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)
A review of Internet security disclosed that users have individual user accounts with Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only the corporate network is used. The organization should FIRST:

A. use a proxy server to filter out Internet sites that should not be accessed.
B. keep a manual log of Internet access.
C. monitor remote access activities.
D. include a statement in its security policy about Internet use.

Answer: D

Explanation:
The first step that the organization should take to ensure that only the corporate network is used for downloading business data is to include a statement in its security policy about Internet use. A security policy is a document that defines the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data1. A security policy should clearly state the acceptable and unacceptable use of Internet resources, such as personal accounts with ISPs, and the consequences of violating the policy. A security policy also helps to guide the implementation of technical controls, such as proxy servers, firewalls, or monitoring tools, that can enforce the policy and prevent or detect unauthorized Internet access.
The other options are not the first step that the organization should take, but rather subsequent or complementary steps that depend on the security policy. Using a proxy server to filter out Internet sites that should not be accessed is a technical control that can help implement the security policy, but it does not address the root cause of why users are using personal accounts with ISPs. Keeping a manual log of Internet access is a monitoring technique that can help audit the compliance with the security policy, but it does not prevent or deter users from using personal accounts with ISPs. Monitoring remote access activities is another monitoring technique that can help detect unauthorized Internet access, but it does not specify what constitutes unauthorized access or how to respond to it.
References:
? ISACA CISA Review Manual 27th Edition (2019), page 247
? What is a Security Policy? Definition, Elements, and Examples - Varonis1

NEW QUESTION 2
- (Topic 3)
Which of the following should an IS auditor ensure is classified at the HIGHEST level of sensitivity?

A. Server room access history
B. Emergency change records
C. IT security incidents
D. Penetration test results

Answer: D

Explanation:
The IS auditor should ensure that penetration test results are classified at the highest level of sensitivity, because they contain detailed information about the vulnerabilities and weaknesses of the IT systems and networks, as well as the methods and tools used by the testers to exploit them. Penetration test results can be used by malicious actors to launch cyberattacks or cause damage to the organization if they are disclosed or accessed without authorization. Therefore, they should be protected with the highest level of confidentiality, integrity and availability. The other options are not as sensitive as penetration test results, because they either do not reveal as much information about the IT security posture, or they are already known or reported by the organization. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

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

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

Answer: B

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

NEW QUESTION 4
- (Topic 3)
Which of the following would an IS auditor recommend as the MOST effective preventive control to reduce the risk of data leakage?

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

Answer: D

Explanation:
Digital watermarks are hidden marks or codes that can be embedded into digital files, such as images, videos, audio, or documents. They can be used to identify the source, owner, or authorized user of the data, as well as to track any unauthorized copying or distribution of the data. Digital watermarks can help prevent data

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

NEW QUESTION 5
- (Topic 3)
A company has implemented an IT segregation of duties policy. In a role-based environment, which of the following roles may be assigned to an application developer?

A. IT operator
B. System administration
C. Emergency support
D. Database administration

Answer: C

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

NEW QUESTION 6
- (Topic 3)
Management receives information indicating a high level of risk associated with potential flooding near the organization's data center within the next few years. As a result, a decision has been made to move data center operations to another facility on higher ground. Which approach has been adopted?

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

Answer: A

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

NEW QUESTION 7
- (Topic 3)
An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

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

Answer: B

Explanation:
Developing a risk-based plan considering each entity's business processes would best help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan. A risk-based plan is a plan that prioritizes the audit activities based on the level of risk associated with each area or process. A risk-based plan can help to allocate the audit resources more efficiently and effectively, and provide more assurance and value to the stakeholders1.
By considering each entity's business processes, the IS audit can identify and assess the specific risks and controls that affect the IT environment of each entity, and tailor the audit objectives, scope, and procedures accordingly. This can help to address the unique needs and expectations of each entity, and ensure that the IS audit covers the key risk areas that are relevant and significant to each entity's operations, performance, and compliance2.
The other options are not as effective as developing a risk-based plan considering each entity's business processes in ensuring that IS audit still covers key risk

areas within the IT environment as part of its annual plan. Option A, increasing the frequency of risk-based IS audits for each business entity, is not a feasible or efficient solution, as it may increase the audit costs and workload, and create duplication or overlap of audit efforts. Option C, conducting an audit of newly introduced IT policies and procedures, is a limited and narrow approach, as it may not cover all the aspects or dimensions of the IT environment that may have changed or been affected by the split. Option D, revising IS audit plans to focus on IT changes introduced after the split, is a reactive and short-term approach, as it may not reflect the current or future state of the IT environment or the business objectives of each entity.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Risk-Based Audit Planning: A Guide for Internal Audit1
? Risk-Based Audit Approach: Definition & Example

NEW QUESTION 8
- (Topic 3)
An IS auditor notes that the previous year's disaster recovery test was not completed within the scheduled time frame due to insufficient hardware allocated by a third-party vendor. Which of the following provides the BEST evidence that adequate resources are now allocated to successfully recover the systems?

A. Service level agreement (SLA)
B. Hardware change management policy
C. Vendor memo indicating problem correction
D. An up-to-date RACI chart

Answer: A

Explanation:
The best evidence that adequate resources are now allocated to successfully recover the systems is a service level agreement (SLA). An SLA is a contract between a service provider and a customer that defines the scope, quality, and terms of the service delivery. An SLA should include measurable and verifiable indicators of the service performance, such as availability, reliability, capacity, security, and recovery. An SLA should also specify the roles, responsibilities, and expectations of both parties, as well as the remedies and penalties for non-compliance. An SLA can help to ensure that the third- party vendor has allocated sufficient hardware and other resources to meet the recovery objectives and requirements of the organization. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 9
- (Topic 3)
A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items lo the inventory system. Which control would have BEST prevented this type of fraud in a retail environment?

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

Answer: A

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

NEW QUESTION 10
- (Topic 3)
An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported the auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

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

Answer: C

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

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

NEW QUESTION 10
- (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 12
- (Topic 3)
Which of the following presents the GREATEST challenge to the alignment of business and IT?

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

Answer: A

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

NEW QUESTION 13
- (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 15
- (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 20
- (Topic 3)
During an exit meeting, an IS auditor highlights that backup cycles are being missed due to operator error and that these exceptions are not being managed. Which of the following is the BEST way to help management understand the associated risk?

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

Answer: A

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

NEW QUESTION 24
- (Topic 3)
Which of the following is the BEST way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster?

A. Prepare detailed plans for each business function.
B. Involve staff at all levels in periodic paper walk-through exercises.
C. Regularly update business impact assessments.
D. Make senior managers responsible for their plan sections.

Answer: B

Explanation:
The best way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster is to involve staff at all levels in periodic paper walk-through exercises. This means that the BCPs are tested and validated by the people who will execute them in a real situation, and any gaps, errors, or inconsistencies can be identified and corrected. Paper walk-through exercises are also a good way to raise awareness and train staff on their roles and responsibilities in a BCP scenario, as well as to evaluate the feasibility and effectiveness of the recovery strategies1.

The other options are not the best ways to ensure that BCPs will work effectively, because they do not involve testing or validating the plans. Preparing detailed plans for each business function is important, but it does not guarantee that the plans are realistic, practical, or aligned with the overall business objectives and priorities2. Regularly updating business impact assessments is also essential, but it does not ensure that the BCPs are aligned with the current business environment and risks2. Making senior managers responsible for their plan sections is a good way to assign accountability and authority, but it does not ensure that the plan sections are coordinated and integrated with each other2.
References:
? Best Practice Guide: Business Continuity Planning (BCP)3
? Best Practices for Creating a Business Continuity Plan1
? Business Continuity Plan Best Practices

NEW QUESTION 28
- (Topic 3)
The PRIMARY objective of value delivery in reference to IT governance is to:

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

Answer: C

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

NEW QUESTION 31
- (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 34
- (Topic 3)
Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

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

Answer: B

Explanation:
The most important factor to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings is to document evidence handling by personnel throughout the forensic investigation. Documentation is essential to establish the chain of custody, prove the integrity and authenticity of the evidence, and demonstrate compliance with legal and ethical standards. Documentation should include information such as the date, time, location, source, destination, method, purpose, result, and authorization of each action performed on the evidence. Documentation should also include any observations, findings, assumptions, limitations, or exceptions encountered during the investigation. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 38
- (Topic 3)
Which of the following should be of GREATEST concern for an IS auditor reviewing an organization's disaster recovery plan (DRP)?

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

Answer: C

Explanation:

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

NEW QUESTION 40
- (Topic 2)
An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?

A. Data with customer personal information
B. Data reported to the regulatory body
C. Data supporting financial statements
D. Data impacting business objectives

Answer: B

Explanation:
To ensure that management concerns are addressed, internal audit should recommend that the data quality team review the data reported to the regulatory body first. This is because this data set is the most relevant and critical to the issue that triggered the enhancement of the data quality program. The data reported to the regulatory body should be accurate, complete, consistent, and timely, as any discrepancies could result in fines, penalties, or reputational damage for the organization. Data with customer personal information is important for data quality, but it is not directly related to the regulatory reporting issue. Data supporting financial statements is important for data quality, but it may not be the same as the data reported to the regulatory body. Data impacting business objectives is important for data quality, but it may not be as urgent or sensitive as the data reported to the regulatory body. References:
? CISA Review Manual, 27th Edition, pages 404-4051
? CISA Review Questions, Answers & Explanations Database, Question ID: 262

NEW QUESTION 45
- (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 49
- (Topic 2)
An organization has assigned two now IS auditors to audit a now system implementation. One of the auditors has an IT-related degree, and one has a business degree. Which ol the following is MOST important to meet the IS audit standard for proficiency?

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

Answer: C

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

way to ensure quality and accuracy of the audit work, but it does not ensure that the new auditors have the necessary proficiency to perform audit tasks independently or competently. References: CISA Review Manual (Digital Version) , Chapter 1: Information Systems Auditing Process, Section 1.4: Audit Skills and Competencies.

NEW QUESTION 50
- (Topic 2)
Which of the following would be an appropriate rote of internal audit in helping to establish an organization's privacy program?

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

Answer: A

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

NEW QUESTION 55
- (Topic 2)
Which of the following is MOST important to verify when determining the completeness of the vulnerability scanning process?

A. The organization's systems inventory is kept up to date.
B. Vulnerability scanning results are reported to the CISO.
C. The organization is using a cloud-hosted scanning tool for Identification of vulnerabilities
D. Access to the vulnerability scanning tool is periodically reviewed

Answer: A

Explanation:
The completeness of the vulnerability scanning process depends on the accuracy and currency of the organization’s systems inventory, which is a list of all the hardware and software assets that are owned or used by the organization. A complete and up-to-date systems inventory can help ensure that all the systems are identified and scanned for vulnerabilities, and that no system is missed or overlooked. Vulnerability scanning results are reported to the CISO is a good practice for ensuring accountability and visibility of the vulnerability management process, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as reporting does not guarantee that all the systems are scanned. The organization is using a cloud-hosted scanning tool for identification of vulnerabilities is a possible option for conducting vulnerability scanning, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as the type of scanning tool does not affect the scope or coverage of the scanning. Access to the vulnerability scanning tool is periodically reviewed is a critical control for ensuring the security and integrity of the vulnerability scanning tool, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as access review does not ensure that all the systems are scanned.

NEW QUESTION 58
- (Topic 2)
Which of the following is the BEST source of information for an IS auditor to use as a baseline to assess the adequacy of an organization's privacy policy?

A. Historical privacy breaches and related root causes
B. Globally accepted privacy best practices
C. Local privacy standards and regulations
D. Benchmark studies of similar organizations

Answer: C

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

NEW QUESTION 61
- (Topic 2)
Which of the following is the BEST audit procedure to determine whether a firewall is configured in compliance with the organization's security policy?

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

Answer: A

Explanation:
The best audit procedure to determine whether a firewall is configured in compliance with the organization’s security policy is reviewing the parameter settings. Parameter settings are values or options that define how a firewall operates and functions, such as rules, filters, ports, protocols, etc. By reviewing the parameter

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

NEW QUESTION 63
- (Topic 2)
An internal audit department recently established a quality assurance (QA) program. Which of the following activities Is MOST important to include as part of the QA program requirements?

A. Long-term Internal audit resource planning
B. Ongoing monitoring of the audit activities
C. Analysis of user satisfaction reports from business lines
D. Feedback from Internal audit staff

Answer: B

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

NEW QUESTION 67
- (Topic 2)
The waterfall life cycle model of software development is BEST suited for which of the following situations?

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

Answer: A

Explanation:
The waterfall life cycle model of software development is best suited for situations where the project requirements are well understood. The waterfall life cycle model is a sequential and linear approach to software development that consists of several phases, such as planning, analysis, design, implementation, testing, and maintenance. Each phase depends on the completion and approval of the previous phase before proceeding to the next phase. The waterfall life cycle model is best suited for situations where the project requirements are well understood, as it assumes that the requirements are clear, stable, and fixed at the beginning of the project, and do not change significantly throughout the project. The project is subject to time pressures is not a situation where the waterfall life cycle model of software development is best suited, as it may not be flexible or agile enough to accommodate changes or adjustments in the project schedule or timeline. The waterfall life cycle model may involve long delays or dependencies between phases, and may not allow for early feedback or delivery of software products. The project intends to apply an object-oriented design approach is not a situation where the waterfall life cycle model of software development is best suited, as it may not be compatible or effective with the object-oriented design approach. The object-oriented design approach is a technique that models software as a collection of interacting objects that have attributes and behaviors. The object-oriented design approach may require iterative and incremental development methods that allow for dynamic and adaptive changes in software design and functionality. The project will involve the use of new technology is not a situation where the waterfall life cycle model of software development is best suited, as it may not be able to cope with the uncertainty or complexity of new technology. The waterfall life cycle model may not allow for sufficient exploration or experimentation with new technology, and may not be able to handle changes or issues that arise from new technology.

NEW QUESTION 72
- (Topic 2)
The IS quality assurance (OA) group is responsible for:

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

Answer: A

Explanation:
The IS quality assurance (QA) group is responsible for ensuring that program changes adhere to established standards. Program changes are modifications made to software applications or systems to fix errors, improve performance, add functionality, or meet changing requirements. Program changes should follow established standards for documentation, authorization, testing, implementation, and review. The IS QA group is responsible for verifying that program changes comply with these standards and meet the expected quality criteria. Designing procedures to protect data against accidental disclosure; ensuring that the output received from system processing is complete; and monitoring the execution of computer processing tasks are not responsibilities of the IS QA group. References: [ISACA CISA Review Manual 27th Edition], page 304.

NEW QUESTION 77
- (Topic 2)

Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

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

Answer: D

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

NEW QUESTION 79
- (Topic 2)
Which of the following is MOST important for an IS auditor to verify when evaluating an organization's firewall?

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

Answer: A

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

NEW QUESTION 80
- (Topic 2)
A project team has decided to switch to an agile approach to develop a replacement for an existing business application. Which of the following should an IS auditor do FIRST to ensure the effectiveness of the protect audit?

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

Answer: C

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

NEW QUESTION 83
- (Topic 2)
In order to be useful, a key performance indicator (KPI) MUST

A. be approved by management.
B. be measurable in percentages.
C. be changed frequently to reflect organizational strategy.
D. have a target value.

Answer: D

Explanation:
A key performance indicator (KPI) is a quantifiable measure of performance over time for a specific objective1. KPIs help organizations and teams track their progress and achievements towards their strategic goals. To be useful, a KPI must have a target value, which is the desired level of performance or outcome that the organization or team aims to achieve. A target value provides a clear direction and a benchmark for measuring success or failure. Without a target value, a KPI is meaningless, as it does not indicate whether the performance is good or bad, or how far or close the organization or team is from reaching their objective.

NEW QUESTION 87
- (Topic 2)
An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

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

Answer: D

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

NEW QUESTION 89
- (Topic 2)
Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm tor potential software vulnerabilities?

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

Answer: D

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

NEW QUESTION 93
- (Topic 2)
Which of the following is the GREATEST risk associated with storing customer data on a web server?

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

Answer: B

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

NEW QUESTION 95
- (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 100
- (Topic 2)
Which of the following should an IS auditor review FIRST when planning a customer data privacy audit?

A. Legal and compliance requirements
B. Customer agreements
C. Data classification
D. Organizational policies and procedures

Answer: D

Explanation:
The organizational policies and procedures are the first source of guidance for an IS auditor when planning a customer data privacy audit. They provide the framework and objectives for ensuring compliance with legal and regulatory requirements, customer agreements and data classification. The IS auditor should review them first to understand the scope, roles and responsibilities, standards and controls related to customer data privacy in the organization. The other options are also important, but they are secondary sources of information that should be reviewed after the organizational policies and
procedures. References: CISA Review Manual (Digital Version) 1, Chapter 2: Governance and Management of Information Technology, Section 2.5: Privacy Principles and Policies.

NEW QUESTION 101
- (Topic 2)
An organization has developed mature risk management practices that are followed across all departments What is the MOST effective way for the audit team to leverage this risk management maturity?

A. Implementing risk responses on management's behalf
B. Integrating the risk register for audit planning purposes
C. Providing assurances to management regarding risk
D. Facilitating audit risk identification and evaluation workshops

Answer: B

Explanation:
The most effective way for the audit team to leverage the risk management maturity of the organization is to integrate the risk register for audit planning purposes. The risk register is a document that records the identified risks, their likelihood, impact, and mitigation strategies for a project or an organization. By using the risk register, the audit team can align their audit objectives, scope, and procedures with the organization's risk profile and priorities. This will help the audit team to provide more value-added and relevant assurance and recommendations to the management and stakeholders.
Some of the web sources that support this answer are:
? Audit Maturity And Risk Management | Ideagen
? Building a Mature Enterprise Risk Management Plan | AuditBoard
? CISA Certified Information Systems Auditor – Question0551

NEW QUESTION 103
- (Topic 2)
The due date of an audit project is approaching, and the audit manager has determined that only 60% of the audit has been completed. Which of the following should the audit manager do FIRST?

A. Determine where delays have occurred
B. Assign additional resources to supplement the audit
C. Escalate to the audit committee
D. Extend the audit deadline

Answer: A

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

NEW QUESTION 105
- (Topic 2)
An organization with many desktop PCs is considering moving to a thin client architecture. Which of the following is the MAJOR advantage?

A. The security of the desktop PC is enhanced.

B. Administrative security can be provided for the client.
C. Desktop application software will never have to be upgraded.
D. System administration can be better managed

Answer: C

Explanation:
The major advantage of moving from many desktop PCs to a thin client architecture is that desktop application software will never have to be upgraded. A thin client architecture is a type of client-server architecture that uses lightweight or minimal devices (thin clients) as clients that connect to a central server that provides most of the processing and storage functions. A thin client architecture can offer several benefits over a traditional desktop PC architecture, such as lower cost, higher security, easier maintenance, etc. One of these benefits is that desktop application software will never have to be upgraded on thin clients, as all the applications are installed and updated on the server, and accessed by thin clients through a network connection. This can save time and money for installing and upgrading software on individual devices, and ensure consistency and compatibility among different devices. The security of the desktop PC is enhanced is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one. A thin client architecture can enhance the security of desktop PCs by reducing the exposure or vulnerability of data and applications on individual devices, and centralizing the security management and control on the server. However, this advantage may depend on other factors such as network security, server security, user authentication, etc. Administrative security can be provided for the client is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one. A thin client architecture can provide administrative security for clients by allowing administrators to configure and manage client devices remotely from the server, and enforce policies and restrictions on client access or usage. However, this advantage may depend on other factors such as network reliability, server availability, user compliance, etc. System administration can be better managed is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one. A thin client architecture can improve system administration by simplifying and streamlining the tasks and activities involved in maintaining and supporting client devices, such as backup, recovery, troubleshooting, etc., and consolidating them on the server. However, this advantage may depend on other factors such as network bandwidth, server capacity, user satisfaction

NEW QUESTION 108
- (Topic 2)
In an online application, which of the following would provide the MOST information about the transaction audit trail?

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

Answer: C

Explanation:
In an online application, data architecture provides the most information about the transaction audit trail, as it describes how data are created, stored, processed, accessed and exchanged among different components of the application. Data architecture includes data models, schemas, dictionaries, metadata, standards and policies that define the structure, quality, integrity, security and governance of data. Data architecture can help the IS auditor to trace the origin, flow, transformation and destination of data in an online transaction, and to identify the key data elements, attributes and relationships that are relevant for audit purposes. A system/process flowchart is a graphical representation of the sequence of steps or activities that are performed by a system or process. A system/process flowchart can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. A system/process flowchart shows the inputs, outputs, decisions and actions of a system or process, but it does not show the data elements, attributes and relationships that are involved in each step or activity. A file layout is a specification of the format and structure of a data file. A file layout can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. A file layout shows the fields, types, lengths and positions of data in a file, but it does not show the origin, flow, transformation and destination of data in an online transaction. Source code documentation is a description of the logic, functionality and purpose of a program or module written in a programming language. Source code documentation can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. Source code documentation shows the instructions, variables and parameters that are used to perform calculations and operations on data, but it does not show the data elements, attributes and relationships that are involved in each instruction or operation. References: CISA Review Manual (Digital Version) 1, Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: Data Administration Practices.

NEW QUESTION 110
- (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 111
- (Topic 2)
Which of the following is MOST important for an IS auditor to consider when performing the risk assessment poor to an audit engagement?

A. The design of controls
B. Industry standards and best practices
C. The results of the previous audit
D. The amount of time since the previous audit

Answer: C

Explanation:
The results of the previous audit are an important source of information for an IS auditor to consider when performing the risk assessment prior to an audit engagement, as they can provide insights into the current state and performance of the auditee, identify any issues or gaps that need to be followed up or addressed, and highlight any areas that require special attention or focus. The design of controls is an important factor to evaluate during an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not reflect the actual implementation or effectiveness of the controls. Industry standards and best practices are useful benchmarks or guidelines for an IS auditor to compare or measure against during an audit engagement, but they are not the most important thing to consider when performing the risk assessment prior to an audit engagement, as they may not be applicable or relevant to the specific context or objectives of the auditee. The amount of time since the previous audit is a relevant criterion to determine the frequency or timing of an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not indicate the level or nature of risk associated with the auditee.

NEW QUESTION 116
- (Topic 2)
The GREATEST benefit of using a polo typing approach in software development is that it helps to:

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

Answer: C

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

NEW QUESTION 119
- (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 124
- (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 127
- (Topic 2)
Which of the following would MOST effectively ensure the integrity of data transmitted over a network?

A. Message encryption
B. Certificate authority (CA)
C. Steganography
D. Message digest

Answer: D

Explanation:
The most effective way to ensure the integrity of data transmitted over a network is to use a message digest. A message digest is a cryptographic function that

generates a unique and fixed-length value (also known as a hash or checksum) from any input data. The message digest can be used to verify that the data has not been altered or corrupted during transmission by comparing it with the message digest generated at the destination. Message encryption is a method of protecting the confidentiality of data transmitted over a network by transforming it into an unreadable format using a secret key. Message encryption does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. Certificate authority (CA) is an entity that issues and manages digital certificates that bind public keys to identities. CA does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. Steganography is a technique of hiding data within other data, such as images or audio files. Steganography does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. References:
? CISA Review Manual, 27th Edition, pages 383-3841
? CISA Review Questions, Answers & Explanations Database, Question ID: 258

NEW QUESTION 130
- (Topic 2)
In data warehouse (DW) management, what is the BEST way to prevent data quality issues caused by changes from a source system?

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

Answer: C

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

NEW QUESTION 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 134
- (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 136
- (Topic 2)
Which of the following would BEST help lo support an auditor's conclusion about the effectiveness of an implemented data classification program?

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

Answer: C

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

? CISA Review Questions, Answers & Explanations Database, Question ID 2042

NEW QUESTION 141
- (Topic 2)
Which of the following are BEST suited for continuous auditing?

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

Answer: B

Explanation:
Continuous auditing is a method of performing audit-related activities on a real-time or near real-time basis. Continuous auditing is best suited for real-time transactions, such as online banking, e-commerce, or electronic funds transfer, that require immediate verification and assurance. Low-value transactions are not necessarily suitable for continuous auditing, as they may not pose significant risks or require frequent monitoring. Irregular transactions are not suitable for continuous auditing, as they may not occur frequently or consistently enough to justify the use of continuous auditing techniques. Manual transactions are not suitable for continuous auditing, as they may not be captured or processed by automated systems that enable continuous auditing. References:
? CISA Review Manual, 27th Edition, pages 307-3081
? CISA Review Questions, Answers & Explanations Database, Question ID: 253

NEW QUESTION 144
- (Topic 2)
Which of the following concerns is BEST addressed by securing production source libraries?

A. Programs are not approved before production source libraries are updated.
B. Production source and object libraries may not be synchronized.
C. Changes are applied to the wrong version of production source libraries.
D. Unauthorized changes can be moved into production.

Answer: D

Explanation:
Unauthorized changes can be moved into production is the best concern that is addressed by securing production source libraries. Production source libraries contain the source code of programs that are used in the production environment. Securing production source libraries means implementing access controls, change management procedures, and audit trails to prevent unauthorized or improper changes to the source code that could affect the functionality, performance, or security of the production programs. The other options are less relevant concerns that may not be directly addressed by securing production source libraries, but rather by other controls such as program approval, version control, or change testing. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.21
? CISA Review Questions, Answers & Explanations Database, Question ID 213

NEW QUESTION 145
- (Topic 2)
An organization that has suffered a cyber-attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

A. An imaging process was used to obtain a copy of the data from each computer.
B. The legal department has not been engaged.
C. The chain of custody has not been documented.
D. Audit was only involved during extraction of the Information

Answer: C

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

NEW QUESTION 148
- (Topic 2)
Which of the following is the PRIMARY role of the IS auditor m an organization's information classification process?

A. Securing information assets in accordance with the classification assigned
B. Validating that assets are protected according to assigned classification
C. Ensuring classification levels align with regulatory guidelines
D. Defining classification levels for information assets within the organization

Answer: B

Explanation:
Validating that assets are protected according to assigned classification is the primary role of the IS auditor in an organization’s information classification process. An IS auditor should evaluate whether the information security controls are adequate and effective in safeguarding the information assets based on their classification levels. The other options are not the primary role of the IS auditor, but rather the responsibilities of the information owners, custodians, or security managers. References:
? CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31

? CISA Review Questions, Answers & Explanations Database, Question ID 206

NEW QUESTION 152
- (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 154
- (Topic 1)
Due to limited storage capacity, an organization has decided to reduce the actual retention period for media containing completed low-value transactions. Which of the following is MOST important for the organization to ensure?

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

Answer: D

Explanation:
The most important thing for the organization to ensure when reducing the actual retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for the quality, security, and availability of the data under their control. They are also responsible for defining and enforcing data retention policies that comply with legal, regulatory, contractual, and business requirements. Data owners should be consulted and involved in any decision that affects the retention period of their data, as they are ultimately liable for any consequences of data loss or breach.
The policy includes a strong risk-based approach, the retention period allows for review during the year-end audit, and the total transaction amount has no impact on financial reporting are not the most important things for the organization to ensure when reducing the actual retention period for media containing completed low-value transactions. These are possible factors or benefits that may influence or justify the decision, but they do not override or replace the data owner responsibilities.

NEW QUESTION 156
- (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 160
- (Topic 1)
When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor's BEST recommendation is to place an intrusion detection system (IDS) between the firewall and:

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

Answer: A

Explanation:
When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor's best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet, as this would provide an additional layer of security and alert the organization of any malicious traffic that bypasses or penetrates the firewall. Placing an IDS between the firewall and the demilitarized zone (DMZ), the organization's web server, or the organization's network would not be as effective, as it would only monitor the traffic that has already passed through the firewall. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.3

NEW QUESTION 162
- (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 165
- (Topic 1)
From an IS auditor's perspective, which of the following would be the GREATEST risk associated with an incomplete inventory of deployed software in an organization?

A. Inability to close unused ports on critical servers
B. Inability to identify unused licenses within the organization
C. Inability to deploy updated security patches
D. Inability to determine the cost of deployed software

Answer: C

Explanation:
The greatest risk associated with an incomplete inventory of deployed software in an organization is the inability to deploy updated security patches. Security patches are updates that fix vulnerabilities or bugs in software that could be exploited by attackers. Without an accurate inventory of software versions and configurations, it is difficult to identify and apply the relevant patches in a timely manner, which exposes the organization to increased security risks. Inability to close unused ports on critical servers, inability to identify unused licenses within the organization, and inability to determine the cost of deployed software are not as critical as security risks. References: ISACA CISA Review Manual 27th Edition, page 308

NEW QUESTION 166
- (Topic 1)
During the design phase of a software development project, the PRIMARY responsibility of an IS auditor is to evaluate the:

A. Future compatibility of the application.
B. Proposed functionality of the application.
C. Controls incorporated into the system specifications.
D. Development methodology employed.

Answer: C

Explanation:
The primary responsibility of an IS auditor during the design phase of a software development project is to evaluate the controls incorporated into the system specifications. Controls are mechanisms or procedures that aim to ensure the security, reliability, or performance of a system or process. System specifications are documents that define and describe the requirements, features, functions, or components of a system or software. Evaluating the controls incorporated into the system specifications is a key responsibility of an IS auditor during the design phase of a software development project, as it helps ensure that the system or software meets the organization’s objectives, standards, and expectations for security, reliability, or performance. The other options are not primary responsibilities of an IS auditor during the design phase of a software development project, as they do not directly relate to evaluating the controls incorporated into the system specifications. Future compatibility of the application is a possible factor that may affect the functionality or usability of the application in different environments or platforms, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. Proposed functionality of the application is a possible factor that may affect the suitability or value of the application for meeting user needs or expectations, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. Development methodology employed is a possible factor that may affect the quality or consistency of the software development process, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION 167
- (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 170
- (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 172
- (Topic 1)
Which of the following should be an IS auditor's GREATEST consideration when scheduling follow-up activities for agreed-upon management responses to remediate audit observations?

A. Business interruption due to remediation
B. IT budgeting constraints
C. Availability of responsible IT personnel
D. Risk rating of original findings

Answer: D

Explanation:
The most important consideration for an IS auditor when scheduling follow- up activities for agreed-upon management responses to remediate audit observations is the risk rating of original findings. The risk rating of original findings is an assessment of the potential impact or likelihood of an audit issue or observation on the organization’s objectives, operations, or reputation. The risk rating of original findings can help determine the priority and urgency of follow-up activities for agreed-upon management responses to remediate audit observations by ensuring that high-risk issues are addressed first and more frequently than low-risk issues. The other options are not as important as the risk rating of original findings in scheduling follow-up activities for agreed-upon management responses to remediate audit observations, as they do not reflect the significance or severity of audit issues or observations. Business interruption due to remediation is a possible consequence of implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. IT budgeting constraints is a possible factor that may affect the availability or feasibility of resources for implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. Availability of responsible IT personnel is a possible factor that may affect the accountability or responsiveness of staff for implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

NEW QUESTION 177
- (Topic 1)
An IS auditor notes that several employees are spending an excessive amount of time using social media sites for personal reasons. Which of the following should the auditor recommend be performed FIRST?

A. Implement a process to actively monitor postings on social networking sites.
B. Adjust budget for network usage to include social media usage.
C. Use data loss prevention (DLP) tools on endpoints.
D. implement policies addressing acceptable usage of social media during working hours.

Answer: D

Explanation:
The first course of action that the auditor should recommend after finding that several employees are spending an excessive amount of time using social media sites for personal reasons is to implement policies addressing acceptable usage of social media during working hours. Policies can help define the scope, purpose, rules, and expectations of using social media in the workplace, both for personal and professional reasons. Policies can also specify the consequences of violating the policies, such as disciplinary actions or termination. Policies can help deter employees from misusing social media at work, which could affect their productivity, performance, or security. Policies can also help protect the organization from legal liabilities or reputational damages that could arise from inappropriate or unlawful employee behavior on social media.

NEW QUESTION 182
- (Topic 1)
An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes. Which of the following recommendations would BEST help to reduce the risk of data leakage?

A. Requiring policy acknowledgment and nondisclosure agreements (NDAs) signed by employees
B. Establishing strong access controls on confidential data
C. Providing education and guidelines to employees on use of social networking sites
D. Monitoring employees' social networking usage

Answer: C

Explanation:

The best recommendation to reduce the risk of data leakage from employee use of social networking sites for business purposes is to provide education and guidelines to employees on use of social networking sites. Education and guidelines can help employees understand the benefits and risks of using social media for business purposes, such as enhancing brand awareness, engaging with customers, or sharing industry insights. They can also inform employees about the dos and don'ts of social media etiquette, such as respecting privacy, protecting intellectual property, avoiding conflicts of interest, or complying with legal obligations. Education and guidelines can also raise awareness of potential data leakage scenarios, such as phishing attacks, malicious links, fake profiles, or oversharing sensitive information, and provide tips on how to prevent or respond to them.

NEW QUESTION 187
- (Topic 3)
Which of the following is the BEST control lo mitigate attacks that redirect Internet traffic to an unauthorized website?

A. Utilize a network-based firewall.
B. Conduct regular user security awareness training.
C. Perform domain name system (DNS) server security hardening.
D. Enforce a strong password policy meeting complexity requirement.

Answer: C

Explanation:
The best control to mitigate attacks that redirect Internet traffic to an unauthorized website is to perform domain name system (DNS) server security hardening. DNS servers are responsible for resolving domain names into IP addresses, and they are often targeted by attackers who want to manipulate or spoof DNS records to redirect users to malicious websites4. By applying security best practices to DNS servers, such as encrypting DNS traffic, implementing DNSSEC, restricting access and updating patches, the organization can reduce the risk of DNS hijacking attacks. A network-based firewall, user security awareness training and a strong password policy are also important controls, but they are not as effective as DNS server security hardening in preventing this specific type of attack.
References:
? CISA Review Manual, 27th Edition, page 4021
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 188
- (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 192
- (Topic 3)
Which of the following is MOST important for an IS auditor to determine during the detailed design phase of a system development project?

A. Program coding standards have been followed
B. Acceptance test criteria have been developed
C. Data conversion procedures have been established.
D. The design has been approved by senior management.

Answer: B

Explanation:
The most important thing for an IS auditor to determine during the detailed design phase of a system development project is that acceptance test criteria have been developed. Acceptance test criteria define the expected functionality, performance and quality of the system, and are used to verify that the system meets the user requirements and specifications. The IS auditor should ensure that the acceptance test criteria are clear, measurable and agreed upon by all stakeholders. Program coding standards have been followed is something that the IS auditor should check during the coding or testing phase, not the detailed design phase. Data conversion procedures have been established or the design has been approved by senior management are things that the IS auditor should verify during the implementation phase, not the detailed design phase. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 323

NEW QUESTION 195
- (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 199
- (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 201
- (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 203
- (Topic 3)
An audit has identified that business units have purchased cloud-based applications without IPs support. What is the GREATEST risk associated with this situation?

A. The applications are not included in business continuity plans (BCFs)
B. The applications may not reasonably protect data.
C. The application purchases did not follow procurement policy.
D. The applications could be modified without advanced notice.

Answer: B

Explanation:
The greatest risk associated with the situation of business units purchasing cloud-based applications without IT support is that the applications may not reasonably protect data. Cloud-based applications are software applications that run on the internet, rather than on a local device or network. Cloud-based applications offer many benefits, such as scalability, accessibility, and cost-effectiveness, but they also pose many challenges and risks, especially for data security1.
Data security is the process of protecting data from unauthorized access, use, modification, disclosure, or destruction. Data security is essential for ensuring the confidentiality, integrity, and availability of data, as well as complying with legal and regulatory requirements. Data security is especially important for cloud-based applications, as data are stored and processed on remote servers that are owned and managed by third-party cloud service providers (CSPs)2.
When business units purchase cloud-based applications without IT support, they may not be aware of or follow the best practices and standards for data security in the cloud. They may not perform adequate risk assessments, vendor evaluations, contract reviews, or audits to ensure that the CSPs and the applications meet the organization’s data security policies and expectations. They may not implement appropriate data encryption, backup, recovery, or disposal methods to protect the data in transit and at rest. They may not
monitor or control the access and usage of the data by internal or external users. They may not report or respond to any data breaches or incidents that may occur3.
These actions or inactions may expose the organization’s data to various threats and vulnerabilities in the cloud, such as cyberattacks, human errors, malicious

insiders, misconfigurations, or legal disputes. These threats and vulnerabilities may result in data loss, leakage, corruption, or compromise, which may have serious consequences for the organization’s reputation, operations, performance, compliance, and liability4.
Therefore, it is essential that business units consult and collaborate with IT support before purchasing any cloud-based applications, and follow the organization’s guidelines and procedures for cloud security. IT support can help business units to select and use cloud- based applications that are suitable and secure for their needs and objectives. References:
? Top 5 Risks With Cloud Software and How to Mitigate Them4
? Mitigate risks and secure your cloud-native applications3
? 12 Risks, Threats & Vulnerabilities in Moving to the Cloud2
? Best Practices to Manage Risks in the Cloud1

NEW QUESTION 208
- (Topic 3)
Which of the following backup schemes is the BEST option when storage media is limited?

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

Answer: C

Explanation:
A differential backup scheme is the best option when storage media is limited, as it only backs up the data that has changed since the last full backup. This reduces the amount of storage space required and also simplifies the restoration process, as only the last full backup and the last differential backup are needed. A real-time backup scheme would require continuous replication of data, which would consume a lot of storage space and network bandwidth. A virtual backup scheme would create a snapshot of the data at a point in time, but it would not reduce the storage space required, as it would still need to store the changes made to the data. A full backup scheme would back up all the data every time, which would require the most storage space and also take longer to complete.
References: ISACA, CISA Review Manual, 27th Edition, 2018, page 405

NEW QUESTION 211
- (Topic 3)
During an audit of an organization's risk management practices, an IS auditor finds several documented IT risk acceptances have not been renewed in a timely manner after the assigned expiration date When assessing the seventy of this finding, which mitigating factor would MOST significantly minimize the associated impact?

A. There are documented compensating controls over the business processes.
B. The risk acceptances were previously reviewed and approved by appropriate senior management
C. The business environment has not significantly changed since the risk acceptances were approved.
D. The risk acceptances with issues reflect a small percentage of the total population

Answer: A

Explanation:
The mitigating factor that would most significantly minimize the impact of not renewing IT risk acceptances in a timely manner is having documented compensating controls over the business processes. Compensating controls are alternative controls that reduce or eliminate the risk when the primary control is not feasible or cost-effective. The other factors, such as previous approval by senior management, unchanged business environment, and small percentage of issues, do not mitigate the risk as effectively as compensating controls. References: ISACA CISA Review Manual 27th Edition Chapter 1

NEW QUESTION 212
......

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/