PassQueen
a.k.a dumpsqueen.com

EC-Council Certified CISO (CCISO)

ECCouncil 712-50

Version Demo

Total Demo Questions: 79

Total Premium Questions: 792

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Governance	223
Topic 2, IS Management Controls and Audit Management	107
Topic 3, Management of Projects, Technology, and Operations	190
Topic 4, Information Security Core Concepts	188
Topic 5, Strategic Planning and Finance	84
Total	792

QUESTION NO: 1

You have been hired as the CISO for a hospital. The hospital currently deploys a hybrid cloud model using a Software as a Service (SaaS) product for healthcare clearinghouse services. The Health Insurance Portability and Accountability Act (HIPAA) require an agreement between Cloud Service Providers (CSP) and the covered entity. Based on HIPAA, once the agreement between the covered entity and the CSP signed, the CSP is _____?

A. Partially liable for compliance with the applicable requirements of the HIPAA Rules

B. Directly liable for compliance with the applicable requirements of the HIPAA Rules

C. Not liable for compliance with the applicable requirements of the HIPAA Rules

D. Indirectly liable for compliance with the applicable requirements of the HIPAA Rules

ANSWER: B

Explanation:

Directly liable for compliance with the applicable requirements of the HIPAA Rules is correct. When a cloud service provider creates, receives, maintains, or transmits protected health information on behalf of a covered entity, it is generally a HIPAA business associate, even if it only stores encrypted information and does not routinely access it. The required agreement is a business associate agreement (BAA), which establishes permitted uses and disclosures of protected health information and the safeguards the business associate must implement.

Importantly, the BAA does not merely transfer contractual duties from the hospital to the provider. HIPAA makes business associates directly accountable to the U.S. Department of Health and Human Services for the applicable provisions of the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule. A CSP must therefore protect electronic protected health information with appropriate administrative, physical, and technical safeguards, report relevant breaches, and meet the other HIPAA obligations that apply to its business-associate role. The covered entity retains its own HIPAA responsibilities, while the CSP has direct responsibility for its applicable HIPAA duties. See HHS guidance on business associates and cloud computing.

QUESTION NO: 2

Payment Card Industry (PCI) compliance requirements are based on what criteria?

A. The size of the organization processing credit card data

B. The types of cardholder data retained

C. The duration card holder data is retained

D. The number of transactions performed per year by an organization

ANSWER: D

Explanation:

The number of transactions performed per year by an organization is the relevant criterion because PCI DSS compliance validation is commonly organized into merchant levels based on annual payment-card transaction volume. The card brands and acquiring banks use those levels to determine the expected validation process, such as whether an organization must complete a Self-Assessment Questionnaire, undergo an onsite assessment by a Qualified Security Assessor, provide an Attestation of Compliance, and/or perform regular vulnerability scans. Transaction volume is generally measured over a twelve-month period and may be calculated separately by card brand, so an organization should confirm its precise obligations with its acquirer and the applicable payment brands.

PCI DSS itself establishes a baseline set of security requirements for entities that store, process, or transmit cardholder data, while the merchant-level thresholds determine the validation and reporting obligations that demonstrate compliance. For example, Visa publishes merchant compliance criteria and annual-volume levels used for PCI DSS validation, and the PCI Security Standards Council explains the standard’s applicability to organizations handling account data. See Visa merchant levels and PCI Security Standards Council merchant guidance.

QUESTION NO: 3

A method to transfer risk is to:

A. Implement redundancy

B. move operations to another region

C. purchase breach insurance

D. Alignment with business operations

ANSWER: C

Explanation:

“purchase breach insurance” is a risk-transfer treatment because it contractually shifts specified financial consequences of a cybersecurity incident from the organization to an insurer, subject to the policy’s coverage terms, limits, exclusions, deductible, and notification conditions. The organization still owns and must manage the underlying operational and security risk: insurance does not prevent a breach, restore disrupted services by itself, or remove legal and regulatory obligations. Instead, it allocates qualifying losses—such as incident-response services, legal defense, forensic investigation, notification, public relations, and certain business-interruption costs—to another party in exchange for a premium. This is the core distinction of risk transfer in enterprise risk management: a third party accepts responsibility for defined loss exposure through a contractual arrangement. A CISO should ensure that cyber-insurance coverage is aligned with the organization’s risk assessment, critical assets, plausible incident scenarios, vendor dependencies, and recovery arrangements. Coverage should also be periodically reviewed as the business, threat landscape, and regulatory obligations change. NIST describes risk transfer as shifting risk-related consequences to another party, including through insurance, in its risk-management guidance. See NIST SP 800-39: Managing Information Security Risk and NIST Cybersecurity Framework FAQs.

QUESTION NO: 4

IT control objectives are useful to IT auditors as they provide the basis for understanding the:

A. Desired results or purpose of implementing specific control procedures.

B. The audit control checklist.

C. Techniques for securing information.

D. Security policy

ANSWER: A

Explanation:

Desired results or purpose of implementing specific control procedures. is correct because a control objective states the outcome a control is intended to achieve. It expresses the business, governance, security, operational, or compliance purpose that control activities must support. For an IT auditor, this objective establishes the evaluation criterion: the auditor first determines the intended result, then assesses whether appropriately designed controls exist and whether those controls operate effectively enough to achieve that result. For example, an access-management control objective may be to ensure that access to systems and information is restricted to authorized users according to business need. The objective is therefore not merely a list of audit steps; it identifies the condition or result that the control environment should deliver. ISACA’s COBIT guidance similarly distinguishes governance and management objectives from the practices and activities used to achieve them, reinforcing the role of objectives in structuring assurance work and evaluating control design and effectiveness. This outcome-focused view enables audits to remain aligned with organizational requirements and risk treatment rather than focusing only on the mechanics of individual procedures. See ISACA COBIT resources and The IIA Global Internal Audit Standards.

QUESTION NO: 5

A CISO is reviewing the organization's security budget. Several proposed initiatives have similar technical benefits, but only one can be funded this year.

Which of the following should be the PRIMARY basis for prioritizing the investment?

A. The expected reduction of business risk

B. The number of features offered by the product

C. The preference of the technology team

D. The lowest implementation cost

ANSWER: A

Explanation:

The expected reduction of business risk is the primary basis because security investments should be selected according to their ability to reduce risks that could materially affect organizational objectives. This requires consideration of the value and criticality of affected assets, the likelihood and impact of relevant threat scenarios, the effectiveness of the proposed control, and the residual risk that will remain.

Technical capability, vendor reputation, and implementation convenience may be relevant considerations, but they do not establish whether an initiative provides the greatest value to the organization. Risk-based prioritization enables the CISO to explain security spending in terms senior management can use for governance and resource-allocation decisions. NIST describes risk management as supporting organizational decisions through assessment of likelihood, impact, and risk response. See NIST SP 800-39.

QUESTION NO: 6

Which of the following intellectual Property components is focused on maintaining brand recognition?

A. Trademark

B. Research Logs

C. Copyright

D. Patent

ANSWER: A

Explanation:

Trademark is correct because trademark law protects the identifiers that distinguish one organization's goods or services from those of another organization. These identifiers can include brand names, logos, slogans, symbols, distinctive packaging, and—in appropriate circumstances—other source-identifying elements. By granting the owner the ability to prevent confusingly similar use by others, trademark protection helps preserve the distinct association between a brand and its commercial source. This is directly tied to maintaining brand recognition, consumer trust, and marketplace goodwill. From an information-security leadership perspective, trademarks are intellectual-property assets that require governance and monitoring, particularly for unauthorized use, impersonation, counterfeit activity, and lookalike branding that may damage the organization's reputation. The United States Patent and Trademark Office explains that a trademark identifies the source of goods or services and distinguishes them from those provided by others. The World Intellectual Property Organization likewise describes trademarks as signs that distinguish one enterprise's goods or services from those of other enterprises. These source-identification and differentiation functions make trademark protection the intellectual-property component focused on brand recognition. See the USPTO trademark basics and WIPO trademarks overview.

QUESTION NO: 7

In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

A. Internal Audit

B. Information Security

C. Compliance

D. Database Administration

ANSWER: B

Explanation:

Information Security is correct because monitoring and reviewing network intrusion detection system logs is a core operational security function. Security personnel, often within a security operations center, use IDS alerts and log data to identify suspicious activity, validate potential attacks, assess their impact, and initiate incident-response procedures. This recurring review supports continuous detection and timely escalation of threats across the organization's environment. The function requires security-specific expertise in attack indicators, alert triage, correlation of events from multiple systems, and response coordination. NIST describes continuous monitoring as maintaining ongoing awareness of information-security risks, including collecting and analyzing security-related information. Its incident-handling guidance also identifies detection and analysis as essential activities for recognizing and evaluating potential incidents. These responsibilities align directly with the Information Security group's daily protective-monitoring role. See NIST SP 800-137, Information Security Continuous Monitoring and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 8

A third-party service provider will process customer personal information on behalf of an organization.

Which of the following is MOST important to include in the contract before processing begins?

A. Defined security, privacy, breach-notification, and audit requirements

B. A commitment to use the organization's corporate logo

C. A requirement that all provider personnel work onsite

D. A fixed contract term of at least five years

ANSWER: A

Explanation:

Defined security, privacy, breach-notification, and audit requirements are most important because the organization remains accountable for ensuring that personal information is processed in accordance with applicable legal, regulatory, contractual, and business requirements. The contract should clearly establish the provider's obligations for safeguarding data, reporting incidents, supporting investigations, managing subcontractors, returning or securely disposing of data, and providing assurance of control operation.

A general statement that the provider will follow industry practices is insufficient because it does not define measurable obligations, accountability, or remedies. Third-party risk management should include due diligence before engagement and ongoing monitoring throughout the relationship. NIST supply-chain risk-management guidance addresses establishing security requirements and oversight for external service providers. See NIST SP 800-161 Rev. 1 and NIST Privacy Framework.

QUESTION NO: 9

Which business stakeholder is accountable for the integrity of a new security system within the Security Operations Center (SOC)?

A. Chief Information Officer (CIO)

B. Chief Executive Officer (CEO)

C. Chief Compliance Officer (CCO)

D. Chief Information Security Officer (CISO)

ANSWER: D

Explanation:

Chief Information Security Officer (CISO) is correct because this executive is the business leader responsible for establishing and governing the organization's information-security program, including the security capabilities operated through a Security Operations Center. Accountability for a new SOC security system means ensuring that the system is appropriately selected, securely implemented, validated, monitored, maintained, and aligned to enterprise risk tolerance and security objectives. The CISO provides the security governance and executive ownership needed to ensure the system produces reliable, trustworthy results and supports effective detection, response, and reporting.

In practice, this accountability includes defining security requirements, approving security architecture and control objectives, ensuring appropriate assurance and testing, assigning operational ownership, and receiving metrics or risk reports on the system's performance. A CISO may delegate technical administration and day-to-day monitoring to SOC personnel or other teams, but delegation of activities does not remove executive accountability for the security capability's integrity and effectiveness. This aligns with the CCISO focus on security governance, risk management, and directing the information-security function. See EC-Council's CCISO certification overview and NIST's guidance on risk-management responsibilities and system security governance.

QUESTION NO: 10

When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

A. When there is a variety of technologies deployed in the infrastructure.

B. When it results in an overall lower cost of operating the security program.

C. When there is a need to develop a more unified incident response capability.

D. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.

ANSWER: D

Explanation:

When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements is correct because decentralized policies and procedures allow security requirements to be tailored to the operational context of each business unit. Units may process different types of information, use specialized technologies, operate in different jurisdictions, and face materially different threat and compliance obligations. A single detailed, enterprise-wide procedure can become impractical in such an environment; it may either fail to address a unit's specific risks or impose unnecessary operational burdens. Decentralization enables accountable local management to define and maintain procedures that implement security objectives appropriately for its assets, risk appetite, legal obligations, and business processes. Effective decentralization still requires enterprise governance: senior leadership should establish common security principles, minimum control requirements, risk-management methodology, oversight, and exception handling, while allowing implementation details to vary by unit. This approach is consistent with the NIST Cybersecurity Framework's emphasis on organizational governance, risk management, and the use of profiles to reflect specific business needs. See the NIST Cybersecurity Framework and NIST's SP 800-53 control catalog, which supports tailoring controls to organizational missions, environments, and risks.

QUESTION NO: 11

The total cost of security controls should:

A. Be equal to the value information resource being protected

B. Should not matter, as long as the information resource is protected

C. Be greater than the value of the information resource being protected

D. Be less than the value of the information resource being protected

ANSWER: D

Explanation:

The total cost of security controls should be less than the value of the information resource being protected. This reflects the fundamental economic principle of security control selection: safeguards must be cost-justified and proportionate to the business value of the asset and the risk being treated. A security leader evaluates not only acquisition cost, but also implementation, integration, operational administration, monitoring, maintenance, training, and eventual replacement costs. The expected reduction in loss exposure delivered by a control must justify that total lifecycle investment.

In practice, this assessment is commonly expressed through cost-benefit analysis, using measures such as annualized loss expectancy and the expected loss reduction from a safeguard. Controls are selected to reduce risk to a level consistent with organizational risk appetite while preserving an economically sound outcome. The principle does not require eliminating every risk; some residual risk is accepted when further treatment would cost more than the loss it is intended to prevent. NIST's risk-management guidance emphasizes selecting and implementing controls that are appropriate to organizational risks and conditions, while ISACA describes cost-benefit considerations as an essential part of risk response decisions. See NIST SP 800-53 and ISACA's risk-management guidance.

QUESTION NO: 12

What is the estimate of all direct and indirect costs associated with an asset or acquisition over its entire life cycle?

A. Total COST of Product

B. Total Cost of Ownership

C. Return on Investment

D. Total Cost of Production

ANSWER: B

Explanation:

Total Cost of Ownership is the estimate of the complete direct and indirect cost of acquiring, deploying, operating, supporting, maintaining, and ultimately retiring an asset throughout its useful life. In an information-security and governance context, this lifecycle perspective is essential because an acquisition's purchase price alone rarely represents its full financial impact. A TCO assessment accounts for costs such as implementation, integration, licensing, infrastructure, personnel time, training, vendor support, upgrades, monitoring, maintenance, downtime, and disposal or replacement. This enables executive leadership to compare alternatives on their actual long-term resource requirements, support sound budgeting, and make informed investment and risk-management decisions. The U.S. Government Accountability Office describes life-cycle cost as the total cost of ownership over a system's life, including research and development, procurement, operations and maintenance, and disposal. The U.S. Department of Energy similarly defines life-cycle cost as the total costs associated with owning, operating, maintaining, and disposing of an asset. These established lifecycle-costing principles align directly with the definition in the question. See the GAO Cost Estimating and Assessment Guide and the U.S. Department of Energy Life-Cycle Cost Analysis.

QUESTION NO: 13

When developing the Business Impact Assessment (BIA), which of the following MOST closely relates to data backup and restoration?

A. Maximum Tolerable Downtime (MTD)

B. Recovery Point Objective (RPO)

C. Mean Time to Delivery (MTD)

D. Recovery Time Objective (RTO)

ANSWER: B

Explanation:

Recovery Point Objective (RPO) most closely relates to data backup and restoration because it defines the maximum acceptable amount of data loss measured in time. For example, an RPO of four hours means that, after a disruption, the organization must be able to restore data to a point no more than four hours before the incident. This requirement directly determines the necessary backup frequency, replication cadence, backup retention design, and restoration capabilities for a business process or system.

During a Business Impact Assessment, stakeholders identify the operational and business consequences of losing data and establish tolerable thresholds. RPO converts that business tolerance into a measurable continuity and recovery requirement. Systems processing high-value or rapidly changing information may require very short RPOs, potentially supported by continuous replication or frequent snapshots, while less critical systems may tolerate longer intervals between backups. NIST defines RPO as the point in time to which data must be recovered after an outage, making it a central metric for backup and restoration planning. See the NIST definition of Recovery Point Objective and NIST's Contingency Planning Guide for Federal Information Systems.

QUESTION NO: 14

Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN.

Recently, members of your organization have been targeted through a number of sophisticated phishing attempts and have compromised their system credentials. What action can you take to prevent the misuse of compromised credentials to change bank account information from outside your organization while still allowing employees to manage their bank information?

A. Turn off VPN access for users originating from outside the country

B. Enable monitoring on the VPN for suspicious activity

C. Force a change of all passwords

D. Block access to the Employee-Self Service application via VPN

ANSWER: D

Explanation:

Block access to the Employee-Self Service application via VPN is the appropriate action because it creates an access boundary around a particularly high-impact self-service function: changing payroll bank-routing and account details. A stolen username and password could still permit an attacker to establish a VPN session, but the attacker would be unable to reach the Employee-Self Service application through that remote-access path. Employees can continue to manage their bank information when connected from the organization's internal network, satisfying the stated operational requirement while removing the exposed remote route used in the scenario.

This is a practical application of restricting access to sensitive resources according to context and minimizing the paths through which a credential can be abused. NIST describes access control as limiting system access to authorized users, processes, and devices, and recognizes the importance of enforcing access restrictions for specific resources and connection methods. See NIST SP 800-53 Rev. 5. CISA similarly emphasizes reducing implicit trust and applying access decisions based on the resource and access context in its Zero Trust Maturity Model. In practice, this control should be

paired with stronger authentication and alerting, but blocking VPN access to this sensitive application directly prevents the described external misuse.

QUESTION NO: 15

SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organizationâ€™s needs.

The CISO is unsure of the information provided and orders a vendor proof of concept to validate the systemâ€™s scalability. This demonstrates which of the following?

A. An approach that allows for minimum budget impact if the solution is unsuitable

B. A methodology-based approach to ensure authentication mechanism functions

C. An approach providing minimum time impact to the implementation schedules

D. A risk-based approach to determine if the solution is suitable for investment

ANSWER: D

Explanation:

A risk-based approach to determine if the solution is suitable for investment is correct because the CISO has identified a material uncertainty: whether the chosen two-factor authentication product can scale to meet organizational requirements. Scalability affects the likelihood of implementation failure, service disruption, unplanned redesign costs, and the ability to realize the expected security benefits. Rather than relying on vendor assertions or proceeding with implementation based on incomplete information, the CISO requests a proof of concept to generate evidence under conditions relevant to the organization.

This is risk-based decision-making: identify an uncertainty that could affect objectives, assess it through targeted validation, and use the resulting information to determine whether the investment and implementation should proceed. A proof of concept is especially appropriate before committing further resources because it can validate technical feasibility, capacity behavior, integration assumptions, and operational suitability. The result supports an informed treatment decision, such as accepting the solution, requiring remediation, selecting a different product, or revising the implementation plan. This aligns with NIST guidance that risk assessments inform organizational decisions and risk responses, as described in NIST SP 800-30 Rev. 1 and the NIST Risk Management Framework.

QUESTION NO: 16

Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

A. Reduction of budget

B. Decreased security awareness

C. Improper use of information resources

D. Fines for regulatory non-compliance

ANSWER: D

Explanation:

Fines for regulatory non-compliance represents the highest negative impact because an ineffective security governance program can leave an organization unable to demonstrate that it has assigned accountability, assessed risk, implemented required controls, and monitored compliance with applicable legal and regulatory obligations. When a regulator identifies material non-compliance, penalties can be substantial and immediate, affecting financial results, operational priorities, and executive or board oversight. The impact also extends beyond the fine itself: regulatory enforcement commonly requires remediation commitments, independent assessments, reporting, and sustained governance improvements. Effective security

governance establishes decision rights, oversight, policies, risk management, and performance monitoring so that security activities remain aligned with both business objectives and compliance duties. This makes preventing and detecting compliance failures a core governance outcome rather than merely an operational security task. NIST's Cybersecurity Framework emphasizes that governance provides oversight, expectations, and accountability for managing cybersecurity risk, including legal and regulatory requirements. Regulatory authorities also demonstrate that security and privacy failures can lead to significant civil monetary penalties. See the NIST Cybersecurity Framework and the FTC Rite Aid enforcement action.

QUESTION NO: 17

A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?

A. Poorly configured firewalls

B. Malware

C. Advanced Persistent Threat (APT)

D. An insider

ANSWER: D

Explanation:

An insider is the most probable threat actor because a rapid compromise involving many accounts on a hardened system strongly suggests access or knowledge that is already within the organization's trust boundary. An insider—such as an employee, contractor, administrator, or other person with authorized access—may possess privileged credentials, understand account-management processes, know where sensitive information is stored, or be able to bypass normal controls. That access can be used maliciously or mishandled in a way that exposes numerous accounts to an external party. Hardened systems commonly have layered technical protections, so widespread and sudden account exposure is particularly consistent with misuse of legitimate access, privileged account abuse, or disclosure of credentials by someone who already has trusted access.

NIST describes insider threat as the potential for individuals with authorized access to use that access, intentionally or unintentionally, in a manner that harms the organization. Effective response should therefore include immediate credential containment, review of privileged and account-management activity, preservation of relevant logs, and investigation of unusual data transfers or authentication events. See NIST's definition of insider threat and CISA's insider-threat mitigation guidance.

QUESTION NO: 18

Which of the following is the MOST logical method of deploying security controls within an organization?

A. Obtain funding for all desired controls and then create project plans for implementation

B. costly controls

C. Apply the least costly controls to demonstrate positive program activity

D. Obtain business unit buy-in through close communication and coordination

ANSWER: D

Explanation:

Obtain business unit buy-in through close communication and coordination is the most logical approach because security controls affect how business processes operate, how information is handled, and what responsibilities users and process owners must assume. Effective deployment therefore requires collaboration with the leaders and staff who own the affected processes. Early communication enables the security function to understand operational requirements, explain the control

objectives and expected impact, coordinate implementation timing, establish accountable owners, and obtain acceptance of any residual risk. This support also improves adoption: controls that are understood and incorporated into normal workflows are more likely to be used consistently and sustained after implementation. At the executive level, a CISO is expected to align information-security initiatives with business objectives and communicate risk and security requirements to stakeholders. This governance-focused, stakeholder-engagement approach is reflected in the CCISO role description from EC-Council. It is also consistent with NIST guidance that emphasizes organization-wide preparation, stakeholder roles, and ongoing communication throughout risk-management activities; see NIST SP 800-37 Rev. 2. Funding and implementation planning remain important, but they should be carried out with informed business participation rather than as an isolated security exercise.

QUESTION NO: 19

A key cybersecurity feature of a Personal Identification Verification (PIV) Card is:

A. Inability to export the private key

B. It can double as physical identification at the DMV

C. It has the user's photograph to help ID them

D. It can be used as a secure flash drive

ANSWER: A

Explanation:

Inability to export the private key is a core cybersecurity property of a PIV credential. A PIV card is a hardware-based credential used to support strong authentication, digital signatures, and key establishment. Its private cryptographic keys are intended to remain protected within the card's secure cryptographic boundary rather than being copied to a workstation, removable media device, or another system. When the card performs a cryptographic operation, such as signing an authentication challenge, the relying system receives the resulting cryptographic output, not the private key material itself.

This design substantially reduces the risk that malware, unauthorized users, or compromise of an endpoint can steal and reuse the credential's private key. Use of the key is also normally gated by card possession and user verification, such as a PIN, providing a practical combination of something the user has and something the user knows. Certificates, which contain public keys and identity information, can be distributed to enable signature validation; the protected asset is specifically the associated private key. NIST's PIV specifications describe the card as a secure platform for PIV credentials and cryptographic key operations. See NIST SP 800-73-4 and FIPS 201-3.

QUESTION NO: 20

Which of the following would be used to measure the effectiveness of an Information Security Management System (ISMS)?

A. Information Technology Infrastructure Library (ITIL)

B. Control Objectives for Information and Related Technology (COBIT)

C. International Organization for Standardization (ISO) 27004

D. International Organization for Standardization (ISO) 27005

ANSWER: C

Explanation:

International Organization for Standardization (ISO) 27004 is the appropriate standard for measuring the effectiveness of an Information Security Management System because it specifically addresses information-security measurement. An ISMS is not complete merely because controls have been implemented; leadership needs reliable evidence that those controls, processes, and objectives are achieving their intended information-security outcomes. ISO/IEC 27004 provides guidance for establishing and operating a measurement program that produces this evidence.

Its focus includes defining useful measures, identifying the data needed for those measures, collecting and analyzing results, and reporting information that supports management decisions and continual improvement. This directly supports the ISMS performance-evaluation expectations in ISO/IEC 27001, which require an organization to determine what needs monitoring and measurement, the methods used, when results are analyzed, and who evaluates them. Metrics developed using ISO/IEC 27004 can help management assess whether security objectives are being met, whether controls operate as intended, and where corrective improvement is warranted.

This makes International Organization for Standardization (ISO) 27004 the specialized and authoritative choice for ISMS effectiveness measurement. See the ISO overview of ISO/IEC 27004 and the ISMS requirements described in ISO/IEC 27001.

QUESTION NO: 21

Which of the following provides an independent assessment of a vendor's internal security controls and overall posture?

A. Alignment with business goals

B. ISO27000 accreditation

C. PCI attestation of compliance

D. Financial statements

ANSWER: B

Explanation:

ISO27000 accreditation is the best answer because independent certification against the ISO/IEC 27001 information security management system standard gives a customer meaningful assurance that a vendor's security program has been assessed by an accredited external certification body. The assessment evaluates whether the vendor has established, implemented, maintained, and continually improved an information security management system, including a risk-based approach to selecting and operating security controls. This provides evidence beyond a vendor's own statements: the certification process includes audit activities, documented findings, and periodic surveillance or recertification audits to confirm continuing conformity.

In third-party risk management, an ISO/IEC 27001 certificate can therefore serve as a broadly applicable indicator of the maturity and governance of a vendor's internal security controls and overall security posture. A customer should still validate the certificate's scope, issuing certification body, validity dates, and relevance to the specific services being procured, because certification applies only to the stated scope of the management system. ISO describes ISO/IEC 27001 and certification at ISO/IEC 27001 — Information security management systems, while the International Accreditation Forum explains the role of accredited certification at IAF: Accredited Certification.

QUESTION NO: 22

The PRIMARY objective for information security program development should be:

A. Reducing the impact of the risk to the business.

B. Establishing strategic alignment with bunsiness continuity requirements

C. Establishing incident response programs.

D. Identifying and implementing the best security solutions.

ANSWER: A

Explanation:

Reducing the impact of the risk to the business is the primary objective because an information security program exists to preserve the organization's ability to achieve its mission and business objectives despite threats, vulnerabilities, and security incidents. Effective program development starts with understanding the business context, identifying information-related

risks, and selecting governance, technical, and operational measures that keep residual risk within leadership's risk tolerance. The intended result is not security for its own sake; it is the protection of business processes, information assets, stakeholders, financial performance, reputation, and operational resilience. A risk-based program also enables management to prioritize limited people, budget, and technology resources according to the potential business consequences of adverse events. This approach supports continual measurement and improvement as the threat landscape and organizational objectives change. NIST describes risk management as an organization-wide activity that provides a disciplined, structured, and flexible process for managing security and privacy risk in support of organizational missions and business functions. See NIST SP 800-39: Managing Information Security Risk. Similarly, the NIST Cybersecurity Framework emphasizes managing cybersecurity risk in a manner that supports organizational objectives. Accordingly, reducing business risk impact is the guiding objective for the overall information security program.

QUESTION NO: 23

You have recently drafted a revised information security policy. From whom should you seek endorsement in order to have the GREATEST chance for adoption and implementation throughout the entire organization?

A. Chief Executive Officer

B. Chief Information Officer

C. Chief Information Security Officer

D. Chief Information Officer

ANSWER: A

Explanation:

Endorsement from the **Chief Executive Officer** gives a revised information security policy the strongest authority for organization-wide adoption and implementation. Information security is an enterprise governance matter: it affects every business unit, workforce member, process, information asset, and technology environment. The CEO is positioned to communicate that the policy is a business requirement rather than merely an IT or security-team initiative, establish accountability among senior leaders, and ensure that adequate resources and cross-functional cooperation are available for implementation.

Visible executive sponsorship also helps embed policy requirements into organizational priorities, management objectives, operational procedures, and compliance expectations. While policy development and administration may be delegated to security and technology leadership, endorsement by the highest executive authority creates the broad management commitment needed to drive consistent behavior across functions. NIST describes information-security governance as requiring executive-level direction and support, including management commitment to security policy and program responsibilities. This aligns with the governance focus of senior executive leadership in an enterprise security program. See NIST SP 800-100, Information Security Handbook and NIST SP 800-12 Rev. 1, Introduction to Information Security.

QUESTION NO: 24

A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding.

Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?

A. The organization has purchased cyber insurance

B. The risk tolerance of the organization permits this risk

C. The CIO of the organization disagrees with the finding

D. The auditors have not followed proper auditing processes

ANSWER: B

Explanation:

The risk tolerance of the organization permits this risk is the most likely reason to reject the recommended implementation. An audit finding identifies a condition that deviates from a required control, policy, standard, or expected practice, and the recommendation normally proposes a way to reduce the related risk. However, management is responsible for deciding how risk will be treated. Where the residual risk associated with a control exception is understood, assessed, and remains within the organization's approved risk tolerance, the organization may formally accept that risk rather than invest in new technology or processes.

This decision should be made through the established risk-governance process by an appropriately authorized risk owner, with the rationale, risk assessment, acceptance period, and any required monitoring documented. Risk tolerance provides practical boundaries for decision-making: it recognizes that eliminating every risk is neither feasible nor economically justified. The recommendation may therefore be declined when its expected risk reduction does not warrant its cost or operational impact, provided the residual exposure stays within approved tolerance. NIST's Risk Management Framework describes risk acceptance as an authorized risk response following assessment and treatment decisions; see NIST SP 800-37 Rev. 2. NIST also discusses organizational risk tolerance in NIST SP 800-39.

QUESTION NO: 25

What does a security control objective provide for auditors?

A. Policy guidance for controls and implementations

B. Desired results or purpose of implementing a specific control

C. Techniques that were used for securing information

D. The framework for the audit control object checklist

ANSWER: B

Explanation:

Desired results or purpose of implementing a specific control is correct because a control objective states the intended security, compliance, or risk-management outcome that the control is meant to achieve. It gives auditors a clear evaluation criterion: the auditor can determine whether the control is appropriately designed and operating in a manner that supports the stated outcome. For example, an access-control objective may be to ensure that only authorized individuals can access sensitive information. The specific technologies, procedures, and configurations used to implement that objective can vary, but the objective remains the benchmark for audit assessment.

This distinction is central to risk-based assurance. Auditors use control objectives to connect a business or security risk with expected control outcomes, then gather evidence to assess whether those outcomes are being achieved consistently. NIST describes security controls as safeguards or countermeasures prescribed to meet security requirements, while assessment evaluates the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome. See NIST's definition of a security control and NIST SP 800-53A control-assessment guidance. Thus, the control objective provides auditors with the intended result against which control effectiveness can be assessed.

QUESTION NO: 26

What is the relationship between information protection and regulatory compliance?

A. That all information in an organization must be protected equally.

B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.

C. There is no relationship between the two.

D. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protected based on business need.

ANSWER: D

Explanation:

The correct relationship is that the protection of some information, such as National ID information, is mandated by regulation, while other information, such as trade secrets, is protected based on business need. An information-protection program must account for both sources of obligation. Regulatory compliance establishes mandatory safeguards for defined data types and processing activities, including personally identifiable information, health data, payment data, or government-issued identity information, depending on the applicable jurisdiction and sector. These obligations typically require risk-appropriate technical and organizational measures, governance, and demonstrable accountability.

Business needs extend protection beyond the minimum legal baseline. Trade secrets, proprietary designs, strategic plans, source code, pricing, and intellectual property may not be subject to a specific privacy regulation, but their disclosure, alteration, or loss could create substantial competitive, operational, and financial harm. A sound classification policy therefore identifies information according to legal, regulatory, contractual, and business-value requirements, then applies handling rules and controls appropriate to each classification. This approach helps a CISO demonstrate compliance while also preserving the confidentiality and value of critical organizational assets. The GDPR's security principle is described in GDPR Article 32, and NIST discusses categorizing information systems according to impact in FIPS Publication 199.

QUESTION NO: 27

Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

A. Implementation of business-enabling information security

B. Use within an organization to ensure compliance with laws and regulations

C. To enable organizations that adopt it to obtain certifications

D. Use within an organization to formulate security requirements and objectives

ANSWER: A

Explanation:

ISO/IEC 27001's primary purpose is the implementation of business-enabling information security through a risk-based information security management system (ISMS). It establishes requirements for an organization to identify information-security risks, select and operate appropriate controls, monitor their effectiveness, and continually improve the management system. This approach protects the confidentiality, integrity, and availability of information while ensuring that security activities support organizational objectives rather than operating as an isolated technical function.

"Implementation of business-enabling information security" correctly reflects the management-system focus of the standard. ISO/IEC 27001 is designed to embed information security into governance, processes, risk treatment, and continual improvement, allowing an organization to manage information risk in a manner appropriate to its business context and stakeholder needs. Certification may be available after independent assessment, but the standard's fundamental value is the operation and improvement of an effective ISMS that supports resilient, trustworthy business operations. ISO describes ISO/IEC 27001 as specifying requirements for establishing, implementing, maintaining, and continually improving an ISMS. See ISO's ISO/IEC 27001 overview and the ISO Online Browsing Platform entry for ISO/IEC 27001.

QUESTION NO: 28

Who is responsible for securing networks during a security incident?

A. Chief Information Security Officer (CISO)

B. Security Operations Center (SOC)

C. Disaster Recovery (DR) manager

D. Incident Response Team (IRT)

ANSWER: D

Explanation:

The **Incident Response Team (IRT)** is responsible for coordinating and executing the operational actions needed to secure networks during a security incident. This includes quickly determining the incident's scope, identifying affected network segments and systems, collecting and preserving relevant evidence, containing malicious activity, and implementing eradication and recovery actions. Network-securing measures may include isolating hosts, disabling compromised accounts, blocking malicious indicators, changing credentials, applying emergency controls, and validating that systems can safely return to normal operation.

This responsibility aligns with the incident-response lifecycle used in security governance and management programs: preparation, detection and analysis, containment, eradication, recovery, and post-incident activity. The IRT brings together the technical, forensic, operational, and communications capabilities required to make timely, controlled decisions while minimizing business impact. In a CCISO context, the CISO establishes governance, authority, policy, and executive oversight, while the IRT performs the incident-handling work under established procedures and escalation paths.

NIST describes incident response as encompassing containment, eradication, and recovery activities in its Computer Security Incident Handling Guide. EC-Council's CCISO program overview likewise emphasizes incident-management and security-operations leadership responsibilities.

QUESTION NO: 29

In terms of supporting a forensic investigation, it is now imperative that managers, firstresponders, etc., accomplish the following actions to the computer under investigation:

A. Immediately place hard drive and other components in an anti-static bag

B. Secure the area and attempt to maintain power until investigators arrive

C. Secure the area and shut down the computer until investigators arrive

D. Secure the area

ANSWER: B

Explanation:

Secure the area and attempt to maintain power until investigators arrive is correct because preserving the system's running state is central to effective digital-forensic handling. A powered-on computer may contain volatile evidence that is lost when power is removed, including the contents of RAM, active processes, logged-on user sessions, network connections, encryption keys, and temporary artifacts. Maintaining power gives trained forensic personnel the opportunity to make a controlled decision about live acquisition and to collect this information using documented, repeatable procedures.

First responders should protect the physical scene, prevent unauthorized access or use, and promptly escalate to qualified investigators. They should preserve the system's condition and record relevant observations, such as the screen state, connected devices, date and time, and visible applications, while maintaining chain-of-custody records. The decision to disconnect a system from networks or undertake a live response must be made in accordance with the organization's incident-response and forensic procedures so that evidence integrity and admissibility are protected. NIST's guidance on integrating forensic techniques into incident response emphasizes collecting and preserving data appropriately, including volatile information when relevant: NIST SP 800-86. Additional incident-handling guidance is available in NIST SP 800-61 Rev. 2.

QUESTION NO: 30

As the CISO for your company you are accountable for the protection of information resources commensurate with:

A. Risk of exposure

B. Cost and time to replace

C. Insurability tables

D. Customer demand

ANSWER: A

Explanation:

Risk of exposure is correct because a CISO's accountability for protecting information resources is risk-based: safeguards must be selected and applied in proportion to the potential exposure of an asset and the business impact if its confidentiality, integrity, or availability is compromised. This requires identifying relevant threat sources and vulnerabilities, estimating the likelihood and impact of adverse events, and treating risk within the organization's approved risk appetite. Higher-risk information and systems therefore warrant stronger or more extensive administrative, technical, and physical controls, as well as closer monitoring and governance.

This approach supports efficient use of security resources while ensuring that protection reflects the value and sensitivity of information, applicable legal and contractual obligations, and the consequences of a security incident. NIST describes risk management as an organization-wide process used to frame, assess, respond to, and monitor risk, and it emphasizes tailoring controls to the system's risk environment. Similarly, the NIST Cybersecurity Framework organizes cybersecurity outcomes around managing risk to organizational operations and assets. These principles align with the CISO's responsibility to ensure information-resource protection is commensurate with risk exposure. See NIST SP 800-37 Rev. 2 and the NIST Cybersecurity Framework.

QUESTION NO: 31

What is the name of a formal statement that defines the strategy, approach, or expectations related to specific concerns within an organization:

A. Policy

B. standard

C. Procedure

D. Guideline

ANSWER: A

Explanation:

Policy is the correct term because it is a formal, management-approved statement that establishes the organization's direction, intent, expectations, and rules for addressing a particular area of concern. For example, an information security policy establishes leadership's expectations for protecting information assets and managing security responsibilities. Policies operate at a strategic level: they communicate what the organization requires and why it matters, while supporting documents translate that direction into more detailed, actionable requirements and processes. In a CISO governance program, policies provide the authoritative basis for consistent decision-making, accountability, compliance alignment, and risk management across business units. They should be approved by appropriate leadership, communicated to relevant personnel, periodically reviewed, and maintained as organizational objectives, regulations, threats, and technology evolve. NIST describes policy as high-level statements of management intent that guide information security activities; see NIST SP 800-12 Rev. 1. ISO/IEC 27001 likewise requires top management to establish an information security policy appropriate to the organization's purpose and supportive of its strategic direction; see ISO/IEC 27001.

QUESTION NO: 32

At what level of governance are individual projects monitored and managed?

A. Program

B. Milestone

C. Enterprise

D. Portfolio

ANSWER: D

Explanation:

Portfolio is correct because portfolio-level governance provides the organizational oversight used to monitor, prioritize, authorize, and manage individual projects in relation to strategic objectives. A portfolio is a collection of projects, programs, and other work that are managed together to achieve business goals; its governance processes enable leaders to assess performance, allocate resources, manage risk, and decide whether work should continue, change, or stop. This consolidated view is essential because a project can be successful in isolation while still failing to support enterprise priorities or compete appropriately for limited funding and personnel. Portfolio governance therefore connects project execution to strategy, ensuring that the organization invests in the most valuable and appropriately balanced set of initiatives. In the CCISO governance domain, this reflects the executive responsibility to establish decision-making structures, oversight, and performance measurement that align information-security and organizational initiatives with business direction. PMI similarly describes portfolio management as the centralized management of portfolios to achieve strategic objectives. See PMI's portfolio management overview and EC-Council's CCISO certification information.

QUESTION NO: 33

A security project gets a great deal of resistance across the organization. Which of the following represents the MOST likely reason for this situation?

A. The project is no longer required for securing the organization

B. The organization was not properly trained on security and privacy requirements

C. Software licenses were out of synchronization with other systems

D. The project was initiated without support from the affected business units

ANSWER: D

Explanation:

The project was initiated without support from the affected business units is the most likely reason for widespread organizational resistance. Security initiatives commonly alter business processes, introduce controls that affect daily work, require budget or staff time, and can create perceived operational friction. If affected business leaders and stakeholders were not engaged early, they may not understand the business rationale, have not contributed requirements, and may view the project as an externally imposed technical mandate rather than a shared risk-management effort. A CISO should build sponsorship and stakeholder commitment before and throughout the project by identifying impacted groups, communicating risk and business value in terms meaningful to them, incorporating their requirements, and establishing clear governance and accountability. This creates ownership and substantially improves adoption of security controls. NIST's guidance on organizational preparation for cybersecurity risk management emphasizes the importance of understanding organizational context, stakeholders, and risk priorities when establishing and operating cybersecurity governance. ISACA also identifies stakeholder engagement as a core component of effective governance, ensuring that enterprise objectives and stakeholder needs inform decisions. See NIST Cybersecurity Framework 2.0 and ISACA COBIT governance resources.

QUESTION NO: 34

You have been promoted to the CISO of a retail store. Which of the following compliance standards is the MOST important to the organization?

A. Payment Card Industry (PCI) Data Security Standard (DSS)

B. ISO 27002

C. NIST Cybersecurity Framework

D. The Federal Risk and Authorization Management Program (FedRAMP)

ANSWER: A

Explanation:

Payment Card Industry (PCI) Data Security Standard (DSS) is the most important compliance standard for a retail store because retailers commonly accept, process, store, or transmit payment-card information as part of normal sales operations. PCI DSS establishes a baseline of technical and operational security requirements intended to protect cardholder data and reduce payment-card fraud. Its applicability is determined by the organization's involvement with payment-card account data, not by its size or industry label; a retail business that accepts card payments therefore has a direct need to identify its cardholder-data environment, limit its scope, and maintain the controls required by the standard. As CISO, prioritizing PCI DSS supports protection of customer payment data, contractual compliance with acquiring banks and payment brands, and evidence of security control operation through the applicable validation process. The PCI Security Standards Council describes PCI DSS as a global baseline for protecting payment account data and specifies that entities storing, processing, or transmitting such data, or that can affect the security of the cardholder-data environment, are in scope. See the PCI Security Standards Council's PCI DSS overview and its merchant guidance.

QUESTION NO: 35

Smith, the project manager for a larger multi-location firm, is leading a software project team that has 18 members, 5 of which are assigned to testing. Due to recent recommendations by an organizational quality audit team, the project manager is convinced to add a quality professional to lead to test team at additional cost to the project.

The project manager is aware of the importance of communication for the success of the project and takes the step of introducing additional communication channels, making it more complex, in order to assure quality levels of the project. What will be the first project management document that Smith should change in order to accommodate additional communication channels?

A. WBS document

B. Scope statement

C. Change control document

D. Risk management plan

E. Communications management plan

ANSWER: E

Explanation:

Communications management plan is correct because it defines how project information will be created, collected, distributed, stored, monitored, and controlled. Introducing a quality professional and intentionally adding communication channels changes the project's communication environment: there may be new reporting relationships, recipients, communication methods, frequencies, escalation paths, formats, and responsibilities. The communications management plan is therefore the project management document that must be updated to ensure those new channels are purposeful, understood by stakeholders, and managed consistently across the multi-location team.

Effective communication planning is especially important when project complexity increases. The plan should identify the information needs of the new quality lead and testing function, specify who sends and receives quality-related status information, establish appropriate mechanisms for sharing test results and defects, and define feedback or escalation routes. Updating this plan provides a practical basis for coordinating the expanded team while preserving timely, reliable communication. Any required change-control actions should be processed according to the organization's governance approach, but the document directly affected by the need for additional communication channels is the communications

management plan. PMI identifies planning communications management as the process of developing an appropriate communications approach and plan for project activities. See PMI's PMBOK Guide and Standards and PMI guidance on effective project communications.

QUESTION NO: 36

The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is _____.

A. External Audit

B. Forensic experts

C. Internal Audit

D. Penetration testers

ANSWER: A

Explanation:

External Audit is correct because it provides an assessment performed by parties outside the organization being reviewed, supporting the independence and objectivity needed for a credible opinion on the design and operation of security controls. An external audit can assess controls across the environment against defined criteria, collect and evaluate evidence, and issue a formal report or attestation that stakeholders such as customers, regulators, boards, and business partners can rely on. Where a recognized standard is in scope, an appropriately accredited certification body can conduct the independent conformity assessment required for certification, such as ISO/IEC 27001 certification of an information security management system. This makes external audit the best fit for the question's combined requirements of comprehensive coverage, independence, and a certifiable perspective. ISO explains that certification is undertaken by independent certification bodies and is distinct from an organization merely self-declaring conformance: ISO Certification. ISACA also identifies independence and objectivity as foundational characteristics of effective audit assurance: ISACA: Assurance and Advisory Services in the Digital Age.

QUESTION NO: 37

Which of the following international standards can be BEST used to define a Risk Management process in an organization?

A. International Organization for Standardizations – 27005 (ISO-27005)

B. National Institute for Standards and Technology 800-50 (NIST 800-50)

C. Payment Card Industry Data Security Standards (PCI-DSS)

D. International Organization for Standardizations – 27004 (ISO-27004)

ANSWER: A

Explanation:

ISO/IEC 27005 is the best choice because it provides dedicated guidance for establishing, implementing, maintaining, and continually improving an information-security risk-management process. In a CISO context, risk management must be integrated with the organization's information security management system, business objectives, risk appetite, and treatment decisions. ISO/IEC 27005 supplies a structured lifecycle for defining context, identifying risks, analyzing and evaluating them, selecting and monitoring risk treatments, communicating risk information, and continually reviewing the process.

The standard is designed to support ISO/IEC 27001-based information security management. This makes it especially relevant to an organization seeking a repeatable, defensible process for managing risks to the confidentiality, integrity, and availability of information. It supports management decisions by ensuring that security controls and treatment plans are selected in response to documented and assessed risks rather than being implemented in isolation. ISO describes ISO/IEC 27005 as guidance for managing information-security risks, including how that activity supports an ISMS; see the ISO/IEC

27005 standard page. Additional context on the ISO/IEC 27000 family and its information-security management purpose is available from ISO's ISO/IEC 27001 overview.

QUESTION NO: 38

Which of the following items is discretionary?

A. Procedures

B. Policies

C. Guidelines

D. Standards

ANSWER: C

Explanation:

Guidelines are discretionary because they provide recommended, optional approaches for meeting organizational objectives or implementing controls. They help personnel make consistent and well-informed decisions, but they normally allow professional judgment and adaptation to the circumstances. For example, a security guideline may recommend preferred methods for creating secure configurations or handling sensitive information while permitting an alternative method when it achieves the same required outcome. This flexible role distinguishes guidelines within the policy framework: they translate organizational intent into useful advice without creating an absolute compliance obligation. In a mature information-security governance program, guidelines are still valuable because they communicate proven practices, reduce uncertainty, promote consistency, and support users in applying mandatory requirements effectively. Their discretionary nature also allows the organization to update recommendations as technology, threats, and operational conditions evolve, without necessarily changing its mandatory governance requirements. This treatment is consistent with NIST's description of guidance as material that provides recommendations and is typically nonmandatory, while organizational policy establishes direction for the information-security program. See NIST CSRC: Guidance and NIST SP 800-12 Rev. 1.

QUESTION NO: 39

Acceptable levels of information security risk tolerance in an organization should be determined by?

A. Corporate compliance committee

B. CEO and board of director

C. CISO with reference to the company goals

D. Corporate legal counsel

ANSWER: B

Explanation:

CEO and board of director is correct because risk tolerance is an expression of the organization's overall risk appetite: the amount and type of risk it is willing to accept while pursuing strategic and business objectives. Establishing that boundary is a governance responsibility requiring authority over organizational strategy, resources, priorities, and accountability to stakeholders. The board provides oversight and sets the organization's risk direction, while executive management operationalizes this direction throughout the enterprise. Information-security leaders, including the CISO, translate the approved tolerance into security policies, risk-assessment criteria, control requirements, monitoring thresholds, and risk-treatment decisions. They should advise decision-makers with technical and business context, but they should not independently define the level of enterprise risk the organization accepts. NIST describes risk appetite and risk tolerance as inputs from senior leaders and executives that guide risk management decisions across the organization. Similarly, ISACA's governance model emphasizes that governing bodies evaluate stakeholder needs and set direction, while management plans and executes in accordance with that direction. See NIST Special Publication 800-39 and ISACA COBIT resources.

QUESTION NO: 40

The Information Security Management program MUST protect:

A. all organizational assets

B. critical business processes and /or revenue streams

C. intellectual property released into the public domain

D. against distributed denial of service attacks

ANSWER: B

Explanation:

An Information Security Management program must protect **critical business processes and /or revenue streams** because information security is a business-enabling discipline, not merely a technical function. Its purpose is to manage information-related risk so the organization can continue delivering essential products and services, meeting obligations, making sound decisions, and sustaining the activities that generate value and revenue. This requires identifying the processes whose disruption, compromise, or manipulation would have an unacceptable business impact, then applying proportionate governance, risk treatment, controls, monitoring, and incident-response capabilities to preserve their confidentiality, integrity, and availability.

This business-process focus is consistent with the CCISO role, which emphasizes aligning information-security strategy and governance with organizational objectives and risk management. It also aligns with the NIST Cybersecurity Framework's Govern function, which establishes and monitors cybersecurity risk-management strategy, expectations, and policy in support of organizational mission and objectives. Protecting critical operations and the revenue they support gives security leadership a defensible basis for prioritizing investments and resilience requirements. See EC-Council's CCISO certification overview and the NIST Cybersecurity Framework.

QUESTION NO: 41

Which of the following is the MOST important benefit of an effective security governance process?

A. Senior management participation in the incident response process

B. Better vendor management

C. Reduction of security breaches

D. Reduction of liability and overall risk to the organization

ANSWER: D

Explanation:

Reduction of liability and overall risk to the organization is the most important benefit because security governance establishes the decision-making structure, accountability, policies, oversight, and risk-management processes needed to align security with business objectives. Effective governance ensures that leadership evaluates information-security risks in terms the organization can act on, assigns ownership for risk treatment, monitors whether controls remain effective, and makes informed decisions about risk acceptance. This reduces the likelihood and business impact of security-related events while also demonstrating due care and due diligence to regulators, customers, auditors, insurers, and other stakeholders.

Liability is reduced when the organization can show that it has a repeatable and accountable process for identifying risks, implementing proportionate safeguards, monitoring compliance, and improving controls. The resulting risk reduction is broader than any individual operational improvement: it supports legal and regulatory compliance, protects organizational assets and reputation, and helps management make defensible decisions regarding residual risk. NIST describes governance as a means of establishing and monitoring cybersecurity risk-management strategy and policies, while ISO/IEC 27001 emphasizes managing information-security risks through a structured management system. See NIST Cybersecurity Framework and ISO/IEC 27001.

QUESTION NO: 42

The main purpose of the SOC is:

A. An organization which provides Tier 1 support for technology issues and provides escalation when needed

B. A distributed organization which provides intelligence to governments and private sectors on cyber-criminal activities

C. The coordination of personnel, processes and technology to identify information security events and provide timely response and remediation

D. A device which consolidates event logs and provides real-time analysis of security alerts generated by applications and network hardware

ANSWER: C

Explanation:

The main purpose of a Security Operations Center (SOC) is the coordination of people, processes, and technology to continuously monitor for, identify, investigate, and respond to information-security events. A SOC centralizes operational security activities so that alerts are assessed in context, significant incidents are escalated and contained promptly, and remediation activities can be coordinated to reduce business impact. Its scope is therefore broader than a particular tool or a basic technology-support function: it encompasses ongoing detection and response capabilities, supported by defined procedures, skilled analysts, threat intelligence, and relevant security technologies. Effective SOC operations also create feedback that improves defensive controls, incident playbooks, and the organization's overall security posture. This purpose aligns with EC-Council's description of a SOC as a centralized function responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents. NIST similarly describes continuous monitoring as maintaining ongoing awareness of security posture to support risk-management decisions. See EC-Council: What Is a SOC? and NIST SP 800-137, Information Security Continuous Monitoring.

QUESTION NO: 43

What type of control is used when assigning information assurance requirements to an independent security group?

A. Detective

B. Organizational

C. Preemptive

D. Proactive

ANSWER: B

Explanation:

Organizational is correct because assigning information-assurance requirements to an independent security group establishes an organizational structure, defined responsibility, accountability, and appropriate separation of duties. The control is implemented through governance: management designates a security function with the authority and independence needed to oversee, assess, and report on assurance requirements without being unduly influenced by the operational teams whose activities it reviews. This supports objective risk decisions and reliable escalation to executive leadership.

In common security-control classifications, organizational (also called managerial or administrative) controls govern how the security program is directed and managed, including the assignment of security roles, responsibilities, authority, and oversight. NIST's security-control framework includes program-management controls for establishing an information security program and assigning program responsibilities, reflecting that these are governance-level measures rather than system mechanisms. See NIST SP 800-53 Rev. 5 and the related NIST SP 800-12 Rev. 1. An independent security group is therefore an organizational control that embeds assurance responsibilities into the enterprise's security governance model.

QUESTION NO: 44

Which of the following terms is used to describe the unexpected expansion of project deliverables?

A. Vendor management

B. Scope compression

C. Scope creep

D. Results management

ANSWER: C

Explanation:

Scope creep is the term for an uncontrolled or unapproved expansion of a project's scope, including its deliverables, requirements, features, or objectives after the scope baseline has been established. It often occurs when stakeholders request seemingly small additions that are accepted without a formal change-control assessment. Although individual changes may appear minor, their cumulative effect can materially increase the work required, consume budget and schedule reserves, introduce security or operational risk, and impair the project team's ability to meet agreed objectives.

For a CISO or senior security leader, controlling scope creep is particularly important in security programs because added integrations, compliance requirements, data sources, or technical capabilities can alter the risk profile and resource needs of an initiative. Effective project governance establishes a clear scope statement and baseline, requires proposed changes to be documented, assesses effects on cost, schedule, resources, risk, and benefits, and obtains appropriate authorization before incorporating changes. This preserves accountability and ensures that project commitments remain aligned with organizational priorities. PMI describes scope control and formal management of changes in its project-management standards and practice guidance. See PMI's guidance on scope creep and PMI's PMBOK Guide overview.

QUESTION NO: 45

Which of the following is an example of risk transference?

A. Writing specific language in an agreement that puts the burden back on the other party

B. Outsourcing the function on run 3rd party

C. Implementing changes to current operating procedure

D. Purchasing cyber insurance

ANSWER: D

Explanation:

Purchasing cyber insurance is an example of risk transference because the organization contractually shifts a defined portion of the potential financial loss from a cyber incident to an insurer. In exchange for a premium, the insurer agrees to cover eligible costs up to the policy's limits and subject to its terms, conditions, exclusions, and deductibles. Depending on the policy, those costs can include incident-response services, legal expenses, notification and credit-monitoring costs, business interruption losses, and certain liability claims. This treatment does not eliminate the underlying cyber threat, vulnerability, or management responsibility; rather, it changes who bears specified financial consequences if the event occurs. Risk transference is therefore particularly useful where residual loss exposure remains after appropriate security controls have been implemented and where the organization needs to limit the financial volatility of a material incident. NIST identifies risk transfer as a risk-response approach in which an organization shifts risk-associated consequences to another party, commonly through insurance or contractual mechanisms. The organization should still assess coverage scope, insurer requirements, exclusions, retention amounts, and whether the remaining residual risk fits its risk appetite. See NIST SP 800-30 Rev. 1 and the NIST Cybersecurity Framework.

QUESTION NO: 46

Scenario: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.

After determining the audit findings are accurate, which of the following is the MOST logical next activity?

A. Validate gaps with the Information Technology team

B. Begin initial gap remediation analyses

C. Review the security organization's charter

D. Create a briefing of the findings for executive management

ANSWER: B

Explanation:

Begin initial gap remediation analyses is the most logical next activity because the CISO has already established that the audit findings are accurate. The organization must now turn validated observations into an actionable remediation plan. Initial analysis determines the business and security impact of each gap, identifies affected systems, processes, owners, dependencies, resource needs, and estimates the effort required to correct the condition. It also enables risk-based prioritization: high-rated gaps may require expedited treatment or compensating controls, while medium- and low-rated items can be scheduled according to accepted risk, available resources, and strategic priorities.

This analysis produces the evidence needed for accountable decisions on remediation, risk acceptance, transfer, or avoidance, as well as for establishing milestones and tracking progress. A CISO should ensure that remediation work is tied to governance and risk-management processes rather than treating every audit observation as an isolated technical task. NIST describes plans of action and milestones as a mechanism for documenting remediation actions, required resources, and scheduled completion dates; this is the practical output that follows assessment findings. See NIST SP 800-53A and the EC-Council Certified CISO program.

QUESTION NO: 47

You are the CISO for an investment banking firm. The firm is using artificial intelligence (AI) to assist in approving clients for loans.

Which control is MOST important to protect AI products?

A. Hash datasets

B. Sanitize datasets

C. Delete datasets

D. Encrypt datasets

ANSWER: B

Explanation:

Sanitize datasets is the most important control because the quality, integrity, and provenance of data directly determine the trustworthiness of an AI model's decisions. In a loan-approval use case, training or inference data that contains maliciously crafted, manipulated, malformed, biased, or unauthorized records can cause the model to produce unreliable approval outcomes. Dataset sanitization includes validating data sources, enforcing schemas and allowable values, detecting anomalies and duplicates, screening for poisoning or adversarial content, removing unnecessary sensitive fields, and maintaining traceable data lineage. These measures reduce the risk that compromised data will influence model training, tuning, retrieval, or live decision inputs.

This is particularly important for a financial institution because AI-assisted lending decisions must be dependable, auditable, and governed throughout the data lifecycle. NIST's AI Risk Management Framework identifies data-related risks and emphasizes practices that improve the validity, reliability, safety, security, and accountability of AI systems. Similarly, OWASP identifies training-data poisoning as a significant machine-learning security concern, reinforcing the need to validate

and sanitize the data used by AI systems. Effective sanitization should be implemented as a repeatable pipeline control, supported by documented provenance, monitoring, and review of high-risk data changes. See the NIST AI Risk Management Framework and the OWASP Machine Learning Security Top 10.

QUESTION NO: 48

A consultant is hired to do physical penetration testing at a large financial company. In the first day of his

assessment, the consultant goes to the companyâ€™s building dressed like an electrician and waits in the lobby for

an employee to pass through the main access gate, then the consultant follows the employee behind to get into

the restricted area. Which type of attack did the consultant perform?

A. Shoulder surfing

B. Tailgating

C. Social engineering

D. Mantrap

ANSWER: B

Explanation:

Tailgating is the correct answer because the consultant gained entry to a restricted physical area by closely following an authorized employee through an access-controlled gate without independently authenticating or presenting authorization. This physical-security attack exploits normal human behavior and the practical difficulty of ensuring that every person passing through an entrance is individually validated. The consultant's electrician disguise may make the attempt more believable, but the defining action is entering immediately behind a person who has already been granted access. Physical penetration tests commonly assess whether an organization's access-control procedures, employee awareness, visitor controls, and entry design can prevent this form of unauthorized piggyback entry. Effective protections include security awareness training, staff challenging unknown persons, turnstiles or optical barriers, badge-enforced access procedures, and access-control vestibules. NIST identifies tailgating as a physical access threat that organizations should address through physical access controls and monitoring. Guidance on physical access control principles is available from NIST SP 800-53, Physical and Environmental Protection controls. Additional practical physical-security guidance, including access-control considerations, is available from CISA Physical Security.

QUESTION NO: 49

Which of the following is the MOST logical method of deploying security controls within an organization?

A. Obtain funding for all desired controls and then create project plans for implementation

B. Apply the simpler controls as quickly as possible and use a risk-based approach for the more difficult and costly controls

C. Apply the least costly controls to demonstrate positive program activity

D. Obtain business unit buy-in through close communication and coordination

ANSWER: B

Explanation:

“Apply the simpler controls as quickly as possible and use a risk-based approach for the more difficult and costly controls” is the most logical deployment method because it combines prompt risk reduction with disciplined prioritization. Organizations can often implement straightforward, high-value safeguards quickly, reducing exposure while broader control initiatives are planned, funded, integrated, and governed. This creates early security benefits without treating control deployment as an all-or-nothing exercise.

For controls that require substantial cost, architectural change, operational disruption, or cross-functional ownership, a risk-based approach ensures that implementation order reflects the organization's risk appetite and the relative impact and likelihood of threats. Risk information helps leadership direct limited resources toward the systems, processes, and scenarios where additional controls will provide the greatest reduction in risk. This approach also supports accountable decision-making, realistic implementation roadmaps, and ongoing adjustment as threats, business priorities, and technology environments change. NIST describes risk management as an organization-wide process for framing, assessing, responding to, and monitoring risk, while its control guidance supports selecting and tailoring safeguards according to mission and risk context. See NIST SP 800-39 and NIST SP 800-53 Rev. 5.

QUESTION NO: 50

When managing the critical path of an IT security project, which of the following is MOST important?

A. Knowing who all the stakeholders are.

B. Knowing the people on the data center team.

C. Knowing the threats to the organization.

D. Knowing the milestones and timelines of deliverables.

ANSWER: D

Explanation:

Knowing the milestones and timelines of deliverables is most important because the critical path is the sequence of dependent activities that establishes the earliest possible completion date for the project. Each activity on that path has no scheduling flexibility: a delay to a critical-path deliverable directly delays the project's planned completion unless corrective action is taken. A CISO managing an IT security initiative must therefore have clear, current visibility into scheduled milestones, delivery dates, task dependencies, and progress against the approved baseline. This visibility supports timely escalation and decisions such as reallocating resources, resequencing feasible work, or addressing an emerging blocker before it affects a key security outcome or compliance commitment.

Milestones provide measurable control points for confirming that essential deliverables—such as design approval, control implementation, testing, and authorization—are achieved when required. Timelines establish the schedule against which performance and slippage can be assessed. Together, they enable disciplined monitoring of the project activities that determine the end date, which is the central purpose of critical-path management. The Project Management Institute describes critical-path analysis as a scheduling method used to identify the chain of activities that determines project duration; see PMI's critical-path-method overview. EC-Council's CCISO program also includes governance and project-management responsibilities relevant to directing security initiatives: CCISO certification information.

QUESTION NO: 51

How often should an environment be monitored for cyber threats, risks, and exposures?

A. Weekly

B. Daily

C. Monthly

D. Quarterly

E. Continuously

ANSWER: E

Explanation:

Continuously is correct because cyber threats, vulnerabilities, exposed services, and configuration changes can arise at any time. Effective security monitoring is therefore an ongoing operational capability, not a task deferred to a daily, weekly,

monthly, or quarterly schedule. Continuous monitoring enables the organization to collect and analyze security-relevant telemetry from endpoints, networks, identities, cloud workloads, applications, and external attack-surface sources as events occur. This supports rapid detection, triage, containment, and response before a developing exposure becomes a material incident.

This approach also gives leadership current risk information for governance and decision-making. In a CCISO context, continuous monitoring helps ensure that security controls remain effective as the business, technology environment, threat landscape, and regulatory obligations evolve. NIST defines information security continuous monitoring as maintaining ongoing awareness of information-security, vulnerability, and threat status to support risk-management decisions; see NIST SP 800-137. CISA likewise describes continuous diagnostics and mitigation as an approach for improving visibility into cybersecurity risks and prioritizing mitigation activities; see CISA Continuous Diagnostics and Mitigation.

QUESTION NO: 52

One of the MAIN goals of a Business Continuity Plan is to_____.

A. Ensure all infrastructure and applications are available in the event of a disaster

B. Assign responsibilities to the technical teams responsible for the recovery of all data

C. Provide step by step plans to recover business processes in the event of a disaster

D. Allow all technical first-responders to understand their roles in the event of a disaster.

ANSWER: C

Explanation:

A Business Continuity Plan's central purpose is to enable the organization to continue and restore its prioritized business processes to an acceptable level following a disruption. Therefore, "Provide step by step plans to recover business processes in the event of a disaster" correctly captures a main BCP goal: translating business-impact priorities, recovery objectives, dependencies, resources, communications, and assigned actions into documented procedures that personnel can execute during an incident. The plan is business-focused, meaning it addresses how critical products and services will be maintained or resumed, including the sequence for recovering the processes that support them. Effective continuity planning also requires that these procedures be tested, maintained, and aligned with organizational recovery time and recovery point objectives. NIST describes contingency planning as establishing procedures for system recovery and reconstitution that support the continuity of mission and business processes. Similarly, ISO's business continuity guidance emphasizes preparing for, responding to, and recovering from disruptive incidents so that delivery of products and services can continue at an acceptable predefined capacity. These principles make documented, actionable recovery plans for business processes a core BCP outcome. See NIST SP 800-34 Rev. 1 and ISO 22301:2019.

QUESTION NO: 53

Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

A. Human Resources and Budget

B. Audit and Legal

C. Budget and Compliance

D. Legal and Human Resources

ANSWER: B

Explanation:

Audit and Legal is correct because formal information-security governance reporting must provide both independent assurance and appropriate handling of legal, regulatory, contractual, and evidentiary obligations. The audit function supplies

objective assessment of whether security controls, risk-management activities, and governance processes are designed appropriately and operating effectively. This assurance gives executive management and the governing body credible information on the organization's security posture and on whether remediation is required. The legal function ensures that reporting and escalation account for applicable laws, regulations, contractual duties, privacy requirements, records preservation, and potential litigation or breach-notification considerations. Including these functions in the reporting structure helps ensure that security decisions are defensible, appropriately governed, and communicated to the right authority level. This aligns with the NIST Cybersecurity Framework governance outcome that organizational roles, responsibilities, and authorities are established and communicated, including for oversight and risk decisions. It also reflects ISACA's governance emphasis on stakeholder needs, oversight, and assurance as core elements of enterprise governance. See the NIST Cybersecurity Framework and ISACA's COBIT governance resources.

QUESTION NO: 54

Which is the BEST solution to monitor, measure, and report changes to critical data in a system?

A. SNMP traps

B. Syslog

C. File integrity monitoring

D. Application logs

ANSWER: C

Explanation:

File integrity monitoring is the best solution because it is specifically designed to establish a trusted baseline for critical files, directories, configurations, and other designated data objects, then continuously or periodically detect and report unauthorized or unexpected modifications. A file integrity monitoring implementation uses cryptographic hashes and associated metadata, such as permissions, ownership, size, and timestamps, to identify changes reliably. It can generate alerts and audit evidence showing what changed, when it changed, and, where integrated with identity and logging systems, the account or process associated with the change. This makes it directly useful for protecting sensitive system data and demonstrating that integrity controls are operating effectively.

For a CISO, file integrity monitoring supports security monitoring, incident investigation, change-control validation, and compliance obligations. PCI DSS, for example, requires change-detection mechanisms to alert personnel to unauthorized modification of critical system files, configuration files, or content files, and identifies file-integrity monitoring tools as an example. NIST also treats integrity monitoring as an important capability for detecting unauthorized changes and supporting auditability. Effective deployment focuses on defining critical assets, maintaining approved baselines, tuning approved-change workflows, protecting the monitoring system itself, and ensuring alerts are reviewed and retained. See PCI DSS Document Library and NIST SP 800-53 Rev. 5.

QUESTION NO: 55

Ciphertext is encrypted with the same key used by the recipient to decrypt it. What encryption method is being used?

A. Private key

B. Key pairing

C. Shared key

D. Discrete key

ANSWER: C

Explanation:

Shared key is correct because it describes symmetric-key encryption: the same secret cryptographic key is used to transform plaintext into ciphertext and to recover the plaintext from that ciphertext. Both communicating parties must therefore have access to the identical key before protected data can be exchanged. This model is commonly used for efficient protection of substantial volumes of information, since symmetric algorithms are generally designed for high-performance bulk encryption.

From a governance and CISO perspective, the critical control issue is the lifecycle of that shared secret. The key must be generated with sufficient strength, distributed only through a protected mechanism, stored securely, available only to authorized entities, rotated as required, and destroyed when no longer needed. If an unauthorized party obtains the shared key, that party can decrypt data protected with it and potentially create valid ciphertext using the same key. Consequently, secure key establishment and centralized key-management controls are essential parts of operating a shared-key cryptosystem.

NIST defines a symmetric key as a cryptographic key used with a symmetric-key cryptographic algorithm, and its key-management guidance addresses the protection and lifecycle management of such keys. See the NIST definition of a symmetric key and NIST SP 800-57 Part 1 on key management.

QUESTION NO: 56

Which of the following is the MOST effective method for discovering common technical vulnerabilities within the IT environment?

A. Reviewing system administrator logs

B. Auditing configuration templates

C. Checking vendor product releases

D. Performing system scans

ANSWER: D

Explanation:

Performing system scans is the most effective method for discovering common technical vulnerabilities across an IT environment because vulnerability scanners systematically evaluate in-scope hosts, operating systems, services, applications, and configurations against extensive vulnerability intelligence and known weakness checks. A properly governed scanning program can identify missing security patches, exposed or obsolete services, insecure configurations, weak encryption protocols, default credentials, and software versions associated with publicly disclosed vulnerabilities. It also produces repeatable, measurable results that security teams can prioritize by severity, asset criticality, exploitability, and exposure, then track through remediation and verification scans.

For effective coverage, scans should be performed regularly and after material environmental changes, using authenticated scanning where feasible. Authenticated scans provide deeper visibility into installed software, patch levels, and local configuration settings than unauthenticated network-only checks. Scanning results should be validated where appropriate, correlated with asset inventory and threat intelligence, and incorporated into the organization's vulnerability-management lifecycle. NIST describes vulnerability scanning as a core technical assessment activity for identifying vulnerabilities and configuration weaknesses, while CISA provides guidance and resources for continuous vulnerability identification and remediation. See NIST SP 800-115 and CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 57

An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in sever revenue disruptions.

Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

A. Audit and Compliance

B. The CFO

C. The CISO

D. The business owner

ANSWER: D

Explanation:

The business owner is most likely responsible for accepting this risk temporarily because that role owns the affected manufacturing process, its business objectives, and the resulting operational and financial consequences. Risk acceptance is a business decision: it requires an authorized individual to determine that the residual risk of temporarily not blocking the traffic is tolerable when balanced against the unacceptable production disruption and revenue loss that immediate implementation would cause. The business owner should make that decision with documented input from the CISO, security team, risk management, and relevant control owners. This documentation should clearly define the risk, the rationale for accepting it, the interim safeguards or compensating controls, the responsible parties, an expiration or review date, and the plan for implementing the required mitigating controls. The CISO can advise on the threat exposure and proposed safeguards, but accountability for accepting a risk that directly affects business operations rests with the owner who has authority over that business process. This aligns with NIST guidance that organizational risk decisions are made by designated authorizing officials or senior leaders with the appropriate mission/business authority. See NIST SP 800-37 Rev. 2 and NIST Cybersecurity Framework 2.0.

QUESTION NO: 58

Who should be involved in the development of an internal campaign to address email phishing?

A. Business unit leaders, CIO, CEO

B. Business Unit Leaders, CISO, CIO and CEO

C. All employees

D. CFO, CEO, CIO

ANSWER: B

Explanation:

Business Unit Leaders, CISO, CIO and CEO should be involved in developing an internal phishing-awareness campaign because effective security awareness requires both security expertise and organization-wide executive sponsorship. The CISO defines the threat-focused objectives, required behaviors, measurement approach, and alignment with the organization's security program. The CIO helps ensure that the campaign reflects the actual email, identity, reporting, and technical-control environment used by personnel. Business unit leaders contribute operational context, identify role-specific phishing risks, and help make the campaign relevant and actionable within their teams. CEO participation establishes visible tone from the top, reinforces that phishing resistance is a business priority rather than merely an IT activity, and encourages broad organizational support. This combined leadership group can set policy expectations, allocate resources, approve communications, and ensure that training, simulations, reporting procedures, and metrics are coordinated across the enterprise. EC-Council's CCISO program emphasizes executive-level governance and alignment of information-security initiatives with business objectives. NIST similarly identifies awareness and training as an organization-wide program that needs management support and defined responsibilities. See EC-Council CCISO and NIST SP 800-50.

QUESTION NO: 59

Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

A. Security managers

B. Security analysts

C. Security technicians

D. Security administrators

ANSWER: A

Explanation:

Security managers are accountable for the day-to-day operation of the information security program. This role translates the organization's security strategy, policies, risk decisions, and regulatory obligations into managed operational activities. In practice, security managers coordinate security personnel and services; oversee implementation and maintenance of security controls; monitor operational performance; manage security-related projects, budgets, and priorities; and provide status, risk, and incident information to senior leadership. They also ensure that security processes operate consistently across the organization and that issues requiring escalation receive appropriate management attention.

This accountability is broader than performing individual technical tasks. It requires management ownership of the continuing security program, including assigning work, maintaining procedures, tracking control effectiveness, and aligning operational security efforts with organizational objectives. NIST describes the senior information-security role as having responsibility for the organization's information-security program and its implementation, while operational management is necessary to ensure that program requirements are carried out in practice. This is consistent with the management focus expected of information-security leadership under CCISO domains. See NIST SP 800-100: Information Security Handbook and NIST Cybersecurity Framework resources.

QUESTION NO: 60

When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

A. Vendor uses their own laptop and logs in using two-factor authentication with their own unique credentials

B. Vendor uses a company-supplied laptop and logs in using two-factor authentication with the same admin credentials your security team uses

C. Vendor uses a company-supplied laptop and logs in using two-factor authentication with their own unique credentials

D. Vendor uses their own laptop and logs in with the same admin credentials your security team uses

ANSWER: C

Explanation:

Vendor uses a company-supplied laptop and logs in using two-factor authentication with their own unique credentials is the best choice because it combines control of the access endpoint with strong, individually attributable authentication. A company-managed laptop can be configured to the organization's security baseline, including supported endpoint protection, encryption, patching, device-management controls, logging, and restrictions on administrative tools or data transfer. This materially improves the organization's ability to monitor and manage the device from which privileged remote access is performed.

Requiring the vendor to use unique credentials establishes clear accountability for each action taken during support activity. It enables access to be limited to the specific systems, roles, time periods, and privileges necessary for the engagement, while allowing security teams to revoke that vendor's access immediately when the work ends or the relationship changes. Two-factor authentication adds a second proof of identity and reduces the likelihood that a stolen password alone can be used to access critical security infrastructure. These controls support least privilege, traceability, secure remote administration, and effective incident investigation. NIST's guidance on authenticator assurance and multifactor authentication is available in NIST SP 800-63B; endpoint and telework-device security considerations are covered by NIST SP 800-46 Rev. 2.

QUESTION NO: 61

You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

A. Risk Mitigation

B. Risk Acceptance

C. Risk Avoidance

D. Risk Transfer

ANSWER: D

Explanation:

Purchasing an insurance policy is **Risk Transfer**. In a risk-transfer arrangement, the organization does not eliminate the underlying event or necessarily reduce its likelihood; instead, it contractually shifts all or part of the financial consequences of a covered loss to another party. The insurer agrees, subject to policy terms, limits, exclusions, deductibles, and conditions, to compensate the insured organization for specified losses in return for a premium. This lets management manage potentially significant financial exposure while retaining responsibility for operating appropriate controls and meeting any policy obligations.

For a CISO, insurance is commonly considered within the broader risk-treatment plan for exposures such as cyber incidents, business interruption, liability, or property damage. Sound governance requires evaluating the residual risk that remains after insurance, because coverage may be limited and may not address reputational damage, operational disruption, regulatory duties, or every type of loss. The risk register should document the transfer decision, insurer and policy details, coverage limits, and any retained risk. NIST describes risk transfer as shifting responsibility or liability for risk to another party, including through insurance, while ISO/IEC 27005 recognizes risk sharing as a risk-treatment approach. See NIST's definition of risk transfer and ISO/IEC 27005 guidance on information-security risk management.

QUESTION NO: 62

At which point should the identity access management team be notified of the termination of an employee?

A. Immediately so the employee account(s) can be disabled

B. During the monthly review cycle

C. At the end of the day once the employee is off site

D. Before an audit

ANSWER: A

Explanation:

The identity access management team should be notified immediately so the employee account(s) can be disabled. Termination is a high-risk identity-lifecycle event because an individual may otherwise retain access to enterprise systems, data, facilities, cloud services, and privileged resources after their employment relationship ends. Prompt notification enables the organization to execute its offboarding procedure in coordination with Human Resources, the employee's manager, physical security, and IT. The procedure should revoke or disable accounts at the appropriate effective time, terminate active sessions and remote access where feasible, recover organizational devices and credentials, and preserve records needed for legal, audit, or investigation purposes. Immediate notification does not necessarily mean access is removed before the authorized termination time; rather, it ensures IAM has the required notice to perform deprovisioning without delay at that time. Effective joiner-mover-leaver controls rely on a timely, authoritative HR event and automation or documented workflow to prevent orphaned accounts and excessive access. NIST describes account management controls that require organizations to disable accounts within defined organizational time periods when users are terminated or no longer need access. See NIST SP 800-53 Rev. 5, Account Management (AC-2) and CISA Insider Threat Mitigation Resources.

QUESTION NO: 63

Which of the following compliance standards is the MOST common among retail businesses?

A. Payment Card Industry (PCI) Data Security Standard (DSS)

B. NIST Cybersecurity Framework

C. Federal Risk and Authorization Management Program (FedRAMP)

D. ISO 27002

ANSWER: A

Explanation:

Payment Card Industry (PCI) Data Security Standard (DSS) is the most common compliance standard among retail businesses because retailers routinely accept payment cards and therefore commonly store, process, or transmit cardholder data, or can affect the security of the cardholder-data environment. PCI DSS establishes a baseline of technical and operational safeguards for protecting payment account data, including network security controls, secure configuration, vulnerability management, access control, logging and monitoring, security testing, and security-policy governance. Compliance is driven by the payment-card ecosystem: merchants' acquiring banks and payment brands require validation at a level appropriate to the merchant's transaction volume and risk profile. As a result, PCI DSS is a practical and broadly applicable security obligation across physical stores, e-commerce merchants, and omnichannel retail operations. Its relevance is not limited to organizations that directly retain full card numbers; systems that support payment processing or can impact the security of those systems may also fall within scope. Retail leadership should therefore treat PCI DSS as an ongoing risk-management and assurance program, maintaining scope awareness, evidence of control operation, and remediation processes rather than viewing it as a one-time certification exercise. The PCI Security Standards Council describes PCI DSS as the global standard intended to protect payment account data, and its official materials provide the current requirements and assessment resources. See the PCI Security Standards Council PCI DSS overview and the PCI SSC document library.

QUESTION NO: 64

A security project is over a year behind schedule and over budget. Which of the following is MOST important to review and verify?

A. Constraints

B. Scope

C. Technologies

D. Milestones

ANSWER: B

Explanation:

Scope is the most important item to review and verify because it establishes the approved boundaries of the security project: the required deliverables, capabilities, exclusions, and acceptance criteria. A project that is substantially late and over budget may be suffering from unapproved or poorly controlled additions to requirements, incomplete definition of what must be delivered, or a mismatch between current work and the originally authorized business objectives. Reviewing the scope baseline and associated change records enables the project sponsor and security leadership to determine whether the work remains justified, whether changes were formally approved, and what work must be prioritized, deferred, or removed to regain control. This review also provides the factual basis for revising the schedule, cost estimate, resource plan, and stakeholder commitments. Formal scope management is a core project-control discipline because approved scope is the reference point used to assess change and measure delivery. PMI describes scope management as the processes used to ensure that a project includes all—and only—the work required for successful completion; see PMI's project scope management guidance. The CCISO role likewise emphasizes governance and management oversight of security programs and initiatives; see the EC-Council CCISO certification overview.

QUESTION NO: 65

What type of attack requires the least amount of technical equipment and has the highest success rate?

A. War driving

B. Operating system attacks

C. Social engineering

D. Shrink wrap attack

ANSWER: C

Explanation:

Social engineering is correct because it targets people rather than relying primarily on a technical vulnerability in a device, network, or application. An attacker can conduct social engineering with minimal equipment: a phone call, email account, messaging application, convincing pretext, or even an in-person conversation may be sufficient. The method works by influencing a person to disclose information, approve an action, open a malicious attachment, reset a credential, or permit physical access. Its effectiveness stems from exploiting normal human behaviors such as trust, helpfulness, urgency, fear, authority, and curiosity.

For a CISO, this highlights that security controls cannot be limited to technology. A mature security program should combine ongoing, role-appropriate awareness training with phishing simulations, clear reporting channels, identity-verification procedures for sensitive requests, and technical safeguards such as multifactor authentication. These layers reduce the likelihood that a successful manipulation attempt becomes unauthorized access or a material incident. The CISA phishing guidance describes phishing as social engineering intended to steal information or deploy malware. The NIST Cybersecurity Framework 2.0 also supports governance and risk-management practices that address human-focused threats alongside technical risks.

QUESTION NO: 66

Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

A. Vulnerability

B. Threat

C. Exploitation

D. Attack vector

ANSWER: A

Explanation:

Vulnerability is correct because it is the established information-security term for a weakness in an asset, system, process, control, or group of assets that a threat can exploit. An asset can include information, software, hardware, services, personnel, facilities, or supporting processes. A vulnerability may arise from a technical flaw, such as unpatched software or insecure configuration, or from an organizational or procedural weakness, such as inadequate access-review processes. Its security significance is that it creates an exposure that can be acted upon when a relevant threat exists, potentially causing harm to confidentiality, integrity, availability, or other business objectives. ISO/IEC 27005 defines vulnerability as a weakness of an asset or control that can be exploited by one or more threats, which directly matches the wording in the question. NIST likewise treats vulnerabilities as weaknesses that can be exploited by threat sources and considers them in risk assessment alongside threat sources, likelihood, and impact. Identifying vulnerabilities is therefore a core activity in risk management: organizations evaluate the affected assets, assess exposure and potential consequences, and select appropriate controls or remediation measures. See ISO/IEC 27005:2022—Information security risk management and NIST CSRC glossary: Vulnerability.

QUESTION NO: 67

What standard would you use to help determine key performance indicators?

A. ITIL

B. FIPS140-2

C. NI5TSP800-53

D. NIST SP 800-55

ANSWER: D

Explanation:

NIST SP 800-55 is the appropriate publication because it is specifically a guide for developing and implementing information-security performance measurement programs. It provides a structured method for translating security goals and requirements into measurable indicators, including identifying what should be measured, defining measures that produce meaningful data, collecting that data, analyzing results, and reporting them to decision-makers. This is precisely the work involved in determining useful key performance indicators: KPIs must be tied to organizational objectives, be consistently measurable, and support management decisions about the effectiveness and efficiency of the security program.

The guide distinguishes measurement development from merely selecting technical controls. It emphasizes establishing measures that demonstrate whether security activities and controls are achieving intended results, such as compliance, implementation progress, operational effectiveness, or risk-related outcomes. A CISO can use this approach to ensure that KPIs are relevant to governance and are actionable rather than simply reporting raw operational statistics. NIST identifies SP 800-55 Rev. 1 as its *Performance Measurement Guide for Information Security*; its publication record is available through the NIST Computer Security Resource Center, and the complete guide is available as a NIST PDF publication.

QUESTION NO: 68

Which business stakeholder is accountable for the integrity of a new information system?

A. Compliance Officer

B. CISO

C. Project manager

D. Board of directors

ANSWER: B

Explanation:

CISO is correct because the Chief Information Security Officer is the executive stakeholder responsible for directing and governing the organization's information-security program, including protection of information-system integrity. Integrity means safeguarding systems and data from unauthorized or improper modification, deletion, or destruction, and ensuring that system processing remains accurate, complete, and trustworthy. For a new information system, the CISO establishes or approves the security requirements, architecture expectations, risk-management activities, control baseline, assurance activities, and security authorization inputs needed to protect that integrity throughout the system life cycle.

This accountability is exercised through governance and delegation: technical teams may implement controls, and project personnel may coordinate delivery, but the CISO provides security leadership and ensures that integrity risks are identified, treated, monitored, and communicated to senior leadership. NIST describes the CISO as a key senior security official responsible for developing, implementing, and maintaining an organization-wide information-security program. The integrity objective and corresponding controls are central to that program, particularly during system development and acquisition. See NIST SP 800-100, Information Security Handbook and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

QUESTION NO: 69

A business unit within your organization intends to deploy a new technology in violation of information security standards. As a security leader, what would be your BEST course of action?

A. Enforce the existing security standards and block deployment of the new system

B. Assure that the standards align to the new system

C. Create an exception for 6 months, then have the business request exception extensions

D. Perform a risk analysis and provide the results to the business for a decision

ANSWER: D

Explanation:

Perform a risk analysis and provide the results to the business for a decision is the best course because it applies risk-based governance while maintaining the appropriate division of accountability between the security function and business management. The security leader should identify the technology's departure from approved standards, assess the likelihood and impact of resulting threats, evaluate legal, regulatory, operational, and financial consequences, and document feasible treatment choices such as compensating controls, redesign, deferral, or a time-bound exception. The analysis should be communicated in business terms so the accountable business owner can make an informed decision and formally accept any residual risk at the proper authority level.

This approach supports security as a business enabler rather than treating standards as an end in themselves. Standards establish the organization's expected security baseline, but a proposed deviation requires transparent evaluation through the established risk-management and exception-governance process. A documented decision also creates an auditable record of the risk, ownership, approval, and any required remediation milestones. NIST's Risk Management Framework describes risk assessment and authorization as core activities for making informed organizational decisions, while NIST guidance on risk assessment explains the need to evaluate threats, vulnerabilities, likelihood, and impact. See NIST Risk Management Framework and NIST SP 800-30 Rev. 1.

QUESTION NO: 70

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls

B. A compliance test of program library controls

C. A compliance test of the program compiler controls

D. A substantive test of the program compiler controls

ANSWER: B

Explanation:

A compliance test of program library controls is correct because the auditor is testing whether established library-management procedures operate as intended. Program library controls maintain the integrity and traceability of program components, including source code and the corresponding compiled object or executable version. Selecting a sample and comparing the source and object versions provides evidence that the organization's controlled promotion, compilation, versioning, and retention process has been followed. This is a compliance test because it evaluates adherence to a required control procedure, rather than directly measuring the business-processing accuracy of application output or transaction balances. Effective configuration and change-management practices require organizations to identify configuration items, control changes, and maintain records that establish the current approved version. Those practices support the expectation that production object code can be traced to its authorized source version. NIST's configuration-management control guidance describes the need to establish and maintain configuration baselines and control changes to system components; source and executable artifacts are key components of such baselines. See NIST SP 800-53 CM-3, Configuration Change Control and NIST SP 800-128, Guide for Security-Focused Configuration Management.

QUESTION NO: 71

What organizational structure combines the functional and project structures to create a hybrid of the two?

A. Traditional

B. Composite

C. Project

D. Matrix

ANSWER: D

Explanation:

The **Matrix** organizational structure is the hybrid model that combines functional departments with project-based management. In a matrix environment, employees retain alignment with their functional area, such as information security, finance, engineering, or operations, while also being assigned to one or more projects. This arrangement enables an organization to preserve deep functional expertise and consistent professional standards while directing resources across initiatives that require cross-functional coordination.

For a CISO or security leader, this model can be particularly useful when security programs involve multiple business units and specialized capabilities. A security architect, for example, may report through the security function for professional development and technical governance, yet work under a project manager's coordination for an enterprise cloud migration or regulatory compliance project. Matrix structures therefore rely on clearly defined authority, responsibilities, escalation paths, and resource-allocation processes because team members commonly have both functional and project-management reporting relationships. The Project Management Institute describes matrix organizations as structures in which functional managers and project managers share authority, with the balance varying among weak, balanced, and strong matrix forms. See the Project Management Institute's discussion of matrix organizational structures and PMI's PMBOK Guide overview.

QUESTION NO: 72

Devising controls for information security is a balance between?

A. Governance and compliance

B. Auditing and security

C. Budget and risk tolerance

D. Threats and vulnerabilities

ANSWER: C

Explanation:

Budget and risk tolerance is correct because information-security controls must be selected and implemented in a way that reduces risk to a level the organization has formally decided it can accept, while remaining feasible within available financial and operational resources. A control is not valuable merely because it is technically strong; its cost, implementation effort, ongoing maintenance, effect on business operations, and expected risk reduction must all be considered. Senior leadership establishes risk appetite and tolerance, which provide the decision boundaries for determining whether additional control investment is justified. Security leaders then prioritize safeguards toward the most significant risks and make defensible trade-offs where resources are finite. This is a core governance responsibility for a CISO: aligning security expenditure with business objectives and the organization's accepted residual risk. NIST describes risk management as integrating risk considerations into organizational decision-making and resource allocation, while its control framework supports tailoring safeguards to organizational needs and risk context. See NIST SP 800-39, Managing Information Security Risk and NIST SP 800-53, Security and Privacy Controls.

QUESTION NO: 73

What are the three stages of an identity and access management system?

A. Authentication, Authorize, Validation

B. Provision, Administration, Enforcement

C. Administration, Validation, Protect

D. Provision, Administration, Authentication

ANSWER: B

Explanation:

Provision, Administration, Enforcement is the correct three-stage IAM model. Provisioning establishes the identity and its initial access entitlements when a person, service, or device enters the environment. This includes creating accounts, assigning identifiers, associating the subject with roles or groups, and granting access based on approved business requirements. Administration is the ongoing governance of those identities and permissions throughout their lifecycle: IAM administrators and system owners maintain attributes, process access requests and changes, perform access reviews, and remove or adjust privileges as job duties change. Enforcement is the operational point at which IAM controls apply policy to an access attempt. It verifies the requesting identity through authentication and evaluates whether that identity is permitted to use the requested resource, typically using authorization rules, roles, attributes, and contextual conditions. Together, these stages ensure that access is established appropriately, governed over time, and consistently applied at the time of use. This lifecycle-oriented model supports the least-privilege and accountability objectives expected of an enterprise IAM program. NIST's Digital Identity Guidelines describe the identity proofing, authentication, and federation concepts that underpin enforcement, while NIST's SP 800-63-3 provides the core digital-identity framework used to design and govern these controls.

QUESTION NO: 74

What two methods are used to assess risk impact?

A. Quantitative and qualitative

B. Qualitative and percent of loss realized

C. Subjective and Objective

D. Cost and annual rate of expectance

ANSWER: A

Explanation:

Quantitative and qualitative is correct because these are the two standard approaches used in information-security risk assessment to evaluate impact. A qualitative assessment characterizes impact through descriptive ratings—such as low, medium, and high—using defined criteria for outcomes including operational disruption, legal exposure, reputational harm, and loss of confidentiality, integrity, or availability. This approach is especially useful where reliable financial data is limited or decisions must account for business context and stakeholder judgment.

A quantitative assessment expresses impact in measurable numerical or monetary terms. It can estimate values such as the financial loss from a security event, recovery costs, lost revenue, and expected annual loss. These estimates support cost-benefit decisions about safeguards, risk treatment, and security investment. In practice, a CISO may use either method or a hybrid approach, but the foundational methods for assessing risk impact remain qualitative and quantitative. NIST describes risk assessments as using qualitative, quantitative, or semi-quantitative techniques, and ISO guidance recognizes qualitative and quantitative analysis methods for evaluating risk consequences and likelihood. See NIST SP 800-30 Rev. 1 and ISO 31010 risk-assessment techniques.

QUESTION NO: 75

A system is designed to dynamically block offending Internet IP-addresses from requesting services from a secure website.

This type of control is considered_____.

A. Preventive detection control

B. Corrective security control

C. Zero-day attack mitigation

D. Dynamic blocking control

ANSWER: B

Explanation:

Corrective security control is correct because the system takes an active response after it identifies offending behavior from an Internet address. Dynamic IP blocking contains the identified threat by changing the website's access posture and preventing the same source from continuing its harmful or unauthorized activity. In control-classification terminology used in security governance, corrective controls act in response to a detected security event to limit its effects, remove or isolate the cause, and return the environment to an acceptable security state. An automated web-application firewall rule, intrusion-prevention action, or threat-intelligence-driven deny-list can implement this response without waiting for manual administrator intervention.

The relevant characteristic is not merely that network access is denied; it is that the denial is dynamically applied as a remediation and containment action against an already observed offending source. This supports incident response by reducing ongoing exposure, protecting the availability and integrity of the website, and creating time for investigation and longer-term remediation. NIST's incident-response guidance describes containment as a key response activity, including actions that prevent an incident from causing further damage. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and the NIST Cybersecurity Framework for the relationship between detection, response, containment, and recovery activities.

QUESTION NO: 76

Dataflow diagrams are used by IT auditors to:

A. Graphically summarize data paths and storage processes.

B. Order data hierarchically

C. Highlight high-level data definitions

D. Portray step-by-step details of data generation.

ANSWER: A

Explanation:

Dataflow diagrams are used to graphically summarize data paths and storage processes. They depict how data enters a system, moves among processes, is retained in data stores, and leaves the system through outputs or interfaces. For an IT auditor, this provides a clear, logical view of the information flow without requiring the implementation-level detail of program code or operational procedures. The diagram helps the auditor identify where data is collected, transformed, transmitted, stored, and potentially exposed to loss, unauthorized access, or integrity failures. It is particularly useful when scoping an audit, understanding system boundaries and interfaces, tracing important business data, and identifying points at which controls over input, processing, storage, or output should operate. A dataflow diagram therefore communicates the movement and handling of data across a process or system, including the relationships between external entities, processes, and repositories. This use aligns with the standard definition of a data-flow diagram as a graphical representation of data movement through an information system. See the IBM documentation on data-flow diagrams and the OMG BPMN specification for related process and information-flow modeling context.

QUESTION NO: 77

Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

How can you reduce the administrative burden of distributing symmetric keys for your employer?

A. Use asymmetric encryption for the automated distribution of the symmetric key

B. Use a self-generated key on both ends to eliminate the need for distribution

C. Use certificate authority to distribute private keys

D. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

ANSWER: A

Explanation:

Use asymmetric encryption for the automated distribution of the symmetric key is correct because it implements a hybrid cryptographic design: symmetric cryptography protects the high-volume telecommunications traffic efficiently, while asymmetric cryptography solves the difficult key-establishment and key-transport problem. Each remote location maintains an asymmetric key pair. A newly generated symmetric session or link key can be encrypted with the intended recipient's public key and transmitted over available communications infrastructure. Only the holder of the matching private key can recover that symmetric key, eliminating the need to physically courier or manually distribute the secret to every worldwide site.

This approach substantially improves scalability and operational efficiency. Symmetric keys may be generated, rotated, and replaced centrally or automatically as part of a key-management process, while the asymmetric keys provide the secure mechanism needed to establish those secrets across untrusted networks. In production, the public keys must be authenticated—for example, through certificates or another trusted public-key distribution method—to ensure the symmetric key is encrypted for the genuine destination. NIST describes public-key key transport and key establishment as mechanisms for securely establishing symmetric keys in its SP 800-57 Part 1 key-management guidance; its SP 800-56A guidance also covers pair-wise key-establishment schemes.

QUESTION NO: 78

What is the next step after defining the conditions under which standard security controls must be applied?

A. Perform an asset inventory and apply classifications

B. Analyze future security control plans

C. Adopt a culture of risk awareness

D. Create risk mitigation plans

ANSWER: D

Explanation:

Create risk mitigation plans is the appropriate next step because defining the conditions for applying standard security controls establishes the decision criteria for risk treatment. Those criteria indicate when a baseline or predefined control set is sufficient and when a risk requires a planned response tailored to the asset, threat, vulnerability, and business impact. A risk mitigation plan translates that decision into actionable treatment: it identifies the control measures to implement, assigns accountable owners, establishes target dates and resources, documents residual risk, and provides a basis for management approval and subsequent monitoring. This makes the security-control decision operational rather than merely policy-level.

Risk management guidance emphasizes selecting and implementing risk responses and documenting the actions needed to reduce risk to an acceptable level. NIST describes risk response as an organizational activity that includes developing and executing courses of action to address identified risks; mitigation is a principal response approach. A documented mitigation plan also supports governance because leadership can track implementation progress, validate that controls achieve their intended risk reduction, and reassess residual exposure as conditions change. See NIST SP 800-39, Managing Information Security Risk and NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.

QUESTION NO: 79

Scenario: Critical servers show signs of erratic behavior within your organization's intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.

In what phase of the response will the team extract information from the affected systems without altering original data?

A. Follow-up

B. Recovery

C. Response

D. Investigation

ANSWER: D

Explanation:

Investigation is the correct phase because it is where the incident response team establishes what happened, identifies affected assets, determines the scope and impact, and gathers evidence in a manner that preserves its integrity. Extracting information without changing the original data is a core digital-forensics requirement. Investigators should use forensically sound collection methods, such as acquiring an image or other verified copy of relevant storage media, documenting handling, calculating hashes where appropriate, and maintaining chain-of-custody records. These practices allow the team to analyze a working copy while retaining the original evidence for validation, internal review, legal needs, or disciplinary proceedings. In an active intrusion, the team may also collect volatile evidence, such as running processes, network connections, and memory contents, using documented procedures designed to minimize changes and clearly record any unavoidable system impact. NIST's incident-handling guidance describes analysis activities as determining the nature, extent, and impact of an incident, while its digital-forensics guidance emphasizes preserving data integrity during collection and examination. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.