Isaca

Exam Questions CISA

Isaca CISA

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (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 2
- (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 3
- (Topic 3)
An IS auditor discovers that an IT organization serving several business units assigns equal priority to all initiatives, creating a risk of delays in securing project funding Which of the following would be MOST helpful in matching demand for projects and services with available resources in a way that supports business objectives?

A. Project management
B. Risk assessment results
C. IT governance framework
D. Portfolio management

Answer: D

Explanation:
The most helpful tool in matching demand for projects and services with available resources in a way that supports business objectives is portfolio management. Portfolio management is the process of selecting, prioritizing, balancing and aligning IT projects and services with the strategic goals and value proposition of the organization3. Portfolio management helps the IT organization to allocate resources efficiently and effectively, to deliver value to the business units, and to align IT initiatives with business strategies. Project management, risk assessment results and IT governance framework are also important tools, but they are not as helpful as portfolio management in matching demand and supply of IT projects and services. References:
? CISA Review Manual, 27th Edition, page 721
? CISA Review Questions, Answers & Explanations Database - 12 Month
Subscription

NEW QUESTION 4
- (Topic 3)
When reviewing a data classification scheme, it is MOST important for an IS auditor to determine if.

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

Answer: B

Explanation:
When reviewing a data classification scheme, it is most important for an IS auditor to determine if the security criteria are clearly documented for each classification. This will help the IS auditor to evaluate if the data classification scheme is consistent, comprehensive, and aligned with the organizational objectives

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

NEW QUESTION 5
- (Topic 3)
An IS auditor finds that the process for removing access for terminated employees is not documented What is the MOST significant risk from this observation?

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

Answer: D

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

NEW QUESTION 6
- (Topic 3)
Which of the following should be the FRST step when developing a data toes prevention (DIP) solution for a large organization?

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

Answer: D

Explanation:
The first step when developing a data loss prevention (DLP) solution for a large organization is to conduct a data inventory and classification exercise. This step is essential to identify the types, locations, owners, and sensitivity levels of the data that need to be protected by the DLP solution. A data inventory and classification exercise helps to define the scope, objectives, and requirements of the DLP solution, as well as to prioritize the data protection efforts based on the business value and risk of the data. A data inventory and classification exercise also enables the organization to comply with relevant laws and regulations regarding data privacy and security.
The other options are not the first step when developing a DLP solution, but rather subsequent steps that depend on the outcome of the data inventory and classification exercise. Identifying approved data workflows across the enterprise is a step that helps to design and implement the DLP policies and controls that match the business processes and data flows. Conducting a threat analysis against sensitive data usage is a step that helps to assess and mitigate the risks associated with data leakage, theft, or misuse. Creating the DLP policies and templates is a step that helps to enforce the data protection rules and standards across the organization.
References:
? ISACA CISA Review Manual 27th Edition (2019), page 247
? Data Loss Prevention—Next Steps - ISACA1
? What is data loss prevention (DLP)? | Microsoft Security

NEW QUESTION 7
- (Topic 3)
An IS auditor reviewing security incident processes realizes incidents are resolved and closed, but root causes are not investigated. Which of the following should be the MAJOR concern with this situation?

A. Abuses by employees have not been reported.
B. Lessons learned have not been properly documented
C. vulnerabilities have not been properly addressed
D. Security incident policies are out of date.

Answer: C

Explanation:
The major concern with the situation where security incidents are resolved and closed, but root causes are not investigated, is that vulnerabilities have not been properly addressed. Vulnerabilities are weaknesses or gaps in the security posture of an organization that can be exploited by threat actors to compromise its systems, data, or operations. If root causes are not investigated, vulnerabilities may remain undetected or unresolved, allowing attackers to exploit them again or use them as entry points for further attacks. This can result in repeated or escalated security incidents that can cause more damage or disruption to the organization.
The other options are not as major as the concern about vulnerabilities, but rather secondary or related issues that may arise from the lack of root cause analysis. Abuses by employees have not been reported is a concern that may indicate a lack of awareness, accountability, or monitoring of insider threats. Lessons learned have not been properly documented is a concern that may indicate a lack of improvement, learning, or feedback from security incidents. Security incident policies are out of date is a concern that may indicate a lack of alignment, review, or update of security incident processes.

References:
? ISACA CISA Review Manual 27th Edition (2019), page 254
? Why Root Cause Analysis is Crucial to Incident Response (IR) - Avertium3
? Root Cause Analysis Steps and How it Helps Incident Response …

NEW QUESTION 8
- (Topic 3)
In response to an audit finding regarding a payroll application, management implemented a new automated control. Which of the following would be MOST helpful to the IS auditor when evaluating the effectiveness of the new control?

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

Answer: B

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

NEW QUESTION 9
- (Topic 3)
Which of the following is MOST critical for the effective implementation of IT governance?

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

Answer: C

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

NEW QUESTION 10
- (Topic 3)
An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

A. Improve the change management process
B. Establish security metrics.
C. Perform a penetration test
D. Perform a configuration review

Answer: D

Explanation:
The best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities is to perform a configuration review. A configuration review is an audit procedure that involves examining and verifying the security settings and parameters of application servers against predefined standards or best practices. A configuration review can help to identify and remediate any deviations, inconsistencies, or misconfigurations that may expose the application servers to unauthorized access, exploitation, or compromise6. A configuration review can also help to ensure compliance with security policies and regulations, as well as enhance the performance and availability of application servers. The other options are less effective or incorrect because:
? A. Improving the change management process is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While improving the change management process may help to prevent future inconsistencies or misconfigurations in application server settings, it does not ensure that the existing ones are detected and corrected.
? B. Establishing security metrics is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While establishing security metrics may help to measure and monitor the security performance and posture of application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected.
? C. Performing a penetration test is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While performing a penetration test may help to simulate and evaluate the impact of an attack on application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected. References: Configuring system to use application server security - IBM, Application Security Risk: Assessment and Modeling - ISACA, Five Key Components of an Application Security Program - ISACA, ISACA Practitioner Guidelines for Auditors - SSH, SCADA Cybersecurity Framework - ISACA

NEW QUESTION 10
- (Topic 3)
Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

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

Answer: B

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

NEW QUESTION 13
- (Topic 3)
Which of the following is necessary for effective risk management in IT governance?

A. Local managers are solely responsible for risk evaluation.
B. IT risk management is separate from corporate risk management.
C. Risk management strategy is approved by the audit committee.
D. Risk evaluation is embedded in management processes.

Answer: D

Explanation:
The necessary condition for effective risk management in IT governance is that risk evaluation is embedded in management processes. Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation should be integrated into the management processes of planning, implementing, monitoring, and reviewing the IT activities and resources. This will ensure that risk management is aligned with the business objectives, strategies, and values, and that risk responses are timely, appropriate, and effective. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 14
- (Topic 3)
Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA> to automate routine business tasks?

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

Answer: A

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

NEW QUESTION 19
- (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 24
- (Topic 3)
An IS auditor follows up on a recent security incident and finds the incident response was not adequate. Which of the following findings should be considered MOST critical?

A. The security weakness facilitating the attack was not identified.
B. The attack was not automatically blocked by the intrusion detection system (IDS).
C. The attack could not be traced back to the originating person.
D. Appropriate response documentation was not maintained.

Answer: A

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

NEW QUESTION 29
- (Topic 3)
During a follow-up audit, an IS auditor finds that some critical recommendations have the IS auditor's BEST course of action?

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

Answer: C

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

NEW QUESTION 31
- (Topic 3)
An audit identified that a computer system is not assigning sequential purchase order numbers to order requests. The IS auditor is conducting an audit follow-up to determine if management has reserved this finding. Which of two following is the MOST reliable follow- up procedure?

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

Answer: C

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

NEW QUESTION 36
- (Topic 3)
Which of the following is MOST important to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition?

A. Role-based access control policies
B. Types of data that can be uploaded to the platform
C. Processes for on-boarding and off-boarding users to the platform
D. Processes for reviewing administrator activity

Answer: B

Explanation:
The most important thing to determine during the planning phase of a cloud- based messaging and collaboration platform acquisition is the types of data that can be uploaded to the platform. This is because different types of data may have different security, privacy, and compliance requirements, depending on the nature, sensitivity, and value of the data. For example, personal data, financial data, health data, or intellectual property data may be subject to various laws and regulations that govern how they can be collected, stored, processed, and shared in the cloud. Therefore, it is essential to identify and classify the types of data that will be uploaded to the platform, and ensure that the platform meets the organization’s policies and standards for data protection1.
The other options are not as important as the types of data that can be uploaded to the platform during the planning phase of a cloud-based messaging and collaboration platform acquisition. Option A, role-based access control policies, is a mechanism that defines who can access what data and resources on the platform based on their roles and responsibilities. Role-based access control policies are important for ensuring data security and accountability, but they can be designed and implemented after the platform is acquired2. Option C, processes for on-boarding and off-boarding users to the platform, are procedures that enable or disable user accounts and access rights on the platform. Processes for on-boarding and off-boarding users are important for managing user identities and lifecycles, but they can be developed and executed after the platform is acquired3. Option D, processes for reviewing administrator activity, are methods that monitor and audit the actions and events performed by administrators on the
platform. Processes for reviewing administrator activity are important for detecting and preventing unauthorized or malicious activities, but they can be established and performed after the platform is acquired4.
References:
? Cloud Messaging and Collaboration Services - Maryland.gov DoIT4
? MessageBird acquires real-time notifications and in-app messaging platform Pusher for $35M | TechCrunch2
? Symphony to lead financial market communications with the acquisition of Cloud9 Technologies3
? Cloud messaging and collaboration | Sumo Logic

NEW QUESTION 40
- (Topic 3)
Which of the following is the PRIMARY advantage of using visualization technology for corporate applications?

A. Improved disaster recovery
B. Better utilization of resources
C. Stronger data security
D. Increased application performance

Answer: B

Explanation:
Visualization technology is the use of software and hardware to create graphical representations of data, such as charts, graphs, maps, images, etc. Visualization technology can help users to understand, analyze, and communicate complex and large amounts of data in an intuitive and engaging way1.
One of the primary advantages of using visualization technology for corporate applications is that it can improve the utilization of resources, such as time, money, human capital, and physical assets. Some of the ways that visualization technology can achieve this are:
? Visualization technology can help users to quickly and easily explore, filter, and
interact with data, reducing the need for manual data processing and analysis1. This can save time and effort for both data producers and consumers, and allow them to focus on more value-added tasks.
? Visualization technology can help users to discover patterns, trends, outliers,
correlations, and causations in data that may otherwise be hidden or overlooked in traditional reports or tables1. This can enable users to make better and faster decisions based on data-driven insights, and optimize their strategies and actions accordingly.
? Visualization technology can help users to communicate and share data more
effectively and persuasively with different audiences, such as customers, partners, investors, regulators, etc1. This can enhance the reputation and credibility of the organization, and foster collaboration and innovation among stakeholders.
? Visualization technology can help users to monitor and measure the performance
and impact of their activities, products, services, or processes1. This can help users to identify problems or opportunities for improvement, and adjust their plans or actions accordingly.
? Visualization technology can help users to create engaging and interactive
experiences for their customers or end-users1. This can increase customer satisfaction and loyalty, and generate more revenue or value for the organization.
Therefore, using visualization technology for corporate applications can help organizations to better utilize their resources and achieve their goals.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? TechRadar Blog, Best data visualization tools of 20232
? IBM Blog, What is Data Visualization?3
? TDWI Blog, Data Visualization Technology4
? Tableau Blog, What are the advantages and disadvantages of data visualization?

NEW QUESTION 45
- (Topic 3)
Which of the following provides the BEST providence that outsourced provider services are being properly managed?

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

Answer: B

Explanation:
Adequate action taken for noncompliance with the service level agreement (SLA) provides the best evidence that outsourced provider services are being properly managed. This shows that the organization is monitoring the performance of the provider and enforcing the terms of the SLA.
The other options are not as convincing as evidence of proper management. Option A, the SLA includes penalties for non-performance, is a good practice but does not guarantee that the penalties are actually applied or that the performance is satisfactory. Option C, the vendor provides historical data to demonstrate its performance, is not reliable because the data may be biased or inaccurate. Option D, internal performance standards align with corporate strategy, is irrelevant to the question of outsourced provider management. References:
? ISACA, CISA Review Manual, 27th Edition, 2019, page 2821
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 1066692

NEW QUESTION 48
- (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 52
- (Topic 3)
An IS auditor has completed the fieldwork phase of a network security review and is preparing the initial following findings should be ranked as the HIGHEST risk?

A. Network penetration tests are not performed
B. The network firewall policy has not been approved by the information security officer.
C. Network firewall rules have not been documented.
D. The network device inventory is incomplete.

Answer: A

Explanation:
The finding that should be ranked as the highest risk is that network penetration tests are not performed. Network penetration tests are simulated cyberattacks that aim to identify and exploit the vulnerabilities and weaknesses of the network security controls, such as firewalls, routers, switches, servers, and devices. Network penetration tests are essential for assessing the effectiveness and resilience of the network security posture, and for providing recommendations for improvement and remediation. If network penetration tests are not performed, the organization may not be aware of the existing or potential threats
and risks to its network, and may not be able to prevent or respond to real cyberattacks, which can result in data breaches, service disruptions, financial losses, reputational damage, and legal or regulatory penalties. The other findings are also important, but not as risky as the lack of network penetration tests, because they either do not directly affect the network security controls, or they can be addressed by documentation or approval processes. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION 53
- (Topic 3)
Which of the following is the BEST metric to measure the alignment of IT and business strategy?

A. Level of stakeholder satisfaction with the scope of planned IT projects
B. Percentage of enterprise risk assessments that include IT-related risk
C. Percentage of stat satisfied with their IT-related roles
D. Frequency of business process capability maturity assessments

Answer: B

Explanation:
The best metric to measure the alignment of IT and business strategy is the percentage of enterprise risk assessments that include IT-related risk. This metric

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

NEW QUESTION 55
- (Topic 3)
An IS auditor has been asked to advise on measures to improve IT governance within the organization. Which at the following is the BEST recommendation?

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

Answer: A

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

NEW QUESTION 56
- (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 59
- (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 60
- (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 65
- (Topic 3)
Which of the following is MOST important when implementing a data classification program?

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

Answer: B

Explanation:
Data classification is the process of organizing data into categories based on its sensitivity, value, and risk to the organization. Data classification helps to ensure that data is protected according to its importance and regulatory requirements. Data classification also enables data owners to make informed decisions about data access, retention, and disposal.
To implement a data classification program, it is most important to formalize data ownership. Data owners are the individuals or business units that have the authority and responsibility for the data they create or use. Data owners should be involved in defining the data classification levels, assigning the appropriate classification to their data, and ensuring that the data is handled according to the established policies and procedures. Data owners should also review and update the data classification periodically or when there are changes in the data or its usage.
The other options are not as important as formalizing data ownership when implementing a data classification program. Understanding the data classification levels is necessary, but it is not sufficient without identifying the data owners who will apply them. Developing a privacy policy is a good practice, but it is not specific to data classification. Planning for secure storage capacity is a technical consideration, but it does not address the business and legal aspects of data classification.
References:
? ISACA, CISA Review Manual, 27th Edition, 2020, page 247
? Data Classification: What It Is and How to Implement It

NEW QUESTION 69
- (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 70
- (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 75
- (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 77
- (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 79
- (Topic 2)
An organization has recently implemented a Voice-over IP (VoIP) communication system. Which ot the following should be the IS auditor's PRIMARY concern?

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

Answer: A

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

NEW QUESTION 80
- (Topic 2)
Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?

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

Answer: A

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

? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.21
? CISA Review Questions, Answers & Explanations Database, Question ID 222

NEW QUESTION 81
- (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 83
- (Topic 2)
While auditing a small organization's data classification processes and procedures, an IS auditor noticed that data is often classified at the incorrect level. What is the MOST effective way for the organization to improve this situation?

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

Answer: B

Explanation:
This is the most effective way for the organization to improve its data classification processes and procedures, because data owners are the ones who are responsible for assigning the appropriate level of classification to the data they create, collect, or manage. Data owners should be aware of the data classification policy, the criteria for each level of classification, and the implications of misclassification. IT security staff can provide tailored training for data owners based on their roles, functions, and types of data they handle.
The other options are not as effective as having IT security staff conduct targeted training for data owners:
? Use automatic document classification based on content. This is a possible option, but it may not be feasible or accurate for a small organization. Automatic document classification is a process that uses artificial intelligence or machine learning to analyze the content of a document and assign a class label based on predefined rules or models. However, this process may require a lot of resources, expertise, and maintenance, and it may not capture all the nuances and context of the data. The IS auditor should also verify the reliability and validity of the automatic document classification system.
? Publish the data classification policy on the corporate web portal. This is a good practice, but it is not enough to improve the data classification situation. Publishing the data classification policy on the corporate web portal can increase the visibility and accessibility of the policy, but it does not ensure that data owners will read, understand, and follow it. The IS auditor should also monitor and enforce the compliance with the policy.
? Conduct awareness presentations and seminars for information classification policies. This is a useful measure, but it is not the most effective one. Conducting awareness presentations and seminars can raise the general awareness and knowledge of information classification policies among all employees, but it may not address the specific needs and challenges of data owners. The IS auditor should also provide more in-depth and practical training for data owners.

NEW QUESTION 85
- (Topic 2)
Which of the following environments is BEST used for copying data and transformation into a compatible data warehouse format?

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

Answer: C

Explanation:
The best environment for copying data and transforming it into a compatible data warehouse format is the staging environment. The staging environment is a temporary area where data from various sources are extracted, transformed, and loaded (ETL) before being moved to the data warehouse. The staging environment allows for data cleansing, validation, integration, and standardization without affecting the source or target systems. The testing environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for verifying and validating the functionality and performance of applications or systems. The replication environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for creating identical copies of data or systems for backup or recovery purposes. The development environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for creating or modifying applications or systems. References:
? CISA Review Manual, 27th Edition, pages 475-4761
? CISA Review Questions, Answers & Explanations Database, Question ID: 2642

NEW QUESTION 90
- (Topic 2)
Which of the following activities provides an IS auditor with the MOST insight regarding potential single person dependencies that might exist within the organization?

A. Reviewing vacation patterns

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

Answer: D

Explanation:
Mapping IT processes to roles is an activity that provides an IS auditor with the most insight regarding potential single person dependencies that might exist within the organization. Single person dependencies occur when only one person has the knowledge, skills, or access rights to perform a critical IT function. Mapping IT processes to roles can help to identify such dependencies and assess their impact on the continuity and security of IT operations. The other activities do not provide as much insight into single person dependencies, as they do not show the relationship between IT processes and roles. References: CISA Review Manual, 27th Edition, page 94

NEW QUESTION 91
- (Topic 2)
Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS audit has been asked to conduct a control assessment. the auditor's BEST course of action would be to determine if:

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

Answer: B

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

NEW QUESTION 92
- (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 95
- (Topic 2)
The BEST way to determine whether programmers have permission to alter data in the production environment is by reviewing:

A. the access control system's log settings.
B. how the latest system changes were implemented.
C. the access control system's configuration.
D. the access rights that have been granted.

Answer: D

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

NEW QUESTION 99
- (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 103
- (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 108
- (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 111
- (Topic 2)
Which of the following represents the HIGHEST level of maturity of an information security program?

A. A training program is in place to promote information security awareness.
B. A framework is in place to measure risks and track effectiveness.
C. Information security policies and procedures are established.

D. The program meets regulatory and compliance requirements.

Answer: B

Explanation:
According to the ISACA's Information Security Governance Guidance for Boards of Directors and Executive Management, the highest level of maturity of an information security program is Level 5: Optimized, which means that the program is aligned with the business objectives and strategy, and continuously monitors and improves its performance and effectiveness. A framework is in place to measure risks and track effectiveness, and the program is proactive, adaptive, and innovative. The other options represent lower levels of maturity:
? A training program is in place to promote information security awareness. This is Level 2: Repeatable, which means that the program has some basic policies and procedures, and provides awareness training to employees.
? Information security policies and procedures are established. This is Level 3:
Defined, which means that the program has formalized policies and procedures, and assigns roles and responsibilities for information security.
? The program meets regulatory and compliance requirements. This is Level 4:
Managed, which means that the program has established metrics and reporting mechanisms, and complies with relevant laws and regulations.
References: : ISACA. (2001). Information Security Governance Guidance for B

NEW QUESTION 116
- (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 118
- (Topic 2)
An IS auditor learns the organization has experienced several server failures in its distributed environment. Which of the following is the BEST recommendation to limit the potential impact of server failures in the future?

A. Redundant pathways
B. Clustering
C. Failover power
D. Parallel testing

Answer: B

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

NEW QUESTION 123
- (Topic 2)
An organization is planning an acquisition and has engaged an IS auditor lo evaluate the IT governance framework of the target company. Which of the following would be MOST helpful In determining the effectiveness of the framework?

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

Answer: C

Explanation:
Recent third-party IS audit reports would be most helpful in determining the effectiveness of the IT governance framework of the target company. IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. A third-party IS audit is an independent and objective examination of an organization's IT governance framework by an external auditor. Recent third-party IS audit reports can provide reliable and unbiased evidence of the strengths, weaknesses, and maturity of the IT governance framework of the target company. The other options are not as helpful as recent third-party IS audit reports, as they may not be as comprehensive, accurate, or current as external audits. References: CISA Review Manual, 27th Edition, page 94

NEW QUESTION 125
- (Topic 2)
Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization's incident management processes?

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

Answer: D

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

NEW QUESTION 126
- (Topic 2)
The IS auditor has recommended that management test a new system before using it in production mode. The BEST approach for management in developing a test plan is to use processing parameters that are:

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

Answer: D

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

NEW QUESTION 128
- (Topic 2)
Which of the following should be an IS auditor's GREATEST concern when an international organization intends to roll out a global data privacy policy?

A. Requirements may become unreasonable.
B. The policy may conflict with existing application requirements.
C. Local regulations may contradict the policy.
D. Local management may not accept the policy.

Answer: C

Explanation:
The greatest concern for an IS auditor when an international organization intends to roll out a global data privacy policy is that local regulations may contradict the policy. Data privacy regulations vary across different countries and regions, and they may impose different or conflicting requirements on how personal data can be collected, processed, stored, transferred, and disclosed. The organization should ensure that its global data privacy policy complies with the applicable local regulations in each jurisdiction where it operates, or risk facing legal sanctions or reputational damage. Requirements may become unreasonable, but this is not a major concern for an IS auditor, as it is a business decision that should be based on a cost-benefit analysis. The policy may conflict with existing application requirements, but this is not a serious concern for an IS auditor, as it can be resolved by modifying or updating the applications to align with the policy. Local management may not accept the policy, but this is not a critical concern for an IS auditor, as it can be mitigated by providing adequate training and awareness on the policy and its benefits. References:
? CISA Review Manual, 27th Edition, pages 406-4071
? CISA Review Questions, Answers & Explanations Database, Question ID: 2592

NEW QUESTION 133
- (Topic 2)
An IS auditor finds that an organization's data loss prevention (DLP) system is configured to use vendor default settings to identify violations. The auditor's MAIN concern should be that:

A. violation reports may not be reviewed in a timely manner.
B. a significant number of false positive violations may be reported.
C. violations may not be categorized according to the organization's risk profile.
D. violation reports may not be retained according to the organization's risk profile.

Answer: C

NEW QUESTION 136
- (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 139
- (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 141
- (Topic 2)
Providing security certification for a new system should include which of the following prior to the system's implementation?

A. End-user authorization to use the system in production
B. External audit sign-off on financial controls
C. Testing of the system within the production environment
D. An evaluation of the configuration management practices

Answer: D

Explanation:
Providing security certification for a new system should include an evaluation of the configuration management practices prior to the system's implementation. Configuration management is a process that ensures that the system's components are identified, controlled, and tracked throughout the system's lifecycle. Configuration management helps to maintain the security and integrity of the system by preventing unauthorized or unintended changes. End-user authorization to use the system in production is not part of security certification, but rather a post-implementation activity that grants access rights to authorized users. External audit sign-off on financial controls is not part of security certification, but rather a verification activity that ensures that the system complies with financial reporting standards. Testing of the system within the production environment is not part of security certification, but rather a validation activity that ensures that the system meets the functional and performance requirements. References:
? CISA Review Manual, 27th Edition, pages 449-4501
? CISA Review Questions, Answers & Explanations Database, Question ID: 2572

NEW QUESTION 144
- (Topic 2)
Which of the following metrics would BEST measure the agility of an organization's IT function?

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

Answer: C

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

NEW QUESTION 149
- (Topic 2)
An IS audit learn is evaluating the documentation related to the most recent application user-access review performed by IT and business management It is determined that the user list was not system-generated. Which of the following should be the GREATEST concern?

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

Answer: C

NEW QUESTION 153
- (Topic 1)
An organization has outsourced its data processing function to a service provider. Which of the following would BEST determine whether the service provider continues to meet the organization s objectives?

A. Assessment of the personnel training processes of the provider
B. Adequacy of the service provider's insurance
C. Review of performance against service level agreements (SLAs)
D. Periodic audits of controls by an independent auditor

Answer: C

Explanation:
Reviewing the performance against service level agreements (SLAs) would best determine whether the service provider continues to meet the organization’s objectives, as SLAs define the expected level of service, quality, availability, and responsibilities of both parties. Assessment of the personnel training processes of the provider, adequacy of the service provider’s insurance, and periodic audits of controls by an independent auditor are important aspects of outsourcing, but they do not directly measure the performance of the service provider against the organization’s objectives. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.5.2

NEW QUESTION 155
- (Topic 1)
Which of the following BEST minimizes performance degradation of servers used to authenticate users of an e-commerce website?

A. Configure a single server as a primary authentication server and a second server as a secondary authentication server.
B. Configure each authentication server as belonging to a cluster of authentication servers.
C. Configure each authentication server and ensure that each disk of its RAID is attached to the primary controller.
D. Configure each authentication server and ensure that the disks of each server form part of a duplex.

Answer: B

Explanation:
Configuring each authentication server as belonging to a cluster of authentication servers is the best way to minimize performance degradation of servers used to authenticate users of an e-commerce website. A cluster is a group of servers that work together to provide high availability, load balancing, and fault tolerance. If one server fails or becomes overloaded, another server in the cluster can take over its workload without disrupting the service. A single server as a primary authentication server and a second server as a secondary authentication server is not as effective as a cluster, because the secondary server is only used when the primary server fails, which means it is idle most of the time and does not improve performance. Configuring each authentication server and ensuring that each disk of its RAID is attached to the primary controller does not address the issue of performance degradation, but rather the issue of data redundancy and reliability. RAID (redundant array of independent disks) is a technology that combines multiple disks into a logical unit that can tolerate disk failures and improve data access speed. Configuring each authentication server and ensuring that the disks of each server form part of a duplex does not address the issue of performance degradation, but rather the issue of data backup and recovery. A duplex is a pair of disks that store identical copies of data, so that if one disk fails, the other disk can be used to restore the data.
References: ISACA CISA Review Manual 27th Edition, page 310

NEW QUESTION 157
- (Topic 1)
The implementation of an IT governance framework requires that the board of directors of an organization:

A. Address technical IT issues.
B. Be informed of all IT initiatives.
C. Have an IT strategy committee.
D. Approve the IT strategy.

Answer: D

Explanation:
IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. The board of directors of an organization is ultimately accountable for IT governance and has the authority to approve the IT strategy. The board of directors does not need to address technical IT issues, be informed of all IT initiatives, or have an IT strategy committee, as these tasks can be delegated to other stakeholders or committees within the organization.

NEW QUESTION 158
- (Topic 1)
Which of the following provides the MOST reliable audit evidence on the validity of transactions in a financial application?

A. Walk-through reviews
B. Substantive testing
C. Compliance testing
D. Design documentation reviews

Answer: B

Explanation:
Substantive testing provides the most reliable audit evidence on the validity of transactions in a financial application. Substantive testing is an audit procedure that examines the financial statements and supporting documentation to see if they contain errors or misstatements. Substantive testing can help to verify that the transactions recorded in the financial application are authorized, complete, accurate, and properly classified. Substantive testing can include methods such as vouching, confirmation, analytical procedures, or physical examination.

NEW QUESTION 163
- (Topic 1)
Coding standards provide which of the following?

A. Program documentation
B. Access control tables
C. Data flow diagrams
D. Field naming conventions

Answer: D

Explanation:
Coding standards provide field naming conventions, which are rules for naming variables, constants, functions, classes, and other elements in a program. Coding standards help to ensure consistency, readability, maintainability, and portability of code. Program documentation, access control tables, and data flow diagrams are not part of coding standards. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.1

NEW QUESTION 165
- (Topic 1)
Which of the following should an IS auditor be MOST concerned with during a post- implementation review?

A. The system does not have a maintenance plan.
B. The system contains several minor defects.
C. The system deployment was delayed by three weeks.
D. The system was over budget by 15%.

Answer: A

Explanation:
A post-implementation review (PIR) is an assessment conducted at the end of a project cycle to determine if the project was indeed successful and to identify any existing flaws in the project1. One of the main objectives of a PIR is to evaluate the outcome and functional value of a project1. Therefore, an IS auditor should be most concerned with whether the system meets the intended requirements and delivers the expected benefits to the stakeholders. A system that does not have a maintenance plan is a major risk, as it may not be able to cope with changing needs, fix errors, or prevent security breaches. A maintenance plan is essential for ensuring the system's reliability, availability, and performance in the long term2.
The other options are less critical for a PIR, as they are more related to the project management aspects than the system quality aspects. The system may contain several minor defects that do not affect its functionality or usability, and these can be resolved in future updates. The system deployment may be delayed by three weeks due to unforeseen circumstances or dependencies, but this does not necessarily mean that the system is faulty or ineffective. The system may be over budget by 15% due to various factors such as scope creep, resource constraints, or market fluctuations, but this does not imply that the
system is not valuable or beneficial.
References: 1: Post-Implementation Review Best Practices - MetaPM 2: What is Post- Implementation Review in Project Management?

NEW QUESTION 170
- (Topic 1)
Which of the following is MOST important for an IS auditor to examine when reviewing an organization's privacy policy?

A. Whether there is explicit permission from regulators to collect personal data
B. The organization's legitimate purpose for collecting personal data
C. Whether sharing of personal information with third-party service providers is prohibited
D. The encryption mechanism selected by the organization for protecting personal data

Answer: B

Explanation:
The most important thing for an IS auditor to examine when reviewing an organization's privacy policy is its legitimate purpose for collecting personal data. A legitimate purpose is a clear and specific reason for collecting personal data that is necessary for the organization's business operations or legal obligations, and that respects the rights and interests of the data subjects. A legitimate purpose is the basis for establishing a lawful and fair processing of personal data, and it should be communicated to the data subjects in the privacy policy. The other options are not as important as the legitimate purpose in reviewing the privacy policy. Explicit permission from regulators to collect personal data is not always required, as there may be other lawful bases for data collection, such as consent, contract, or public interest. Sharing of personal information with third-party service providers is not prohibited, as long as there are adequate safeguards and agreements in place to protect the data. The encryption mechanism selected by the organization for protecting personal data is a technical control that can enhance data security, but it does not determine the legality or fairness of data collection. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

NEW QUESTION 175
- (Topic 1)
Which of the following should be done FIRST when planning a penetration test?

A. Execute nondisclosure agreements (NDAs).
B. Determine reporting requirements for vulnerabilities.
C. Define the testing scope.
D. Obtain management consent for the testing.

Answer: D

Explanation:
The first step when planning a penetration test is to obtain management consent for the testing. This is because a penetration test involves simulating a cyberattack against the organization's systems and networks, which may have legal, ethical, and operational implications. Without proper authorization from management, a penetration test may violate laws, policies, contracts, or service level agreements. Management consent also helps define the objectives, scope, and boundaries of the test, as well as the roles and responsibilities of the testers and the stakeholders. Obtaining management consent for the testing also demonstrates due care and due diligence on the part of the testers and the organization.
Executing nondisclosure agreements (NDAs), determining reporting requirements for vulnerabilities, and defining the testing scope are important steps when

planning a penetration test, but they are not the first step. These steps should be done after obtaining management consent for the testing, as they depend on the approval and involvement of management and other parties.

NEW QUESTION 179
- (Topic 1)
Which of the following should be GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

A. Data conversion was performed using manual processes.
B. Backups of the old system and data are not available online.
C. Unauthorized data modifications occurred during conversion.
D. The change management process was not formally documented

Answer: C

Explanation:
The greatest concern for an IS auditor reviewing data conversion and migration during the implementation of a new application system is unauthorized data modifications occurred during conversion. Unauthorized data modifications are changes or alterations to data that are not authorized, intended, or expected, such as due to errors, fraud, or sabotage. Unauthorized data modifications occurred during conversion can compromise the accuracy, completeness, and integrity of the data being converted and migrated to the new application system, and may result in data loss, corruption, or inconsistency. The other options are not as concerning as unauthorized data modifications occurred during conversion in reviewing data conversion and migration during the implementation of a new application system, as they do not affect the accuracy, completeness, or integrity of the data being converted and migrated. Data conversion was performed using manual processes is a possible factor that may increase the risk or complexity of data conversion and migration, but it does not necessarily imply that unauthorized data modifications occurred during conversion. Backups of the old system and data are not available online is a possible factor that may affect the availability or accessibility of the old system and data for backup or recovery purposes, but it does not imply that unauthorized data modifications occurred during conversion. The change management process was not formally documented is a possible factor that may affect the quality or consistency of the change management process for implementing the new application system, but it does not imply that unauthorized data modifications occurred during conversion. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION 182
- (Topic 1)
Documentation of workaround processes to keep a business function operational during recovery of IT systems is a core part of a:

A. business impact analysis (BIA).
B. threat and risk assessment.
C. business continuity plan (BCP).
D. disaster recovery plan (DRP).

Answer: C

Explanation:
A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A core part of a BCP is the documentation of workaround processes to keep a business function operational during recovery of IT systems. Workaround processes are alternative methods or procedures that can be used to perform a business function when the normal IT systems are unavailable or disrupted2. For example, if an online payment system is down, a workaround process could be to accept manual payments or use a backup system. Workaround processes help to minimize the impact of IT disruptions on the business operations and ensure continuity of service to customers and stakeholders3. References:
? 1 explains what is a business continuity plan and why it is important.
? 2 defines what is a workaround process and how it can be used in a BCP.
? 3 provides examples of workaround processes for different business functions.

NEW QUESTION 185
- (Topic 1)
An incorrect version of the source code was amended by a development team. This MOST likely indicates a weakness in:

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

Answer: C

Explanation:
A weakness in change management is the most likely cause of an incorrect version of source code being amended by a development team. Change management is the process of controlling and documenting changes to IT systems and software. It ensures that changes are authorized, tested, and implemented in a controlled manner. If change management is weak, there is a risk of using outdated or incorrect versions of source code, which can lead to errors, defects, or security vulnerabilities in the software.

NEW QUESTION 190
- (Topic 1)
Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

A. Independent reconciliation
B. Re-keying of wire dollar amounts
C. Two-factor authentication control
D. System-enforced dual control

Answer: D

Explanation:
The best method to prevent wire transfer fraud by bank employees is system-enforced dual control. System-enforced dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity using a system that enforces this requirement. System-enforced dual control can prevent wire transfer fraud by requiring independent verification and approval of payment requests, amounts, and recipients by different bank employees using a system that does not allow any single employee to complete the transaction alone. The other options are not as effective as system-enforced dual control in preventing wire transfer fraud, as they do not involve independent checks or approvals using a system. Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent wire transfer fraud from occurring. Re-keying of wire dollar amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent wire transfer fraud from occurring. Two-factor authentication control is an access control that can help verify the identity and authorization of bank employees, but it does not prevent wire transfer fraud from occurring. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION 192
- (Topic 1)
Which of the following is a social engineering attack method?

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

Answer: B

Explanation:
An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone. This is a social engineering attack method that exploits the trust or curiosity of the employee to obtain sensitive information that can be used to access or compromise the network. According to the web search results, social engineering is a technique that uses psychological manipulation to trick users into making security mistakes or giving away sensitive information1. Phishing, whaling, baiting, and pretexting are some of the common forms of social engineering attacks2. Social engineering attacks are often more effective and profitable than purely technical attacks, as they rely on human error rather than system vulnerabilities

NEW QUESTION 193
- (Topic 1)
An IT balanced scorecard is the MOST effective means of monitoring:

A. governance of enterprise IT.
B. control effectiveness.
C. return on investment (ROI).
D. change management effectiveness.

Answer: A

Explanation:
An IT balanced scorecard is a strategic management tool that aligns IT objectives with business goals and measures the performance of IT processes using key performance indicators (KPIs). It is the most effective means of monitoring governance of enterprise IT, which is the process of ensuring that IT supports the organization’s strategy and objectives. Governance of enterprise IT covers aspects such as IT value delivery, IT risk management, IT resource management, and IT performance measurement. An IT balanced scorecard can help monitor these aspects and provide feedback to improve IT governance. References: ISACA Frameworks: Blueprints for Success, CISA Review Manual (Digital Version)

NEW QUESTION 194
- (Topic 1)
An IS auditor discovers that validation controls m a web application have been moved from the server side into the browser to boost performance This would MOST likely increase the
risk of a successful attack by.

A. phishing.
B. denial of service (DoS)
C. structured query language (SQL) injection
D. buffer overflow

Answer: C

Explanation:
Moving validation controls from the server side into the browser would most likely increase the risk of a successful attack by structured query language (SQL) injection. SQL injection is a technique that exploits a security vulnerability in an application’s database layer by inserting malicious SQL statements into user input fields. Validation controls are used to check and filter user input before sending it to the database. If these controls are moved to the browser, they can be easily bypassed or modified by an attacker, who can then execute arbitrary SQL commands on the database. References: CISA Review Manual, 27th Edition, page 361

NEW QUESTION 195
- (Topic 1)
Secure code reviews as part of a continuous deployment program are which type of control?

A. Detective
B. Logical
C. Preventive
D. Corrective

Answer: C

Explanation:
Secure code reviews as part of a continuous deployment program are preventive controls. Preventive controls are controls that aim to prevent or avoid

undesirable events or outcomes from occurring, such as errors, defects, or incidents. Secure code reviews are activities that examine and evaluate the source code of a software or application to identify and eliminate any vulnerabilities, flaws, or weaknesses that may compromise its security, functionality, or performance. Secure code reviews as part of a continuous deployment program can help prevent or avoid security issues or incidents from occurring by ensuring that the code is secure and compliant before it is deployed to production. The other options are not correct types of controls for secure code reviews as part of a continuous deployment program, as they have different meanings and functions. Detective controls are controls that aim to detect or discover undesirable events or outcomes that have occurred, such as errors, defects, or incidents. Logical controls are controls that use software or hardware mechanisms to regulate or restrict access to IT resources, such as data, systems, or networks. Corrective controls are controls that aim to correct or rectify undesirable events or outcomes that have occurred, such as errors, defects, or incidents. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION 199
- (Topic 3)
Which of the following would be MOST effective to protect information assets in a data center from theft by a vendor?

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

Answer: A

Explanation:
The most effective control to protect information assets in a data center from theft by a vendor is to monitor and restrict vendor activities. A vendor may have legitimate access to the data center for maintenance or support purposes, but they may also have malicious intentions or be compromised by an attacker. By monitoring and restricting vendor activities, the organization can ensure that the vendor only performs authorized tasks and does not access or tamper with sensitive data or equipment. Issuing an access card to the vendor, concealing data devices and information labels, and restricting use of portable and wireless devices are also useful controls, but they are not as effective as monitoring and restricting vendor activities in preventing theft by a vendor. References:
? CISA Review Manual, 27th Edition, page 3381
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 203
- (Topic 3)
Which of the following BEST enables the effectiveness of an agile project for the rapid development of a new software application?

A. Project segments are established.
B. The work is separated into phases.
C. The work is separated into sprints.
D. Project milestones are created.

Answer: C

Explanation:
The best way to enable the effectiveness of an agile project for the rapid development of a new software application is to separate the work into sprints. Sprints are short, time-boxed iterations that deliver a potentially releasable product increment at the end of each sprint. Sprints allow agile teams to work in a flexible and adaptive manner, respond quickly to changing customer needs and feedback, and deliver value faster and more frequently. Sprints also help teams to plan, execute, review, and improve their work in a collaborative and transparent way. Project segments, phases, and milestones are not specific to agile projects and do not necessarily enable the effectiveness of an agile project. References: Agile Project Management [What is it & How to Start] - Atlassian, CISA Review Manual (Digital Version).

NEW QUESTION 205
- (Topic 3)
What is the PRIMARY benefit of an audit approach which requires reported findings to be issued together with related action plans, owners, and target dates?

A. it facilitates easier audit follow-up
B. it enforces action plan consensus between auditors and auditees
C. it establishes accountability for the action plans
D. it helps to ensure factual accuracy of findings

Answer: C

Explanation:
The primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates is that it establishes accountability for the action plans. Accountability means that the individuals or groups who are responsible for implementing the action plans are clearly identified and held liable for their completion within the specified time frame. Accountability also implies that the action plans are monitored and evaluated to ensure that they are effective and efficient in addressing the audit findings and mitigating the associated risks1. Accountability helps to ensure that the audit recommendations are taken seriously and implemented properly, and that the audit value is realized by the organization2. The other options are less relevant or incorrect because:
? A. It facilitates easier audit follow-up is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a secondary or indirect benefit. Audit follow-up is the process of verifying whether the action plans have been implemented and whether they have resolved the audit findings3. While having clear action plans, owners, and target dates may facilitate easier audit follow-up by providing a basis for tracking and reporting the progress and status of the action plans, it does not necessarily guarantee that the action plans will be implemented or effective.
? B. It enforces action plan consensus between auditors and auditees is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a prerequisite or condition for such an approach. Action plan consensus means that the auditors and auditees agree on the audit findings and recommendations, and on the action plans to address them4. While having action plan consensus may enhance the credibility and acceptance of the audit approach, it does not necessarily ensure that the action plans will be implemented or effective.
? D. It helps to ensure factual accuracy of findings is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of an outcome or result of such an approach. Factual accuracy of findings means that the audit findings are based on sufficient, reliable, relevant, and useful evidence5. While having factual accuracy of findings may increase the confidence and trust in the audit approach, it does not necessarily ensure that the action plans will be implemented or effective. References: Accountability - ISACA, Audit Value - ISACA, Audit Follow- up - ISACA, Action Plan Consensus - ISACA, Factual Accuracy of Findings -

ISACA

NEW QUESTION 210
- (Topic 3)
Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

A. Inability to utilize the site when required
B. Inability to test the recovery plans onsite
C. Equipment compatibility issues at the site
D. Mismatched organizational security policies

Answer: A

Explanation:
The greatest risk of using a reciprocal site for disaster recovery is the inability to utilize the site when required. A reciprocal site is an agreement between two organizations to provide backup facilities for each other in case of a disaster. However, this arrangement may not be reliable or enforceable, especially if both organizations are affected by the same disaster or have conflicting priorities. Therefore, the IS auditor should recommend that management consider alternative options for disaster recovery, such as dedicated sites or cloud services12. References:
? CISA Review Manual, 27th Edition, page 3381
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 214
- (Topic 3)
During an IT general controls audit of a high-risk area where both internal and external audit teams are reviewing the same approach to optimize resources?

A. Leverage the work performed by external audit for the internal audit testing.
B. Ensure both the internal and external auditors perform the work simultaneously.
C. Request that the external audit team leverage the internal audit work.
D. Roll forward the general controls audit to the subsequent audit year.

Answer: A

Explanation:
The best approach to optimize resources when both internal and external audit teams are reviewing the same IT general controls area is to leverage the work performed by external audit for the internal audit testing. This can avoid duplication of efforts, reduce audit costs and enhance coordination between the audit teams. The internal audit team should evaluate the quality and reliability of the external audit work before relying on it. Ensuring both the internal and external auditors perform the work simultaneously is not an efficient use of resources, as it would create redundancy and possible interference. Requesting that the external audit team leverage the internal audit work may not be feasible or acceptable, as the external audit team may have different objectives, standards and independence requirements. Rolling forward the general controls audit to the subsequent audit year is not a good practice, as it would delay the identification and remediation of any control weaknesses in a high-risk area. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 247

NEW QUESTION 219
- (Topic 3)
in a controlled application development environment, the MOST important segregation of duties should be between the person who implements changes into the production environment and the:

A. application programmer
B. systems programmer
C. computer operator
D. quality assurance (QA) personnel

Answer: A

Explanation:
In a controlled application development environment, the most important segregation of duties should be between the person who implements changes into the production environment and the application programmer. This segregation of duties ensures that no one person can create and deploy code without proper review, testing, and approval. This reduces the risk of errors, fraud, or malicious code being introduced into the production environment.
The other options are not as important as the segregation between the application programmer and the person who implements changes into production, but they are still relevant for achieving a secure and reliable application development environment. The segregation of duties between the person who implements changes into production and the systems programmer is important to prevent unauthorized or untested changes to system software or configuration. The segregation of duties between the person who implements changes into production and the computer operator is important to prevent unauthorized or uncontrolled access to production data or resources. The segregation of duties between the person who implements changes into production and the quality assurance (QA) personnel is important to ensure independent verification and validation of code quality and functionality.
References:
? ISACA CISA Review Manual 27th Edition (2019), page 247
? Segregation of Duties in an Agile Environment | AKF Partners3
? Separation of Duties: How to Conform in a DevOps World4

NEW QUESTION 223
......

Relate Links

100% Pass Your CISA Exam with Exambible Prep Materials

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

Contact us

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

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