Isaca

Exam Questions CISA

Isaca CISA

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (Topic 3)
Which of the following IT service management activities is MOST likely to help with identifying the root cause of repeated instances of network latency?

A. Change management
B. Problem management
C. incident management
D. Configuration management

Answer: B

Explanation:
Problem management is an IT service management activity that is most likely to help with identifying the root cause of repeated instances of network latency. Problem management involves analyzing incidents that affect IT services and finding solutions to prevent them from recurring or minimize their impact. Change management is an IT service management activity that involves controlling and documenting any modifications to IT services or infrastructure. Incident management is an IT service management activity that involves restoring normal service operation as quickly as possible after an incident has occurred. Configuration management is an IT service management activity that involves identifying and maintaining records of IT assets and their relationships. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 334

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

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

Answer: D

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

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

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

Answer: B

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

NEW QUESTION 4
- (Topic 3)
Which of the following would be an appropriate role of internal audit in helping to establish an organization's privacy program?

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

Answer: A

Explanation:
An appropriate role of internal audit in helping to establish an organization's privacy program is analyzing risks posed by new regulations. A privacy program is a set of policies, procedures, and controls that aim to protect the personal data of individuals from unauthorized or unlawful collection, use, disclosure, or disposal. A privacy program should comply with the applicable laws and regulations that govern the privacy rights and obligations of individuals and organizations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). New regulations may introduce new requirements or changes that

affect the organization's privacy program and expose it to potential compliance risks or penalties. Therefore, internal audit can help to establish an organization's privacy program by analyzing the risks posed by new regulations and providing assurance, advice, or recommendations on how to address them1. The other options are less appropriate or incorrect because:
? B. Developing procedures to monitor the use of personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the effectiveness and efficiency of the organization's privacy program, but not create or execute it2.
? C. Defining roles within the organization related to privacy is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a governance or strategic role. Internal audit should not be involved in setting or approving the organization's privacy strategy, objectives, or policies, as it would compromise its independence and objectivity. Internal audit should provide assurance on the alignment and compliance of the organization's privacy program with its strategy, objectives, and policies, but not define or approve them2.
? D. Designing controls to protect personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the adequacy and effectiveness of the organization's privacy program, but not design or implement it2. References: ISACA Introduces New Audit Programs for Business Continuity/Disaster …, Best Practices for Privacy Audits - ISACA, ISACA Produces New Audit and Assurance Programs for Data Privacy and …

NEW QUESTION 5
- (Topic 3)
Which of the following would BEST ensure that a backup copy is available for restoration of mission critical data after a disaster"

A. Use an electronic vault for incremental backups
B. Deploy a fully automated backup maintenance system.
C. Periodically test backups stored in a remote location
D. Use both tape and disk backup systems

Answer: C

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

NEW QUESTION 6
- (Topic 3)
An IS auditor discovers that an IT organization serving several business units assigns equal priority to all initiatives, creating a risk of delays in securing project funding Which of the following would be MOST helpful in matching demand for projects and services with available resources in a way that supports business objectives?

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

Answer: D

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

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

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

Answer: B

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

NEW QUESTION 8
- (Topic 3)
Which of the following should be the FRST step when developing a data toes prevention (DIP) solution for a large organization?

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

Answer: D

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

NEW QUESTION 9
- (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 10
- (Topic 3)
An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

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

Answer: D

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

NEW QUESTION 10
- (Topic 3)
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 11
- (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 16
- (Topic 3)
Which of the following BEST describes an audit risk?

A. The company is being sued for false accusations.
B. The financial report may contain undetected material errors.
C. Employees have been misappropriating funds.
D. Key employees have not taken vacation for 2 years.

Answer: B

Explanation:
The best description of an audit risk is that the financial report may contain undetected material errors. Audit risk is the risk that the auditor expresses an inappropriate opinion on the financial report when it contains material misstatements or errors. Audit risk consists of three components: inherent risk, control risk, and detection risk. Inherent risk is the susceptibility of an assertion or a control to a material misstatement or error due to factors such as complexity, volatility, fraud, or human error. Control risk is the risk that a material misstatement or error will not be prevented or detected by the internal controls. Detection risk is the risk that the auditor’s procedures will not detect a material misstatement or error that exists in an assertion or a control. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 20
- (Topic 3)
An IS auditor is reviewing the installation of a new server. The IS auditor's PRIMARY objective is to ensure that

A. security parameters are set in accordance with the manufacturer s standards.

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

Answer: C

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

NEW QUESTION 25
- (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 26
- (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 30
- (Topic 3)
Which of the following would BEST detect that a distributed denial of service (DDoS) attack is occurring?

A. Customer service complaints
B. Automated monitoring of logs
C. Server crashes
D. Penetration testing

Answer: B

Explanation:
The best way to detect that a distributed denial of service (DDoS) attack is occurring is to use automated monitoring of logs. A DDoS attack disrupts the operations of a server, service, or network by flooding it with unwanted Internet traffic2. Automated monitoring of logs can help pinpoint potential DDoS attacks by analyzing network traffic patterns, monitoring traffic spikes or other unusual activity, and alerting administrators or security teams of any anomalies or malicious requests, protocols, or IP blocks3. Automated monitoring of logs can also help identify the source, type, and impact of the DDoS attack, and provide evidence for further investigation or mitigation.
The other options are not as effective as automated monitoring of logs for detecting DDoS attacks. Customer service complaints are an indirect and delayed indicator of a DDoS attack, as they rely on users reporting problems with accessing a website or service. Customer service complaints may also be caused by other factors unrelated to DDoS attacks, such as server errors or network issues. Server crashes are an extreme and undesirable indicator of a DDoS attack, as they indicate that the server has already been overwhelmed by the attack and has stopped functioning. Server crashes may also result in data loss or corruption, service disruption, or reputational damage. Penetration testing is a proactive and preventive measure for assessing the security posture of a system or network, but it does not detect ongoing DDoS attacks. Penetration testing may involve simulating DDoS attacks to test the resilience or vulnerability of a system or network, but it does not monitor real-time traffic or identify actual attackers.
References:
? ISACA CISA Review Manual 27th Edition (2019), page 254
? How to prevent DDoS attacks | Methods and tools | Cloudflare2
? Understanding Denial-of-Service Attacks | CISA3

NEW QUESTION 32
- (Topic 3)
Which of the following would be MOST useful when analyzing computer performance?

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

Answer: A

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

NEW QUESTION 35
- (Topic 3)
Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organization's information security policy?

A. IT steering committee minutes
B. Business objectives
C. Alignment with the IT tactical plan
D. Compliance with industry best practice

Answer: B

Explanation:
The most important consideration for an IS auditor when assessing the adequacy of an organization’s information security policy is the business objectives. An information security policy is a document that defines the organization’s approach to protecting its information assets from internal and external threats. It should align with the organization’s mission, vision, values, and goals, and support its business processes and functions1. An information security policy should also be focused on the business needs and requirements of the organization, rather than on technical details or specific solutions2. The other options are not as important as the business objectives, because they do not directly reflect the organization’s purpose and direction. IT steering committee minutes are records of the discussions and decisions made by a group of senior executives who oversee the IT strategy and governance of the organization. They may provide some insights into the information security policy, but they are not sufficient to evaluate its adequacy3. Alignment with the IT tactical plan is a measure of how well the information security policy supports the short-term actions and projects that implement the IT strategy. However, the IT tactical plan itself should be aligned with the business objectives, and not vice versa4. Compliance with industry best practice is a desirable quality of an information security policy, but it is not a guarantee of its

effectiveness or suitability for the organization. Industry best practices are general guidelines or recommendations that may not apply to every organization or situation. An information security policy should be customized and tailored to the specific context and needs of the organization. References:
? The 12 Elements of an Information Security Policy | Exabeam1
? 11 Key Elements of an Information Security Policy | Egnyte2
? What is an IT steering committee? Definition, roles & responsibilities …3
? What is IT Strategy? Definition, Components & Best Practices | BMC …4
? IT Security Policy: Key Components & Best Practices for Every Business

NEW QUESTION 36
- (Topic 3)
Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

A. Apply single sign-on for access control
B. Implement segregation of duties.
C. Enforce an internal data access policy.
D. Enforce the use of digital signatures.

Answer: C

Explanation:
The most appropriate control to prevent unauthorized retrieval of confidential information stored in a business application system is to enforce an internal data access policy. A data access policy defines who can access what data, under what conditions and for what purposes. It also specifies the roles and responsibilities of data owners, custodians and users, as well as the security measures and controls to protect data confidentiality, integrity and availability. By enforcing a data access policy, the organization can ensure that only authorized personnel can retrieve confidential information from the business application system. Applying single sign-on for access control, implementing segregation of duties and enforcing the use of digital signatures are also useful controls, but they are not sufficient to prevent unauthorized data retrieval without a clear and comprehensive data access policy. References:
? CISA Review Manual, 27th Edition, page 2301
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2

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

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

Answer: C

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

NEW QUESTION 42
- (Topic 3)
Which of the following is MOST important when planning a network audit?

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

Answer: D

Explanation:
The most important factor when planning a network audit is to identify the existing nodes on the network. Nodes are devices or systems that are connected to the network and can communicate with each other. Nodes can include servers, workstations, routers, switches, firewalls, printers, scanners, cameras, etc. Identifying the existing nodes on the network will help the auditor to determine the scope, objectives, and methodology of the audit. It will also help the auditor to assess the network topology, architecture, performance, security, and compliance. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 44
- (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 48
- (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 51
- (Topic 3)
Which of the following issues associated with a data center's closed-circuit television (CCTV) surveillance cameras should be of MOST concern to an IS auditor?

A. CCTV recordings are not regularly reviewed.
B. CCTV cameras are not installed in break rooms
C. CCTV records are deleted after one year.
D. CCTV footage is not recorded 24 x 7.

Answer: A

Explanation:
The most concerning issue associated with a data center’s CCTV surveillance cameras is that the recordings are not regularly reviewed. This means that any unauthorized access, theft, vandalism, or other security incidents may go unnoticed and unreported. CCTV recordings are a valuable source of evidence and deterrence for data center security, and they should be monitored and audited periodically to ensure compliance with policies and regulations. If the recordings are not reviewed, the data center may face legal, financial, or reputational risks in case of a security breach or an audit failure.
The other options are less concerning because they do not directly affect the security of the data center. CCTV cameras are not required to be installed in break rooms, as they are not critical areas for data protection. CCTV records can be deleted after one year, as long as they comply with the data retention policy of the organization and the applicable laws. CCTV footage does not need to be recorded 24 x 7, as long as there is sufficient coverage of the data center during operational hours and when access is granted to authorized personnel. References:
? ISACA Journal Article: Physical security of a data center1
? Data Center Security: Checklist and Best Practices | Kisi2
? Video Surveillance Best Practices | Taylored Systems

NEW QUESTION 55
- (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 56
- (Topic 2)
Which of the following is the MOST important reason to classify a disaster recovery plan (DRP) as confidential?

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

Answer: D

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

NEW QUESTION 59
- (Topic 2)
In a RAO model, which of the following roles must be assigned to only one individual?

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

Answer: D

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

NEW QUESTION 63
- (Topic 2)
Due to a recent business divestiture, an organization has limited IT resources to deliver critical projects Reviewing the IT staffing plan against which of the following would BEST guide IT management when estimating resource requirements for future projects?

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

Answer: B

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

NEW QUESTION 65
- (Topic 2)
Which of the following BEST protects an organization's proprietary code during a joint- development activity involving a third party?

A. Statement of work (SOW)
B. Nondisclosure agreement (NDA)
C. Service level agreement (SLA)
D. Privacy agreement

Answer: B

Explanation:
A nondisclosure agreement (NDA) is the best way to protect an organization's proprietary code during a joint-development activity involving a third party. An NDA is a legal contract that binds the parties involved in a joint-development activity to keep confidential any information, data or materials that are shared or exchanged during the activity. An NDA specifies what constitutes confidential information, how it can be used, disclosed or protected, how long it remains confidential, what are the exceptions and remedies for breach of confidentiality, and other terms and conditions. An NDA can help to protect an organization's proprietary code from being copied, modified, distributed or exploited by unauthorized parties without its consent or knowledge. The other options are not as effective as option B, as

they do not address confidentiality issues specifically. A statement of work (SOW) is a document that defines the scope, objectives, deliverables, tasks, roles, responsibilities, timelines and costs of a joint-development activity, but it does not cover confidentiality issues explicitly. A service level agreement (SLA) is a document that defines the quality, performance and availability standards and metrics for a service provided by one party to another party in a joint-development activity, but it does not cover confidentiality issues explicitly. A privacy agreement is a document that defines how personal information collected from customers or users is collected, used, disclosed and protected by one party or both parties in a joint-development activity, but it does not cover confidentiality issues related to proprietary code. References: CISA Review Manual (Digital Version) , Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.2: Project Management Practices.

NEW QUESTION 66
- (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 70
- (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 74
- (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 78
- (Topic 2)
Which of the following is MOST helpful for measuring benefits realization for a new system?

A. Function point analysis

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

Answer: C

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

NEW QUESTION 82
- (Topic 2)
IT disaster recovery time objectives (RTOs) should be based on the:

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

Answer: D

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

NEW QUESTION 85
- (Topic 2)
When testing the adequacy of tape backup procedures, which step BEST verifies that regularly scheduled Backups are timely and run to completion?

A. Observing the execution of a daily backup run
B. Evaluating the backup policies and procedures
C. Interviewing key personnel evolved In the backup process
D. Reviewing a sample of system-generated backup logs

Answer: D

Explanation:
Reviewing a sample of system-generated backup logs is the best step to verify that regularly scheduled backups are timely and run to completion. Backup logs are records that document the details and results of backup operations, such as the date, time, duration, status, errors, and exceptions. By reviewing a sample of backup logs, the IS auditor can check whether the backups are performed according to the schedule and whether they are completed successfully or not. The other steps do not provide as much evidence or assurance as reviewing backup logs, as they do not show the actual outcome or performance of backup operations. References: CISA Review Manual, 27th Edition, page 247

NEW QUESTION 90
- (Topic 2)
A new system is being developed by a vendor for a consumer service organization. The vendor will provide its proprietary software once system development is completed Which of the following is the MOST important requirement to include In the vendor contract to ensure continuity?

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

Answer: C

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

NEW QUESTION 94
- (Topic 2)
Which of the following is a social engineering attack method?

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

Answer: A

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

NEW QUESTION 99
- (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 103
- (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 104
- (Topic 2)
Which of the following would lead an IS auditor to conclude that the evidence collected during a digital forensic investigation would not be admissible in court?

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

Answer: B

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

NEW QUESTION 105
- (Topic 2)
An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives. Which of the following findings should be the IS auditor's GREATEST concern?

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

Answer: C

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

NEW QUESTION 109
- (Topic 2)
During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's NEXT step?

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

Answer: B

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

NEW QUESTION 111
- (Topic 2)
An IS auditor notes that IT and the business have different opinions on the availability of their application servers. Which of the following should the IS auditor review FIRST in order to understand the problem?

A. The exact definition of the service levels and their measurement
B. The alerting and measurement process on the application servers
C. The actual availability of the servers as part of a substantive test
D. The regular performance-reporting documentation

Answer: A

Explanation:
The exact definition of the service levels and their measurement is the first thing that the IS auditor should review in order to understand the problem of different opinions on the availability of their application servers. Service levels are the agreed-upon standards or targets for delivering IT services, such as availability, reliability, performance, and security. Service level measurement is the process of collecting, analyzing, and reporting data related to the achievement of service levels. By reviewing the exact definition of the service levels and their measurement, the IS auditor can identify any gaps, inconsistencies, or ambiguities that may cause confusion or disagreement among IT and the business. The other options are not as important as reviewing the exact definition of the service levels and their measurement, as they do not address the root cause of the problem. References: CISA Review Manual, 27th Edition, page 372

NEW QUESTION 113
- (Topic 2)
Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor's BEST recommendation for a compensating control?

A. Require written authorization for all payment transactions
B. Restrict payment authorization to senior staff members.
C. Reconcile payment transactions with invoices.
D. Review payment transaction history

Answer: A

Explanation:
Requiring written authorization for all payment transactions is the IS auditor’s best recommendation for a compensating control in an environment where segregation of duties (SoD) cannot be enforced in an accounts payable system. SoD is a principle that requires different individuals or functions to perform different tasks or roles in a business process, such as initiating, approving, recording and reconciling transactions. SoD reduces the risk of errors, fraud and misuse of resources by preventing any single person or function from having excessive or conflicting authority or responsibility. A compensating control is a control that mitigates or reduces the risk associated with the absence or weakness of another control. Requiring written authorization for all payment transactions is a compensating control that provides an independent verification and approval of each transaction before it is processed by the accounts payable system. This control can help to detect and prevent unauthorized, duplicate or erroneous payments, and to ensure compliance with policies and procedures. The other options are not as effective as option A, as they do not provide an independent verification or approval of payment transactions. Restricting payment authorization to senior staff members is a control that limits the number of people who can authorize payments, but it does not prevent them from initiating or processing payments themselves, which could violate SoD. Reconciling payment transactions with invoices is a control that verifies that the payments match the invoices, but it does not prevent unauthorized, duplicate or erroneous payments from being processed by the accounts payable system. Reviewing payment transaction history is a control that monitors and analyzes the payment transactions after they have been processed by the accounts payable system, but it does not prevent unauthorized, duplicate
or erroneous payments from occurring in the first place. References: CISA Review Manual
(Digital Version) , Chapter 5: Protection of Information Assets, Section 5.2: Logical Access.

NEW QUESTION 118
- (Topic 2)
Which of the following is a detective control?

A. Programmed edit checks for data entry
B. Backup procedures
C. Use of pass cards to gain access to physical facilities
D. Verification of hash totals

Answer: D

Explanation:
Verification of hash totals is a detective control. A detective control is a control that aims to identify and report errors or irregularities that have already occurred. Verification of hash totals is a technique that compares the hash values of data before and after transmission or processing to detect any changes or corruption. The other options are examples of other types of controls, such as programmed edit checks (preventive), backup procedures (recovery), and use of pass cards (preventive). References: CISA Review Manual, 27th Edition, page 223

NEW QUESTION 120
- (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 123
- (Topic 2)
Which of the following would BEST manage the risk of changes in requirements after the analysis phase of a business application development project?

A. Expected deliverables meeting project deadlines
B. Sign-off from the IT team

C. Ongoing participation by relevant stakeholders
D. Quality assurance (OA) review

Answer: B

NEW QUESTION 124
- (Topic 2)
Which of the following controls BEST ensures appropriate segregation of dudes within an accounts payable department?

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

Answer: D

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

NEW QUESTION 126
- (Topic 2)
For an organization that has plans to implement web-based trading, it would be MOST important for an IS auditor to verify the organization's information security plan includes:

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

Answer: C

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

NEW QUESTION 128
- (Topic 2)
Which of the following activities would allow an IS auditor to maintain independence while facilitating a control sell-assessment (CSA)?

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

Answer: D

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

NEW QUESTION 131
- (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 135
- (Topic 2)
Which of the following is an example of a preventative control in an accounts payable system?

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

Answer: A

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

NEW QUESTION 140
- (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 141
- (Topic 2)
During an IT governance audit, an IS auditor notes that IT policies and procedures are not regularly reviewed and updated. The GREATEST concern to the IS auditor is that policies and procedures might not:

A. reflect current practices.
B. include new systems and corresponding process changes.
C. incorporate changes to relevant laws.
D. be subject to adequate quality assurance (QA).

Answer: A

Explanation:
The greatest concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated is that policies and procedures might not reflect current practices. Policies are documents that define the goals, objectives, and guidelines for an organization’s information systems and resources. Procedures are documents that describe the steps, tasks, or activities for implementing or executing policies. Policies and procedures should be regularly reviewed and updated to ensure that they are relevant, accurate, consistent, and effective for the organization’s information systems and resources. Policies and procedures that are not regularly reviewed and updated might not reflect current practices, as they might be outdated, obsolete, or incompatible with the current state or needs of the organization’s information systems and resources. This can cause confusion, inconsistency, inefficiency, or noncompliance among users or stakeholders who rely on policies and procedures for guidance or direction. Policies and procedures might not include new systems and corresponding process changes is a possible concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated, but it is not the greatest one. Policies and procedures might not include new systems and corresponding process changes, as they might be unaware of or unresponsive to the introduction or modification of information systems or resources within the organization. This can cause gaps, overlaps, or conflicts among policies and procedures that affect different information systems or resources.

NEW QUESTION 143
- (Topic 2)
Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at test?

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

Answer: A

Explanation:
The condition that would be of most concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at rest is short key length. A brute force attack is a method of breaking encryption by trying all possible combinations of keys until finding the correct one. The shorter the key length,

the easier it is for an attacker to guess or crack the encryption. Random key generation, use of symmetric encryption, and use of asymmetric encryption are not conditions that would increase the risk of a successful brute force attack. In fact, random key generation can enhance security by preventing predictable patterns in key selection. Symmetric encryption and asymmetric encryption are different types of encryption that have their own advantages and disadvantages, but neither is inherently more vulnerable to brute force attacks than the other. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION 145
- (Topic 2)
Upon completion of audit work, an IS auditor should:

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

Answer: B

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

NEW QUESTION 146
- (Topic 2)
After the merger of two organizations, which of the following is the MOST important task for an IS auditor to perform?

A. Verifying that access privileges have been reviewed
B. investigating access rights for expiration dates
C. Updating the continuity plan for critical resources
D. Updating the security policy

Answer: A

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

NEW QUESTION 148
- (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 151
- (Topic 2)
Providing security certification for a new system should include which of the following prior to the system's implementation?

A. End-user authorization to use the system in production
B. External audit sign-off on financial controls

C. Testing of the system within the production environment
D. An evaluation of the configuration management practices

Answer: D

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

NEW QUESTION 154
- (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 155
- (Topic 2)
Which of the following would provide the MOST important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program?

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

Answer: D

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

NEW QUESTION 156
- (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 161
- (Topic 1)

Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

A. Identifying relevant roles for an enterprise IT governance framework
B. Making decisions regarding risk response and monitoring of residual risk
C. Verifying that legal, regulatory, and contractual requirements are being met
D. Providing independent and objective feedback to facilitate improvement of IT processes

Answer: D

Explanation:
The most important benefit of involving IS audit when implementing governance of enterprise IT is providing independent and objective feedback to facilitate improvement of IT processes. Governance of enterprise IT is the process of ensuring that IT supports the organization’s strategy, goals, and objectives in an effective, efficient, ethical, and compliant manner. IS audit can provide value to governance of enterprise IT by assessing the alignment of IT with business needs, evaluating the performance and value delivery of IT, identifying risks and issues related to IT, recommending corrective actions and best practices, and monitoring the implementation and effectiveness of IT governance activities. IS audit can also provide assurance that IT governance processes are designed and operating in accordance with relevant standards, frameworks, laws, regulations, and contractual obligations. Identifying relevant roles for an enterprise IT governance framework is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help define and clarify the roles and responsibilities of various stakeholders involved in IT governance, such as board members, senior management, business units, IT function, external parties, etc. IS audit can also help ensure that these roles are aligned with the organization’s strategy, goals, and objectives, and that they have adequate authority, accountability, communication, and reporting mechanisms. However, this benefit is more related to the design phase of IT governance implementation than to the ongoing monitoring and improvement phase. Making decisions regarding risk response and monitoring of residual risk is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help identify and assess the risks associated with IT activities and processes, such as
strategic risks, operational risks, compliance risks, security risks, etc. IS audit can also help evaluate the effectiveness of risk management practices and controls implemented by management to mitigate or reduce these risks. However, this benefit is more related to the assurance function of IS audit than to its advisory function. Verifying that legal, regulatory, and contractual requirements are being met is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help verify that IT activities and processes comply with applicable laws, regulations, and contractual obligations, such as data protection laws, privacy laws, cybersecurity laws, industry standards, service level agreements, etc. IS audit can also help identify and report any instances of noncompliance or violations that could result in legal or reputational consequences for the organization. However, this benefit is more related to the assurance function of IS audit than to its advisory function. References: ISACA CISA Review Manual 27th Edition, page 283

NEW QUESTION 163
- (Topic 1)
Which of the following attack techniques will succeed because of an inherent security weakness in an Internet firewall?

A. Phishing
B. Using a dictionary attack of encrypted passwords
C. Intercepting packets and viewing passwords
D. Flooding the site with an excessive number of packets

Answer: D

Explanation:
Flooding the site with an excessive number of packets is an attack technique that will succeed because of an inherent security weakness in an Internet firewall. This type of attack is also known as a denial-of-service (DoS) attack or a distributed denial-of-service (DDoS) attack if it involves multiple sources. The aim of this attack is to overwhelm the network bandwidth or the processing capacity of the firewall or the target system, rendering it unable to respond to legitimate requests or perform its normal functions. An Internet firewall is a device or software that monitors and controls incoming and outgoing network traffic based on predefined rules. A firewall can block or allow traffic based on various criteria, such as source address, destination address, port number, protocol type, application type, etc. However, a firewall cannot prevent traffic from reaching its interface or distinguish between legitimate and malicious traffic based on its content or behavior. Therefore, a firewall is vulnerable to flooding attacks that exploit its limited resources. Phishing is an attack technique that involves sending fraudulent emails or messages that appear to come from legitimate sources, such as banks, government agencies, online services, etc., in order to trick recipients into revealing their personal or financial information, such as passwords, credit card numbers, bank account details, etc., or into clicking on malicious links or attachments that can infect their systems with malware or ransomware. Phishing does not exploit an inherent security weakness in an Internet firewall, but rather exploits human psychology and social engineering techniques. A firewall cannot prevent phishing emails or messages from reaching their intended targets, unless they contain some identifiable features that can be filtered out by the firewall rules. However, a firewall cannot detect or prevent users from responding to phishing emails or messages or from opening malicious links or attachments. Using a dictionary attack of encrypted passwords is an attack technique that involves trying to guess or crack passwords by using a list of common or likely passwords or by using a brute-force method that tries all possible combinations of characters. This type of attack does not exploit an inherent security weakness in an Internet firewall, but rather exploits weak or poorly chosen passwords or weak encryption algorithms. A firewall cannot prevent a dictionary attack of encrypted passwords, unless it has some mechanisms to detect and block repeated or suspicious login attempts or to enforce strong password policies. However, a firewall cannot protect passwords from being stolen or intercepted by other means, such as phishing, malware, keylogging, etc. Intercepting packets and viewing passwords is an attack technique that involves capturing and analyzing network traffic that contains sensitive information, such as passwords, credit card numbers, bank account details, etc., in order to use them for malicious purposes. This type of attack does not exploit an inherent security weakness in an Internet firewall, but rather exploits insecure or unencrypted
network communication protocols or channels. A firewall cannot prevent packets from being intercepted and viewed by unauthorized parties, unless it has some mechanisms to encrypt or obfuscate the network traffic or to authenticate the source and destination of the traffic. However, a firewall cannot protect packets from being modified or tampered with by other means, such as man-in-the-middle attacks, replay attacks, etc. References: ISACA CISA Review Manual 27th Edition, page 300

NEW QUESTION 168
- (Topic 1)
Which of the following will be the MOST effective method to verify that a service vendor keeps control levels as required by the client?

A. Conduct periodic on-site assessments using agreed-upon criteria.
B. Periodically review the service level agreement (SLA) with the vendor.
C. Conduct an unannounced vulnerability assessment of vendor's IT systems.
D. Obtain evidence of the vendor's control self-assessment (CSA).

Answer: A

Explanation:
The most effective method to verify that a service vendor keeps control levels as required by the client is to conduct periodic on-site assessments using agreed-

upon criteria. On-site assessments can provide direct evidence of whether the vendor's controls are operating effectively and consistently in accordance with the client's expectations and requirements. Agreed-upon criteria can ensure that the assessments are objective, relevant, and reliable. The other options are not as effective as on-site assessments in verifying the vendor's control levels. Periodically reviewing the SLA with the vendor can help monitor whether the vendor meets its contractual obligations and service standards, but it does not provide assurance of whether the vendor's controls are adequate or sufficient. Conducting an unannounced vulnerability assessment of vendor's IT systems can help identify any weaknesses or gaps in the vendor's security controls, but it may violate the terms and conditions of the vendor-client relationship or cause operational disruptions. Obtaining evidence of the vendor's CSA can provide some indication of whether the vendor's controls are self-monitored and reported, but it does not verify whether the vendor's controls are independent or accurate. References:
CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION 173
- (Topic 1)
An online retailer is receiving customer complaints about receiving different items from what they ordered on the organization's website. The root cause has been traced to poor data quality. Despite efforts to clean erroneous data from the system, multiple data quality issues continue to occur. Which of the following recommendations would be the BEST way to reduce the likelihood of future occurrences?

A. Assign responsibility for improving data quality.
B. Invest in additional employee training for data entry.
C. Outsource data cleansing activities to reliable third parties.
D. Implement business rules to validate employee data entry.

Answer: D

Explanation:
Implementing business rules to validate employee data entry is the best way to reduce the likelihood of future occurrences of poor data quality that cause customer complaints about receiving different items from what they ordered on the organization's website. Business rules are logical statements that define the conditions and actions for data validation, such as checking for data completeness, accuracy, consistency, and integrity. Assigning responsibility for improving data quality, investing in additional
employee training for data entry, and outsourcing data cleansing activities to reliable third parties are also possible ways to improve data quality, but they are not as effective as implementing business rules to validate employee data entry. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.1

NEW QUESTION 175
- (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 179
- (Topic 1)
Which of the following MOST effectively minimizes downtime during system conversions?

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

Answer: D

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

NEW QUESTION 182
- (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 187
- (Topic 1)
Which of the following BEST minimizes performance degradation of servers used to authenticate users of an e-commerce website?

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

Answer: B

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

NEW QUESTION 189
- (Topic 1)
Coding standards provide which of the following?

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

Answer: D

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

NEW QUESTION 190
- (Topic 1)
An organization's software developers need access to personally identifiable information (Pll) stored in a particular data format. Which of the following is the BEST way to protect this sensitive information while allowing the developers to use it in development and test environments?

A. Data masking
B. Data tokenization
C. Data encryption
D. Data abstraction

Answer: A

Explanation:
The best way to protect sensitive information such as personally identifiable information (PII) stored in a particular data format while allowing the software developers to use it in development and test environments is data masking. Data masking is a technique that replaces or obscures sensitive data elements with fictitious or modified data elements that retain the original format and characteristics of the data. Data masking can help protect sensitive information such as PII stored in a particular data format while allowing the software developers to use it in development and test environments by preventing the exposure or disclosure of the real data values without affecting the functionality or performance of the software or application. The other options are not as effective as data masking in protecting sensitive information such as PII stored in a particular data format while allowing the software developers to use it in development and test environments, as they have different limitations or drawbacks. Data tokenization is a technique that replaces sensitive data elements with non-sensitive tokens that have no intrinsic value or meaning. Data tokenization can protect sensitive information such as PII from unauthorized access or theft, but it may not retain the original format and characteristics of the data, which may affect the functionality or performance of the software or application. Data encryption is a technique that transforms sensitive data elements into unreadable or unintelligible ciphertext using an algorithm and a key. Data encryption can protect sensitive information such as PII from unauthorized access or modification, but it requires decryption to restore the original data values, which may introduce additional complexity or overhead to the software development process. Data abstraction is a technique that hides the details or complexity of data structures or operations from users or programmers by providing a simplified representation or interface. Data abstraction can help improve the usability or maintainability of software or applications, but it does not protect sensitive information such as PII from exposure or disclosure. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

NEW QUESTION 194
......