Product Questions: 1408
Version: 71.0

Topic 1, Exam Pool A

Question: 1

An IT balanced scorecard is the MOST effective means of monitoring:

A. governance of enterprise IT.

B. control effectiveness.

C. return on investment (ROI).

D. change management effectiveness.

Answer: A

Explanation:

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

Question: 2

When reviewing an organization's information security policies, an IS auditor should verify that the policies have been defined PRIMARILY on the basis of:

A. a risk management process.

B. an information security framework.

C. past information security incidents.

D. industry best practices.

Answer: A

Explanation:

Information security policies are high-level statements that define the organization's approach to protecting its information assets from threats and risks. They should be based primarily on a risk management process, which is a systematic method of identifying, analyzing, evaluating, treating, and monitoring information security risks. A risk management process can help ensure that the policies are aligned with the organization's risk appetite, business objectives, legal and regulatory requirements, and stakeholder expectations. An information security framework is a set of standards, guidelines, and best practices that provide a structure for implementing information security policies. It can support the risk management process, but it is not the primary basis for defining the policies. Past information security incidents and industry best practices can also provide valuable inputs for defining the policies, but they are not sufficient to address the organization's specific context and needs. Reference: Insights and Expertise, CISA Review Manual (Digital Version)

Question: 3

Which of the following would be an IS auditor's GREATEST concern when reviewing the early stages of a software development project?

A. The lack of technical documentation to support the program code

B. The lack of completion of all requirements at the end of each sprint

C. The lack of acceptance criteria behind user requirements.

D. The lack of a detailed unit and system test plan

Answer: C

Explanation:

User requirements are statements that describe what the users expect from the software system in terms of functionality, quality, and usability. They are essential inputs for the software development process, as they guide the design, implementation, testing, and deployment of the system. Therefore, an IS auditor's greatest concern when reviewing the early stages of a software development project would be the lack of acceptance criteria behind user requirements. Acceptance criteria are measurable conditions that define when a user requirement is met or satisfied. They help ensure that the user requirements are clear, complete, consistent, testable, and verifiable. Without acceptance criteria, it would be difficult to evaluate whether the system meets the user expectations and delivers value to the organization. Technical documentation, such as program code, is usually produced in later stages of the software development process. Completion of all requirements at the end of each sprint is not mandatory in agile software development methods, as long as there is a prioritized backlog of requirements that can be delivered incrementally. A detailed unit and system test plan is also important for ensuring software quality, but it depends on well-defined user requirements andacceptance criteria. Reference: Information Systems

Acquisition, Development & Implementation, CISA ReviewManual (Digital Version)

Question: 4

Which of the following is the BEST data integrity check?

A. Counting the transactions processed per day

B. Performing a sequence check

C. Tracing data back to the point of origin

D. Preparing and running test data

Answer: C

Explanation:

Data integrity is the property that ensures that data is accurate, complete, consistent, and reliable throughout its lifecycle. The best data integrity check is tracing data back to the point of origin, which is the source where the data was originally created or captured. This check can verify that data has not been altered or corrupted during transmission, processing, or storage. It can also identify any errors or discrepancies in data entry or conversion. Counting the transactions processed per day is a performance measure that does not directly assess data integrity. Performing a sequence check is a validity check that ensures that data follows a predefined order or pattern. It can detect missing or out-of-order data elements, but it cannot verify their accuracy or completeness. Preparing and running test data is a testing technique that simulates real data to evaluate how a system handles different scenarios. It can help identify errors or bugs in the system logic or functionality, but it cannot ensure data integrity in production environments. Reference: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

Question: 5

Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system. What is the BEST control to ensure that data is accurately entered into the system?

A. Reconciliation of total amounts by project

B. Validity checks, preventing entry of character data

C. Reasonableness checks for each cost type

D. Display the back of the project detail after the entry

Answer: A

Explanation:

Reconciliation of total amounts by project is the best control to ensure that data is accurately entered into the job-costing system from spreadsheets. Reconciliation is a process of comparing two sets of data to identify any differences or discrepancies between them. By reconciling the total amounts by project from spreadsheets with those from the job-costing system, any errors or omissions in data entry can be detected and corrected. Validity checks are controls that verify that data conforms to predefined formats or ranges. They can prevent entry of character data into numeric fields, but they cannot ensure that the numeric data is correct or complete. Reasonableness checks are controls that verify that data is within expected or acceptable limits. They can detect outliers or anomalies in data, but they cannot ensure that the data matches the source. Display back of project detail after entry is a control that allows the user to review and confirm the data entered into the system. It can help reduce human errors, but it cannot guarantee that the data is accurate or consistent with the source. Reference: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

Question: 6

An incorrect version of the source code was amended by a development team. This MOST likely indicates a weakness in:

A. incident management.

B. quality assurance (QA).

C. change management.

D. project management.

Answer: C

Explanation:

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

Question: 7

An organizations audit charier PRIMARILY:

A. describes the auditors' authority to conduct audits.

B. defines the auditors' code of conduct.

C. formally records the annual and quarterly audit plans.

D. documents the audit process and reporting standards.

Answer: A

Explanation:

An organization’s audit charter primarily describes the auditors’ authority to conduct audits.

The audit charter is a formal document that defines the purpose, scope, responsibilities, and reporting relationships of the internal audit function. It also establishes the auditors' right of access to information, records, personnel, and physical properties relevant to their work. The audit charter provides the basis for the auditors' independence and accountability to the governing body and senior management.

Question: 8

The decision to accept an IT control risk related to data quality should be the responsibility of the:

A. information security team.

B. IS audit manager.

C. chief information officer (CIO).

D. business owner.

Answer: D

Explanation:

The decision to accept an IT control risk related to data quality should be the responsibility of the business owner. The business owner is the person who has the authority and accountability for the business process that relies on the data quality. The business owner should understand the impact of data quality issues on the business objectives, performance, and compliance. The business owner should also be involved in defining the data quality requirements, assessing the data quality risks, and implementing the data quality controls or mitigation strategies.

Question: 9

Which of the following data would be used when performing a business impact analysis (BIA)?

A. Projected impact of current business on future business

B. Cost-benefit analysis of running the current business

C. Cost of regulatory compliance

D. Expected costs for recovering the business

Answer: D

Explanation:

The expected costs for recovering the business would be used when performing a business impact analysis (BIA). A BIA is a process of identifying and evaluating the potential effects ofdisruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, strategies, and resources needed to resume normal operations after a disruption. One of the key outputs of a BIA is an estimate of the financial losses or costs associated with different types of disruptions, such as lost revenue, increased expenses, contractual penalties, or regulatory fines.

Question: 10

During the evaluation of controls over a major application development project, the MOST effective use of an IS auditor's time would be to review and evaluate:

A. application test cases.

B. acceptance testing.

C. cost-benefit analysis.

D. project plans.

Answer: A

Explanation:

Reviewing and evaluating application test cases is the most effective use of an IS auditor’s time during the evaluation of controls over a major application development project. Application test cases are designed to verify that the application meets the functional and non-functional requirements and specifications. They also help to identify and correct any errors, defects, or vulnerabilities in the application before it is deployed. By reviewing and evaluating the test cases, the IS auditor can assess the quality, reliability, security, and performance of the application and provide recommendations for improvement.

Question: 11

An IS auditor finds that firewalls are outdated and not supported by vendors. Which of the following should be the auditor's NEXT course of action?

A. Report the mitigating controls.

B. Report the security posture of the organization.

C. Determine the value of the firewall.

D. Determine the risk of not replacing the firewall.

Answer: D

Explanation:

The IS auditor’s next course of action after finding that firewalls are outdated and not supported by vendors should be to determine the risk of not replacing the firewall. Outdated firewalls may have known vulnerabilities that can be exploited by attackers to bypass security controls and access the network. They may also lack compatibility with newer technologies or standards that are required for optimal network performance and protection. Not replacing the firewall could expose the organization to various threats, such as data breaches, denial-of-service attacks, malware infections, or regulatory non-compliance. The IS auditor should assess the likelihood and impact of these threats and quantify the risk level for management to make informed decisions.

Question: 12

Which of the following is the BEST way to determine whether a test of a disaster recovery plan (DRP) was successful?

A. Analyze whether predetermined test objectives were met.

B. Perform testing at the backup data center.

C. Evaluate participation by key personnel.

D. Test offsite backup files.

Answer: A

Explanation:

The best way to determine whether a test of a disaster recovery plan (DRP) was successful is to analyze whether predetermined test objectives were met. Test objectives are specific, measurable, achievable, relevant, and time-bound (SMART) goals that define what the test aims to accomplish and how it will be evaluated. Test objectives should be aligned with the DRP objectives and scope, and should cover aspects such as recovery time objectives (RTOs), recovery point objectives (RPOs), critical business functions, roles and responsibilities, communication channels, backup systems, and contingency procedures. By comparing the actual test results with the expected test objectives, the IS auditor can measure the effectiveness and efficiency of the DRP and identify any gaps or weaknesses that need to be addressed.

Question: 13

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

A. Requiring policy acknowledgment and nondisclosure agreements (NDAs) signed by employees

B. Establishing strong access controls on confidential data

C. Providing education and guidelines to employees on use of social networking sites

D. Monitoring employees' social networking usage

Answer: C

Explanation:

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

Question: 14

An IS auditor notes that several employees are spending an excessive amount of time using social media sites for personal reasons. Which of the following should the auditor recommend be performed FIRST?

A. Implement a process to actively monitor postings on social networking sites.

B. Adjust budget for network usage to include social media usage.

C. Use data loss prevention (DLP) tools on endpoints.

D. implement policies addressing acceptable usage of social media during working hours.

Answer: D

Explanation:

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

Question: 15

Which of the following fire suppression systems needs to be combined with an automatic switch to shut down the electricity supply in the event of activation?

A. Carbon dioxide

B. FM-200

C. Dry pipe

D. Halon

Answer: A

Explanation:

Carbon dioxide fire suppression systems need to be combined with an automatic switch to shut down the electricity supply in the event of activation. This is because carbon dioxide displaces oxygen in the air and can create a suffocation hazard for people in the protected area. Therefore, it is essential to cut off the power source before releasing carbon dioxide to avoid electrical shocks and sparks that could ignite the fire again. Carbon dioxide systems are typically used for total flooding applications in spaces that are not habitable, such as server rooms or data centers.

Question: 16

Which of the following would MOST likely impair the independence of the IS auditor when performing a post-implementation review of an application system?

A. The IS auditor provided consulting advice concerning application system best practices.

B. The IS auditor participated as a member of the application system project team, but did not have operational responsibilities.

C. The IS auditor designed an embedded audit module exclusively for auditing the application system.

D. The IS auditor implemented a specific control during the development of the application system.

Answer: D

Explanation:

The IS auditor’s independence would be most likely impaired if they implemented a specific control during the development of an application system. This is because the IS auditor would be auditing their own work, which creates a self-review threat that could compromise their objectivity and impartiality. The IS auditor should avoid participating in any operational or management activities that could affect their ability to perform an unbiased audit. The other options do not pose a significant threat to the IS auditor’s independence, as long as they follow the ethical standards and guidelines of the profession.

Question: 17

An IS auditor suspects an organization's computer may have been used to commit a crime. Which of the following is the auditor's BEST course of action?

A. Examine the computer to search for evidence supporting the suspicions.

B. Advise management of the crime after the investigation.

C. Contact the incident response team to conduct an investigation.

D. Notify local law enforcement of the potential crime before further investigation.

Answer: C

Explanation:

The IS auditor’s best course of action if they suspect an organization’s computer may have been used to commit a crime is to contact the incident response team to conduct an investigation. The incident response team is a group of experts who are responsible for responding to security incidents, such as data breaches, ransomware attacks, or cybercrimes. The incident response team can help to preserve and collect digital evidence, determine the scope and impact of the incident, contain and eradicate the threat, and restore normal operations. The IS auditor should not examine the computer themselves, as they may inadvertently alter or destroy potential evidence, or compromise the chain of custody. The IS auditor should also not notify local law enforcement before further investigation, as this may escalate the situation unnecessarily or interfere with the internal investigation process. The IS auditor should advise management of the crime after the investigation, or as soon as possible if there is an imminent risk or legal obligation to do so.

Question: 18

Which of the following access rights presents the GREATEST risk when granted to a new member of the system development staff?

A. Write access to production program libraries
B. Write access to development data libraries
C. Execute access to production program libraries
D. Execute access to development program libraries

Answer: A

Explanation:

Write access to production program libraries presents the greatest risk when granted to a new member of the system development staff. Production program libraries contain executable code that runs on live systems and supports critical business functions. Write access allows a user to modify or delete existing programs, or add new programs to the library. If a user were to make unauthorized or erroneous changes to production programs, it could cause serious disruptions, errors, or security breaches in the organization’s operations. Therefore, writeaccess to production program libraries should be restricted to authorized personnel only, and subject to strict change management controls.

Question: 19

An IS auditor is conducting a post-implementation review of an enterprise resource planning (ERP) system. End users indicated concerns with the accuracy of critical automatic calculations made by the system. The auditor's FIRST course of action should be to:

A. review recent changes to the system.
B. verify completeness of user acceptance testing (UAT).
C. verify results to determine validity of user concerns.
D. review initial business requirements.

Answer: C

Explanation:

The IS auditor’s first course of action should be to verify the results of the critical automatic calculations made by the system to determine the validity of user concerns. This is because the IS auditor needs to obtain sufficient and appropriate audit evidence to support the audit findings and conclusions. By verifying the results, the IS auditor can assess whether there are any errors or discrepancies in the system’s calculations that could affect the accuracy and reliability of the financial data. The IS auditor can use various techniques to verify the results, such as re-performing the calculations, comparing them with expected values, or tracing them to source documents.

Question: 20

Which of the following provides the MOST reliable audit evidence on the validity of transactions in a financial application?

A. Walk-through reviews

B. Substantive testing

C. Compliance testing

D. Design documentation reviews

Answer: B

Explanation:

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

Question: 21

During an incident management audit, an IS auditor finds that several similar incidents were logged during the audit period. Which of the following is the auditor's MOST important course of action?

A. Document the finding and present it to management.

B. Determine if a root cause analysis was conducted.

C. Confirm the resolution time of the incidents.

D. Validate whether all incidents have been actioned.

Answer: B

Explanation:

The IS auditor’s most important course of action after finding that several similar incidents were logged during the audit period is to determine if a root cause analysis was conducted. A root cause analysis is a systematic process that identifies the underlying causes of system failures or incidents. A root cause analysis can help to prevent recurrence of similar incidents, improve system performance and reliability, and enhance incident management processes. The IS auditor should evaluate whether a root cause analysis was performed for each incident, whether it was timely and thorough, and whether it resulted in effective corrective actions.

Question: 22

During an external review, an IS auditor observes an inconsistent approach in classifying system criticality within the organization. Which of the following should be recommended as the PRIMARY factor to determine system criticality?

A. Key performance indicators (KPIs)
B. Maximum allowable downtime (MAD)
C. Recovery point objective (RPO)
D. Mean time to restore (MTTR)

Answer: B

Explanation:

The primary factor to determine system criticality within an organization is the maximum allowable downtime (MAD). MAD is the maximum time frame during which recovery must become effective before an outage compromises the ability of an organization to achieve its business objectives and/or survival. MAD reflects the business impact of a system outage onthe organization’s operations, reputation, compliance, and finances. MAD can help to prioritize system recovery efforts, allocate resources, and establish recovery objectives.

Question: 23

An IS auditor discovers an option in a database that allows the administrator to directly modify any table. This option is necessary to overcome bugs in the software, but is rarely used. Changes to tables are automatically logged. The IS auditor's FIRST action should be to:

A. recommend that the option to directly modify the database be removed immediately.
B. recommend that the system require two persons to be involved in modifying the database.
C. determine whether the log of changes to the tables is backed up.
D. determine whether the audit trail is secured and reviewed.

Answer: D

Explanation:

The IS auditor’s first action after discovering an option in a database that allows the administrator to directly modify any table should be to determine whether the audit trail is secured and reviewed. This is because direct modification of database tables can pose a significant risk to data integrity, security, and accountability. An audit trail is a record of all changes made to database tables, including who made them, when they were made, and what was changed. An audit trail can help to detect unauthorized or erroneous changes, provide evidence for investigations or audits, and support data recovery or restoration. The IS auditor should assess whether the audit trail is protected from tampering or deletion, and whether it is regularly reviewed for anomalies or exceptions.

Question: 24

An IS auditor finds that a key Internet-facing system is vulnerable to attack and that patches are not available. What should the auditor recommend be done FIRST?

A. Implement a new system that can be patched.

B. Implement additional firewalls to protect the system.

C. Decommission the server.

D. Evaluate the associated risk.

Answer: D

Explanation:

The first step in addressing a vulnerability is to evaluate the associated risk, which involves assessing the likelihood and impact of a potential exploit. Based on the risk assessment, the appropriate mitigation strategy can be determined, such as implementing a new system, addingfirewalls, or decommissioning the server. Reference: ISACA CISA Review Manual 27th Edition, page 280

Question: 25

IS management has recently disabled certain referential integrity controls in the database management system (DBMS) software to provide users increased query performance. Which of the following controls will MOST effectively compensate for the lack of referential integrity?

A. More frequent data backups

B. Periodic table link checks

C. Concurrent access controls

D. Performance monitoring tools

Answer: B

Explanation:

Referential integrity is a property of data that ensures that all references between tables are valid and consistent. Disabling referential integrity controls can result in orphaned records, data anomalies, and inaccurate queries. The most effective way to compensate for the lack of referential integrity is to perform periodic table link checks, which verify that all foreign keys match existing primary keys in the related tables. More frequent data backups, concurrent access controls, and performance monitoring tools do not address the issue of data consistency and accuracy. Reference: ISACACISA Review Manual 27th Edition, page 291

Question: 26

A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

A. Periodically reviewing log files

B. Configuring the router as a firewall

C. Using smart cards with one-time passwords

D. Installing biometrics-based authentication

Answer: A

Explanation:

The most effective way to detect an intrusion attempt is to periodically review log files, which record the activities and events on a system or network. Log files can provide evidence of unauthorized access attempts, malicious activities, or system errors. Configuring the router as a firewall, using smart cards with one-time passwords, and installing biometrics-basedauthentication are preventive controls that can reduce the likelihood of an intrusion, but they do not detect it. Reference: ISACA CISA Review Manual 27th Edition, page 301

Question: 27

The PRIMARY advantage of object-oriented technology is enhanced:

A. efficiency due to the re-use of elements of logic.

B. management of sequential program execution for data access.

C. grouping of objects into methods for data access.

D. management of a restricted variety of data types for a data object.

Answer: A

Explanation:

The primary advantage of object-oriented technology is enhanced efficiency due to the re-use of elements of logic. Object-oriented technology is a software design model that uses objects, which contain both data and code, to create modular and reusable programs. Objects can be inherited from other objects, which reduces duplication and improves maintainability. Grouping objects into methods for data access, managing sequential program execution for data access, and managing a restricted variety of data types for a data object are not advantages of object-oriented technology. Reference: ISACA CISA Review Manual 27th Edition, page 304

Question: 28

From an IS auditor's perspective, which of the following would be the GREATEST risk associated with an incomplete inventory of deployed software in an organization?

A. Inability to close unused ports on critical servers

B. Inability to identify unused licenses within the organization

C. Inability to deploy updated security patches

D. Inability to determine the cost of deployed software

Answer: C

Explanation:

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

Question: 29

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. Reference: ISACA CISA Review Manual 27th Edition, page 310

Question: 30

During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be MOST concerned with the:

A. allocation of resources during an emergency.

B. frequency of system testing.

C. differences in IS policies and procedures.

D. maintenance of hardware and software compatibility.

Answer: A

Explanation:

During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be most concerned with the allocation of resources during an emergency. A reciprocal disaster recovery agreement is an arrangement by which one organization agrees to use another’s resources in the event of a business continuity event or incident. The IS auditor would need to ensure that both parties have clearly defined their roles and responsibilities, their resource requirements, their priority levels, their communication channels, and their escalation procedures in case of a disaster. The IS auditor would also need to verify that both parties have tested their agreement and have updated it regularly to reflect any changes in their business environments. The frequency of system testing is not as critical as the allocation of resources during an emergency, because system testing can be performed periodically or on demand, while resource allocation is a dynamic and complex process that requires careful planning and coordination. The differences in IS policies and procedures are not as critical as the allocation of resources during an emergency, because both parties can agree on common standards and protocols for their disaster recovery operations, or they can adapt their policies and procedures to suit each other’s needs. The maintenance of hardware and software compatibility is not as critical as the allocation of resources during an emergency, because both parties can use compatible or interoperable systems, or they can use virtualization or cloud computing technologies to overcome any compatibility issues. Reference: ISACACISA Review Manual 27th Edition, page 281

Question: 31

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 andcontrols 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. Reference: ISACA CISA Review Manual 27th Edition, page 300

Question: 32

Which of the following is an executive management concern that could be addressed by the implementation of a security metrics dashboard?

A. Effectiveness of the security program

B. Security incidents vs. industry benchmarks

C. Total number of hours budgeted to security

D. Total number of false positives

Answer: A

Explanation:

The executive management concern that could be addressed by the implementation of a security metrics dashboard is the effectiveness of the security program. A security metrics dashboard is a tool that provides a visual representation of key performance indicators (KPIs) and key risk indicators (KRIs) related to the organization’s information security objectives and activities. A security metrics dashboard can help executive management monitor and evaluate the performance and value delivery of the security program, identify strengths and weaknesses, assess compliance with policies and standards, and support decision making and improvement initiatives. Security incidents vs. industry benchmarks, total number of hours budgeted to security, and total number of false positives are not executive management concerns that could be addressed by the implementation of a security metrics dashboard.

These are more operational or technical aspects of information security that could be measured and reported by other means, such as incident reports, budget reports, or log analysis. Reference: [ISACA CISA Review Manual 27th Edition], page 302

Question: 33

One benefit of return on investment (ROI) analysts in IT decision making is that it provides the:

A. basis for allocating indirect costs.

B. cost of replacing equipment.

C. estimated cost of ownership.

D. basis for allocating financial resources.

Answer: D

Explanation:

One benefit of return on investment (ROI) analysis in IT decision making is that it provides the basis for allocating financial resources. ROI analysis is a method of evaluating the profitability or cost-effectiveness of an IT project or investment by comparing the expected benefits with the required costs. ROI analysis can help IT decision makers prioritize and justify their IT initiatives, allocate their financial resources optimally, and demonstrate the value contribution of IT to the organization’s goals and objectives. Basis for allocating indirect costs, cost of replacing equipment, and estimated cost of ownership are not benefits of ROI analysis in IT decision making. These are more inputs or outputs of ROI analysis that could be used to calculate or estimate the costs or benefits of an IT project or investment. Reference: [ISACA CISA Review Manual 27th Edition], page 307

Question: 34

Which of the following is an audit reviewer's PRIMARY role with regard to evidence?

A. Ensuring unauthorized individuals do not tamper with evidence after it has been captured

B. Ensuring evidence is sufficient to support audit conclusions

C. Ensuring appropriate statistical sampling methods were used

D. Ensuring evidence is labeled to show it was obtained from an approved source

Answer: B

Explanation:

The primary role of an audit reviewer with regard to evidence is to ensure that evidence is sufficient to support audit conclusions. Evidence is the information obtained by the auditor to provide a reasonable basis for the audit opinion or findings. Evidence should be sufficient, reliable, relevant, and useful to support the audit objectives and criteria. The audit reviewer should evaluate the quality and quantity of evidence collected by the auditor and determine if