PassQueen
a.k.a dumpsqueen.com

EC-Council Information Security Manager (E|ISM)

ECCouncil 512-50

Version Demo

Total Demo Questions: 44

Total Premium Questions: 445

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Information Security Management	102
Topic 2, Governance and Risk Management	153
Topic 3, Information Security Program	90
Topic 4, Security Operations Management	77
Topic 5, Information Security Incident Management	23
Total	445

QUESTION NO: 1

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 the organization contractually shifts a defined portion of the financial consequences of a security incident to an insurer in exchange for a premium. Cyber or breach insurance can cover specified costs such as incident response, forensic investigation, legal services, notification obligations, credit monitoring, business interruption, and certain liabilities, subject to the policy's terms, limits, exclusions, deductibles, and retention requirements. The organization still owns and manages the underlying information-security risk: it must maintain appropriate controls, satisfy policy conditions, and respond to the incident. However, insurance reallocates qualifying financial loss to another party, which is the essential characteristic of risk transfer. Risk-management guidance recognizes transfer or sharing as a treatment in which the burden of loss is allocated contractually, often through insurance. NIST's risk-management guidance describes risk transfer as shifting some or all risk to another party, while CISA identifies cyber insurance as a tool that can help organizations manage the financial impact of cyber incidents. See NIST SP 800-39, Managing Information Security Risk and CISA Cyber Insurance resources.

QUESTION NO: 2

The newly appointed CISO of an organization is reviewing the IT security strategic plan. Which of the following is the MOST important component of the strategic plan?

A. There is integration between IT security and business staffing.

B. There is a clear definition of the IT security mission and vision.

C. There is an auditing methodology in place.

D. The plan requires return on investment for all security projects.

ANSWER: B

Explanation:

There is a clear definition of the IT security mission and vision. A security strategic plan must first establish the intended security end state and the purpose of the security function. The mission expresses the enduring purpose of the security program—such as protecting organizational information, systems, and services in support of business objectives—while the vision describes the desired future capability or maturity. Together, they provide the direction against which strategic goals, priorities, governance decisions, investment roadmaps, staffing needs, and performance measures can be aligned.

For a CISO, this clarity is especially important because information security is not an isolated technical activity; it must enable the organization's mission and risk objectives. A well-defined mission and vision lets leadership assess whether proposed initiatives advance the agreed strategic direction and provides a consistent basis for communicating the program's value to stakeholders. The NIST Cybersecurity Framework emphasizes that cybersecurity governance should establish organizational context, direction, and risk-management expectations. NIST also describes security program planning as a management responsibility that must be aligned with organizational objectives. See the NIST Cybersecurity Framework and NIST Special Publication 800-100.

QUESTION NO: 3

When updating the security strategic planning document what two items must be included?

A. Alignment with the business goals and the vision of the CIO

B. The risk tolerance of the company and the company mission statement

C. The executive summary and vision of the board of directors

D. The alignment with the business goals and the risk tolerance

ANSWER: D

Explanation:

The alignment with the business goals and the risk tolerance must be included when updating a security strategic planning document. An information-security strategy exists to enable the organization's mission and strategic objectives, so its priorities, investments, control objectives, and security initiatives need to be explicitly traceable to current business goals. This alignment helps ensure that security is managed as a business enabler and that leadership can make informed decisions about funding, sequencing, and acceptable exposure.

Risk tolerance is equally essential because it establishes the level and types of risk the organization is prepared to accept while pursuing its objectives. The strategic plan should use that tolerance to guide security priorities and determine the appropriate balance among risk reduction, risk transfer, risk avoidance, and risk acceptance. As business conditions, regulatory obligations, technology, and threats change, revisiting both business alignment and risk tolerance keeps the security strategy relevant and appropriately governed. NIST describes risk tolerance as a key organizational input to risk-management decisions, while ISACA emphasizes aligning information and technology governance with enterprise objectives. See NIST SP 800-39 and ISACA COBIT resources.

QUESTION NO: 4

This occurs when the quantity or quality of project deliverables is expanded from the original project plan.

A. Scope creep

B. Deadline extension

C. Scope modification

D. Deliverable expansion

ANSWER: A

Explanation:

Scope creep is the uncontrolled or insufficiently controlled expansion of a project's scope beyond what was defined and approved in the original project plan. It can involve additional deliverables, features, functions, requirements, or increased quality expectations. The defining characteristic is that work is added beyond the approved baseline, frequently without corresponding adjustments to budget, staffing, schedule, risk planning, or formal authorization. In an information-security program or project, scope creep may occur when stakeholders request extra security controls, additional systems for assessment, broader compliance coverage, or expanded reporting after the work has begun. Effective scope management requires a documented scope baseline and an integrated change-control process so proposed changes can be evaluated for their effect on objectives, resources, time, cost, and risk before approval and implementation. This protects delivery commitments while allowing legitimate business-driven changes to be managed transparently. The Project Management Institute describes scope management as the processes used to ensure a project includes all required work, and only the required work; uncontrolled additions undermine that objective. See the Project Management Institute's discussion of scope creep and the PMBOK Guide overview.

QUESTION NO: 5

During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:

A. Identify and evaluate the existing controls.

B. Disclose the threats and impacts to management.

C. Identify information assets and the underlying systems.

D. Identify and assess the risk assessment process used by management.

ANSWER: A

Explanation:

Identify and evaluate the existing controls. is the appropriate next activity because risk analysis must determine the extent to which identified threats and impacts are already mitigated by safeguards in the current environment. The auditor should document relevant administrative, technical, and physical controls, then evaluate their design and operating effectiveness in relation to the affected assets, threat events, and potential business impacts. This establishes the residual exposure rather than merely describing the inherent exposure. For example, access controls, monitoring, backup arrangements, change controls, supplier controls, and incident-response procedures may reduce either the likelihood of a threat event, its resulting impact, or both. The control evaluation also identifies gaps, weaknesses, or dependencies that require treatment and provides evidence for subsequent risk-rating and risk-treatment decisions. NIST describes risk assessment as considering threats, vulnerabilities, likelihood, impact, and existing controls when determining risk, while NIST control-assessment guidance emphasizes evaluating whether safeguards are correctly implemented and effective in achieving their intended outcomes. See NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments and NIST SP 800-53A Rev. 5, Assessing Security and Privacy Controls.

QUESTION NO: 6

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. Response

B. Investigation

C. Recovery

D. Follow-up

ANSWER: B

Explanation:

Investigation is the correct phase because it is where the Incident Response Team determines what occurred, identifies affected assets and attack scope, and collects the evidence needed to support technically sound decisions. A core requirement of this work is preserving the integrity of original data. Responders should acquire information using forensically sound procedures, such as creating verified forensic images, collecting volatile data in a controlled manner when appropriate, documenting every action, and maintaining chain-of-custody records. Analysis is then performed on copies whenever possible rather than directly modifying the affected system's original evidence. This enables the organization to establish a reliable timeline, identify indicators of compromise, understand attacker activity, and retain evidence that may support legal, regulatory, disciplinary, or insurance requirements. NIST incident-handling guidance emphasizes collecting and analyzing incident-related data as part of effective incident analysis, while its forensic guidance stresses preserving evidence integrity throughout 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.

QUESTION NO: 7

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 organization's needs.

The CISO is unsure of the information provided and orders a vendor proof of concept to validate the system'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 material uncertainty about a security control's ability to scale to the organization's operational requirements. Scalability affects whether the two-factor authentication service can support the required user population, transaction volume, geographic footprint, availability targets, and future growth. If that assumption is incorrect, proceeding could create financial loss, schedule disruption, security exposure, and the need to replace the control after deployment.

Ordering a vendor proof of concept is a practical risk-treatment and due-diligence activity. It uses representative testing to obtain evidence about the product's actual capabilities before the organization commits further resources to implementation. The outcome enables the CISO to make an informed investment decision: proceed if performance and scaling requirements are demonstrated, require remediation or contractual assurances if gaps are manageable, or select another solution if the risk remains unacceptable. This aligns with the NIST risk-management process, which calls for assessing risks and selecting appropriate responses using reliable information. See NIST SP 800-37 Rev. 2 and NIST Risk Management Framework.

QUESTION NO: 8

What two methods are used to assess risk impact?

A. Cost and annual rate of expectance

B. Subjective and Objective

C. Qualitative and percent of loss realized

D. Quantitative and qualitative

ANSWER: D

Explanation:

Risk impact is assessed using **quantitative and qualitative** methods. Quantitative assessment expresses risk in measurable numerical or financial terms. It commonly estimates the value of an affected asset, the expected loss from a single occurrence, the likelihood or annualized rate of occurrence, and the resulting annualized loss expectancy. This approach helps security managers compare risk-treatment costs with the anticipated financial consequences of a risk event.

Qualitative assessment evaluates impact through descriptive ratings, such as low, medium, high, or critical. These ratings draw on expert judgment and defined criteria that can include operational disruption, legal and regulatory exposure, reputational harm, safety implications, and effects on confidentiality, integrity, and availability. It is particularly useful where dependable financial data is unavailable or where consequences cannot reasonably be reduced to a monetary amount.

Using these two approaches enables an organization to assess risks in a manner appropriate to the available information and the decision being made. NIST describes both qualitative and quantitative risk-assessment approaches in NIST SP 800-30 Rev. 1, while ISO guidance recognizes that risk analysis may use qualitative, quantitative, or mixed methods in ISO 31010:2019.

QUESTION NO: 9

Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

A. Poses a strong technical background

B. Understand all regulations affecting the organization

C. Understand the business goals of the organization

D. Poses a strong auditing background

ANSWER: C

Explanation:

Understand the business goals of the organization is the most important factor because an effective security leader must position security as an enabler of the organization's mission, strategy, and operational priorities. Security culture is influenced when employees and leadership see that security practices support meaningful business outcomes, such as customer trust, reliable service delivery, innovation, resilience, and protection of critical assets. Understanding goals also lets the security leader communicate risk in terms that executives and business teams can act on, prioritize investments according to business value, and establish policies that are practical within real operational workflows. This alignment makes security a shared organizational responsibility rather than a purely technical or compliance-driven function. A security program that reflects business objectives is more likely to gain executive sponsorship, receive appropriate resources, and be adopted consistently by personnel throughout the organization. NIST's Cybersecurity Framework emphasizes that cybersecurity risk management should be integrated with organizational mission, objectives, and risk-management processes. ISACA likewise describes business alignment as a central component of effective enterprise information and technology governance. See the NIST Cybersecurity Framework and ISACA COBIT resources.

QUESTION NO: 10

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

A. The types of cardholder data retained

B. The duration card holder data is retained

C. The size of the organization processing credit card data

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 correct because PCI DSS compliance validation requirements are commonly assigned through merchant levels based primarily on the organization's annual payment-card transaction volume. Payment brands and acquiring banks use these volume thresholds to determine the expected validation approach, such as whether an organization must submit a Self-Assessment Questionnaire, obtain an on-site assessment performed by a Qualified Security Assessor, provide an Attestation of Compliance, or complete regular vulnerability scans. The precise thresholds and validation procedures can vary by payment brand and acquirer, but annual transaction count is the fundamental criterion used to categorize merchants for compliance-validation purposes. For example, Visa's merchant-level descriptions classify merchants according to the number of Visa transactions processed annually and tie those levels to validation expectations. PCI DSS itself establishes the security controls for protecting account data, while the payment brands and acquirers determine the validation level applicable to a particular merchant. See Visa's PCI DSS compliance guidance and the PCI Security Standards Council PCI DSS document library.

QUESTION NO: 11

During the 3rd quarter of a budget cycle, the CISO noticed she spent more than was originally planned in her annual budget. What is the condition of her current budgetary posture?

A. The budget is in a temporary state of imbalance

B. The budget is operating at a deficit

C. She can realign the budget through moderate capital expense (CAPEX) allocation

D. She has a surplus of operational expenses (OPEX)

ANSWER: B

Explanation:

The budget is operating at a deficit. A deficit exists when actual spending exceeds the amount authorized or planned in the budget for the applicable period. Here, the CISO has identified that spending is higher than the annual budget originally planned, which represents an unfavorable budget variance and places the security function in a deficit position. Recognizing this condition during the third quarter is important because the CISO can forecast the full-year variance, identify the specific drivers of excess spending, and escalate the projected shortfall through established financial-governance processes. Appropriate follow-up includes validating whether the excess is due to timing, unplanned operational needs, contract costs, incident response, or other business requirements; updating the forecast; and seeking approved corrective action, such as reprioritization or a formally authorized budget adjustment. Budget management guidance commonly treats variance analysis as the process of comparing actual results with budgeted amounts so that management can identify and respond to differences. See the U.S. GAO's Standards for Internal Control in the Federal Government for the importance of monitoring actual performance against planned results, and the CFA Institute corporate-finance resources for budgeting and financial-control concepts.

QUESTION NO: 12

Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?

A. Control Objective for Information Technology (COBIT)

B. Committee of Sponsoring Organizations (COSO)

C. Payment Card Industry (PCI)

D. Information Technology Infrastructure Library (ITIL)

ANSWER: A

Explanation:

Control Objective for Information Technology (COBIT) is correct because COBIT is specifically designed as an enterprise governance and management framework for information and technology. Developed by ISACA, it gives managers and governance bodies a structured way to translate business objectives and risk considerations into information-and-technology governance objectives, processes, controls, performance measures, and accountability structures. This directly supports the stated need to bridge business risks, control requirements, and technical matters: leadership can define the outcomes and acceptable risk levels, while IT teams can implement and measure the associated practices and controls. COBIT also supports assurance by providing a common language for evaluating whether information-and-technology activities are aligned with enterprise goals, delivering expected value, optimizing risk, and using resources responsibly. Its governance-system approach makes it useful across an organization rather than limiting it to one technology, regulatory domain, or operational service area. ISACA describes COBIT as a framework for the governance and management of enterprise information and technology, with principles and objectives that help organizations create value while balancing benefits, risk, and resources. See ISACA's COBIT resource page and the COBIT framework overview.

QUESTION NO: 13

Acme Inc. has engaged a third party vendor to provide 99.999% up-time for their online web presence and had them contractually agree to this service level agreement. What type of risk tolerance is Acme exhibiting? (choose the BEST answer):

A. low risk-tolerance

B. high risk-tolerance

C. moderate risk-tolerance

D. medium-high risk-tolerance

ANSWER: A

Explanation:

low risk-tolerance is correct because a contractual requirement for 99.999% availability—commonly called “five nines”—allows only about 5.26 minutes of unavailability over an entire year. This exceptionally stringent service-level target indicates that Acme considers disruption to its online presence highly unacceptable and is willing to impose substantial resilience and availability obligations on its provider. Risk tolerance expresses the amount of risk an organization is prepared to accept in pursuit of its objectives. Here, Acme’s very limited acceptable downtime reflects a minimal willingness to accept availability risk. Contractually documenting the target also establishes accountability, measurable performance expectations, and a basis for monitoring the vendor’s delivery of this critical service. Availability requirements should be tied to business impact and incorporated into third-party risk management and service-level governance. NIST explains that availability means timely, reliable access to and use of information, while its contingency-planning guidance emphasizes defining recovery objectives based on organizational needs and impact. See NIST’s definition of availability and NIST SP 800-34 Rev. 1, Contingency Planning Guide.

QUESTION NO: 14

What is meant by password aging?

A. An expiration date set for passwords

B. A Single Sign-On requirement

C. Time in seconds a user is allocated to change a password

D. The amount of time it takes for a password to activate

ANSWER: A

Explanation:

Password aging is the policy of assigning a defined maximum lifetime to a password, after which the password expires and the user must create a new one to continue authentication. Therefore, *An expiration date set for passwords* accurately describes password aging. In practice, an organization configures a maximum password age, such as a specified number of days; once that period elapses, the account holder is prompted or required to change the password. This control has historically been used to limit the duration for which a disclosed or compromised password remains usable and to support organizational access-control policy. Microsoft defines the maximum password age setting as the period a password can be used before the system requires the user to change it: Microsoft Maximum password age policy. Modern password policy should also be risk-based: NIST advises against arbitrary periodic password changes unless there is evidence of compromise, because forced changes can lead users to choose predictable variations. That guidance affects whether and how an organization implements the control, but the term itself still means setting a password validity period or expiration date. See NIST SP 800-63B.

QUESTION NO: 15

You have implemented the new controls. What is the next step?

A. Document the process for the stakeholders

B. Monitor the effectiveness of the controls

C. Update the audit findings report

D. Perform a risk assessment

ANSWER: B

Explanation:

After new safeguards have been put into operation, the appropriate next step is to **monitor the effectiveness of the controls**. Implementation alone establishes that a control exists; it does not demonstrate that the control operates as intended, consistently meets its stated objective, or continues to address the risk within the organization's accepted tolerance. Ongoing monitoring produces evidence about control performance, such as whether required activities occur, whether exceptions are identified and handled, and whether changes to systems, threats, or business processes have reduced the control's effectiveness.

This activity supports the continual-improvement cycle of an information security management program. Results from monitoring can trigger corrective action, control tuning, management reporting, reassessment of residual risk, or future audit activity. It also ensures that the organization can detect control degradation promptly rather than waiting for a periodic review or an incident. NIST describes information-security continuous monitoring as maintaining ongoing awareness of security, vulnerabilities, and threats to support risk-management decisions. See NIST SP 800-137: Information Security Continuous Monitoring. The broader control-assessment lifecycle is also described in NIST SP 800-53A Rev. 5, which emphasizes assessing implemented controls and monitoring their continued effectiveness.

QUESTION NO: 16

What is the main purpose of the Incident Response Team?

A. Ensure efficient recovery and reinstate repaired systems

B. Create effective policies detailing program activities

C. Communicate details of information security incidents

D. Provide current employee awareness programs

ANSWER: A

Explanation:

The main purpose of an Incident Response Team is to coordinate and carry out a timely, controlled response to an information security incident so that affected services and systems can be safely recovered and returned to normal operation. Therefore, *Ensure efficient recovery and reinstate repaired systems* best captures the team's central operational objective. Incident response is not limited to technical remediation: the team assesses the incident, contains its effects, eliminates the cause where possible, validates that systems are trustworthy, and supports restoration of business operations. Efficient recovery matters because incidents can disrupt availability, compromise information, and create ongoing organizational risk; restoring systems without appropriate validation could allow the incident to recur or remain undetected. The team also preserves relevant evidence and records lessons learned during this process, helping the organization strengthen future resilience. NIST describes incident response as a lifecycle that includes containment, eradication, and recovery, with recovery focused on restoring affected systems and services while monitoring for signs of residual compromise. This aligns directly with the stated purpose of ensuring repaired systems are reinstated efficiently and securely. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and CISA Incident Response resources.

QUESTION NO: 17

A Security Operations Centre (SOC) manager is informed that a database containing highly sensitive corporate strategy information is under attack. Information has been stolen and the database server was disconnected. Who must be informed of this incident?

A. Internal audit

B. The data owner

C. All executive staff

D. Government regulators

ANSWER: B

Explanation:

The data owner must be informed because the data owner is accountable for the classification, authorized use, protection requirements, and business impact of the information asset. In this case, the affected database contains highly sensitive corporate strategy information, and theft of that information creates a potentially material business, legal, competitive, and reputational incident. The SOC manager's immediate technical containment action—disconnecting the server—helps limit further loss, but it does not replace the data owner's responsibility to direct business decisions concerning the affected data.

Notification enables the data owner to validate the sensitivity and scope of the compromised information, assess its business consequences, determine required handling and recovery priorities, and engage the appropriate internal incident-management, legal, privacy, communications, and executive escalation processes under the organization's incident-response plan. NIST states that incident response involves coordination among technical and organizational stakeholders and that reporting and communication procedures should be defined in advance. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide. Accountability for information assets is also consistent with established information-security management practice, including ISO/IEC 27001, which emphasizes assigned roles and responsibilities for protecting organizational information.

QUESTION NO: 18

Which of the following defines the boundaries and scope of a risk assessment?

A. The risk assessment schedule

B. The risk assessment framework

C. The risk assessment charter

D. The assessment context

ANSWER: D

Explanation:

The assessment context defines the boundaries and scope of a risk assessment. Establishing context is an essential early activity because it states what is being assessed, why the assessment is being performed, the organizational or system boundary, relevant assets and processes, stakeholders, assumptions, constraints, risk criteria, and the timeframe to be considered. These parameters ensure that assessment activities and conclusions are relevant to the intended decision and are not applied beyond the environment or business objective under review.

NIST SP 800-30 describes risk assessment preparation as establishing the context for the assessment, including its purpose, scope, assumptions, constraints, sources of threat information, and risk model. Scope specifically identifies the organizational applicability, systems, functions, or other elements included in the assessment. Defining this context enables an organization to select appropriate information sources, identify applicable threats and vulnerabilities, and communicate risk results in a manner decision-makers can use. This aligns with ISO-based risk-management practice, in which the internal and external context and the scope of risk-management activities are determined before risk analysis is performed. See NIST SP 800-30 Rev. 1 and ISO 31000:2018 Risk management.

QUESTION NO: 19

Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

A. Plan-Check-Do-Act

B. Plan-Do-Check-Act

C. Plan-Select-Implement-Evaluate

D. SCORE (Security Consensus Operational Readiness Evaluation)

ANSWER: B

Explanation:

Plan-Do-Check-Act is correct because it is the continual-improvement cycle historically associated with ISO/IEC 27001 information security management systems (ISMSs). In the planning stage, the organization establishes ISMS objectives, identifies information-security risks, and determines the controls and processes needed to treat those risks. It then implements and operates those arrangements in the doing stage. The checking stage evaluates performance through monitoring, measurement, internal audit, management review, and assessment of whether the ISMS is achieving intended results. Finally, the acting stage addresses nonconformities and drives corrective action and ongoing improvement. This cyclic management approach ensures information security is maintained as an evolving business-management discipline rather than treated as a one-time technical project. Although modern ISO/IEC 27001 editions organize requirements into clauses and do not present PDCA as a mandatory clause-by-clause model, the cycle remains a well-established and useful way to understand the standard's risk-based, continual-improvement approach. ISO describes ISO/IEC 27001 as defining requirements for establishing, implementing, maintaining, and continually improving an ISMS: ISO/IEC 27001. ISO also explains the standard's role in managing information-security risks: ISO information security management overview.

QUESTION NO: 20

As the Chief Information Security Officer, you are performing an assessment of security posture to understand

what your Defense-in-Depth capabilities are. Which network security technology examines network traffic flows

to detect and actively stop vulnerability exploits and attacks?

A. Gigamon

B. Intrusion Prevention System

C. Port Security

D. Anti-virus

ANSWER: B

Explanation:

Intrusion Prevention System is correct because an IPS is a network security control designed to inspect traffic as it traverses the network, identify malicious activity or exploit attempts, and take immediate preventive action. Unlike a monitoring-only capability, an IPS operates inline or is otherwise integrated so that it can actively enforce a security decision. Its detection methods commonly include signature-based detection for known threats, protocol and policy analysis, and behavioral or anomaly-based methods. When traffic matches an exploit signature, violates a defined security policy, or displays indicators of an attack, the IPS can block packets, terminate a connection, or otherwise prevent the traffic from reaching the intended target. This directly supports defense in depth by adding a network-layer control that can reduce exposure to attacks targeting unpatched vulnerabilities and known attack patterns. NIST describes intrusion prevention systems as technologies that monitor events and can attempt to stop detected incidents, while CISA identifies network intrusion prevention as a key defensive capability. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and CISA guidance on intrusion detection and prevention systems.

QUESTION NO: 21

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 company'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 obtained physical access to a restricted area by following an authorized employee through an access-controlled gate. In a tailgating incident, an unauthorized person enters a secured location immediately behind someone who has valid authorization, taking advantage of the authorized person's access event rather than presenting their own credential. The consultant's electrician disguise may make the entry seem plausible, but the defining action described is following an employee through the main access gate. This is a common scenario assessed during physical penetration tests because it evaluates whether personnel verify that each person entering a controlled area has independently authenticated and whether access controls prevent more than one individual from passing on a single authorization event. Organizations can reduce this exposure through awareness training, visitor-management procedures, security guards, badge checks, turnstiles, and anti-passback or single-person entry controls. NIST describes physical access control as limiting access to facilities and systems to authorized individuals, including mechanisms and procedures that enforce authorized entry. See NIST's physical access control definition and the physical and environmental protection guidance in NIST SP 800-53 Rev. 5.

QUESTION NO: 22

Risk appetite directly affects what part of a vulnerability management program?

A. Staff

B. Scope

C. Schedule

D. Scan tools

ANSWER: B

Explanation:

Scope is correct because risk appetite establishes the amount and type of risk an organization is prepared to accept while pursuing its objectives. In a vulnerability management program, that tolerance directly informs the boundaries of the program: which business services, asset classes, environments, data types, internet-facing systems, and third-party connections require the most comprehensive assessment and treatment. A low risk appetite for exposure of regulated or sensitive data, for example, calls for a broad and rigorous vulnerability-management scope around the systems that store, process, or transmit that data. Conversely, an organization may formally accept more residual risk for isolated, low-value systems, affecting the level of coverage and treatment required for those assets. Risk appetite therefore provides governance direction for aligning vulnerability-management coverage with business priorities and the organization's risk strategy. NIST describes risk appetite as the types and amount of risk an organization is willing to accept, and its risk-management framework emphasizes using organizational risk decisions to guide security activities. See NIST SP 800-39: Managing Information Security Risk and CISA Vulnerability Management.

QUESTION NO: 23

Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered. What tool could Simon and his administrators implement to accomplish this?

A. They need to use Nessus.

B. They can implement Wireshark.

C. Snort is the best tool for their situation.

D. They could use Tripwire.

ANSWER: D

Explanation:

Tripwire is the appropriate tool because it provides file integrity monitoring, which is specifically designed to identify unauthorized changes to critical files. It establishes a trusted baseline of protected files and their attributes, such as cryptographic hashes, permissions, ownership, and configuration details. During subsequent scans or continuous monitoring, Tripwire compares the current state against that baseline and alerts administrators when a protected website file, system binary, configuration file, or other essential asset has been modified.

This capability directly addresses the stated need to detect alterations that occurred despite existing perimeter firewalls and IDS/IPS controls. File integrity monitoring supplies evidence of what changed and when, helping incident responders scope the compromise, identify potentially malicious modifications, and restore approved versions of affected files. It is also an important integrity control for sensitive systems and web servers. NIST identifies integrity verification as a system-information-integrity control, including tools that detect unauthorized changes to software, firmware, and information. Tripwire describes file integrity monitoring as continuous detection and reporting of changes to critical files and configurations. See NIST SP 800-53 SI-7: Software, Firmware, and Information Integrity and Tripwire File Integrity Monitoring.

QUESTION NO: 24

The formal certification and accreditation process has four primary steps, what are they?

A. Evaluating, describing, testing and authorizing

B. Evaluating, purchasing, testing, authorizing

C. Auditing, documenting, verifying, certifying

D. Discovery, testing, authorizing, certifying

ANSWER: A

Explanation:

Evaluating, describing, testing and authorizing correctly reflects the core activities of a formal certification and accreditation process. The process begins by evaluating the information system and its security context to identify applicable requirements, risks, and controls. It then describes the system, its environment, interconnections, and implemented

safeguards in formal security documentation. Testing follows to produce evidence that security controls are implemented properly and operate as intended. Finally, an accountable senior official reviews the resulting risk information and authorizes operation, accepting the residual risk at an appropriate organizational level. These activities establish a documented, evidence-based basis for deciding whether a system may operate and under what conditions. Modern risk-management guidance continues this essential model by requiring security-control assessment and an explicit authorization decision based on documented system and risk information. See the NIST Risk Management Framework, SP 800-37 Rev. 2 and the NIST Risk Management Framework overview.

QUESTION NO: 25

An example of professional unethical behavior is:

A. Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation

B. Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material

C. Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes

D. Storing client lists and other sensitive corporate internal documents on a removable thumb drive

ANSWER: C

Explanation:

Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes is professional unethical behavior because an employee's personal belief in an ownership interest does not authorize self-help access, copying, or removal of organizational records. Intellectual-property ownership, work-product rights, confidentiality obligations, and permitted access are determined through employment agreements, applicable law, and formal dispute-resolution processes—not by unilaterally taking files from a corporate system. A security professional is expected to protect information entrusted to them, respect proprietary rights, and act only within authorized boundaries, particularly when handling documents that may contain confidential business information, trade secrets, customer data, or internal strategy. If an ownership dispute exists, the appropriate professional response is to preserve evidence and pursue it through management, legal counsel, contractual procedures, or a competent authority. This approach maintains integrity, safeguards organizational assets, and avoids compromising the confidentiality and evidentiary integrity of the disputed material. Professional ethics codes emphasize maintaining high standards of conduct and supporting the protection of confidential and proprietary information; see the ISACA Code of Professional Ethics. The U.S. Patent and Trademark Office also describes trade secrets as commercially valuable information protected through reasonable secrecy measures: USPTO Trade Secret Policy.

QUESTION NO: 26

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 that stores cryptographic keys and performs operations such as authentication and digital signing on the card itself. The private key is designed to remain protected within the card's secure cryptographic boundary rather than being

copied to a workstation, removable media device, or other system. This substantially reduces the risk that malware, endpoint compromise, or unauthorized users can obtain the key and impersonate the cardholder.

In normal use, a relying system can receive the cardholder's public certificate and validate it, but the private key remains under card control. The cardholder unlocks use of protected key functions with a PIN, and the card performs the requested cryptographic operation without disclosing the private-key material. This hardware protection is central to PIV's support for strong, phishing-resistant certificate-based authentication and signing. NIST's PIV specifications define the card interfaces, credential containers, and key-management requirements that support this model. See NIST SP 800-73-4, Interfaces for Personal Identity Verification and FIPS 201-3, Personal Identity Verification of Federal Employees and Contractors.

QUESTION NO: 27

The success of the Chief Information Security Officer is MOST dependent upon:

A. favorable audit findings

B. following the recommendations of consultants and contractors

C. development of relationships with organization executives

D. raising awareness of security issues with end users

ANSWER: C

Explanation:

development of relationships with organization executives is correct because a Chief Information Security Officer must operate as a business leader as well as a security specialist. Executive relationships provide the influence, sponsorship, and communication channels needed to align security strategy with organizational objectives, risk appetite, regulatory obligations, and investment priorities. Through trusted engagement with senior leaders, the CISO can present cyber risk in business terms, obtain decisions on risk treatment, secure appropriate funding and resources, and ensure that accountability for important risks is assigned to the relevant business owners.

Security is an enterprise-wide responsibility, so the CISO's effectiveness depends heavily on collaboration across leadership functions such as finance, legal, operations, technology, and human resources. This executive alignment enables security requirements to be embedded in strategic planning, major initiatives, governance processes, and organizational culture rather than treated as an isolated technical activity. The NIST Cybersecurity Framework emphasizes governance, including establishing organizational context, risk-management strategy, and oversight for cybersecurity risk. NIST also identifies leadership commitment and clear communication as essential to managing enterprise risk effectively. See the NIST Cybersecurity Framework and NIST SP 800-39: Managing Information Security Risk.

QUESTION NO: 28

Which of the following provides an independent assessment of a vendorâ€™s internal security controls and overall posture?

A. Alignment with business goals

B. ISO/IEC 27001 certification

C. PCI attestation of compliance

D. Financial statements

ANSWER: B

Explanation:

ISO/IEC 27001 certification provides an independent assessment because an accredited certification body audits whether the vendor's information security management system (ISMS) conforms to the requirements of ISO/IEC 27001. The assessment considers the organization's systematic approach to managing information-security risk, including its governance, risk treatment, security policies, operational controls, performance evaluation, and continual improvement.

Certification is not merely a vendor assertion: the external auditor evaluates documented evidence and implementation of the ISMS, then performs periodic surveillance audits to maintain certification. This makes ISO/IEC 27001 certification a useful third-party due-diligence artifact when evaluating a vendor's overall security-management posture. It also establishes that security controls are selected and managed through a risk-based management framework rather than being assessed solely against one narrow regulatory requirement. ISO describes ISO/IEC 27001 as the standard defining requirements for an ISMS and notes that organizations can demonstrate conformity through certification. See ISO/IEC 27001:2022 and ISO's overview of ISO/IEC 27001.

QUESTION NO: 29

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 project activities that determines the earliest possible completion date. A security-project manager must identify the required deliverables, their durations, dependency relationships, milestone dates, and any schedule constraints in order to determine which activities have little or no scheduling flexibility. This makes it possible to focus oversight and resources on work that could delay the overall project, such as deployment prerequisites, security testing, approvals, remediation activities, or implementation cutovers.

Maintaining an accurate schedule of milestones and delivery timelines also supports continuous monitoring of progress against the approved project plan. When a critical activity slips, the manager can assess the impact promptly, update forecasts, escalate as appropriate, and pursue corrective actions such as resequencing work or assigning additional resources. This is especially important in security initiatives because a delayed control implementation may extend organizational exposure to risk. The Project Management Institute describes critical-path analysis as a scheduling technique used to identify the activities that directly control project duration; see PMI's critical path method overview. Further scheduling terminology and concepts are available in the PMBOK Guide resources.

QUESTION NO: 30

Which of the following information would MOST likely be reported at the board-level within an organization?

A. System scanning trends and results as they pertain to insider and external threat sources

B. The capabilities of a security program in terms of staffing support

C. Significant risks and security incidents that have been discovered since the last assembly of the membership

D. The numbers and types of cyberattacks experienced by the organization since the last assembly of the membership

ANSWER: C

Explanation:

Significant risks and security incidents that have been discovered since the last assembly of the membership are the information most appropriate for board-level reporting. A board's governance role is to provide oversight of enterprise risk, ensure that management is addressing material threats, and make informed decisions about risk appetite,

strategic priorities, resource allocation, and regulatory or stakeholder obligations. Accordingly, security reporting to the board should concentrate on matters that could materially affect organizational objectives, finances, operations, legal responsibilities, or reputation. Significant incidents should be communicated in a business-oriented form: their impact or likely impact, the affected services or data, management's response and recovery status, residual risk, and any decisions or support needed from the board. This enables directors to exercise meaningful oversight without being drawn into operational security management. The U.S. Securities and Exchange Commission's cybersecurity disclosure guidance also reflects the importance of governance-level visibility into material cybersecurity risks and incidents. See the SEC final rule on cybersecurity risk management, strategy, governance, and incident disclosure and the NIST Cybersecurity Framework for risk-governance context.

QUESTION NO: 31

What process defines the framework of rules and practices by which a board of directors ensure accountability, fairness and transparency in an organization's relationship with its shareholders?

A. Internal Audit

B. Corporate governance

C. Risk Oversight

D. Key Performance Indicators

ANSWER: B

Explanation:

Corporate governance is the framework of rules, practices, processes, and relationships through which an organization is directed and controlled. It establishes how a board of directors exercises accountability and oversight while balancing the interests of shareholders and other stakeholders. A sound governance framework defines decision-making authority, board responsibilities, ethical expectations, disclosure practices, and mechanisms for monitoring organizational performance and conduct.

In an information-security management context, corporate governance provides the senior-level direction that enables security strategy, risk appetite, policy oversight, and accountability to be aligned with organizational objectives. The board is responsible for ensuring transparent reporting and appropriate oversight of significant risks, including cyber and information-security risks. Governance is therefore not merely a control activity; it is the overarching system that establishes responsibility, fairness, transparency, and accountability between the organization and its shareholders.

The OECD describes corporate governance as involving relationships among management, the board, shareholders, and other stakeholders, while the International Finance Corporation emphasizes the structures and processes for company direction and control. See the OECD corporate governance resources and the IFC corporate governance overview.

QUESTION NO: 32

When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

A. Daily

B. Hourly

C. Weekly

D. Monthly

ANSWER: A

Explanation:

Daily is correct because PCI DSS requires audit logs to be reviewed at least once each day for security events and other specified system components. This recurring review is intended to identify suspicious activity, security control failures,

unauthorized access attempts, and other indicators of compromise promptly enough to support effective incident response. PCI DSS treats logging as an active security-monitoring control rather than merely a record-retention obligation: organizations must collect relevant audit data, protect it from alteration, and review it consistently. A daily cadence creates an accountable operational process in which anomalies can be investigated while supporting evidence is still timely and useful. The requirement applies to relevant logs in the cardholder data environment and systems that could affect its security, with organizations maintaining documented procedures and evidence that reviews occurred. Automated log-management or SIEM tooling can assist by aggregating, correlating, and alerting on events, but it does not remove the need for the required review process. See the PCI Security Standards Council's PCI DSS Document Library and the PCI DSS merchant resources for current standard materials and implementation guidance.

QUESTION NO: 33

SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:

A. ' OR 1=1 --

B. /../../../../

C. "DROPTABLE USERNAME"

D. NOPS

ANSWER: A

Explanation:

`' OR 1=1 --` is a classic basic SQL-injection payload. It begins by closing a quoted string in a vulnerable SQL statement, then introduces an always-true Boolean condition, `OR 1=1`. When an application concatenates untrusted input directly into a query, that condition can cause a query's filtering logic to evaluate as true for every row. The double hyphen is a common SQL single-line comment marker; where supported and correctly formatted for the database dialect, it comments out the remaining portion of the original query, such as a trailing quote or password comparison. The payload is therefore a concise demonstration of how user-controlled input can alter query syntax and intended authorization logic.

Its practical purpose in security testing and awareness training is to illustrate why applications must use parameterized queries (prepared statements), enforce server-side input handling, and ensure database accounts have only the permissions they need. OWASP describes SQL injection as occurring when an attacker can interfere with database queries through unsafely handled input and recommends parameterized queries as a primary defense. See the OWASP SQL Injection guidance and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 34

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 sudden compromise involving a large number of accounts on an otherwise hardened system strongly indicates access or knowledge that was already available within the organization. An insider may be an employee, contractor, administrator, service provider, or other trusted party with legitimate access to

systems, credentials, account-management processes, or sensitive authentication data. That access can be deliberately abused or can be exploited through negligence, coercion, or credential theft from an internal user.

In a hardened environment, controls such as restricted administration, hardened configurations, segmentation, and monitoring generally make broad compromise through ordinary external access more difficult. A trusted individual can bypass or undermine those protections by exporting account data, sharing credentials, creating unauthorized access paths, changing permissions, or disclosing information that enables an external party to take over many accounts quickly. The key indicator is the scale and abruptness of the account compromise despite the system's hardened state, which makes misuse of trusted access the most plausible explanation. NIST describes insider threats as risks arising when individuals with authorized access use that access in a manner that harms the organization. See NIST SP 800-53 and CISA's Insider Threat Mitigation guidance.

QUESTION NO: 35

What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

A. Test every three years to ensure that things work as planned

B. Conduct periodic tabletop exercises to refine the BC plan

C. Outsource the creation and execution of the BC plan to a third party vendor

D. Conduct a Disaster Recovery (DR) exercise every year to test the plan

ANSWER: B

Explanation:

Conduct periodic tabletop exercises to refine the BC plan is correct because a business continuity plan must be regularly exercised, reviewed, and improved to remain practical as business processes, personnel, technologies, dependencies, and threats change. A tabletop exercise brings the relevant stakeholders together to walk through a realistic disruption scenario, assess decision-making, communications, roles, escalation paths, recovery priorities, and dependencies without interrupting production operations. The outcomes identify gaps and result in documented updates to the plan, supporting continual improvement rather than treating continuity planning as a one-time documentation exercise.

This approach aligns with recognized business-continuity practice. NIST states that contingency-plan testing exercises the plan and identifies deficiencies that should be corrected through plan maintenance. The ISO business-continuity standard likewise emphasizes exercising and testing continuity procedures and evaluating results to drive improvement. Tabletop exercises are particularly valuable because they can be conducted periodically and efficiently with business and technical owners, helping demonstrate that the BC plan is usable and understood across the organization. References: NIST SP 800-34 Rev. 1, Contingency Planning Guide; ISO 22301:2019 Business Continuity Management Systems.

QUESTION NO: 36

A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how

hardware and software is implemented and managed within the organization. Which of the following principles

does this best demonstrate?

A. Effective use of existing technologies

B. Create a comprehensive security awareness program and provide success metrics to business units

C. Proper budget management

D. Leveraging existing implementations

ANSWER: D

Explanation:

Leveraging existing implementations is the principle demonstrated because the CISO is first examining the organization's current infrastructure, including the way its hardware and software are deployed, configured, operated, and managed. This establishes the technical and operational context in which security controls must function. A security program should build on and integrate with established platforms, administrative processes, architectures, and technology investments where appropriate, rather than treating security solutions as isolated additions. This approach helps ensure that controls are compatible with the organization's environment and can be implemented in a manner that supports sustainable operations and governance.

The NIST Cybersecurity Framework emphasizes understanding organizational context and using that context to establish and manage cybersecurity outcomes. Existing systems, dependencies, resources, and operating practices are material inputs to selecting and implementing appropriate safeguards. Likewise, NIST guidance on security and privacy controls recognizes that control implementation must be tailored to the system and organizational environment. Analyzing the current implementation and management of technology is therefore directly aligned with leveraging what is already implemented as the foundation for security decisions. See the NIST Cybersecurity Framework and NIST SP 800-53 Rev. 5.

QUESTION NO: 37

Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings you discover that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.

To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?

A. Business Impact Analysis

B. Business Continuity plan

C. Security roadmap

D. Annual report to shareholders

ANSWER: A

Explanation:

Business Impact Analysis is the appropriate document to review before changing non-performing controls because it identifies the business consequences of disruption to processes, systems, services, and information assets. A remediation plan should not merely restore technical control operation; it must ensure that the revised controls protect the organization in accordance with current business priorities, recovery needs, critical dependencies, and impact tolerances. Reviewing the Business Impact Analysis allows the CISO to determine which deficient controls affect the most critical business functions and therefore require the fastest remediation, strongest compensating measures, or executive risk acceptance while permanent corrections are implemented.

This review also supports an executive-level briefing by connecting audit results to measurable business impact rather than presenting the findings as isolated technical issues. The plan can then clearly state the affected business services, the risk posed by inadequate control performance, remediation ownership, target dates, and any interim safeguards. NIST describes the business impact analysis as a process for identifying and prioritizing critical systems and components based on the impact of a disruption. This makes it essential input when prioritizing corrective action after an audit. See NIST SP 800-34 Rev. 1 and NIST Cybersecurity Framework resources.

QUESTION NO: 38

Who in the organization determines access to information?

A. Legal department

B. Compliance officer

C. Data Owner

D. Information security officer

ANSWER: C

Explanation:

Data Owner is correct because the data owner is the business role accountable for a particular information asset and is responsible for determining its classification, acceptable use, handling requirements, and who should be authorized to access it. Access decisions should be based on business need, the sensitivity of the information, and the duties individuals must perform. Although technical teams administer identities and enforce permissions through systems, their implementation must follow the access rules and authorization criteria established by the accountable owner of the data.

This responsibility is central to effective information governance: the data owner understands the information's business value, regulatory relevance, confidentiality needs, and the consequences of improper disclosure or modification. The owner can therefore approve, modify, or revoke access as job responsibilities change, while ensuring that permissions remain aligned with least privilege and need-to-know principles. NIST's access-control guidance identifies information owners as responsible for specifying access-control requirements for information and systems. NIST also describes system and information owners' accountability in its control catalog. See NIST's definition of an information owner and NIST SP 800-53 Rev. 5.

QUESTION NO: 39

Which of the following is considered one of the most frequent failures in project management?

A. Overly restrictive management

B. Excessive personnel on project

C. Failure to meet project deadlines

D. Insufficient resources

ANSWER: C

Explanation:

Failure to meet project deadlines is a frequent and widely recognized project-management failure because delivering the agreed scope within the approved schedule is a core measure of project performance. A missed deadline can delay expected business benefits, disrupt dependent initiatives and operational plans, increase costs through extended staffing or vendor work, and require stakeholders to revise commitments. In information-security programs, schedule failure can be especially consequential when it postpones remediation, compliance activities, security-control deployment, or response to identified risks.

Effective project management therefore establishes a realistic baseline schedule, identifies dependencies and critical-path work, assigns accountable owners, monitors milestones, and manages schedule changes through governance. Schedule performance should be tracked continuously rather than assessed only at the planned completion date. Earned value management, milestone reviews, and timely corrective actions provide managers with indicators of whether work is progressing as planned and whether forecast completion dates remain achievable. The Project Management Institute describes schedule performance as an important element of integrated project performance measurement, while the U.S. Government Accountability Office's schedule-assessment guidance emphasizes that reliable schedules are necessary for credible planning and oversight. See PMI's earned value management guidance and the GAO Schedule Assessment Guide.

QUESTION NO: 40

A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?

A. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions

B. A clear set of security policies and procedures that are more concept-based than controls-based

C. A complete inventory of Information Technology assets including infrastructure, networks, applications and data

D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in

ANSWER: D

Explanation:

A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in is the foundational requirement because risk management is an enterprise governance activity, not merely a technical security exercise. A sponsor at the executive level provides the authority to establish risk appetite, resolve ownership disputes, prioritize remediation funding, and require business units to participate in risk identification and treatment. This sponsorship is particularly important for a CISO entering an immature program, since meaningful improvements often require changes to processes, accountability, investment, and organizational behavior across departments. Executive backing also ensures that risk decisions are aligned with business objectives and that accepted risks are formally owned by the appropriate business leaders. NIST describes risk management as an organization-wide responsibility integrated into governance and decision-making, requiring senior-leadership involvement and accountability. Similarly, governance frameworks emphasize leadership commitment as the basis for establishing direction, assigning responsibilities, and sustaining an information-security management program. With an empowered champion, the organization can then establish scope, identify assets and risks, define policies, and allocate resources in a coordinated manner. See NIST SP 800-37 Rev. 2 and ISO/IEC 27001.

QUESTION NO: 41

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

A. Weekly

B. Monthly

C. Quarterly

D. Daily

ANSWER: D

Explanation:

Daily is the correct choice because security conditions can change rapidly as new vulnerabilities, threat intelligence, suspicious activities, configuration changes, and exposed assets emerge. A daily monitoring cadence enables the security team to identify meaningful changes promptly, assess their potential business impact, and initiate investigation or remediation before exposure becomes a successful incident. In practice, many security controls—such as SIEM alerting, endpoint detection, vulnerability intelligence, and cloud-security monitoring—operate continuously or near real time. Daily review is therefore an appropriate minimum management-level cadence for ensuring that collected telemetry, alerts, risk indicators, and exposure findings receive regular attention.

This approach aligns with the NIST Cybersecurity Framework's emphasis on continuous monitoring to detect cybersecurity events and to maintain awareness of systems, assets, vulnerabilities, and threats. Daily monitoring also supports timely risk reporting and informed decisions by the information security manager, particularly where high-value data, internet-facing services, or changing cloud environments are involved. See the NIST Cybersecurity Framework and NIST guidance on Information Security Continuous Monitoring.

QUESTION NO: 42

A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

A. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.

B. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.

C. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.

D. If the findings do not impact regulatory compliance, review current security controls.

ANSWER: C

Explanation:

If the findings impact regulatory compliance, remediate the high findings as quickly as possible. This is the best immediate course because high-impact findings represent the greatest potential harm to the organization and, when they also affect regulatory obligations, can expose it to significant legal, financial, operational, and reputational consequences. A CISO should apply risk-based prioritization: validate the finding, identify the affected compliance requirement and business assets, assign accountable owners, and initiate remediation with an accelerated target date. Where a permanent correction cannot be completed immediately, the organization should document a time-bound remediation plan and implement compensating controls that reduce exposure until the corrective action is complete. This approach creates clear evidence of governance and due diligence for auditors and regulators while directing scarce security resources to the most material issue first. It also aligns with the expectation that assessment findings feed a formal plan of action and milestones process, with remediation prioritized according to risk. NIST's control-assessment guidance discusses documenting findings and managing remediation through plans of action and milestones: NIST SP 800-53A Rev. 5. NIST also describes risk management as an ongoing organizational process: NIST SP 800-37 Rev. 2.

QUESTION NO: 43

The MOST effective way to validate that a business continuity plan can support recovery objectives is to:

A. Exercise the plan using realistic disruption scenarios

B. Store multiple printed copies of the plan

C. Require all employees to sign the plan annually

D. Replace the plan whenever a security incident occurs

ANSWER: A

Explanation:

Exercise the plan using realistic disruption scenarios is correct because an exercise tests whether assigned personnel understand their responsibilities and whether documented procedures, communication channels, dependencies, resources, and recovery arrangements work in practice. Exercises can reveal gaps that are not apparent during document review, enabling the organization to correct the plan before a real disruption occurs.

Continuity plans should be maintained and tested on a defined schedule and after material changes to business processes, systems, suppliers, or recovery strategies. NIST contingency-planning guidance emphasizes testing, training, and exercises to validate plan effectiveness, while ISO 22301 requires exercising and evaluating continuity procedures. See NIST SP 800-34 Rev. 1 and ISO 22301:2019.

QUESTION NO: 44

With respect to the audit management process, management response serves what function?

A. placing underperforming units on notice for failing to meet standards

B. determining whether or not resources will be allocated to remediate a finding

C. adding controls to ensure that proper oversight is achieved by management

D. revealing the "root cause" of the process failure and mitigating for all internal and external units

ANSWER: B

Explanation:

In the audit-management process, a management response formally states how management will address an audit finding. This includes deciding whether remediation will be undertaken, identifying the accountable owner, establishing a target date, and committing the budget, personnel, technology, or other resources needed to implement corrective action. Therefore, “determining whether or not resources will be allocated to remediate a finding” best reflects the essential governance function of the response: management evaluates the finding and accepts responsibility for an appropriately resourced action plan, or documents its risk-based decision concerning the issue.

This response is important because auditors identify and communicate risks, control gaps, and recommendations, but management owns the business processes and the associated risk-treatment decisions. A clear response creates an auditable record of management’s commitment and allows subsequent follow-up to validate that agreed remediation has been implemented and is operating as intended. The Institute of Internal Auditors’ Global Internal Audit Standards describe communicating conclusions and management action plans, while GAO guidance emphasizes that management is responsible for designing, implementing, and monitoring corrective actions for identified deficiencies. See the IIA Global Internal Audit Standards and GAO Green Book.