that outlines the security objectives, requirements, and guidelines for an organization’s information systems and resources. Reviewing the system log is a possible audit procedure to determine whether a firewall is configured in compliance with the organization’s security policy, but it is not the best one, as a system log records events or activities that occur on a firewall, such as connections, requests, responses, errors, alerts, etc., and may not indicate whether they comply with the organization’s security policy. Interviewing the firewall administrator is a possible audit procedure to determine whether a firewall is configured in compliance with the organization’s security policy, but it is not the best one, as a firewall administrator may not provide accurate or reliable information about the firewall configuration, and may have conflicts of interest or ulterior motives. Reviewing the actual procedures is a possible audit procedure to determine whether a firewall is configured in compliance with the organization’s security policy, but it is not the best one, as actual procedures describe how a firewall is configured and maintained, such as installation, testing, updating, etc., and may not reflect whether they comply with the organization’s security policy.

NEW QUESTION 74
- (Topic 2)
Which of the following BEST Indicates that an incident management process is effective?

A. Decreased time for incident resolution
B. Increased number of incidents reviewed by IT management
C. Decreased number of calls lo the help desk
D. Increased number of reported critical incidents

Answer: A

Explanation:
Decreased time for incident resolution is the best indicator that an incident management process is effective. Incident management is a process that aims to restore normal service operation as quickly as possible after an incident, which is an unplanned interruption or reduction in quality of an IT service. Decreased time for incident resolution means that the incident management process is able to identify, analyze, respond to, and resolve incidents efficiently and effectively. The other indicators do not necessarily reflect the effectiveness of the incident management process, as they may depend on other factors such as the nature, frequency, and severity of incidents. References: CISA Review Manual, 27th Edition, page 372

NEW QUESTION 76
- (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 80
- (Topic 2)
Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

A. The job scheduler application has not been designed to display pop-up error messages.
B. Access to the job scheduler application has not been restricted to a maximum of two staff members
C. Operations shift turnover logs are not utilized to coordinate and control the processing environment
D. Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor

Answer: D

Explanation:
Changes to the job scheduler application’s parameters are not approved and reviewed by an operations supervisor. This is a serious control weakness that could compromise the integrity, availability, and security of the IT operations. An IS auditor should be concerned about the lack of oversight and accountability for such changes, which could result in unauthorized, erroneous, or malicious modifications that affect the processing environment. The other options are less critical issues that may not have a significant impact on the IT operations. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.11
? CISA Review Questions, Answers & Explanations Database, Question ID 202

NEW QUESTION 81
- (Topic 2)
A project team has decided to switch to an agile approach to develop a replacement for an existing business application. Which of the following should an IS auditor do FIRST to ensure the effectiveness of the protect audit?

A. Compare the agile process with previous methodology.
B. Identify and assess existing agile process control
C. Understand the specific agile methodology that will be followed.
D. Interview business process owners to compile a list of business requirements

Answer: C

Explanation:
Understanding the specific agile methodology that will be followed is the first step that an IS auditor should do to ensure the effectiveness of the project audit. An IS auditor should familiarize themselves with the agile approach, principles, practices, and tools that will be used by the project team, as well as the roles and responsibilities of the project stakeholders. This will help the IS auditor to identify and assess the relevant risks and controls for the project audit. The other options are not the first steps that an IS auditor should do, but rather possible subsequent actions that may depend on the specific agile methodology. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.21
? CISA Review Questions, Answers & Explanations Database, Question ID 211

NEW QUESTION 85
- (Topic 2)
A now regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditor's BEST recommendation to facilitate compliance with the regulation?

A. Establish key performance indicators (KPIs) for timely identification of security incidents.
B. Engage an external security incident response expert for incident handling.
C. Enhance the alert functionality of the intrusion detection system (IDS).
D. Include the requirement in the incident management response plan.

Answer: D

Explanation:
The best recommendation for the IS auditor to facilitate compliance with the new regulation is to include the requirement in the incident management response plan. An incident management response plan is a document that defines the roles, responsibilities, processes, and procedures for responding to security incidents. By including the new regulation in the plan, the IS auditor can ensure that the organization is aware of the reporting obligation, has a clear workflow for notifying the regulator within 24 hours, and has the necessary documentation and evidence to support the report.
The other options are not as effective as including the requirement in the incident management response plan:
? Establishing key performance indicators (KPIs) for timely identification of security incidents is a good practice, but it does not guarantee compliance with the regulation. KPIs are metrics that measure the performance of a process or activity, but they do not specify how to perform it. The IS auditor should also provide guidance on how to identify and report security incidents within 24 hours.
? Engaging an external security incident response expert for incident handling is a possible option, but it may not be feasible or cost-effective. The organization may not have the budget or time to hire an external expert, or may prefer to handle the incidents internally. The IS auditor should also evaluate the qualifications and trustworthiness of the external expert, and ensure that they comply with the regulation and other contractual or legal obligations.
? Enhancing the alert functionality of the intrusion detection system (IDS) is a useful measure, but it is not sufficient to comply with the regulation. An IDS is a tool that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. However, an IDS may not detect all types of security incidents, or may generate false positives or negatives. The IS auditor should also consider other sources of incident detection, such as logs, reports, audits, or user feedback.

NEW QUESTION 90
- (Topic 2)
An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

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

Answer: D

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

NEW QUESTION 93
- (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 98
- (Topic 2)
Which of the following is MOST helpful for measuring benefits realization for a new system?

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

Answer: C

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

NEW QUESTION 99
- (Topic 2)
IT disaster recovery time objectives (RTOs) should be based on the:

A. maximum tolerable loss of data.
B. nature of the outage
C. maximum tolerable downtime (MTD).
D. business-defined criticality of the systems.

Answer: D

Explanation:
IT disaster recovery time objectives (RTOs) are the maximum acceptable
time that an IT system can be unavailable after a disaster before it causes unacceptable consequences for the business. IT RTOs should be based on the business-defined criticality of the systems, which reflects how important they are for supporting the business processes and functions. The maximum tolerable loss of data, the nature of the outage, and the maximum tolerable downtime (MTD) are also factors that affect the IT RTOs, but they are not the primary basis for determining them.

NEW QUESTION 102
- (Topic 2)
A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon The MOST effective plan of action would be to:

A. evaluate replacement systems and performance monitoring software.
B. restrict functionality of system monitoring software to security-related events.
C. re-install the system and performance monitoring software.
D. use analytical tools to produce exception reports from the system and performance monitoring software

Answer: D

Explanation:
Using analytical tools to produce exception reports from the system and performance monitoring software is the most effective plan of action for a company that purchased and implemented system and performance monitoring software. Exception reports are reports that highlight deviations or anomalies from predefined thresholds or standards. Using analytical tools to produce exception reports can help to reduce the size and complexity of the system and performance monitoring reports, as well as to focus on the most relevant and critical information for review and action. The other options are less effective plans of action, as they may involve unnecessary costs, risks, or efforts. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21
? CISA Review Questions, Answers & Explanations Database, Question ID 219

NEW QUESTION 104
- (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 107
- (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 109
- (Topic 2)
To enable the alignment of IT staff development plans with IT strategy, which of the following should be done FIRST?

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

Answer: C

Explanation:
Identifying required IT skill sets that support key business processes is the first step to enable the alignment of IT staff development plans with IT strategy. An IT strategy is a plan that defines how IT will support the organization’s goals and objectives. Identifying required IT skill sets means determining the knowledge, abilities, and competencies that IT staff need to perform their roles and responsibilities effectively and efficiently. This can help to align IT staff development plans with IT strategy, as well as to identify and address any skill gaps or needs within the IT workforce. The other options are not the first steps to enable alignment, but rather possible subsequent actions that may depend on the required IT skill sets. References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.11
? CISA Review Questions, Answers & Explanations Database, Question ID 229

NEW QUESTION 112
- (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 117
- (Topic 2)
Stress testing should ideally be earned out under a:

A. test environment with production workloads.
B. production environment with production workloads.
C. production environment with test data.
D. test environment with test data.

Answer: A

Explanation:
Stress testing is a type of performance testing that evaluates the behavior and reliability of a system under extreme conditions, such as high workload, limited resources, or concurrent users. Stress testing should ideally be carried out under a test environment with production workloads, as this would simulate the most realistic and demanding scenario for the system without affecting the actual production environment. A production environment with production workloads is not suitable for stress testing, as it could cause disruption or damage to the system and its users. A production environment with test data is not suitable for stress testing, as it could compromise the integrity and security of the production data. A test environment with test data is not suitable for stress testing, as it could underestimate the potential issues and risks that could occur in the production environment. References:
? CISA Review Manual, 27th Edition, pages 471-4721
? CISA Review Questions, Answers & Explanations Database, Question ID: 261

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

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

Answer: B

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

NEW QUESTION 125
- (Topic 2)
Which of the following would lead an IS auditor to conclude that the evidence collected during a digital forensic investigation would not be admissible in court?

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

Answer: B

Explanation:
The evidence collected during a digital forensic investigation would not be admissible in court if the logs failed to identify the person handling the evidence. This would violate the chain of custody principle, which requires that the evidence be properly documented, secured, and tracked throughout the investigation process. The chain of custody ensures that the evidence is authentic, reliable, and trustworthy, and that it has not been tampered with or altered. The person who collected the evidence, whether qualified or not, is not relevant to the admissibility of the evidence, as long as they followed the proper procedures and protocols. The evidence collected by the internal forensics team can be admissible in court, as long as they are independent, objective, and competent. The evidence does not need to be fully backed up using a cloud-based solution prior to the trial, as long as it is preserved and protected from damage or loss. References: ISACA Journal Article: Digital Forensics: Chain of Custody

NEW QUESTION 128
- (Topic 2)
An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives. Which of the following findings should be the IS auditor's GREATEST concern?

A. Users are not required to sign updated acceptable use agreements.
B. Users have not been trained on the new system.
C. The business continuity plan (BCP) was not updated.
D. Mobile devices are not encrypted.

Answer: C

Explanation:
This should be the IS auditor’s greatest concern, because it means that the organization has not considered the potential impact of the cloud document storage solution on its ability to continue its operations in the event of a disruption or disaster. A BCP is a document that outlines the procedures and actions to be taken in order to maintain or resume critical business functions during and after a crisis. A BCP should be updated whenever there is a significant change in the organization’s IT infrastructure, systems, processes, or dependencies, such as implementing a cloud document storage solution. The IS auditor should verify that the BCP reflects the current state of the organization’s IT environment, and that it addresses the risks, challenges, and opportunities associated with the cloud document storage solution.
The other options are not as concerning as the BCP not being updated:
? Users are not required to sign updated acceptable use agreements. This is a minor concern, but it does not pose a major threat to the organization’s business continuity. Acceptable use agreements are documents that define the rules and guidelines for using IT resources, such as the cloud document storage solution. Users should sign updated acceptable use agreements to acknowledge their responsibilities and obligations, and to comply with the organization’s policies and standards. However, this does not affect the organization’s ability to continue its operations in a crisis.
? Users have not been trained on the new system. This is a moderate concern, but it does not jeopardize the organization’s business continuity. Training users on the new system is important to ensure that they can use it effectively and efficiently, and to avoid errors or misuse that could compromise the security or performance of the system. However, this does not prevent the organization from accessing or restoring its data in a crisis.
? Mobile devices are not encrypted. This is a serious concern, but it does not directly impact the organization’s business continuity. Encrypting mobile devices is a security measure that protects the data stored on them from unauthorized access or disclosure in case of loss or theft. However, this does not affect the availability or integrity of the data stored in the cloud document storage solution, which should have its own encryption mechanisms.

NEW QUESTION 132
- (Topic 2)
During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's NEXT step?

A. Perform substantive testing of terminated users' access rights.
B. Perform a review of terminated users' account activity
C. Communicate risks to the application owner.
D. Conclude that IT general controls ate ineffective.

Answer: B

Explanation:
The IS auditor’s next step after determining that many terminated users’ accounts were not disabled is to perform a review of terminated users’ account activity. This means that the IS auditor should check whether any of the terminated users’ accounts were accessed or used after their termination date, which could indicate unauthorized or fraudulent activity. The IS auditor should also assess the impact and risk of such activity on the confidentiality, integrity, and availability of IT resources and data. The other options are not as appropriate as performing a review of terminated users’ account activity, as they do not provide sufficient evidence or assurance of the extent and effect of the problem.
References: CISA Review Manual, 27th Edition, page 240

NEW QUESTION 135
- (Topic 2)
Which of the following is the BEST way for an organization to mitigate the risk associated with third-party application performance?

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

Answer: D

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

NEW QUESTION 136
- (Topic 2)
An IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer payments. The IS auditor should FIRST

A. document the exception in an audit report.
B. review security incident reports.
C. identify compensating controls.
D. notify the audit committee.

Answer: C

Explanation:
The first action that an IS auditor should take when finding a high-risk vulnerability in a public-facing web server used to process online customer payments is to identify compensating controls. Compensating controls are alternative or additional controls that provide reasonable assurance of mitigating the risk of exploiting the vulnerability. The IS auditor should assess the effectiveness of the compensating controls and determine whether they reduce the risk to an acceptable level. If not, the IS auditor should recommend remediation actions to address the vulnerability. Documenting the exception in an audit report is an important action, but it should not be the first action, as it does not address the urgency of the situation. Reviewing security incident reports is a useful action, but it should not be the first

action, as it does not provide assurance of preventing future incidents. Notifying the audit committee is a necessary action, but it should not be the first action, as it does not involve taking any corrective measures. References:
? CISA Review Manual, 27th Edition, pages 295-2961
? CISA Review Questions, Answers & Explanations Database, Question ID: 260

NEW QUESTION 141
- (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 143
- (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 144
- (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 147
- (Topic 2)
An IS auditor is analyzing a sample of accesses recorded on the system log of an application. The auditor intends to launch an intensive investigation if one exception is found Which sampling method would be appropriate?

A. Discovery sampling

B. Judgmental sampling
C. Variable sampling
D. Stratified sampling

Answer: A

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

NEW QUESTION 151
- (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 152
- (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 154
- (Topic 2)
An IS auditor should ensure that an application's audit trail:

A. has adequate security.
B. logs ail database records.
C. Is accessible online
D. does not impact operational efficiency

Answer: A

Explanation:
An application's audit trail is a record of all actions or events that occur within or affect an application, such as user activities, system operations, data changes, errors, exceptions, etc. An audit trail can provide evidence and accountability for an application's functionality and performance, and support auditing, monitoring, troubleshooting, and investigation purposes. An IS auditor should ensure that an application's audit trail has adequate security, which means that it is protected from unauthorized access, modification, deletion, or disclosure. Adequate security can help ensure that an audit trail maintains its integrity, reliability, and availability, and prevents tampering or manipulation by attackers or insiders who want to hide their tracks or evidence of their actions. Logs all database records is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as logging all database records may not be necessary or feasible for some applications, and may generate excessive or irrelevant data that can affect the storage or analysis of the audit trail. Is accessible online is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as online accessibility may not be required or desirable for some applications, and may introduce security or privacy risks for the audit trail. Does not impact operational efficiency is a desirable outcome of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as operational efficiency may not be the primary objective or concern of an application's audit trail, and may depend on other factors or trade-offs such as storage capacity, performance speed, or data quality.

NEW QUESTION 155
- (Topic 2)
During an audit of a multinational bank's disposal process, an IS auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

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

Answer: C

Explanation:
During an audit of a multinational bank's disposal process, an IS auditor should be most concerned about backup media being disposed before the end of the retention period. This is because backup media contain sensitive and critical data that may be required for business continuity, legal compliance, or forensic purposes. Disposing backup media prematurely may result in data loss, unavailability, or corruption, which may have severe consequences for the bank's reputation, operations, and security. Backup media not being reviewed before disposal, degaussing being used instead of physical shredding, and hardware not being destroyed by a certified vendor are also findings that may pose some risks to the bank's disposal process, but they are not as critical as backup media being disposed before the end of the retention period. References: ISACA CISA Review Manual 27th Edition, page 302.

NEW QUESTION 156
- (Topic 2)
Which of the following activities would allow an IS auditor to maintain independence while facilitating a control sell-assessment (CSA)?

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

Answer: D

Explanation:
Developing the CSA questionnaire is an activity that would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA). An IS auditor can design and provide a CSA questionnaire to help the business units or process owners to evaluate their own controls and identify any issues or improvement opportunities. This will enable an IS auditor to support and guide the CSA process without compromising their objectivity or independence. The other options are activities that would impair an IS auditor's independence while facilitating a CSA, as they involve implementing, completing, or developing remediation actions for control issues. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.41
? CISA Review Questions, Answers & Explanations Database, Question ID 215

NEW QUESTION 158
- (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 163
- (Topic 2)
The GREATEST benefit of using a polo typing approach in software development is that it helps to:

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

Answer: C

Explanation:
The greatest benefit of using a prototyping approach in software development is that it helps to conceptualize and clarify requirements. A prototyping approach is a method of creating a simplified or partial version of a software product to demonstrate its features and functionality. A prototyping approach can help to elicit, validate, and refine the requirements of the software product, as well as to obtain feedback from the users and stakeholders. The other options are not the greatest benefits of using a prototyping approach, but rather possible outcomes or advantages of doing so. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.11
? CISA Review Questions, Answers & Explanations Database, Question ID 227

NEW QUESTION 164
- (Topic 2)
Which of the following is an example of a preventative control in an accounts payable system?

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

Answer: A

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

NEW QUESTION 166
- (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 169
- (Topic 2)
Upon completion of audit work, an IS auditor should:

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

Answer: B

Explanation:
Upon completion of audit work, an IS auditor should distribute a summary of general findings to the members of the auditing team. This is to ensure that the audit team members are aware of the audit results, have an opportunity to provide feedback, and can agree on the audit conclusions and recommendations. Providing a report to senior management prior to discussion with the auditee, providing a report to the auditee stating the initial findings, and reviewing the working papers with the auditee are not appropriate actions for an IS auditor to take upon completion of audit work, as they may compromise
the audit independence, objectivity, and quality. References: ISACA CISA Review Manual 27th Edition, page 221

NEW QUESTION 171
- (Topic 2)
Which of the following should be of MOST concern to an IS auditor reviewing the public key infrastructure (PKI) for enterprise email?

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

Answer: A

NEW QUESTION 174
- (Topic 2)
In data warehouse (DW) management, what is the BEST way to prevent data quality issues caused by changes from a source system?

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

Answer: C

Explanation:

Including the data warehouse in the impact analysis for any changes in the source system is the best way to prevent data quality issues caused by changes from a source system. A data warehouse is a centralized repository of integrated data from one or more source systems. An impact analysis is a technique of assessing the potential effects and consequences of a change on the existing system or environment. Including the data warehouse in the impact analysis can help to identify and mitigate any data quality issues that may arise from changes in the source system, such as data inconsistency, incompleteness, or inaccuracy. The other options are less effective ways to prevent data quality issues, as they may involve data quality alerts, approval for changes, or access restrictions. References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.41
? CISA Review Questions, Answers & Explanations Database, Question ID 226

NEW QUESTION 179
- (Topic 2)
During an exit interview, senior management disagrees with some of me facts presented m the draft audit report and wants them removed from the report. Which of the following would be the auditor's BEST course of action?

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

Answer: D

Explanation:
The auditor's best course of action when senior management disagrees with some of the facts presented in the draft audit report is to gather evidence to analyze senior management's objections. The auditor should not revise the assessment, escalate the issue, or finalize the report without changes until they have evaluated the validity and relevance of senior management's objections and resolved any discrepancies or misunderstandings. The auditor should maintain a professional and objective attitude and seek to present a fair and accurate audit report based on sufficient and appropriate evidence. References:
? CISA Review Manual (Digital Version), page 372
? CISA Questions, Answers & Explanations Database, question ID 3338

NEW QUESTION 180
- (Topic 2)
During the implementation of a new system, an IS auditor must assess whether certain automated calculations comply with the regulatory requirements Which of the following is the BEST way to obtain this assurance?

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

Answer: C

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

NEW QUESTION 183
- (Topic 2)
Which of the following Is the BEST way to ensure payment transaction data is restricted to the appropriate users?

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

Answer: C

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

NEW QUESTION 187
- (Topic 2)
Which of the following would BEST help lo support an auditor's conclusion about the effectiveness of an implemented data classification program?

A. Purchase of information management tools
B. Business use cases and scenarios
C. Access rights provisioned according to scheme

D. Detailed data classification scheme

Answer: C

Explanation:
Access rights provisioned according to scheme would best help to support an auditor’s conclusion about the effectiveness of an implemented data classification program. This would indicate that the data classification program has been properly implemented and enforced, and that the data is protected according to its sensitivity and value. The other options are not sufficient to demonstrate the effectiveness of a data classification program, as they do not show how the data is actually accessed and used by authorized users. References:
? CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
? CISA Review Questions, Answers & Explanations Database, Question ID 2042

NEW QUESTION 191
......