PassQueen
a.k.a dumpsqueen.com

Certified Information Systems Security Professional (CISSP)

ISC2 CISSP

Version Demo

Total Demo Questions: 156

Total Premium Questions: 1562

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security and Risk Management	292
Topic 2, Asset Security	113
Topic 3, Security Architecture and Engineering	179
Topic 4, Communication and Network Security	224
Topic 5, Identity and Access Management (IAM)	228
Topic 6, Security Assessment and Testing	133
Topic 7, Security Operations	253
Topic 8, Software Development Security	140
Total	1562

QUESTION NO: 1

Which of the following virtual network configuration options is BEST to protect virtual machines (VM)?

A. Data segmentation

B. Data encryption

C. Traffic filtering

D. Traffic throttling

ANSWER: C

Explanation:

Traffic filtering is the best virtual network configuration option to protect virtual machines because it directly controls which network communications may enter and leave each VM. In virtualized environments, this control is commonly implemented through virtual firewalls, security groups, hypervisor or distributed-firewall policies, and access control lists. These controls can enforce least privilege by permitting only explicitly authorized source and destination addresses, ports, protocols, and services.

Applying traffic filtering close to an individual workload is especially valuable because it reduces each VM's exposed network attack surface and helps contain unauthorized lateral movement between virtual workloads. It also remains effective when VMs are moved, cloned, or dynamically provisioned, provided the policy follows the workload or is applied through the virtual networking layer. This aligns with the virtualization-security principle of isolating workloads and controlling inter-VM traffic rather than relying only on protections at the physical network perimeter.

NIST identifies virtual network security controls, including firewalls and traffic isolation mechanisms, as important protections for virtualized infrastructure. NIST's firewall guidance also describes filtering traffic according to defined policy as a foundational network security function. See NIST SP 800-125, Guide to Security for Full Virtualization Technologies and NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy.

QUESTION NO: 2

A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air

Conditioning (HVAC) intakes on the ground level that have ultraviolet light fi lters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

A. Remove the ultraviolet light filters on the HVAC intake and replace the fire suppression system on the upper floors with a dry system.

B. Elevate the HVAC intake by constructing a plenum or external shaft over it and convert the server room fire suppression to a pre-action system.

C. Add additional ultraviolet light fi lters to the HVAC intake supply and return ducts and change server room fire suppression to FM-200.

D. Apply additional physical security around the HVAC intakes and update upper floor fire suppression to FM-200.

ANSWER: B

Explanation:

Elevate the HVAC intake by constructing a plenum or external shaft over it and convert the server room fire suppression to a pre-action system. This recommendation addresses the two relevant risks using complementary physical and environmental controls. Outdoor air intakes located at ground level are particularly exposed to contaminants, vehicle exhaust, flooding, and deliberate introduction of harmful material. Ultraviolet filtration can help control certain biological contaminants but does not prevent physical access to the intake or reliably protect against the broad range of airborne chemical and particulate hazards. Routing the intake upward through a protected plenum or shaft materially reduces its accessibility and exposure.

A pre-action system is also appropriate for a server room because it requires a detection event before water is admitted to the sprinkler piping. This detection-driven design provides fire protection while reducing the likelihood of an inadvertent water discharge damaging sensitive IT equipment. It is especially useful where both life safety and preservation of critical processing equipment are important. The combined recommendation therefore reduces exposure at a building-air entry point and improves the control of fire-suppression activation within the critical facility area. Guidance on protecting critical infrastructure physical systems is available from CISA; sprinkler-system requirements and pre-action system treatment are addressed by NFPA 13.

QUESTION NO: 3

Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

A. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools.

B. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools.

C. Maintaining the inventory through a combination of on premise storage configuration, cloud management, and partner management tools.

D. Maintaining the inventory through a combination of system configuration, network management, and license management tools.

ANSWER: D

Explanation:

Maintaining the inventory through a combination of system configuration, network management, and license management tools is the best method because it provides a comprehensive, continuously maintained view of both hardware and software assets. System configuration tools collect detailed endpoint information, such as installed software, operating-system versions, device identifiers, and relevant configuration attributes. Network-management and discovery capabilities complement this information by identifying devices that are connected to the environment, including systems that may not be enrolled in centralized endpoint-management processes. License-management tools reconcile discovered software installations with purchased entitlements, supporting software asset management, audit readiness, and compliance with licensing obligations.

Together, these tool categories provide more reliable inventory maintenance than a periodic, manually assembled record. They support the configuration-management objective of keeping an accurate, complete, and current inventory of system components, which is necessary for vulnerability management, incident response, change control, and risk decisions. NIST SP 800-53 control CM-8 specifically calls for developing, documenting, reviewing, and updating an inventory of system components, including relevant component details. The CIS Controls likewise identify active inventory management as a foundational security practice. See NIST SP 800-53 Rev. 5, CM-8 and CIS Control: Inventory and Control of Enterprise Assets.

QUESTION NO: 4

What is called the formal acceptance of the adequacy of a system's overall security by the management?

A. Certification

B. Acceptance

C. Accreditation

D. Evaluation.

ANSWER: C

Explanation:

Accreditation is the formal management decision that a system's security is adequate for operation in its intended environment and that the remaining, or residual, risk is acceptable. Historically, this term described the governance step following a technical security evaluation: responsible management reviews the available assessment evidence, understands the system's risk posture, and explicitly accepts accountability for authorizing its use. The decision is documented rather than being an informal statement of confidence.

Modern risk-management terminology, particularly in U.S. federal guidance, more often uses *authorization* in place of accreditation. The underlying concept remains the same: a senior official makes a risk-based decision to permit system operation after considering security and privacy assessment results, plans of action, and residual risk. This decision may result in an Authorization to Operate (ATO). For CISSP purposes, "accreditation" remains the classic term for management's formal acceptance of a system's overall security adequacy. NIST SP 800-37 describes authorization as a senior official's acceptance of security and privacy risk, and the NIST glossary defines the associated ATO decision: NIST SP 800-37 Rev. 2; NIST Glossary: Authorization to Operate.

QUESTION NO: 5

Which of the following reports provides the BEST attestation of detailed controls when evaluating an Identity as a Service (IDaaS) solution?

A. Service Organization Control (SOC) 1.

B. Service Organization Control (SOC) 2.

C. Service Organization Control (SOC) 3

D. Statement on Auditing Standards (SAS) 70.

ANSWER: B

Explanation:

Service Organization Control (SOC) 2 is the best choice because it is specifically intended to provide assurance over a service organization's controls using the AICPA Trust Services Criteria. Those criteria address security, availability, processing integrity, confidentiality, and privacy—areas directly relevant to an IDaaS provider that manages authentication, authorization, identity data, privileged access, logging, and service resilience. For vendor due diligence, the most useful form is ordinarily a SOC 2 Type II report. It includes the service auditor's testing and opinion on whether described controls operated effectively throughout a defined review period, rather than merely documenting their design at a single point in time. This gives the customer evidence that important identity-service controls are not only documented but have been consistently performed in production. The report can also identify the scope of the system, applicable criteria, complementary customer controls, testing procedures, and any exceptions, allowing the customer to evaluate residual risk in the planned IDaaS use case. The AICPA describes SOC 2 examinations as reports focused on controls relevant to the Trust Services Criteria, and its criteria provide the framework for evaluating those controls. See the AICPA SOC suite of services and the AICPA Trust Services Criteria.

QUESTION NO: 6

What Hypertext Transfer Protocol (HTTP) response header can be used to disable the execution of inline JavaScript and the execution of eval()-

type functions?

A. X-XSS-Protection

B. Content-Security-Policy

C. X-Frame-Options

D. Strict-Transport-Security

ANSWER: B

Explanation:

`Content-Security-Policy` is the HTTP response header that controls which sources of content a browser may load and, importantly, which script execution behaviors it permits. A policy using the `script-src` directive disables ordinary inline JavaScript unless the policy explicitly allows it with `'unsafe-inline'`, or selectively authorizes a specific script using a nonce or cryptographic hash. It also blocks `eval()` and similar string-to-code mechanisms unless `'unsafe-eval'` is explicitly present. Therefore, a properly configured policy such as `Content-Security-Policy: script-src 'self'` prevents both unapproved inline scripts and eval-type execution while allowing externally hosted same-origin scripts. CSP is a key browser-enforced defense-in-depth mechanism for reducing the exploitability and impact of cross-site scripting vulnerabilities. In practice, organizations often first deploy a `Content-Security-Policy-Report-Only` header to identify legitimate resources that would be blocked, then move to an enforcing `Content-Security-Policy` header. The CSP specification defines `script-src` and its source expressions, including the restrictions related to inline script and dynamic evaluation. See MDN Web Docs: CSP script-src and W3C Content Security Policy Level 3.

QUESTION NO: 7

A large human resources organization wants to integrate their identity management with a trusted partner organization. The human resources organization wants to maintain the creation and management of the identities and may want to share with other partners in the future. Which of the following options BEST serves their needs?

A. Federated identity

B. Cloud Active Directory (AD)

C. Security Assertion Markup Language (SAML)

D. Single sign-on (SSO)

ANSWER: A

Explanation:

Federated identity best meets this requirement because it lets the human resources organization remain the authoritative identity provider while establishing trust with an external partner that consumes identity assertions. The organization can continue to create, maintain, update, and disable its users' identities in its own identity-management environment. When a user needs access to a partner's service, the partner relies on an assertion or token issued by the organization rather than maintaining an independently managed account for that user.

This model is designed for cross-organizational access and can be extended as additional trusted partners are added. Each service provider can establish a trust relationship with the same identity provider, allowing controlled sharing of only the identity attributes and claims necessary for a particular service. This supports centralized lifecycle management, reduces duplicate identity administration, and improves consistency when access must be changed or revoked. Federation is an architectural trust model; standards such as SAML and OpenID Connect can implement it. NIST describes federation as the process in which a credential service provider asserts subscriber identity information to a relying party: NIST SP 800-63C, Federation and Assertions. It also aligns with the Identity and Access Management coverage in the ISC2 CISSP Examination Content Outline.

QUESTION NO: 8

An organization is designing a large enterprise-wide document repository system. They plan to have several different classification level areas with increasing levels of controls. The BEST way to ensure document confidentiality in the repository is to

A. encrypt the contents of the repository and document any exceptions to that requirement.

B. utilize Intrusion Detection System (IDS) set drop connections if too many requests for documents are detected.

C. keep individuals with access to high security areas from saving those documents into lower security areas.

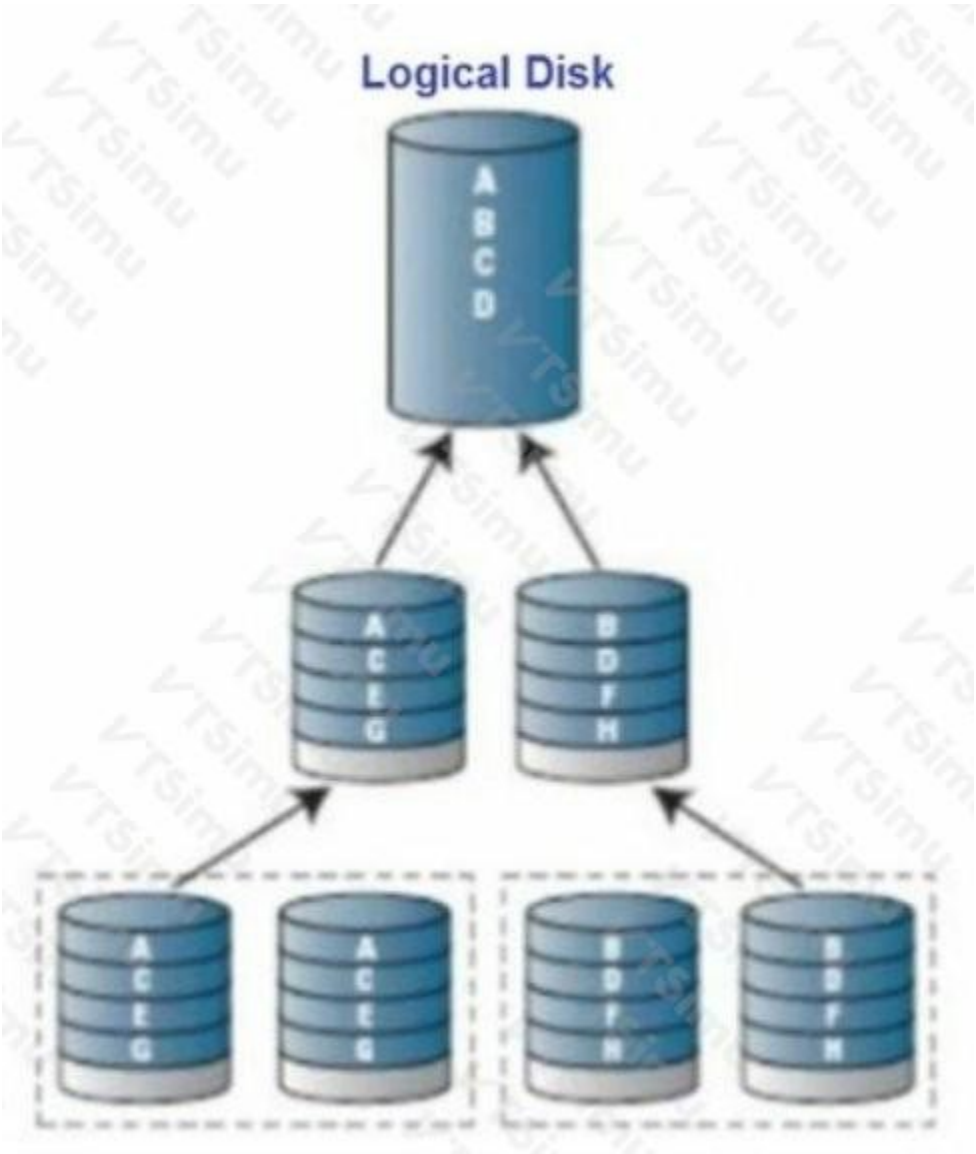
D. require individuals with access to the system to sign Non-Disclosure Agreements (NDA).

ANSWER: C

Explanation:

“keep individuals with access to high security areas from saving those documents into lower security areas” is the best control because the repository is explicitly organized around multiple classification levels. Confidentiality depends not only on restricting access to higher-classified material, but also on preventing that material from being moved, copied, or saved into a lower-classification area where it could become available to less-authorized users. This is the central confidentiality-preserving principle expressed by the Bell-LaPadula mandatory access control model’s *star* property: a subject may not write information to a lower security level (“no write down”). Applied to an enterprise repository, labels and enforced information-flow rules must follow the document and prevent a user with high-level access from downgrading its storage location without an authorized declassification process. This preserves separation between the repository’s classification domains and prevents accidental or intentional disclosure through an improperly chosen destination. NIST describes mandatory access control as restricting access according to security labels and formal authorization, which supports this type of classification-based enforcement. See the NIST definition of mandatory access control and NIST’s SP 800-53 access-control guidance.

QUESTION NO: 9



Which Redundant Array of Independent Disks (RAID) Level does the following diagram represent?

A. RAID 0.

B. RAID 1.

C. RAID 5.

D. RAID 10.

ANSWER: D

Explanation:

The diagram represents RAID 10, also called RAID 1+0. This nested RAID design combines two mechanisms in a specific order: disks are organized as mirrored pairs, and data is then striped across those pairs. Each write is therefore duplicated within its mirror pair, providing redundancy, while striping distributes I/O across multiple pairs to improve throughput and responsiveness.

RAID 10 requires at least four drives. Its capacity is effectively half of the total raw disk capacity because each block has a mirrored copy. Its resilience is determined by the mirror-pair layout: the array can continue operating after a disk failure provided the failed disks are not both members of the same mirrored pair. This arrangement is widely used for performance-sensitive systems that also need strong availability, including database and virtualization workloads. It is particularly useful where fast recovery is important, because replacing a failed drive generally requires copying data only from its surviving mirror partner rather than recalculating data from distributed parity.

The key visual characteristic is striping across sets that are themselves mirrored, which identifies RAID 10. See the Storage Networking Industry Association RAID overview and TechTarget RAID 10 definition for further details.

QUESTION NO: 10

Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?

A. Process isolation.

B. Data hiding and abstraction.

C. Use of discrete layering and Application Programming Interfaces (API).

D. Virtual Private Network (VPN).

ANSWER: B

Explanation:

Data hiding and abstraction. is the primary mechanism because it constrains a subject's view of a system to only the objects, attributes, and operations that the subject needs in its current execution domain. Abstraction presents a simplified, defined interface for interacting with an object while concealing unnecessary implementation details. Data hiding prevents the subject from directly viewing or manipulating internal object state and exposes only authorized methods or services. Together, these concepts reduce the accessible object set and establish controlled boundaries between execution domains.

This approach supports least privilege: a subject should receive only the access necessary for its authorized task, rather than broad visibility into system resources. It also promotes separation of duties and supports a smaller, more manageable trusted computing base by limiting what must be exposed and protected at each boundary. The control is architectural: the object model and its interfaces are designed so that access to protected functionality is mediated through constrained abstractions. NIST defines least privilege as restricting privileges to the minimum necessary to perform assigned tasks; this principle is directly implemented through carefully designed abstraction and data-hiding boundaries. See the NIST definition of least privilege and NIST SP 800-160, Systems Security Engineering.

QUESTION NO: 11

What security principle addresses the issue of "Security by Obscurity"?

A. Open design.

B. Role Based Access Control (RBAC)

C. Segregation of duties (SoD)

D. Least privilege.

ANSWER: A

Explanation:

Open design. is the security-engineering principle that directly addresses security by obscurity. It holds that a system must remain secure even when its architecture, algorithms, interfaces, and implementation details are known to an attacker. Security should instead rely on properly protected secrets, such as cryptographic keys, passwords, or other credentials. This concept is closely associated with Kerckhoffs's principle: the security of a cryptographic system should depend on the secrecy of the key, rather than secrecy of the algorithm or system design.

Applying open design produces controls that can be independently reviewed, tested, and validated. For example, an organization should use established cryptographic algorithms and publicly scrutinized protocols, with securely generated and managed keys, rather than depend on an unpublished algorithm remaining unknown. This approach recognizes that attackers can reverse-engineer software, observe network behavior, obtain documentation, or learn internal implementation details. Designing under that assumption provides more durable assurance and makes the system less dependent on a fragile hidden detail. NIST describes Kerckhoffs's principle as the requirement that cryptographic security reside in the key, not the secrecy of the algorithm. See the NIST CSRC definition of Kerckhoffs's principle and the NIST FIPS 197 specification for AES, an example of a publicly specified algorithm intended to be secure with secret keys.

QUESTION NO: 12

Which of the following is the strongest physical access control?

A. Biometrics, a password, and personal identification number (PIN).

B. Individual password for each user.

C. Biometrics and badge reader.

D. Biometrics, a password, and badge reader.

ANSWER: D

Explanation:

Biometrics, a password, and badge reader. is the strongest physical access control because it requires three distinct authentication-factor categories before permitting entry. A biometric verifies something the individual is, such as a fingerprint or iris characteristic. A password verifies something the individual knows. A badge reader verifies something the individual has, namely an issued physical credential. Requiring independent factors provides substantially greater assurance than relying on one factor alone, because compromise of a badge, disclosure of a password, or attempted biometric impersonation by itself does not grant access.

This layered approach is especially appropriate for high-value or high-risk physical locations, such as data centers, telecommunications rooms, research facilities, and areas containing sensitive records. It supports defense in depth by making unauthorized entry dependent on defeating multiple separate safeguards. For CISSP purposes, the essential point is that authentication strength increases when controls are based on different factor types rather than multiple instances of the same type. NIST defines multifactor authentication as use of more than one distinct authentication factor, and its digital identity guidance describes the categories of something known, possessed, and inherent. See the NIST definition of multifactor authentication and NIST SP 800-63B Digital Identity Guidelines.

QUESTION NO: 13

Which of the following is an attacker MOST likely to target to gain privileged access to a system?

A. Programs that write to system resources

B. Programs that write to user directories

C. Log files containing sensitive information

D. Log files containing system calls

ANSWER: A

Explanation:

Programs that write to system resources are the most likely target because operations affecting protected operating-system resources commonly require elevated privileges. System resources include protected configuration locations, service and startup settings, executable files, device interfaces, system libraries, and other components whose modification can influence how the operating system or privileged processes run. If an attacker can exploit a weakness in such a program—for example, unsafe handling of file paths, permissions, input, or an update mechanism—the attacker may cause a privileged process to write attacker-controlled content or alter a security-relevant resource. This can enable privilege escalation, persistence, or execution of code in a higher-integrity security context. The core security concern is the combination of a privileged execution context and the ability to modify resources that affect system behavior. Secure design therefore applies least privilege, strict authorization checks, protected paths, and safe handling of all resource references used by elevated programs. ISC2 identifies security architecture and secure application design as core CISSP knowledge areas, including the application of least privilege and protection mechanisms. MITRE also documents improper privilege management as a weakness that can permit unauthorized elevation of privilege. See the ISC2 CISSP Exam Outline and MITRE CWE-269: Improper Privilege Management.

QUESTION NO: 14

A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

A. Data sanitization.

B. Data validation.

C. Service accounts removal.

D. Logging and monitoring.

ANSWER: B

Explanation:

Data validation is the best control because it enforces integrity rules before information is accepted, processed, or committed to the financial application's database. A validation control can confirm that data has the required format, type, range, completeness, consistency, and permitted business values. For example, it can reject a transaction containing an invalid account identifier, an amount outside authorized limits, an impossible date, or a value that violates a defined business rule. By rejecting unauthorized, malformed, or manipulated input before it changes a record, validation acts as a preventive integrity control.

For a production financial system, validation should be applied server-side and enforced through both application logic and database constraints where appropriate. Database controls such as data types, referential-integrity constraints, check constraints, stored procedures, and controlled transaction processing provide a reliable enforcement point even if a client-side control is bypassed. This supports the core security objective of integrity: protecting data from unauthorized or improper modification. NIST identifies validation of input as a security measure for protecting systems against maliciously crafted or invalid data, and OWASP recommends allowlist-based server-side input validation as a primary defense. See NIST SP 800-53 Rev. 5, SI-10: Information Input Validation and the OWASP Input Validation Cheat Sheet.

QUESTION NO: 15

Which of the following management processes allots ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

A. Compliance

B. Configuration

C. Identity

D. Patch

ANSWER: B

Explanation:

Configuration is correct because configuration management establishes, documents, implements, and maintains the approved secure settings of systems and their components throughout their lifecycle. This includes defining a hardened baseline that enables only the services and features users or systems genuinely need to perform authorized functions. Applying that baseline includes replacing vendor-supplied default passwords, disabling unnecessary services, and configuring operational settings such as approved antivirus update sources and schedules. These activities are not isolated one-time actions; they are controlled configuration decisions that should be recorded, reviewed, and monitored so that systems remain in their intended secure state after deployment and change. The principle of least functionality is central to this work: systems should provide only essential capabilities, ports, protocols, and services, reducing attack surface while preserving the organization's required business functionality. NIST describes configuration management as managing security-related configuration settings and maintaining secure configurations, while its least-functionality control specifically calls for configuring systems to provide only essential capabilities. See NIST SP 800-128, Guide for Security-Focused Configuration Management and NIST SP 800-53 CM-7, Least Functionality.

QUESTION NO: 16

A packet filtering firewall looks at the data packet to get information about the source and destination addresses of an incoming packet, the protocol (TCP, UDP, or

ICMP), and the source and destination port for the:

A. desired service.

B. dedicated service.

C. delayed service.

D. distributed service.

ANSWER: A

Explanation:

The correct completion is "desired service." A packet-filtering firewall applies rules using network- and transport-layer header information, including source and destination IP addresses, the IP protocol value, and, for TCP or UDP traffic, source and destination port numbers. Port numbers conventionally identify the network service a client is attempting to use. For example, TCP port 443 is commonly associated with HTTPS, TCP port 25 with SMTP, and UDP port 53 with DNS. By matching the protocol and port values against its access-control rules, the firewall can determine whether traffic associated with the requested service is permitted between the specified source and destination. This is the core operation of traditional stateless packet filtering: the decision is based on individual packet header fields rather than on application payload inspection or an established connection's full context. The rule set therefore expresses policy such as allowing a particular desired service to a server while limiting that service to approved source networks. NIST describes packet filtering as controlling traffic based on packet header information, including addresses, protocols, and ports. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and Cloudflare's packet-filtering firewall overview.

QUESTION NO: 17

A security practitioner is tasked with securing the organizationâ€™s Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

A. Enable Wi-Fi Protected Access 2 (WPA2) encryption on the wireless access point

B. Disable the broadcast of the Service Set Identifier (SSID) name

C. Change the name of the Service Set Identifier (SSID) to a random value not associated with the organization

D. Create Access Control Lists (ACL) based on Media Access Control (MAC) addresses

ANSWER: A

Explanation:

Enable Wi-Fi Protected Access 2 (WPA2) encryption on the wireless access point is the most effective listed control because it enforces cryptographic protection and access authentication at the wireless network boundary. WPA2 uses AES-based CCMP protection to provide confidentiality and integrity for wireless traffic, preventing an unauthenticated party from simply joining the protected WLAN or reading protected communications. In an enterprise deployment, WPA2-Enterprise with IEEE 802.1X and EAP is especially appropriate because each user or device can authenticate with distinct credentials or certificates through an authentication server. This supports authorization decisions, centralized account administration, and prompt removal of access when a user or device is no longer authorized. Where a shared credential model is used, WPA2-Personal still requires knowledge of the pre-shared key before association is permitted, though enterprise authentication provides stronger operational control. NIST wireless-security guidance identifies strong authentication and encryption as fundamental protections for WLAN access and communications. While modern deployments should generally prefer WPA3 where it is supported, WPA2 is the strongest access-control mechanism among the choices presented. See NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks and the Wi-Fi Alliance security overview.

QUESTION NO: 18

Which of the following cloud computing service model provides a way to rent operating systems, storage and network capacity over the Internet?

A. Software as a service.

B. Data as a service.

C. Platform as a service

D. Infrastructure as a service.

ANSWER: D

Explanation:

Infrastructure as a service is correct because it delivers fundamental, on-demand computing resources—including processing, storage, and networking—over the internet. Under this service model, a customer can provision virtual machine instances that run an operating system, allocate storage, and establish virtual network capacity without purchasing or operating the underlying physical data-center infrastructure. The cloud provider manages the facilities, physical hardware, and virtualization foundation, while the customer typically retains responsibility for configuring, securing, patching, and administering the guest operating system and everything installed on it. This allocation of responsibilities is central to the shared-responsibility model assessed in CISSP cloud-security topics. NIST defines Infrastructure as a Service as the capability to provision processing, storage, networks, and other fundamental computing resources, with the consumer able to deploy and run software that can include operating systems and applications. Therefore, the wording describing rented OS-level computing, storage, and network capacity directly identifies Infrastructure as a service. See NIST SP 800-145, The NIST Definition of Cloud Computing and CISA Cloud Security Technical Reference Architecture.

QUESTION NO: 19

When performing an investigation with the potential for legal action, what should be the analyst's FIRST consideration?

A. Data decryption.

B. Chain-of-custody.

C. Authorization to collect.

D. Court admissibility.

ANSWER: C

Explanation:

Authorization to collect is the analyst's first consideration because any investigative activity with possible legal consequences must begin under valid authority and a clearly defined scope. Before accessing a system, acquiring logs, imaging storage, or taking custody of a device, the analyst must establish who authorized the work and what sources, accounts, locations, and types of data that authorization covers. The required authority can arise from organizational policy and delegated management authority, informed consent, contractual terms, or legal process such as a warrant, subpoena, or court order, depending on the investigation and jurisdiction.

Confirming authority first protects the rights of individuals and the organization while ensuring that evidence collection is lawful and defensible. It also defines the boundaries within which the examiner may operate, helping preserve the evidentiary value of material from the outset. Once collection is authorized, the analyst can use validated forensic procedures, document each action, preserve integrity, and maintain an appropriate chain of custody. NIST describes legal and organizational considerations as foundational to integrating forensic techniques into incident response in NIST SP 800-86. Additional guidance on the legal authority needed to search and seize electronic evidence appears in the U.S. Department of Justice's Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.

QUESTION NO: 20

A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

A. Update the contract to require the vendor to perform security code reviews.

B. Update the service level agreement (SLA) to provide the organization the right to audit the vendor.

C. Update the contract so that the vendor is obligated to provide security capabilities.

D. Update the service level agreement (SLA) to require the vendor to provide security capabilities.

ANSWER: C

Explanation:

Update the contract so that the vendor is obligated to provide security capabilities. The contract is the primary legally enforceable instrument for a custom software-development engagement, so it should establish security as a required deliverable rather than as an informal expectation. The organization can use the contract to incorporate detailed security requirements, including a secure development life cycle, protection of sensitive healthcare-related data, secure design and coding practices, security testing, vulnerability severity definitions, remediation time frames, security acceptance criteria, incident notification, and consequences if the vendor does not meet the requirements. These terms make it possible to objectively verify whether the delivered application satisfies the organization's security needs before acceptance and payment. This is especially important when the application may create, receive, maintain, or transmit protected health information, because the organization must ensure appropriate safeguards are implemented by parties performing work on its behalf. NIST's Secure Software Development Framework recommends that suppliers communicate and meet secure-development requirements throughout acquisition and delivery. NIST supply-chain guidance likewise emphasizes defining cybersecurity requirements in procurement and contractual relationships. See NIST SP 800-218, Secure Software Development Framework and NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices.

QUESTION NO: 21

Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

A. Mandatory Access Control (MAC).

B. Access Control List (ACL).

C. Discretionary Access Control (DAC).

D. Authorized user control.

ANSWER: A

Explanation:

Mandatory Access Control (MAC) is the policy in which the system uses fixed security attributes, commonly called security labels, to make access decisions. A subject, such as a user or process, is assigned attributes such as a security clearance, while an object, such as a file, is assigned a classification or label. The operating system's trusted security mechanism compares those attributes against centrally defined rules before allowing access. This control is mandatory because individual users, including an object's owner, cannot independently alter permissions or override the policy. MAC is therefore appropriate where access decisions must be consistently enforced according to an organization-wide classification scheme, especially in environments handling sensitive or classified information. This system-enforced use of subject and object attributes is the defining characteristic described in the question. NIST describes attribute-based access-control concepts and the use of subject, object, and environmental attributes in access decisions in NIST SP 800-162, Guide to Attribute Based Access Control. Additional guidance on policy enforcement for access control is available in NIST SP 800-53 Rev. 5.

QUESTION NO: 22

Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

A. File hashing.

B. Storage encryption.

C. Data retention policy.

D. Data processing.

ANSWER: B

Explanation:

Storage encryption is the best control because the confidentiality Trust Services Category used in SOC examinations addresses protection of information designated as confidential from unauthorized disclosure. SSAE No. 18 establishes the attestation framework under which service auditors perform SOC engagements, while the applicable confidentiality criteria focus on safeguards that prevent unauthorized parties from reading or obtaining sensitive information. Encryption of stored data provides a direct, technically enforceable safeguard: data on disks, databases, object storage, backups, and snapshots is rendered unreadable unless the requester also possesses or can use the required cryptographic key.

As an auditable control, storage encryption can be supported with evidence such as enabled encryption configurations, encryption coverage inventories, key-management procedures, access restrictions to keys, key rotation settings, and monitoring of encryption-related events. These artifacts help demonstrate that confidential data remains protected during storage and that the organization has implemented controls relevant to the confidentiality commitment. Effective implementation also requires sound cryptographic key management, since protection depends on keeping keys appropriately secured and available only to authorized systems and personnel. See the AICPA SOC suite of services overview and NIST guidance on storage encryption technologies.

QUESTION NO: 23

When developing the entitlement review process, which of the following roles is responsible for determining who has a need for the information?

A. Data Custodian

B. Data Owner

C. Database Administrator

D. Information Technology (IT) Director

ANSWER: B

Explanation:

Data Owner is responsible for determining who has a business need to access information. In CISSP governance terminology, the data owner has organizational accountability for a data set and makes the business decisions governing its classification, acceptable use, handling requirements, and authorization for access. An entitlement review is therefore not merely a technical validation of whether an account remains active; it must confirm that each granted entitlement remains appropriate for the person's current job responsibilities and legitimate business purpose. The data owner, often working with business managers and application owners, defines or approves the criteria used to make that determination. This responsibility directly supports the principles of least privilege and need to know: access should be limited to information required to perform authorized duties, and it should be revisited when duties, projects, employment status, or the sensitivity of the information changes. Technical teams can operate review tooling and provide evidence of current permissions, but the decision about whether access is justified is a business-data ownership decision. This separation of accountability helps ensure that access approvals reflect the value, sensitivity, and intended use of the information rather than only operational convenience. See the ISC2 CISSP Examination Outline for Identity and Access Management coverage and NIST's SP 800-53 Rev. 5 access-control guidance.

QUESTION NO: 24

Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

A. Write a Service Level Agreement (SLA) for the two companies.

B. Set up a Virtual Private Network (VPN) between the two companies.

C. Configure a firewall at the perimeter of each of the two companies.

D. Establish a File Transfer Protocol (FTP) connection between the two companies.

ANSWER: B

Explanation:

Set up a Virtual Private Network (VPN) between the two companies. A business-to-business VPN provides a protected communications path across an untrusted network, such as the Internet, for the systems exchanging inventory data and purchase orders. In this supplier-client scenario, a site-to-site VPN is particularly appropriate because it can securely connect defined networks or application environments at each organization without requiring every individual user to establish a separate remote-access connection.

A properly implemented VPN uses strong mutual authentication and encryption to protect the confidentiality of order and inventory information while it is in transit. It also supplies integrity protection, helping each organization detect unauthorized modification of transmitted records. Security teams can restrict the tunnel's permitted traffic to only the necessary hosts, ports, and business applications, and can log and monitor the connection as part of normal security operations. This creates an encrypted extranet-style connection suited to an ongoing interorganizational relationship, while allowing each company to retain control of its own internal network and access policies. NIST's guidance describes VPNs as mechanisms for protecting communications over public networks; see NIST SP 800-77, Guide to IPsec VPNs. Additional practical guidance on securely configuring VPN services is available from the UK NCSC VPN security collection.

QUESTION NO: 25

In a data classification scheme, the data is owned by the

A. system security managers

B. business managers

C. Information Technology (IT) managers

D. end users

ANSWER: B

Explanation:

In a data classification scheme, the data is owned by the **business managers**. More precisely, this role is commonly called the data owner or information owner, and it is normally a business role rather than an IT or security operations role. The owner has organizational authority and accountability for the information and is therefore best positioned to determine its business value, sensitivity, criticality, and the harm that could result from unauthorized disclosure, alteration, unavailability, or destruction. Based on that assessment, the business manager establishes the information's classification and defines the protection requirements, including appropriate handling, access, retention, and disposal expectations. Technical teams then implement and operate controls consistent with those requirements, but accountability for classification remains with the business function that owns and uses the information to accomplish the organization's mission. This allocation supports appropriate risk-based decisions because classification is driven by the information's business impact—not merely the technology on which it resides. NIST describes system and information owners as organizational officials with responsibility for information and associated security requirements; CISSP governance practice similarly distinguishes business ownership from operational custody and administration. See NIST SP 800-60, Volume I and NIST SP 800-37 Rev. 2.

QUESTION NO: 26

When should an application invoke re-authentication in addition to initial user authentication?

A. At the application sign-off

B. Periodically during a session

C. After a period of inactivity

D. For each business process

ANSWER: C

Explanation:

After a period of inactivity is correct because an inactive authenticated session can be exposed if a user leaves a workstation, mobile device, browser, or application session unattended. Re-authentication confirms that the person resuming activity is still the originally authenticated user before access continues. This is particularly important when the session can expose sensitive information, enable privileged actions, or permit transactions with security or business impact. An application enforces this through an inactivity timeout: after no user activity for a defined period, it terminates or locks the active session and requires the user to authenticate again before resuming. The appropriate duration depends on the system's risk level, data sensitivity, user environment, and organizational policy. Re-authentication following inactivity reduces the opportunity for someone with physical or logical access to an unattended session to act under the legitimate user's identity. NIST digital identity guidance specifically addresses session inactivity and requires reauthentication or termination when the inactivity limit is reached. OWASP likewise recommends expiring idle sessions and requiring authentication again before continued use. See NIST SP 800-63B: Authentication and Authenticator Management and the OWASP Session Management Cheat Sheet.

QUESTION NO: 27

Which of the following technologies would provide the BEST alternative to anti-malware software?

A. Host-based Intrusion Detection Systems (HIDS)

B. Application whitelisting

C. Host-based firewalls

D. Application sandboxing

ANSWER: B

Explanation:

Application whitelisting is the best alternative because it uses a default-deny execution model: software is permitted to execute only when it has been explicitly approved under an organization's policy. This shifts protection from attempting to recognize every malicious file to controlling which code may run in the first place. As a result, it can prevent execution of previously unseen malware, including threats for which no anti-malware signature, reputation record, or behavioral detection rule yet exists. This is especially valuable on fixed-function, high-value, or tightly managed systems where the set of required applications is known and changes are controlled.

For CISSP purposes, application whitelisting is a preventive technical control that directly addresses unauthorized code execution. Effective deployment includes maintaining an approved software inventory; defining rules based on trusted publishers, file hashes, paths, or certificates; protecting the policy-management process; and implementing a controlled process to approve legitimate application updates. It is not necessarily a complete replacement for defense in depth, but among the listed technologies it is the strongest alternative to traditional anti-malware because it most directly stops unapproved and potentially malicious executables from running. NIST describes application whitelisting as allowing execution only of authorized software in SP 800-167, Guide to Application Whitelisting. Related executable-code control guidance is also available in CISA's Application Control resource.

QUESTION NO: 28

A breach investigation found a website was exploited through an open source component. What is the FIRST step in the process that could have

prevented this breach?

A. Application whitelisting

B. Vulnerability remediation

C. Web application firewall (WAF)

D. Software inventory

ANSWER: D

Explanation:

Software inventory is the essential first step because an organization must know which software components, versions, dependencies, and deployment locations it uses before it can manage their security. Open-source libraries are frequently incorporated transitively, meaning developers may not directly install every component present in a web application. A complete inventory, often supported by a software bill of materials (SBOM), establishes the visibility needed to identify affected applications promptly when a vulnerability is disclosed. The organization can then correlate component versions with vulnerability intelligence, assess exposure and business impact, prioritize the resulting risks, and apply patches, upgrades, removals, or compensating controls. This makes the inventory foundational to an effective vulnerability-management and software-supply-chain security process. NIST SP 800-53's CM-8 control calls for maintaining an inventory of system components, including relevant component information needed for management and security. Likewise, NIST's SSDF describes maintaining provenance and component information to support identification and response to vulnerabilities in software dependencies. A current software inventory must be maintained continuously as applications and dependencies change, rather than created only after an incident occurs. References: NIST SP 800-53 Rev. 5, CM-8 System Component Inventory; NIST SP 800-218, Secure Software Development Framework.

QUESTION NO: 29

The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

A. System acquisition and development

B. System operations and maintenance

C. System initiation

D. System implementation

ANSWER: D

Explanation:

System implementation is correct. In the traditional SDLC security framework, accreditation is the formal management decision to authorize a system to operate after security controls have been implemented, assessed, and documented. This decision is made at the conclusion of implementation, when the system is ready to transition into its operational environment. By this point, the organization has completed activities such as security testing and evaluation, risk assessment, preparation of authorization documentation, and the formal review of residual risk by the designated authorizing official.

Current NIST terminology generally uses *authorization* rather than *accreditation*, but the underlying concept remains the same: an accountable senior official accepts the assessed risk and grants approval for the information system to operate. NIST's system development life cycle guidance places security authorization activities within the implementation phase before the system enters operations and maintenance. This timing ensures that operational use begins only after the organization has made an informed risk-based authorization decision. See NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle and NIST SP 800-37 Rev. 2, Risk Management Framework.

QUESTION NO: 30

What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

A. Policy creation.

B. Information Rights Management (IRM)

C. Data classification.

D. Configuration management (CM).

ANSWER: C

Explanation:

Data classification is the first step because a DLP program can protect information effectively only after the organization understands what information it holds, which data is sensitive, who owns it, and what handling restrictions apply. Classification assigns business-relevant labels—such as public, internal, confidential, or regulated—to information based on its value, sensitivity, and potential impact if disclosed, altered, or unavailable. Those labels supply the context needed to define DLP detection criteria and enforcement actions across endpoints, email, cloud services, networks, and data repositories. For example, a DLP policy may identify regulated personal data or confidential intellectual property through labels, content patterns, and associated handling rules, then alert, encrypt, quarantine, or block an attempted transfer according to the defined risk. Classification also supports consistent data ownership, retention, access, and sharing decisions, allowing DLP controls to be prioritized around the organization's most consequential data risks. ISC2's CISSP domains emphasize classifying information and determining handling requirements as foundational information-security governance activities. NIST similarly defines security categorization as determining information types and impact levels, providing a basis for selecting and applying appropriate protections. See NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

QUESTION NO: 31

Which of the following statements pertaining to disaster recovery is incorrect?

A. A recovery team's primary task is to get the pre-defined critical business functions at the alternate backup processing site.

B. A salvage team's task is to ensure that the primary site returns to normal processing conditions.

C. The disaster recovery plan should include how the company will return from the alternate site to the primary site.

D. When returning to the primary site, the most critical applications should be brought back first.

ANSWER: D

Explanation:

“When returning to the primary site, the most critical applications should be brought back first.” is the incorrect statement. A return from an alternate processing facility to the repaired primary facility is a planned reconstitution, or failback, activity. Its sequence must be based on technical dependencies, availability of the restored infrastructure, data synchronization, validation, and an approved cutover plan—not solely on each application’s business criticality. Before production workloads can safely return, the organization must ensure that essential underlying capabilities at the primary site, such as facilities, network connectivity, identity services, storage, backup capability, monitoring, and security controls, are operational and validated. It must also reconcile or synchronize data produced while operating at the alternate site so that the transition does not create inconsistent records or lost transactions.

Critical business functions are prioritized when initially recovering services because their outage has the greatest business impact. During failback, however, moving a critical application prematurely can create a second outage if its dependencies, data, or operational support are not fully ready. The disaster recovery plan should therefore define tested criteria, sequencing, rollback procedures, and management authorization for reconstitution. NIST describes reconstitution as returning system operations to normal after recovery and emphasizes validation and restoration activities in contingency planning. See NIST SP 800-34 Rev. 1 and CISA Continuity Planning.

QUESTION NO: 32

Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

A. Length of Initialization Vector (IV)

B. Protection against message replay

C. Detection of message tampering

D. Built-in provision to rotate keys

ANSWER: A

Explanation:

Length of Initialization Vector (IV) is correct because WEP uses a 24-bit IV with the RC4 stream cipher. An IV is transmitted with each protected frame and is combined with the shared WEP key to produce the RC4 keystream. A 24-bit value provides only 16,777,216 possible IVs, which is a small space for an active wireless network. Consequently, IV values repeat relatively quickly as traffic grows. Reuse is especially damaging for a stream cipher because frames encrypted using the same IV and secret key reuse related keystream material. An attacker can passively capture a sufficient number of frames and repeated IVs, then apply known statistical key-recovery techniques against WEP’s RC4 key scheduling to derive the shared key. Once the key is recovered, the attacker can decrypt traffic and create frames that appear to be protected by WEP. This weakness is fundamental to WEP’s design rather than merely an implementation configuration concern, which is why WEP has been deprecated and replaced by stronger Wi-Fi security mechanisms such as WPA2 and WPA3. NIST describes WEP as having known security vulnerabilities and recommends stronger WLAN protections in NIST SP 800-153. The IEEE 802.11 working group also documents modern Wi-Fi security standards at IEEE 802.11.

QUESTION NO: 33

Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users' internal control over financial reporting?

A. Statement on Auditing Standards (SAS) 70.

B. Service Organization Control 1 (SOC1).

C. Service Organization Control 2 (SOC2).

D. Service Organization Control 3 (SOC3).

ANSWER: B

Explanation:

Service Organization Control 1 (SOC1) is the appropriate reporting type because it addresses controls at a service organization that are relevant to user entities' internal control over financial reporting (ICFR). A SOC 1 examination is conducted under the AICPA attestation standards for reporting on controls at service organizations. Management prepares a description of the system used to provide the service, identifies the applicable control objectives, and describes the controls designed to achieve those objectives. This information enables user entities and their financial-statement auditors to understand and assess controls that may affect financial reporting assertions.

SOC 1 reports are particularly applicable where a provider performs a financially significant outsourced process, such as payroll administration, transaction processing, benefits administration, or claims processing. Depending on the report type, the examination addresses either whether controls are suitably designed as of a specified date or whether they were suitably designed and operated effectively throughout a stated period. The decisive scope indicator is the relationship to users' ICFR, not a general review of technology, security, or privacy practices. The AICPA identifies SOC 1 as reporting on controls relevant to user entities' financial reporting; see the AICPA SOC suite of services and its SOC reporting overview.

QUESTION NO: 34

During the change management process, which of the following is used to identify and record new risks?

A. Risk assessment

B. Lessons learned register

C. Risk register.

D. Risk report.

ANSWER: C

Explanation:

The **Risk register.** is the appropriate repository for documenting newly identified risks arising during change management. A proposed change can introduce security, operational, compliance, availability, or business risks; these must be identified as part of evaluating the change and then recorded so they can be assigned, assessed, treated, monitored, and communicated. The risk register is a living record that commonly captures the risk description, affected assets or processes, likelihood, impact, overall risk level, assigned risk owner, planned response, treatment status, and residual risk. Maintaining this record through the lifecycle of a change provides traceability between a change decision and its risk-management obligations. It also supports governance and auditability by demonstrating that risk decisions were documented and that responsible parties were assigned to manage the resulting exposure. NIST's risk-management guidance emphasizes ongoing risk assessment and monitoring as systems and operating environments change; the register provides the practical mechanism for retaining and managing the identified risk information over time. See NIST SP 800-37 Rev. 2 for continuous risk management and monitoring concepts, and PMI's risk register overview for the purpose and typical contents of a risk register.

QUESTION NO: 35

Which of the following BEST ensures the integrity of transactions to intended recipients?

A. Public key infrastructure (PKI).

B. Blockchain technology.

C. Pre-shared key (PSK).

D. Web of trust.

ANSWER: A

Explanation:

Public key infrastructure (PKI) best ensures transaction integrity when parties must reliably transact with intended, identifiable recipients. PKI combines asymmetric cryptography with digital certificates that bind a validated identity to a public key. A sender can digitally sign transaction data using its private key; the recipient then validates the signature with the sender's certified public key. Successful verification provides evidence that the signed transaction has not changed since signing and that it originated from the holder of the associated private key. This makes digital signatures a core PKI mechanism for integrity, origin authentication, and support for nonrepudiation.

PKI also provides a scalable trust model through certificate authorities and certificate-path validation. Before relying on a signature or establishing a protected session, a recipient can validate the certificate chain, certificate status, validity period, and identity information associated with the public key. This trusted binding is particularly important when transactions occur across networks where parties do not share a prior secret. In operational systems, PKI underpins technologies such as TLS, S/MIME, signed documents, and code signing, enabling recipients to verify the integrity and authenticated source of important data exchanges. See RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile and NIST SP 800-57 Part 1 Rev. 5.

QUESTION NO: 36

An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

A. Perform a compliance review

B. Perform a penetration test

C. Train the technical staff

D. Survey the technical staff

ANSWER: A

Explanation:

Perform a compliance review is the appropriate way to verify that a firewall hardening standard has been implemented as required. A compliance review compares the actual firewall configuration, supporting implementation records, and applicable operational evidence against the organization's approved baseline or standard. The reviewer can validate specific requirements such as permitted services and ports, rule-set approval and documentation, default-deny behavior, administrative access restrictions, logging configuration, secure management protocols, firmware requirements, and configuration-change controls. The result is objective evidence of whether the implemented configuration conforms to the newly adopted standard, along with documented findings and remediation actions for any deviations.

This is a verification activity: it measures the deployed technical state against defined organizational requirements. Effective assessment also includes sampling relevant devices, examining configuration exports and change tickets, and confirming that approved exceptions have been formally authorized. NIST describes firewall policy and configuration as central elements of firewall security and recommends documenting, implementing, and reviewing firewall configurations as part of ongoing management. NIST control-assessment guidance likewise emphasizes examining evidence to determine whether

control requirements are implemented. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and NIST SP 800-53A Rev. 5, Assessing Security and Privacy Controls.

QUESTION NO: 37

As a design principle, which one of the following actors is responsible for identifying and approving data security requirement in a cloud ecosystem?

A. Cloud auditor.

B. Cloud broker.

C. Cloud provider.

D. Cloud consumer.

ANSWER: D

Explanation:

Cloud consumer is correct because the consumer is the organization that owns or is accountable for the information processed in the cloud, as well as the business objectives, legal duties, risk tolerance, and data classifications that determine required protections. Accordingly, the consumer identifies required safeguards for its data—such as confidentiality and integrity needs, retention periods, encryption and key-management expectations, geographic residency, access-control requirements, and audit logging—and approves those requirements before selecting and using a cloud service. These needs are then translated into contractual, service-level, and technical requirements that the cloud environment must support. This is consistent with the cloud shared-responsibility approach: although security activities are divided between the customer and service provider according to the service model, the consumer remains accountable for making risk-based decisions about its data and for defining the protection objectives it needs. NIST notes that organizations remain ultimately accountable for maintaining the security and privacy of data placed in public cloud environments and must assess provider controls against their own requirements. The Cloud Security Alliance likewise frames cloud governance around the customer's responsibility to understand requirements and manage cloud-related risk. See NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing and the Cloud Security Alliance Security Guidance v4.

QUESTION NO: 38

An organization needs to evaluate the effectiveness of security controls implemented on a new system. Which of the following roles should the organization entrust to conduct the evaluation?

A. Authorizing Official (AO).

B. System owner.

C. Control assessor.

D. Information System Security Officer (ISSO).

ANSWER: C

Explanation:

Control assessor is the appropriate role because this function is specifically responsible for evaluating whether security and privacy controls have been implemented correctly, operate as intended, and achieve the required security outcomes. A control assessment is evidence based: the assessor examines documentation and configurations, interviews responsible personnel, and tests technical or procedural controls. The resulting assessment findings identify control weaknesses, deficiencies, and residual risk, giving organizational leadership reliable information for risk decisions and system authorization.

Independence and objectivity are important characteristics of this role. The evaluator should be sufficiently separate from the personnel who implemented or operate the controls so that the assessment provides credible assurance rather than a self-

review. This supports sound governance, accountability, and defensible authorization decisions. NIST describes control assessors as conducting comprehensive assessments of implemented controls and documenting results to support ongoing authorization and risk management. See NIST SP 800-37 Rev. 2 and NIST SP 800-53A Rev. 5.

QUESTION NO: 39

In what way can violation of clipping levels assist in violation tracking and analysis?

A. Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.

B. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.

C. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status.

D. Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations.

ANSWER: A

Explanation:

Clipping levels establish a threshold for behavior that is ordinarily expected or tolerated, such as a limited number of routine user errors. When activity exceeds that defined threshold, the violation is significant enough to be recorded, flagged, or escalated for review. This makes violation tracking more useful because analysts can concentrate on patterns that depart from the established baseline rather than being overwhelmed by isolated, low-value events. For example, a small number of failed authentication attempts may be normal, while repeated failures crossing the clipping level can create an audit record or alert that supports investigation of possible password guessing, misuse, or user training issues. The resulting records provide evidence for determining who performed the activity, when it occurred, how often it occurred, and what circumstances contributed to the threshold being exceeded. This supports both operational monitoring and later forensic or compliance analysis. NIST log-management guidance emphasizes defining logging, analysis, and alerting processes that produce actionable information, while continuous-monitoring practices use thresholds and indicators to identify conditions requiring assessment. See NIST SP 800-92, Guide to Computer Security Log Management and NIST SP 800-137, Information Security Continuous Monitoring.

QUESTION NO: 40

To protect auditable information, which of the following MUST be configured to only allow read access?

A. Logging configurations

B. Transaction log files

C. User account configurations

D. Access control lists (ACL)

ANSWER: B

Explanation:

Transaction log files are the correct choice because they contain the audit trail: recorded events, transactions, timestamps, identities, actions, and outcomes that may be needed for monitoring, investigations, compliance evidence, and recovery activities. Protecting this evidence requires preventing unauthorized alteration, deletion, or overwriting after events have been recorded. Configuring transaction log files so that ordinary users and reviewers have read-only access preserves the integrity and reliability of the recorded information while still permitting authorized personnel to inspect it. In practice, the logging process or a tightly controlled service identity requires narrowly scoped write or append capability to create records; that privilege should not be broadly granted to users who consume or review the logs. This separation supports

accountability because evidence remains trustworthy when an incident, suspected misuse, or control failure must be reconstructed. NIST SP 800-53 control AU-9 specifically requires protection of audit information and controls access to it, including protection from unauthorized modification and deletion. NIST's AU-9: Protection of Audit Information control describes these requirements, and the related AU-11: Audit Record Retention control reinforces retaining audit records for defined periods.

QUESTION NO: 41

A hospital has allowed virtual private networking (VPN) access to remote database developers. Upon auditing the internal configuration, the network administrator discovered that split-tunneling was enabled. What is the concern with this configuration?

A. The network intrusion detection system (NIDS) will fail to inspect Secure Sockets Layer (SSL) traffic.

B. Remote sessions will not require multi-layer authentication.

C. Remote clients are permitted to exchange traffic with the public and private network.

D. Multiple Internet Protocol Security (IPSec) tunnels may be exploitable in specific circumstances.

ANSWER: C

Explanation:

Remote clients are permitted to exchange traffic with the public and private network. This is the defining security concern of VPN split tunneling. With split tunneling enabled, traffic intended for the hospital's internal network is sent through the VPN tunnel, while traffic for Internet destinations continues through the remote developer's local network connection. Consequently, the endpoint is connected simultaneously to a trusted private environment and a potentially untrusted public or local network. If the remote device is compromised, or if its local network is hostile, it can become a bridge or pivot point through which an attacker attempts to access hospital systems over the established VPN connection. This weakens the organization's ability to apply centralized inspection, egress filtering, and monitoring consistently to all traffic from that endpoint. The risk is particularly important for remote database developers because their access may reach sensitive systems containing regulated patient information. Organizations commonly disable split tunneling for privileged access, or compensate with managed-device requirements, endpoint detection and response, host firewalls, network access controls, and strong authentication. Microsoft's VPN security guidance discusses the security implications of VPN configurations, and Cisco describes how split tunneling permits simultaneous VPN and direct Internet connectivity.

QUESTION NO: 42

One of Canada's leading pharmaceutical firms recently hired a Chief Data Officer (CDO) to oversee its data privacy program. The CDO has discovered the firm's marketing department has been collecting information from individuals without their knowledge and consent via the company website. Which of the following privacy regulations should concern the CDO regarding this practice?

A. The Health Insurance Portability and Accountability Act (HIPAA).

B. The Privacy Act of 1974.

C. The Fair Information Practice Principles (FIPPs).

D. The Personal Information Protection and Electronic Documents Act (PIPEDA).

ANSWER: D

Explanation:

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the relevant Canadian federal private-sector privacy law for an organization collecting personal information during commercial activities. PIPEDA's fair information principles require an organization to identify the purposes for collecting personal information at or before collection and obtain meaningful consent, subject to limited statutory exceptions. Website collection by a pharmaceutical company's

marketing function is a commercial activity, so collecting individuals' information without their knowledge or consent raises a direct PIPEDA compliance concern.

Meaningful consent depends on providing information in a form the individual can reasonably understand, including what information is collected, the purposes of collection, and any material consequences. The appropriate form of consent depends on contextual factors, notably the sensitivity of the information and the individual's reasonable expectations. This is especially important for a pharmaceutical firm because online marketing data may reveal or be associated with health-related interests, which can elevate sensitivity. The CDO should therefore ensure transparent privacy notices, documented purposes, and consent mechanisms that are appropriate to the data and intended uses. See Canada's Personal Information Protection and Electronic Documents Act and the Office of the Privacy Commissioner of Canada's guidance on meaningful consent.

QUESTION NO: 43

A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

A. Provide students with Internet Protocol Security (IPSec) Virtual Private Network (VPN) client software.

B. Use Secure Sockets Layer (SSL) VPN technology.

C. Use Secure Shell (SSH) with public/private keys.

D. Require students to purchase home router capable of VPN.

ANSWER: B

Explanation:

Use Secure Sockets Layer (SSL) VPN technology is the best choice because it supports remote access with minimal endpoint administration and broad compatibility for a large, diverse student population. An SSL VPN, more commonly described today as a TLS VPN, can provide secure encrypted access through a standard web browser for portal-based services, or through a lightweight client when specific applications require it. This substantially reduces the burden of distributing, configuring, updating, and troubleshooting full VPN software across thousands of personally owned devices with differing operating systems and security configurations.

For a university, browser-based access also enables centralized management: access policies, authentication requirements, and authorization to particular university resources can be maintained at the VPN gateway rather than individually configured on student devices. The university can integrate the service with institutional identity systems and multifactor authentication, apply granular access controls, and make services available without requiring students to acquire or manage specialized home-network equipment. This combination of centralized control, simple user onboarding, and support for unmanaged endpoints directly satisfies the requirements for low maintenance and ease of deployment. NIST's remote-access guidance discusses the need to secure and centrally manage remote-access technologies, while the CISSP exam outline includes secure remote-access concepts within Communication and Network Security. See NIST SP 800-46 Rev. 2 and the ISC2 CISSP Examination Outline.

QUESTION NO: 44

What is the PRIMARY objective of the post-incident phase of the incident response process in the security operations center (SOC)?

A. improve the IR process.

B. Communicate the IR details to the stakeholders.

C. Validate the integrity of the IR.

D. Finalize the IR.

ANSWER: A

Explanation:

The primary objective of the post-incident phase is to **improve the IR process.** After operational response activities have concluded, the organization should convert the incident experience into measurable improvements to its incident-handling capability and overall security posture. This includes conducting a lessons-learned review; documenting the incident's timeline, root cause, impact, decisions, and outcomes; identifying control or process gaps; and tracking corrective actions through completion. Findings can lead to updates to incident response plans, playbooks, escalation paths, monitoring and detection use cases, technical controls, training, and exercises. The purpose is not simply to close an administrative record, but to reduce the probability, scope, and impact of similar future incidents while improving response speed and effectiveness. NIST describes post-incident activity as including lessons learned and using the results to improve incident response procedures and security controls. This continuous-improvement focus aligns with the CISSP Security Operations domain's incident-handling expectations. See NIST's Computer Security Incident Handling Guide (SP 800-61 Rev. 2) and ISC2's CISSP Certification Exam Outline.

QUESTION NO: 45

Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this IAM action?

A. Clothing retailer acts as User Self Service, confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

B. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends a signed assertion or token to partner businesses that act as service providers and allow access to services.

C. Clothing retailer acts as Service Provider, confirms identity of user using industry standards, then sends credentials to partner businesses that act as an identity provider (IdP) and allows access to resources.

D. Clothing retailer acts as Access Control Provider, confirms access of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to resources.

ANSWER: B

Explanation:

Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends a signed assertion or token to partner businesses that act as service providers and allow access to services. This reflects federated, or extended, identity management: the employee's home organization maintains the authoritative identity and performs authentication, while external partner organizations rely on that authentication result to provide access to their own applications and resources.

In this flow, the identity provider authenticates the employee and issues a cryptographically protected assertion or token containing identity information and, where appropriate, attributes or claims. The partner service provider receives and validates the assertion or token according to the agreed federation protocol, such as SAML or OpenID Connect. It then uses the validated identity and claims to apply its own authorization rules before granting access. This model supports cross-organizational access without requiring each partner to maintain the employee's password or duplicate the retailer's identity-proofing process. It also permits interoperability where the organizations' underlying IAM implementations differ, provided they support common federation standards. SAML defines the exchange of security assertions between identity and service providers, while OpenID Connect specifies an identity layer built on OAuth 2.0. See the OASIS SAML 2.0 Core specification and the OpenID Connect Core specification.

QUESTION NO: 46

An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

A. Limits and scope of the testing.

B. Physical location of server room and wiring closet.

C. Logical location of filters and concentrators.

D. Employee directory and organizational chart.

ANSWER: A

Explanation:

Limits and scope of the testing. is correct because an authorized penetration test must begin with clear, written authorization and mutually agreed rules of engagement. The organization provides the test scope to define the permitted targets, such as networks, applications, facilities, or cloud resources, as well as exclusions and prohibited activities. It also establishes boundaries for test timing, acceptable techniques, handling of sensitive data, communications and escalation contacts, evidence collection, reporting requirements, and conditions requiring the test to pause or stop. These limits ensure that the tester's actions remain authorized and that testing produces useful results without creating unacceptable operational, legal, safety, or business risk. In CISSP terms, penetration testing is an authorized form of security assessment; its scope and rules of engagement distinguish it from unauthorized activity. The scope should be sufficiently specific to enable the firm to plan and execute the assessment while ensuring the organization retains control over what systems and actions are in bounds. The resulting agreement provides accountability for both the organization and the security services firm. See the ISC2 CISSP Exam Outline for security assessment and testing coverage, and NIST's SP 800-115, Technical Guide to Information Security Testing and Assessment for planning, authorization, and rules-of-engagement considerations.

QUESTION NO: 47

What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?

A.Accountability controls

B. Mandatory access controls

C. Assurance procedures

D. Administrative controls.

Answer: C

Explanation:

A. Mandatory access controls

B. Assurance procedures

C. Administrative controls.

D. Accountability controls

ANSWER: B

Explanation:

Assurance procedures are correct because assurance is the confidence, supported by evidence, that an information system's security controls correctly enforce its stated security policy. This confidence is not limited to a point-in-time implementation decision. It is established and maintained throughout the system development life cycle, including security requirements definition, architecture and design review, implementation, testing, authorization, configuration and change management, ongoing assessment, monitoring, maintenance, and retirement. Assurance activities verify that the implemented mechanisms match the policy and continue to do so as the system, its environment, threats, and operational requirements change. In a CISSP context, assurance connects the intended security objectives to demonstrable evidence that safeguards operate correctly and consistently over time. A system can have well-defined policies and selected controls, but assurance procedures provide the validation, verification, and continued oversight needed to establish justified confidence that those mechanisms implement policy as intended for the full life cycle. NIST frames trustworthy secure-system engineering as an integrated life-cycle activity in NIST SP 800-160, Volume 1. Similarly, the RMF defines life-cycle

activities for selecting, implementing, assessing, authorizing, and continuously monitoring controls in NIST SP 800-37 Rev. 2.

QUESTION NO: 48

Which element of software supply chain management has the GREATEST security risk to organizations?

A. Unsupported libraries are often used.

B. Applications with multiple contributors are difficult to evaluate.

C. Vulnerabilities are difficult to detect.

D. New software development skills are hard to acquire.

ANSWER: A

Explanation:

Unsupported libraries are often used. This presents the greatest security risk because an unsupported dependency no longer has a dependable maintainer responsible for issuing security fixes, testing compatibility, or responding to newly disclosed vulnerabilities. Applications commonly inherit substantial functionality from direct and transitive third-party components, so an unmaintained library can remain embedded throughout development, build, and production environments long after its support ends. If a vulnerability is discovered in that component, the organization may have no patch path other than replacing or extensively refactoring the dependency, which can be slow and operationally risky.

From a CISSP risk-management perspective, unsupported components create sustained exposure: publicly known flaws can be readily identified and targeted by attackers, while incomplete component inventories can delay discovery of where the vulnerable library is used. Effective software supply chain management therefore requires maintaining a component inventory or software bill of materials, tracking component lifecycle and support status, monitoring vulnerability disclosures, and promptly upgrading, replacing, or isolating unsupported dependencies. NIST's Secure Software Development Framework calls for managing third-party software components and responding to vulnerabilities throughout the software lifecycle. NIST also identifies software supply chain risks associated with components that are no longer supported or maintained. See NIST SP 800-218, Secure Software Development Framework and CISA: Software Bill of Materials (SBOM).

QUESTION NO: 49

Which of the following statements pertaining to disaster recovery planning is incorrect?

A. Every organization must have a disaster recovery plan.

B. A disaster recovery plan contains actions to be taken before, during and after a disruptive event.

C. The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.

D. A disaster recovery plan should cover return from alternate facilities to primary facilities.

ANSWER: A

Explanation:

Every organization must have a disaster recovery plan is the incorrect statement because disaster recovery planning is not a universal, one-size-fits-all requirement. An organization's continuity and recovery capabilities must be selected through business impact analysis and risk assessment. The scope of those capabilities depends on the organization's mission, reliance on information systems, critical processes, threat environment, legal or contractual obligations, recovery objectives, and available resources. For example, an organization with no internally operated technology services may address its recovery needs through supplier arrangements, manual workarounds, contractual service-level commitments, or broader continuity procedures rather than maintaining a distinct, formal IT disaster recovery plan.

ISC2-aligned practice is to ensure that appropriate and proportionate recovery strategies exist for business-critical services, not to impose an identical disaster recovery plan on every organization regardless of risk. NIST contingency-planning guidance likewise directs organizations to conduct a business impact analysis, identify preventive controls, develop recovery strategies, and create plans appropriate to the system and organizational requirements. This risk-based approach supports recovery capabilities that meet defined recovery time and recovery point objectives while avoiding unsupported categorical requirements. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and Ready.gov guidance on business continuity planning.

QUESTION NO: 50

The stringency of an Information Technology (IT) security assessment will be determined by the

A. system's past security record.

B. size of the system's database.

C. sensitivity of the system's data.

D. age of the system.

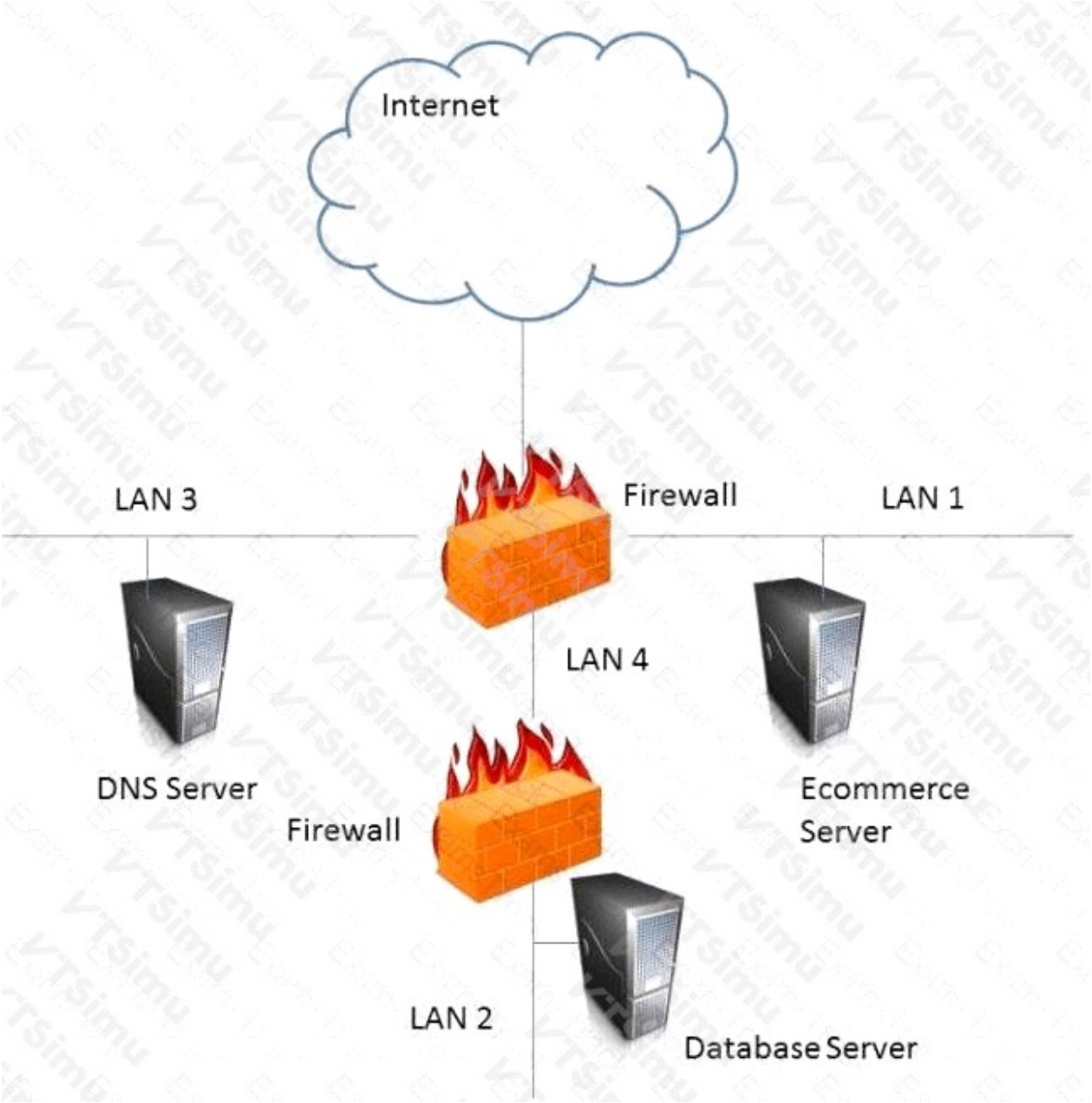
ANSWER: C

Explanation:

The correct answer is **sensitivity of the system's data.** Assessment stringency should be commensurate with the risk associated with the information system, particularly the potential impact of a loss of confidentiality, integrity, or availability. Data sensitivity is a central input to that determination because it reflects the harm that unauthorized disclosure, alteration, or loss could cause to the organization, individuals, operations, or other affected parties. A system that processes highly sensitive information therefore requires more rigorous assessment procedures, greater assessment depth and coverage, stronger evidence, and closer scrutiny of implemented security and privacy controls. This risk-based approach ensures that assessment resources are directed toward systems where control failure would have the greatest consequence. FIPS 199 establishes that information and information systems are categorized according to the potential impact of security objectives being compromised; those impact levels drive proportionate security requirements. NIST assessment guidance likewise frames assessment procedures around the controls selected according to the system’s security and privacy requirements. See NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and NIST SP 800-53A Rev. 5, Assessing Security and Privacy Controls.

QUESTION NO: 51 - (SIMULATION)

In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?



ANSWER: See the explanation for the answer

Explanation:

Deploy the contractor WAP on LAN 4.

LAN 4 is the isolated segment between the perimeter firewall and the internal firewall. Placing the WAP here enables firewall rules to permit contractors' Internet access and only explicitly authorized enterprise services, while preventing direct access to the more trusted internal LANs.

LAN 1 hosts the e-commerce server and should not expose that server segment to contractor wireless clients.
LAN 2 contains the database server and is the most sensitive internal segment.
LAN 3 contains DNS infrastructure and should not be used for untrusted contractor access.

Therefore, configure the WAP connection on **LAN 4** and enforce least-privilege access policies at the firewalls.

QUESTION NO: 52

What is the MOST effective method to enhance security of a single sign-on (SSO) solution that interfaces with critical systems?

A. Two-factor authentication.

B. Reusable tokens for application level authentication.

C. High performance encryption algorithms.

D. Secure Sockets Layer (SSL) for all communications.

ANSWER: A

Explanation:

Two-factor authentication is the most effective enhancement because an SSO implementation concentrates authentication at a central identity provider. This provides substantial usability and administrative benefits, but it also means that compromise of one primary credential could grant access to numerous integrated applications, including critical systems. Requiring a second, independent authentication factor materially strengthens the access decision by requiring evidence beyond a password or other memorized secret. For example, a phishing-resistant cryptographic authenticator can help ensure that possession of a stolen password alone does not enable account takeover.

For critical systems, the second factor should be enforced by the identity provider and used consistently for sign-in, privileged access, and sensitive transactions. Organizations can also apply adaptive or step-up authentication when contextual risk increases, while retaining centralized policy enforcement across relying applications. NIST's Digital Identity Guidelines describe multi-factor authentication requirements and emphasize phishing-resistant authentication at higher assurance levels. This supports defense in depth at the primary trust boundary of an SSO architecture, reducing the likelihood that password reuse, credential stuffing, or password phishing leads to broad unauthorized access. See NIST SP 800-63B, Digital Identity Guidelines and CISA guidance on implementing phishing-resistant MFA.

QUESTION NO: 53

What security management control is MOST often broken by collusion?

A. Job rotation

B. Separation of duties

C. Least privilege model

D. Increased monitoring

ANSWER: B

Explanation:

Separation of duties is the security management control most directly undermined by collusion. This control deliberately divides a sensitive process, transaction, or set of privileges among multiple individuals so that no one person can independently complete the entire action. For example, one person may initiate a financial transaction while another must approve it, or an administrator may implement a change that requires separate review and authorization. Its protective value depends on the participating people acting independently and providing meaningful oversight of one another.

Collusion occurs when the individuals assigned separate responsibilities secretly cooperate to circumvent those required checks. Because the participants collectively hold all portions of the process, they can approve, execute, and conceal an unauthorized activity that the separation was intended to prevent. Therefore, separation of duties reduces the opportunity for a single insider to commit fraud or misuse authority, but it cannot fully protect against coordinated misconduct by multiple insiders. This relationship is reflected in control guidance that identifies separation of duties as a control for reducing fraud and error risk and recognizes collusion as a residual risk. See NIST CSRC: separation of duties and ISC2 CISSP Exam Outline.

QUESTION NO: 54

Which of the following is the BEST mitigation from phishing attacks?

A. Network activity monitoring

B. Security awareness training

C. Corporate policy and procedures

D. Strong file and directory permissions

ANSWER: B

Explanation:

Security awareness training is the best mitigation because phishing is a social-engineering attack that targets human judgment rather than solely a technical weakness. Effective training teaches personnel to recognize common phishing indicators, such as unexpected requests for credentials or payments, spoofed sender domains, deceptive links, malicious attachments, and messages designed to create urgency or fear. It should also establish a clear, simple process for reporting suspected messages so the security team can investigate and protect other users quickly.

For best results, awareness training is continuous rather than a one-time compliance exercise. Organizations should reinforce it with realistic phishing simulations, role-specific guidance for higher-risk functions such as finance and administration, and feedback that helps users make safer decisions in real situations. ISC2 identifies security awareness, education, and training as an important administrative control that helps personnel understand threats and fulfill security responsibilities. The CISA phishing guidance similarly emphasizes training users to identify and report phishing. NIST's SP 800-50 describes awareness and training as foundational for reducing human-related security risk.

QUESTION NO: 55

What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

A. ICS often run on UNIX operating systems.

B. ICS often do not have availability requirements.

C. ICS are often sensitive to unexpected traffic.

D. ICS are often isolated and difficult to access.

ANSWER: C

Explanation:

ICS are often sensitive to unexpected traffic. This is the primary consideration because industrial environments control physical processes that frequently have strict real-time, safety, and availability requirements. Many ICS assets—including programmable logic controllers, remote terminal units, human-machine interfaces, and older industrial network devices—were not designed to tolerate the volume or characteristics of active IT security-testing traffic. Port scans, service discovery, malformed packets, fuzzing, or high-rate vulnerability scans can consume constrained device resources, interrupt communications, cause a controller or interface to fault, or potentially affect the process being controlled. Security testing therefore must be planned jointly with engineering, operations, and safety personnel, with a tightly defined scope and approved methods. Testing commonly emphasizes passive asset discovery and monitoring where possible, uses representative lab systems for intrusive techniques, and schedules any required active assessment during authorized maintenance windows with rollback and incident-response procedures available. NIST explains that ICS security objectives prioritize safety and availability and that conventional IT assessment methods require careful adaptation to avoid operational impacts. CISA likewise advises organizations to manage assessment activity carefully in operational technology environments. See NIST SP 800-82 Rev. 3, Guide to Operational Technology Security and CISA Industrial Control Systems guidance.

QUESTION NO: 56

Physical Access Control Systems (PACS) allow authorized security personnel to manage and monitor access control for subjects through which function?

A. Remote access administration.

B. Personal Identity Verification (PIV).

C. Access Control List (ACL)

D. Privileged Identity Management (PIM).

ANSWER: A

Explanation:

Remote access administration is correct because a Physical Access Control System is designed to give authorized security personnel centralized operational control over physical-entry permissions and related events. Through a management workstation, client application, or protected web interface, administrators can administer credential holders, assign or change access privileges, establish time-based access schedules, disable lost or revoked credentials, and review access activity without having to be physically present at each door or facility. PACS management platforms also commonly provide monitoring capabilities, including controller and reader status, forced-door or door-held alarms, access-event logs, and reporting. This centralized and often network-enabled administrative function supports consistent enforcement of physical-access policy across one or many locations, while retaining audit records for investigation and accountability. NIST describes physical access control systems as mechanisms for controlling entry and supporting the management of physical access credentials and authorization decisions. Its guidance on identity credentials and access control further addresses the use of systems and processes that manage physical access privileges. See NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems and NIST SP 800-53, Physical and Environmental Protection controls.

QUESTION NO: 57

What is the BEST location in a network to place Virtual Private Network (VPN) devices when an internal review reveals network design flaws in remote access?

A. In a dedicated Demilitarized Zone (DMZ)

B. In its own separate Virtual Local Area Network (VLAN)

C. At the Internet Service Provider (ISP)

D. Outside the external firewall

ANSWER: A

Explanation:

In a dedicated Demilitarized Zone (DMZ) is the best placement because a VPN gateway is an internet-facing service that must accept connections from untrusted external networks while providing controlled access to protected internal resources. A dedicated DMZ creates a separate security zone for the VPN device, allowing firewall policies to tightly restrict traffic entering from the internet and traffic permitted onward to internal networks. This segmentation supports defense in depth: compromise of the VPN gateway does not automatically place an attacker directly on the internal network.

The DMZ design also enables administrators to apply distinct monitoring, logging, intrusion-detection, authentication, and access-control policies to remote-access traffic. After a remote user authenticates and the encrypted tunnel terminates at the VPN device, only explicitly authorized connections should be allowed from that security zone to the required internal applications or network segments. This placement limits exposure, reduces lateral-movement opportunities, and makes the trust boundary for remote access clear and enforceable. NIST's remote-access guidance emphasizes controlled remote access, strong authentication, and appropriate boundary protection; its network-security guidance describes DMZs as isolated perimeter subnetworks for systems requiring external connectivity. See NIST SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and BYOD Security and NIST SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy.

QUESTION NO: 58

Which of the following goals represents a modern shift in risk management according to National Institute of Standards and Technology (NIST)?

A. Provide an improved mission accomplishment approach.

B. Focus on operating environments that are changing, evolving, and full of emerging threats.

C. Enable management to make well-informed risk-based decisions justifying security expenditure.

D. Secure information technology (IT) systems that store, mass, or transmit organizational information.

ANSWER: B

Explanation:

Focus on operating environments that are changing, evolving, and full of emerging threats represents the modern NIST risk-management shift because risk is not a fixed condition that can be addressed only through periodic assessments or a one-time authorization decision. NIST's Risk Management Framework integrates risk-management activities throughout the system development life cycle and emphasizes continuous monitoring of controls, system changes, threats, vulnerabilities, and organizational risk posture. This allows risk information to remain current as missions, technologies, interconnections, supply-chain dependencies, and adversary capabilities change.

NIST also describes information-security risk management as an organization-wide, ongoing process that supports mission and business objectives. In this approach, leaders and system owners use timely risk information to adapt safeguards and risk responses as the operating context evolves. The emphasis on a dynamic environment is therefore central to modern risk management: security and privacy activities must continuously account for emerging threats and changing conditions while sustaining resilient organizational operations. This perspective is documented in NIST SP 800-37 Rev. 2, Risk Management Framework and NIST SP 800-39, Managing Information Security Risk.

QUESTION NO: 59

What can be BEST defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?

A. Risk management

B. Risk analysis.

C. Threat analysis.

D. Due diligence.

ANSWER: C

Explanation:

Threat analysis. is correct because the wording describes the focused activity of relating potential threat sources to known or potential vulnerabilities in a specific information system and its actual operating context. The purpose is to identify the threats that are relevant to that system, rather than merely listing generic hazards or adversaries. A threat source may be intentional, accidental, environmental, or structural; its relevance depends on whether it could exploit a vulnerability under the system's particular technical, physical, organizational, and operational conditions.

This use of the term is consistent with NIST risk-assessment terminology. NIST defines threat analysis as examining threat sources against vulnerabilities to determine threats for a particular system in a particular operational environment. That resulting system-specific understanding supplies essential input to subsequent risk determination, including estimates of likelihood and adverse impact. In CISSP practice, this distinction matters because security assessments must be grounded in the assets, exposure, controls, dependencies, and environment actually being evaluated. A generic threat catalog alone does not establish which threats apply; threat analysis makes that connection between source, vulnerability, and system context. See the NIST CSRC definition of threat analysis and NIST SP 800-30 Rev. 1.

QUESTION NO: 60

Which of the following are the FIRST two steps to securing employees from threats involving workplace violence and acts of terrorism?

A. Physical barriers impeding unauthorized access and security guards at each entrance.

B. Physical barriers and the ability to identify people as they enter the workplace.

C. Security guards and metal detectors posted at each entrance.

D. Metal detectors and the ability to identify people as they enter the workplace.

ANSWER: B

Explanation:

Physical barriers and the ability to identify people as they enter the workplace are the foundational first measures because they establish an enforceable boundary and a controlled decision point for admission. Barriers such as perimeter fencing, exterior doors, gates, turnstiles, and reception boundaries deter and delay unauthorized entry, while also directing entrants through designated access points. At those points, identification measures—including employee credentials, visitor registration, badge checks, and access-control authentication—allow personnel or systems to distinguish authorized people from unknown or unauthorized individuals before granting access to the facility or sensitive areas.

This reflects the CISSP physical-security principle of defense in depth: controls at the perimeter and entry point reduce exposure early, create accountability for who is present, and support subsequent monitoring and incident response. Effective workplace-violence and terrorism risk reduction begins with managing access to the site, rather than assuming every person who reaches an entrance is entitled to proceed. CISA's physical-security guidance emphasizes layered protective measures and access control as key components of facility protection, while OSHA identifies workplace-violence prevention as requiring practical controls tailored to the work environment. See CISA Physical Security and OSHA Workplace Violence.

QUESTION NO: 61

A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed

to have gratuitous Address Resolution Protocol (ARP) disabled.

Why did the network architect likely design the VoIP system with gratuitous ARP disabled?

A. Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1.

B. Gratuitous ARP requires the use of insecure layer 3 protocols.

C. Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone.

D. Gratuitous ARP presents a risk of a Man-in-the-Middle (MITM) attack.

ANSWER: D

Explanation:

Gratuitous ARP presents a risk of a Man-in-the-Middle (MITM) attack because it is an unsolicited ARP announcement that can cause hosts on the local broadcast domain to update their ARP caches. ARP normally maps an IPv4 address to a Layer 2 MAC address, but it has no inherent authentication mechanism to verify that an ARP announcement genuinely came from the owner of the claimed IP address. An attacker able to send forged gratuitous ARP messages on the voice VLAN can attempt to associate the IP address of a VoIP endpoint, gateway, or call-control service with the attacker's MAC address. This can redirect local traffic through the attacker, enabling interception or manipulation of signaling and, where media protection is absent or insufficient, voice traffic. Disabling gratuitous ARP is therefore a defensive design decision intended to reduce opportunities for ARP-cache poisoning in the VoIP environment. RFC 5227 describes ARP announcements and notes that hosts may update cached link-layer mappings after receiving them. In enterprise networks, this control is commonly complemented by switch protections such as Dynamic ARP Inspection, which validates ARP packets against trusted binding information. See RFC 5227: IPv4 Address Conflict Detection and Cisco's Dynamic ARP Inspection overview.

QUESTION NO: 62

Which of the following is the BEST reason for writing an information security policy?

A. To support information security governance

B. To reduce the number of audit findings

C. To deter attackers

D. To implement effective information security controls

ANSWER: A

Explanation:

To support information security governance is the best reason for writing an information security policy. Governance establishes the direction, oversight, accountability, and decision-making structure through which an organization manages information-security risk in alignment with its business objectives and risk appetite. An approved policy expresses management's intent and commitment; it defines the organization's high-level security requirements, assigns responsibilities, and provides the authority for supporting standards, procedures, and control implementation. It therefore gives the security program a consistent, management-sanctioned basis for directing behavior and evaluating whether security activities meet organizational expectations. Policies should be approved by appropriate leadership, communicated to relevant personnel, and reviewed as business, technology, regulatory, and risk conditions change. This governance purpose is broader and more fundamental than any particular operational result: it enables accountable management of the security program across the organization. NIST describes policies as management directives that establish roles, responsibilities, and compliance requirements within an information security program, while ISO/IEC 27001 requires top management to establish an information security policy appropriate to the organization's purpose and direction. See NIST SP 800-12 Rev. 1 and ISO/IEC 27001.

QUESTION NO: 63

An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is MOST effective for the SMP?

A. Security controls driven assessment that focuses on controls management.

B. Business processes based risk assessment with a focus on business goals.

C. Asset driven risk assessment with a focus on the assets.

D. Data driven risk assessment with a focus on data.

ANSWER: B

Explanation:

Business processes based risk assessment with a focus on business goals is the most effective approach because a Security Management Program must be driven by the organization's mission, objectives, risk appetite, and operational priorities. Assessing risk through business processes identifies the services and activities the organization depends on, the stakeholders affected by disruption, and the consequences that matter to management, such as financial loss, regulatory exposure, safety impacts, service interruption, and reputational damage. This creates a defensible basis for deciding which risks require treatment first and for selecting safeguards proportionate to business impact.

A business-process perspective also supports effective governance. It enables security objectives, control investments, accountability, and performance measures to be connected directly to outcomes executives and process owners understand. The resulting program can be integrated with enterprise risk management and adjusted as business operations, threats, dependencies, and priorities change. NIST risk-assessment guidance emphasizes that risk is determined by the potential adverse impact on organizational operations, assets, and individuals, supporting a context-driven assessment of business consequences. ISO 31000 likewise frames risk management around achieving objectives and integrating risk practices into organizational activities and decision-making. See NIST SP 800-30 Rev. 1 and ISO 31000 Risk Management.

QUESTION NO: 64

Which of the following statements pertaining to PPTP (Point-to-Point Tunneling Protocol) is NOT true?

A. PPTP allows the tunneling of any protocols that can be carried within PPP.

B. PPTP does not provide strong encryption.

C. PPTP does not support any token-based authentication method for users.

D. PPTP is derived from L2TP.

ANSWER: D

Explanation:

PPTP is derived from L2TP is the statement that is not true. The historical relationship runs in the opposite direction: PPTP was an earlier tunneling protocol, documented by the PPTP Forum in 1999, whereas L2TP was developed from work involving both Cisco Layer 2 Forwarding and elements of Microsoft PPTP. L2TP was subsequently standardized by the IETF as a separate Layer 2 tunneling protocol. PPTP establishes a control channel over TCP and carries PPP frames using GRE; its use of PPP permits the transport of network-layer protocols supported by PPP. This protocol lineage is relevant because PPTP is a legacy VPN technology with well-known security limitations, while L2TP is ordinarily deployed with IPsec to supply confidentiality, integrity, and peer authentication. The IETF's L2TP specification explicitly describes L2TP as combining features of L2F and PPTP, rather than describing PPTP as a derivative of L2TP. See RFC 2661, Layer Two Tunneling Protocol and the PPTP Forum specification (RFC 2637).

QUESTION NO: 65

Which of the following is a major component of the federated identity management (FIM) implementation model and used to establish a network between dozens of organizations?

A. Identity as a Service (IDaaS)

B. Attribute-based access control (ABAC)

C. Cross-certification.

D. Trusted third party (TTP).

ANSWER: C

Explanation:

Cross-certification is correct because it is a PKI-based federation approach that establishes trust among independent organizations without requiring a single organization to own every participant's identity infrastructure. Under this model, certification authorities from participating organizations create certification relationships with one another. These relationships allow a relying party in one organization to build and validate a certification path to a user's certificate issued under another organization's PKI. The result is a scalable trust network in which participants can recognize credentials originating outside their own administrative domain.

This approach is particularly associated with federated environments involving multiple autonomous organizations, such as business partners, government entities, or consortium members. Rather than replacing each organization's local identity authority, cross-certification connects those authorities through documented, cryptographically verifiable trust relationships. Certificate policies and path-validation rules govern the extent to which credentials may be accepted across the federation. NIST describes cross-certification as a mechanism for establishing trust between PKI domains in its Introduction to Public Key Technology and the Federal PKI Infrastructure. The certificate-path concepts that make this trust validation possible are standardized in RFC 5280.

QUESTION NO: 66

When designing a new Voice over Internet Protocol (VoIP) network, an organization's top concern is preventing unauthorized users accessing the VoIP network.

Which of the following will BEST help secure the VoIP network?

A. 802.11g.

B. Web application firewall (WAF)

C. Transport Layer Security (TLS)

D. 802.1x.

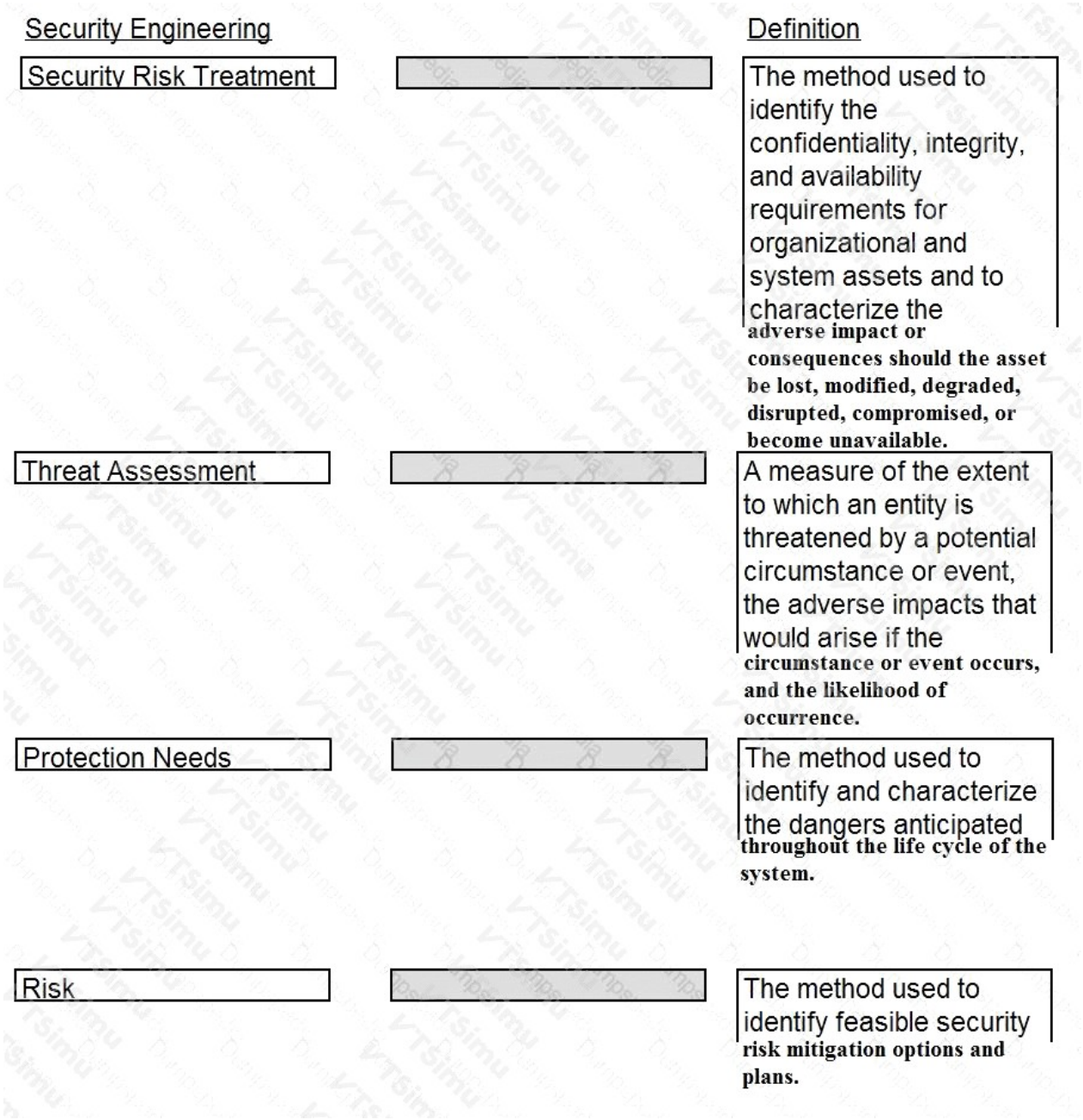
ANSWER: D

Explanation:

802.1X is the best control because the stated security objective is to prevent unauthorized devices or users from obtaining access to the VoIP network. IEEE 802.1X provides port-based network access control: before an endpoint connected to a switch port is granted normal network access, it must authenticate successfully to an authentication service, commonly using EAP and a RADIUS server. This is particularly valuable in a VoIP deployment at the access layer, where an IP phone—and sometimes a workstation connected through that phone—may be physically connected to an available Ethernet jack. Authentication allows the organization to enforce identity-based admission decisions before allowing access to voice-network resources. Following successful authentication, the network can apply authorized connectivity parameters, such as assigning the appropriate VLAN or enforcing policy-based access restrictions. This makes 802.1X a foundational control against rogue or unapproved endpoints joining the environment. The Extensible Authentication Protocol framework used with 802.1X is defined in RFC 3748. For practical implementation concepts, including the roles of supplicant, authenticator, and authentication server, see Cisco's 802.1X authentication overview.

QUESTION NO: 67 - (SIMULATION)

Drag the following Security Engineering terms on the left to the BEST definition on the right.



ANSWER: See the explanation for the answer

Explanation:

Correct drag-and-drop matches:

Security Risk Treatment → "The method used to identify feasible security risk mitigation options and plans."
Threat Assessment → "The method used to identify and characterize the dangers anticipated throughout the life cycle of the system."
Protection Needs → "The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable."
Risk → "A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence."

The key distinction is that **risk** combines potential adverse impact with likelihood, while **threat assessment** identifies and characterizes anticipated dangers. **Protection needs** establish CIA requirements and consequences of asset loss or compromise.

QUESTION NO: 68

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

What MUST the access control logs contain in addition to the identifier?

A. Time of the access

B. Security classification

C. Denied access attempts

D. Associated clearance

ANSWER: A

Explanation:

Time of the access is required in addition to the identifier because an access-control record must establish both *who* performed an activity and *when* it occurred. A timestamp gives each authentication, authorization, or resource-access event a position in a reliable chronological sequence. This allows reviewers to reconstruct activity during independent audits, correlate access events with system, network, and application logs, and establish an incident timeline when investigating suspected misuse. It also supports accountability by associating a uniquely identified subject with a specific event at a specific time, rather than merely showing that the subject had a session or entitlement at some unspecified point. For timestamps to be useful across wired, wireless, remote, and branch-office environments, systems should synchronize clocks to an authoritative time source and consistently record the relevant date, time, and time zone or equivalent offset. NIST guidance identifies the date and time of an event as fundamental log-record information and emphasizes time synchronization to enable correlation among records from different sources. These practices support the CISSP objectives of auditability, accountability, monitoring, and effective investigation. See NIST SP 800-92, Guide to Computer Security Log Management and NIST SP 800-53, Audit and Accountability controls.

QUESTION NO: 69

What is the BEST approach for maintaining ethics when a security professional is

unfamiliar with the culture of a country and is asked to perform a questionable task?

A. Exercise due diligence when deciding to circumvent host government requests.

B. Become familiar with the means in which the code of ethics is applied and considered.

C. Complete the assignment based on the customer's wishes.

D. Execute according to the professional's comfort level with the code of ethics.

ANSWER: B

Explanation:

Become familiar with the means in which the code of ethics is applied and considered. is the best approach because ethical conduct requires both adherence to professional principles and an informed understanding of the context in which work is performed. When working in an unfamiliar country, a security professional may encounter different legal requirements, social expectations, business practices, and interpretations of professional responsibilities. Before acting on a questionable request, the professional should research the applicable local laws and regulations, understand relevant cultural considerations, and seek informed guidance through appropriate organizational, legal, or professional channels. This enables a decision that respects local context without abandoning core professional duties such as protecting society, acting honorably, providing diligent service, and advancing the profession.

The ISC2 Code of Ethics is intended to guide members' professional judgment and conduct, including when circumstances are complex or uncertain. Familiarity with how ethical standards are applied in the local environment helps the professional identify conflicts, document concerns, escalate matters appropriately, and make a defensible decision grounded in both ethical obligations and applicable requirements. See the ISC2 Code of Ethics and the CISSP examination outline.

QUESTION NO: 70

Which of the following is the MOST effective corrective control to minimize the effects of a physical intrusion?

A. Rapid response by guards or police to apprehend a possible intruder.

B. Sounding a loud alarm to frighten away a possible intruder.

C. Automatic videotaping of a possible intrusion.

D. Activating bright lighting to frighten away a possible intruder.

ANSWER: A

Explanation:

Rapid response by guards or police to apprehend a possible intruder is the most effective corrective control because it is an active response taken after an intrusion is detected or underway. Corrective controls are intended to contain an incident, limit its consequences, restore a secure condition, and support recovery. A prompt, trained guard or law-enforcement response can physically intervene, prevent further access to protected areas or assets, preserve the scene, initiate escalation procedures, and reduce the time available for theft, sabotage, or compromise. Its effectiveness depends on response time, defined procedures, reliable communications, and personnel authorized and prepared to act. In a layered physical-security program, detection mechanisms are valuable only when they trigger an effective response capability; this response is what directly reduces the intrusion's impact. NIST describes physical and environmental protection controls, including monitoring and response-related capabilities, in NIST SP 800-53 Rev. 5, Update 1. NIST incident-response guidance likewise emphasizes containment as a core activity for limiting the scope and impact of an event; see NIST SP 800-61 Rev. 2.

QUESTION NO: 71

For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

A. Hash functions

B. Data segregation

C. File system permissions

D. Non-repudiation controls

ANSWER: B

Explanation:

Data segregation most effectively addresses cloud customers' confidentiality concerns because cloud environments commonly use multitenancy, in which infrastructure, platforms, or services are shared by distinct customers. The provider must enforce logical isolation so that one tenant's users, workloads, processes, storage, backups, and management paths cannot access another tenant's information. Effective segregation is implemented through a combination of strong tenant-aware identity and access controls, network and compute isolation, separate logical storage boundaries, secure virtualization or container controls, and encryption with appropriate key-management practices. These controls reduce the risk of cross-tenant data exposure while allowing the provider to operate shared services at scale. Segregation also supports customers' contractual, privacy, and regulatory obligations by establishing clear boundaries around data handling and access. In a shared-responsibility model, the provider is generally responsible for securing the underlying cloud infrastructure and for delivering service features that enable tenant isolation; customers then configure and use those features appropriately. NIST identifies resource pooling and multitenancy as fundamental cloud characteristics, making isolation between consumers a

central provider security requirement. See NIST SP 800-145, The NIST Definition of Cloud Computing and the CISA Cloud Security guidance.

QUESTION NO: 72

As part of an application penetration testing process, session hijacking can BEST be achieved by which of the following?

A. Known-plaintext attack

B. Denial of Service (DoS)

C. Cookie manipulation

D. Structured Query Language (SQL) injection

ANSWER: C

Explanation:

Cookie manipulation is the best answer because web applications commonly use a session identifier stored in a browser cookie to associate subsequent HTTP requests with an authenticated user session. If an authorized penetration test demonstrates that a session cookie can be obtained, predicted, modified, or replayed without adequate server-side validation and session controls, the tester may be able to submit requests in the context of the legitimate user. This is the core mechanism of session hijacking: taking over an already authenticated session by abusing its session token rather than independently authenticating as that user.

Effective session management therefore requires session identifiers with sufficient entropy, secure transport protection, and appropriate cookie attributes. The `Secure` attribute limits cookie transmission to HTTPS connections, while `HttpOnly` helps prevent client-side scripts from reading the cookie. Applications should also regenerate session identifiers after authentication and privilege changes, enforce expiration, and invalidate sessions at logout. These safeguards reduce the likelihood that a captured or manipulated session cookie can be replayed successfully. OWASP's guidance describes session IDs as the link between the user and server-side session state and details the protections needed for secure session handling. See the OWASP Session Management Cheat Sheet and the OWASP session hijacking overview.

QUESTION NO: 73

Which of the following events prompts a review of the disaster recovery plan (DRP)?

A. Change in senior management.

B. Completion of the security policy review.

C. Organizational merger.

D. New members added to the steering committee.

ANSWER: C

Explanation:

Organizational merger. is the correct answer because a disaster recovery plan must be maintained as a living document that reflects the organization's current business requirements, technology environment, dependencies, and risk profile. A merger is a substantial organizational change that can alter all of these plan inputs at once. For example, the combined organization may acquire additional data centers, cloud services, applications, suppliers, personnel, business units, and regulatory obligations. It may also redefine critical business services and their recovery time and recovery point objectives. These changes directly affect recovery strategies, alternate-site arrangements, emergency communications, roles and responsibilities, contact lists, and plan activation procedures. Consequently, the DRP should be reviewed, updated, and then appropriately exercised to ensure that it remains feasible and supports the newly combined organization's recovery priorities. NIST contingency-planning guidance identifies organizational and system changes as circumstances requiring plan maintenance, including updates to ensure plans remain current and effective. This reflects the CISSP principle that continuity

and recovery capabilities must stay aligned with material changes in business operations and supporting assets. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and ISO 22301: Security and resilience — Business continuity management systems.

QUESTION NO: 74

Which of the following initiates the systems recovery phase of a disaster recovery plan?

A. Issuing a formal disaster declaration

B. Activating the organization's hot site

C. Evacuating the disaster site

D. Assessing the extent of damage following the disaster

ANSWER: A

Explanation:

Issuing a formal disaster declaration initiates the systems recovery phase because it is the authorized management decision that activates the disaster recovery plan and commits the organization to recovery actions. Before this declaration, responders may conduct emergency response, protect life and safety, perform initial damage assessment, and gather information needed to determine whether normal operations can be restored within established recovery objectives. Once the authorized individual or team formally declares a disaster, recovery teams can be mobilized, recovery procedures can be executed, vendors and stakeholders can be notified, and alternate processing arrangements can be used where required. This formal authorization is important because recovery can involve substantial cost, contractual commitments, controlled changes, and the use of alternate facilities. The specific recovery capability used—such as an alternate site, replicated environment, backups, or cloud-based recovery resources—depends on the organization's approved recovery strategy; it is not itself the universal initiating event. NIST describes contingency-plan activation and notification as the point at which the organization determines that recovery is required and begins executing recovery procedures. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and ISC2 CISSP Certification Exam Outline.

QUESTION NO: 75

Which software defined networking (SDN) architectural component is responsible for translating network requirements?

A. SDN Controller

B. SDN Datapath

C. SDN Northbound Interfaces

D. SDN Application

ANSWER: A

Explanation:

SDN Controller is responsible for translating network requirements into the policies, forwarding behavior, and device-level instructions needed to implement them. The controller is the logically centralized control-plane entity that maintains a broader view of network state and makes decisions about how traffic should be handled. It receives high-level intent or policy requests from applications through northbound interfaces, interprets those requirements in light of topology and operational constraints, and determines the appropriate network behavior. It then communicates the resulting control instructions to SDN datapaths through southbound interfaces and protocols.

This translation role is central to SDN's separation of the control plane from the data plane: applications describe the desired outcome, while the controller converts that outcome into enforceable network policy and flow-handling rules. RFC 7426 describes the SDN controller as a control-plane entity that manages and controls resources exposed by SDN datapaths. The Open Networking Foundation likewise characterizes the SDN control plane as the layer that provides centralized control and

abstracts underlying network infrastructure. See RFC 7426: SDN Layers and Architecture Terminology and the Open Networking Foundation SDN definition.

QUESTION NO: 76

The stringency of an Information Technology (IT) security assessment will be determined by the

A. system's past security record.

B. size of the system's database.

C. sensitivity of the system's data.

D. age of the system.

ANSWER: C

Explanation:

The **sensitivity of the system's data** determines how stringent an IT security assessment needs to be because the potential impact of a compromise is driven primarily by the value, classification, and criticality of the information being processed, stored, or transmitted. Systems handling highly sensitive information—such as regulated personal data, financial records, authentication data, classified information, or mission-critical business information—require deeper assessment scope and more rigorous testing. The assessment must establish whether safeguards adequately protect the confidentiality, integrity, and availability requirements associated with that data and whether residual risk is acceptable to the organization.

This is consistent with risk-based security assessment practices. NIST defines risk as a function of the likelihood of a threat event and the adverse impact that could result; data sensitivity and information impact directly influence that adverse-impact determination. Higher-impact information systems therefore warrant more comprehensive control assessment, stronger assurance evidence, and greater scrutiny of identified weaknesses. CISSP risk-management principles likewise focus security decisions and control rigor on business impact and the value of information assets. See NIST SP 800-30 Rev. 1 and the ISC2 CISSP Exam Outline.

QUESTION NO: 77

Which of the following Secure Shell (SSH) remote access practices is MOST suited for scripted functions?

A. Restricting authentication by Internet Protocol (IP) address.

B. Requiring multi-factor authentication (MFA).

C. Implementing access credentials management tools.

D. Using public key-based authentication method.

ANSWER: D

Explanation:

Using public key-based authentication method is most suited to scripted SSH functions because it provides strong, non-interactive authentication. Automated jobs, configuration-management processes, scheduled tasks, and deployment pipelines generally cannot depend on a person being present to enter a password or complete an interactive challenge. With public-key authentication, the automated account holds a private key and the SSH server verifies that key against the associated public key configured for the target account. The private key should be protected appropriately, such as through restrictive file permissions, a dedicated service account, secure storage, and managed rotation. Where an interactive session can initialize an agent, a passphrase-protected key and `ssh-agent` provide additional protection. Public-key access can also be constrained to the operational purpose of the script through `authorized_keys` settings, including forced commands, source-address restrictions, and disabling forwarding or pseudo-terminal allocation. These controls support least privilege while retaining the reliability required for unattended execution. OpenSSH documents public-key authentication and

the server-side authorization controls available in the `authorized_keys` file; see the OpenBSD sshd(8) manual and the OpenBSD sshd_config(5) manual.

QUESTION NO: 78

Which of the following is MOST important to follow when developing information security controls for an organization?

A. Use industry standard best practices for security controls in the organization.

B. Exercise due diligence with regard to all risk management information to tailor appropriate controls.

C. Review all local and international standards and choose the most stringent based on location.

D. Perform a risk assessment and choose a standard that addresses existing gaps.

ANSWER: B

Explanation:

Exercise due diligence with regard to all risk management information to tailor appropriate controls is the most important principle because information security controls must be selected in the context of the organization's specific risks, mission, business objectives, legal obligations, assets, threat environment, and risk appetite. Due diligence means decision-makers use relevant and current risk information to make informed, reasonable choices and can demonstrate appropriate care in protecting organizational information and systems. This produces controls that are proportionate to the likelihood and impact of adverse events, practical to operate, and capable of reducing risk to an approved level.

A risk-based process also supports tailoring: controls are not applied as a generic checklist, but are implemented, adjusted, or supplemented according to the organization's architecture, operational needs, inherited controls, and identified risk treatment decisions. This directly reflects the NIST Risk Management Framework, which integrates risk assessment, control selection, implementation, assessment, authorization, and ongoing monitoring. NIST control guidance likewise requires organizations to tailor control baselines and document risk-based decisions. These practices help governance leaders prioritize investment in controls that provide meaningful protection and remain aligned with changing business and threat conditions. See NIST SP 800-37 Rev. 2, Risk Management Framework and NIST SP 800-53 Rev. 5, Security and Privacy Controls.

QUESTION NO: 79

What is the term commonly used to refer to a technique of authentication one machine to another by forging packets from a trusted source?

A. Smurfing.

B. Man-in-the-Middle (MITM) attack.

C. Session redirect.

D. Spoofing.

ANSWER: D

Explanation:

Spoofing. is the correct term. In this context, spoofing means falsifying source-identifying information in network traffic so that a receiving system treats the packets as though they originated from a trusted machine. More specifically, this is commonly called IP spoofing when the forged attribute is the source IP address in an IP packet. The attack takes advantage of trust decisions based on claimed network identity: if a host or service accepts traffic because it appears to come from an authorized peer, forged packets can impersonate that peer.

This concept is particularly important in discussions of legacy host-to-host trust relationships and network protocols that did not strongly authenticate each message with cryptographic protections. A forged source address does not itself prove that an

attacker can complete every interaction, because many protocols require responses or sequence information; nevertheless, the defining act of impersonating a source by forging packet identity is spoofing. Modern security architecture addresses this risk through cryptographic mutual authentication, integrity protection, ingress and egress filtering, and avoiding source-address-based trust. RFC 2827 describes network ingress filtering intended to reduce packets sent with forged source addresses, while NIST defines spoofing as masquerading as another entity by falsifying data or identity information. See RFC 2827: Network Ingress Filtering and NIST CSRC: Spoofing.

QUESTION NO: 80

Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.

Which of the following could have MOST likely prevented the Peer-to-Peer (P2P) program from being installed on the computer?

A. Removing employee's full access to the computer

B. Supervising their child's use of the computer

C. Limiting computer's access to only the employee

D. Ensuring employee understands their business conduct guidelines

ANSWER: A

Explanation:

Removing employee's full access to the computer is the most likely preventive control because it applies the principle of least privilege. A standard user account should have only the permissions required for normal business work and should not have standing local administrator rights. Most software installations that make system-wide changes, such as writing to protected program directories, adding services, changing security settings, or installing device components, require elevated privileges. Removing full administrator access therefore prevents the employee's normal account from authorizing such an installation without an approved elevation process.

For legitimate business software, the organization can use centrally managed deployment tools or require temporary, controlled elevation after IT approval. This preserves employee productivity while ensuring that software is reviewed for licensing, security, malware exposure, and policy compliance before it is installed. Least privilege is a foundational access-control practice: permissions are restricted to the minimum necessary to perform authorized duties, reducing the impact of mistakes or misuse on an endpoint. NIST identifies least privilege as requiring only the minimum access needed for assigned tasks in its least privilege glossary definition. This approach also aligns with the access-control and security-principles areas assessed in the ISC2 CISSP Exam Outline.

QUESTION NO: 81

What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

A. Standardize specifications between software security products.

B. Achieve organizational compliance with international standards.

C. Improve vulnerability assessment capabilities.

D. Save security costs for the organization.

ANSWER: A

Explanation:

Standardize specifications between software security products is correct because SCAP's fundamental purpose is to provide a common, interoperable framework for communicating security-related information in machine-readable forms. Developed by NIST, SCAP is a suite of specifications that supports automated vulnerability management, configuration assessment, and compliance measurement. Its value begins with the use of shared data models, identifiers, and checklists, allowing security tools from different vendors to consume, produce, and exchange comparable security content.

For example, SCAP incorporates component specifications such as Common Vulnerabilities and Exposures (CVE) for vulnerability identifiers, Common Platform Enumeration (CPE) for product naming, Common Configuration Enumeration (CCE) for configuration issues, Open Vulnerability and Assessment Language (OVAL) for assessment logic, and Extensible Configuration Checklist Description Format (XCCDF) for checklists and reporting. This shared structure permits an organization to reuse assessment content and correlate results across heterogeneous platforms rather than relying on proprietary formats unique to each product.

Consequently, automated assessment and reporting capabilities are enabled by SCAP's central benefit: standardization and interoperability among security products. NIST describes SCAP as a method for using standards to enable automated vulnerability management, measurement, and policy compliance evaluation. See NIST's SCAP project page and NIST SP 800-126 Rev. 3.

QUESTION NO: 82

Which of the following teams should be included in an organization's contingency plan?

A. Damage assessment team.

B. Hardware salvage team

C. Tiger team.

D. Legal affairs team.

ANSWER: A

Explanation:

Damage assessment team. is correct because contingency planning requires defined personnel and responsibilities to evaluate the effects of a disruption promptly and reliably. Following an incident, this team determines the nature, location, and extent of damage to facilities, information systems, data, and supporting infrastructure. It also identifies immediate safety or stabilization needs and communicates its findings to the personnel responsible for activating and directing recovery activities.

This assessment provides the factual basis for consequential contingency decisions. For example, leadership needs timely information about service impacts, resource requirements, and the likely duration of an outage to determine whether to activate recovery procedures, invoke an alternate site, prioritize specific business functions, or escalate to a disaster declaration. Preassigning this function avoids ad hoc decision-making during a high-pressure event and supports coordinated, repeatable recovery operations.

NIST contingency-planning guidance identifies damage assessment as an activity during contingency plan activation and recovery, with results used to determine the appropriate recovery actions. Assigning a damage assessment team therefore reflects the CISSP principle that contingency plans must establish clear recovery roles, responsibilities, communications, and decision criteria before an incident occurs. See NIST SP 800-34 Rev. 1 and Ready.gov continuity planning guidance.

QUESTION NO: 83

Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

A. Trusted Platform Module (TPM)

B. Preboot eXecution Environment (PXE)

C. Key Distribution Center (KDC)

D. Simple Key-Management for Internet Protocol (SKIP)

ANSWER: A

Explanation:

Trusted Platform Module (TPM) is correct because it is a tamper-resistant hardware-based cryptoprocessor designed to securely generate, protect, and use cryptographic keys. In a full-disk encryption deployment, the disk's volume encryption key is commonly protected (or "sealed") by a key safeguarded by the TPM. The TPM releases access to that protected key only when expected platform integrity conditions are met, such as measurements of firmware and boot components held in Platform Configuration Registers. This binds access to the encrypted disk to the authorized device and its trusted boot state, helping protect the data if the drive is removed and connected to another system. TPM-backed full-disk encryption can also be configured to require an additional user factor, such as a PIN or startup key, before the key is released. Microsoft describes how BitLocker uses the TPM to help verify system integrity before releasing the key material needed to unlock an encrypted operating-system drive. The Trusted Computing Group provides the TPM specifications defining this hardware root of trust and its protected key capabilities. See Microsoft BitLocker documentation and the Trusted Computing Group TPM Library Specification.

QUESTION NO: 84

Which of the following teams should NOT be included in an organization's contingency plan?

A. Damage assessment team.

B. Hardware salvage team.

C. Tiger team.

D. Legal affairs team.

ANSWER: C

Explanation:

Tiger team. is correct because a contingency plan needs predefined, durable roles that activate during a disruption to assess damage, coordinate recovery, preserve assets, restore services, and support the organization's return to normal operations. A tiger team is instead an ad hoc group of specialists assembled to investigate or solve a narrowly defined, usually difficult technical problem. Although its expertise could be requested during an emergency, it is not a standard functional team or a defined recovery responsibility in a contingency-planning structure.

Effective contingency planning assigns personnel to established recovery functions in advance, documents their authority and responsibilities, and provides procedures for activation, notification, coordination, and recovery. This ensures that the organization can respond quickly without first having to create a technical problem-solving group and determine its scope. NIST contingency-planning guidance emphasizes identifying teams, recovery roles, and responsibilities as part of plan development and implementation. A tiger team's temporary and problem-specific nature does not satisfy this core requirement for an established contingency-plan team. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and Ready.gov business continuity planning guidance.

QUESTION NO: 85

An organization has been collecting a large amount of redundant and unusable data and filling up the storage area network (SAN). Management has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

A. Compression.

B. Caching.

C. Replication.

D. Deduplication.

ANSWER: D

Explanation:

Deduplication is the best technical solution because the stated ongoing storage issue is the accumulation of redundant data in the SAN. Data deduplication detects repeated instances of the same data and retains one unique copy, replacing additional identical copies with references to that retained copy. This directly reduces the capacity consumed by duplicate files, blocks, virtual-machine images, backup content, and commonly repeated attachments. It can operate at file, block, or subfile levels, depending on the storage implementation, and may be applied inline as data is written or as a post-process operation. Either approach helps control future growth while also enabling reclamation of capacity occupied by existing duplicates. This is a technical storage-efficiency control that is particularly valuable in environments where users, applications, and backup processes produce multiple copies of the same information. Its ongoing operation makes it appropriate for a continuing capacity-management problem rather than a one-time cleanup activity. The underlying principle is that eliminating redundant copies reduces physical storage requirements while preserving logical access to the data. See the Microsoft Data Deduplication overview and IBM documentation on data deduplication.

QUESTION NO: 86

What does a Synchronous (SYN) flood attack do?

A. Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state

B. Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections

C. Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests

D. Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

ANSWER: D

Explanation:

Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections is correct because a SYN flood exhausts the resources that a TCP service uses to maintain pending connection requests. TCP normally begins a connection through the three-way handshake: a client sends a SYN segment, the server responds with SYN-ACK, and the client completes the process with an ACK. In a SYN flood, an attacker sends a high volume of SYN requests, often with spoofed source addresses or without sending the final acknowledgment. The target retains state for each incomplete handshake in its backlog, also called the half-open connection queue, while it waits for the handshake to finish or time out. Once that finite queue and associated system resources are consumed, legitimate clients cannot establish new TCP connections. The resulting loss of availability is why SYN flooding is a denial-of-service technique. The attack does not require successfully completing many connections; its effect comes from overwhelming the capacity reserved for new, incomplete connection attempts. SYN cookies, backlog tuning, rate limiting, and upstream filtering are common measures used to reduce this exposure. See Cloudflare's SYN flood overview and CISA guidance on denial-of-service attacks.

QUESTION NO: 87

Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

A. Transport layer handshake compression

B. Application layer negotiation

C. Peer identity authentication

D. Digital certificate revocation

ANSWER: C

Explanation:

Peer identity authentication is correct because TLS authenticates the identity of the endpoint with which a remote client is establishing a protected connection. During the TLS handshake, the remote access server presents an X.509 digital certificate. The client validates that certificate by checking such elements as its trust chain, validity period, and whether its subject name or subject alternative name corresponds to the server name the client intended to reach. This gives the client cryptographic assurance that it is communicating with the legitimate remote access server rather than an impersonating system.

TLS can also support client authentication when the server requests and validates a client certificate. This mutual-authentication capability is particularly valuable for administrative remote access and other environments requiring strong assurance of both endpoint identities. After authentication and key establishment, TLS protects the remote-access session using negotiated cryptographic algorithms, providing confidentiality and integrity for the application data carried in the connection. Thus, endpoint identity authentication is a fundamental TLS security service and directly supports secure remote access. The TLS 1.3 standard specifies the certificate-based authentication messages exchanged in the handshake, while NIST describes TLS as a mechanism for protecting communications and authenticating communicating parties. See RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3 and NIST SP 800-52 Rev. 2.

QUESTION NO: 88

A system has been scanned for vulnerabilities and has been found to contain a number of communication ports that have been opened without authority. To which of the following might this system have been subjected?

A. Trojan horse

B. Denial of Service (DoS)

C. Spoofing

D. Man-in-the-Middle (MITM)

ANSWER: A

Explanation:

Trojan horse is correct because a Trojan is malicious software that appears to be legitimate but executes concealed, unauthorized functions after it runs on a host. A common Trojan capability is to install or activate a backdoor service. That service listens on a network port selected by the malware or attacker, enabling command-and-control communications, remote administration, data exfiltration, or later access to the compromised system. Consequently, a vulnerability scan or port scan may reveal unexpected listening ports that are not approved for the system's intended role or baseline configuration. The unauthorized open ports are therefore an important indicator that the host could have been compromised by a Trojan with backdoor functionality. Incident responders should validate the listening process and its executable path, service configuration, persistence mechanisms, active network connections, and endpoint telemetry; then isolate the affected host and follow the organization's incident-response procedures. NIST describes malware as software or firmware intended to perform an unauthorized process that adversely affects confidentiality, integrity, or availability, and its incident-handling guidance includes containment and eradication activities for compromised systems. See NIST's malware definition and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 89

Which of the following contributes MOST to the effectiveness of a security officer?

A. Developing precise and practical security plans.

B. Integrating security into the business strategies.

C. Understanding the regulatory environment.

D. Analyzing the strengths and weakness of the organization.

ANSWER: B

Explanation:

Integrating security into the business strategies contributes most to a security officer's effectiveness because it makes security an enabler of organizational objectives rather than an isolated technical or compliance function. CISSP governance principles emphasize aligning the security program with business goals, enterprise risk appetite, strategic priorities, and available resources. This alignment enables the security officer to communicate risk in terms executives can use for decisions, such as financial exposure, operational resilience, legal obligations, customer trust, and mission impact.

When security is incorporated into business strategy, security requirements can be considered early in planning, architecture, procurement, product delivery, and organizational change. The security officer can then help leaders make informed risk-treatment decisions and ensure that security investments support measurable business outcomes. Strategic integration also creates executive sponsorship and accountability, which are essential to implementing policies, managing risk consistently, and sustaining an enterprise security program. NIST identifies governance as the mechanism through which an organization establishes and communicates cybersecurity risk-management expectations in support of organizational objectives. See the NIST Cybersecurity Framework and the ISC2 CISSP Exam Outline.

QUESTION NO: 90

The overall goal of a penetration test is to determine a system's

A. ability to withstand an attack.

B. capacity management.

C. error recovery capabilities.

D. reliability under stress.

ANSWER: A

Explanation:

The correct answer is **ability to withstand an attack.** A penetration test is an authorized, controlled simulation of adversarial activity against an in-scope environment. Its purpose is to determine whether identified weaknesses can actually be exploited, how far an attacker could progress after initial compromise, what sensitive assets or business processes could be affected, and whether preventive, detective, and response controls operate effectively under attack conditions. In other words, it evaluates the practical resilience of the system and its surrounding security controls against a realistic attack path—not merely the existence of vulnerabilities in isolation. Results help the organization prioritize remediation according to demonstrated exploitability and potential impact, while documenting evidence and recommendations for strengthening its security posture. This aligns with NIST guidance that penetration testing attempts to circumvent security features and gain access to systems, thereby identifying vulnerabilities that could be exploited. ISC2's CISSP examination outline includes security testing as a means of assessing the effectiveness of security controls. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and the ISC2 CISSP Certification Exam Outline.

QUESTION NO: 91

What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

A. Implementation Phase

B. Initialization Phase

C. Cancellation Phase

D. Issued Phase

ANSWER: B

Explanation:

Initialization Phase is correct in the life-cycle sequence used by this question, where pre-certification activities occur first and initialization prepares the subject and keying material for certificate enrollment. During initialization, the end entity's identity and registration context are established, and the cryptographic key pair and certificate-signing request can be created or prepared according to the organization's certificate policy and certification-practice requirements. The public key and verified subject information are then available for the certification authority's subsequent validation and certificate-issuance processes. Secure handling of the private key is fundamental at this point because the assurance provided by the future certificate depends on the subject retaining exclusive control of that private key. This reflects the broader key-management principle that keying material must be generated, protected, and administered under defined controls throughout its life cycle. NIST describes key management as covering the generation, establishment, storage, use, and destruction of cryptographic keys, with controls appropriate to each stage. PKI certificate policies also define the practices governing registration, certificate application, issuance, and related life-cycle services. See NIST SP 800-57 Part 1 and RFC 3647: Certificate Policy and Certification Practices Framework.

QUESTION NO: 92

The use of private and public encryption keys is fundamental in the implementation of which of the following?

A. Diffie-Hellman algorithm

B. Secure Sockets Layer (SSL)

C. Advanced Encryption Standard (AES)

D. Message Digest 5 (MD5)

ANSWER: B

Explanation:

Secure Sockets Layer (SSL) is the intended answer because secure web-session protocols use public-key cryptography, meaning a mathematically related public key and private key, during the handshake phase to establish an authenticated secure connection. In a typical certificate-based deployment, the server presents an X.509 certificate containing its public key. The client validates the certificate and uses the public-key material to authenticate the server and securely negotiate or protect key-establishment information. The resulting session normally uses symmetric cryptography for bulk application-data encryption because it is substantially more efficient, but the public/private key pair remains fundamental to establishing trust and protecting the initial exchange. Although SSL has been deprecated due to known security weaknesses, it is historically the protocol named by this question; its successor, TLS, follows the same essential model of certificates and public-key cryptography during connection setup. The IETF describes TLS as providing privacy and data integrity between communicating applications, while NIST explains that public-key cryptography uses a public key and a corresponding private key for cryptographic operations. See RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3 and NIST: Public-Key Cryptography.

QUESTION NO: 93

What is the foundation of cryptographic functions?

A. Encryption

B. Cipher

C. Hash

D. Entropy

ANSWER: D

Explanation:

Entropy is the foundation of secure cryptographic functions because it represents the unpredictability available for security-critical values, particularly cryptographic keys, initialization vectors, nonces, salts, and random challenges. Cryptographic algorithms can be mathematically sound, but their security depends on adversaries being unable to predict the secret values used with them. High-quality entropy ensures that generated values have sufficient randomness and cannot feasibly be guessed, reproduced, or enumerated by an attacker.

In practical cryptographic systems, entropy is collected from unpredictable physical or operating-system events and processed by a cryptographically secure random bit generator. The resulting random output is then used to create keys and related parameters. NIST describes entropy as a measure associated with the uncertainty or unpredictability of a source and provides requirements for validating entropy sources used by random bit generators. This makes entropy a prerequisite for establishing trustworthy cryptographic material and, therefore, for the effective operation of encryption, hashing-related authentication mechanisms, and other cryptographic services. See NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation and NIST CSRC's definition of entropy.

QUESTION NO: 94

Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organizationâ€™s Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.

Which of the following documents explains the proper use of the organization's assets?

A. Human resources policy

B. Acceptable use policy

C. Code of ethics

D. Access control policy

ANSWER: B

Explanation:

Acceptable use policy is correct because it establishes the authorized, appropriate, and prohibited uses of an organization's information assets, including organization-issued laptops, software, internet access, email, messaging, and network services. In this scenario, it would communicate whether personal use is permitted, whether nonemployees such as family members may use a company device, and whether users may install peer-to-peer applications or other unapproved software. It also normally informs personnel that organizational systems remain subject to security controls, monitoring, and potential disciplinary action for policy violations. An acceptable use policy is an administrative control that defines user responsibilities and expected behavior before misuse occurs, helping protect corporate devices, data, networks, and legal interests. Users should acknowledge this policy as part of onboarding and whenever it is materially updated. ISC2's CISSP Exam Outline includes security policy and standards as governance topics within Security and Risk Management, and acceptable-use requirements are a practical expression of that governance for end users. NIST likewise describes rules of behavior as defining acceptable system use and user responsibilities, which directly aligns with the purpose of an acceptable use policy. See the ISC2 CISSP Certification Exam Outline and NIST SP 800-18 Rev. 1.

QUESTION NO: 95

Which of the following is the MOST crucial for a successful audit plan?

A. Defining the scope of the audit to be performed

B. Identifying the security controls to be implemented

C. Working with the system owner on new controls

D. Acquiring evidence of systems that are not compliant

ANSWER: A

Explanation:

Defining the scope of the audit to be performed is the most crucial element because it establishes the audit's boundaries and provides the foundation for all subsequent planning. Scope specifies the subject matter to be examined, organizational units and locations involved, systems or processes included, relevant time period, and any exclusions. With these boundaries established, auditors can align the audit objectives, applicable criteria, required skills, schedule, testing approach, and resource allocation to the risks and obligations that the audit is intended to address. A clearly defined scope also enables effective communication with stakeholders and helps preserve auditor independence by setting agreed expectations about what the engagement will assess. It supports an evidence-based audit because the auditor can determine what evidence is needed to reach conclusions within the stated boundaries. The Institute of Internal Auditors' Global Internal Audit Standards require engagement planning to establish objectives, scope, timing, and resource allocations, with scope defining the focus and boundaries of the engagement. Similarly, ISO guidance for management-system auditing treats audit scope as a core component for defining the extent and boundaries of an audit. These principles make scope definition essential to an audit plan that is focused, feasible, and capable of producing meaningful results. See the IIA Global Internal Audit Standards and ISO 19011 auditing guidelines.

QUESTION NO: 96

What capability would typically be included in a commercially available software package designed for access control?

A. Password encryption

B. File encryption

C. Source library control

D. File authentication.

ANSWER: A

Explanation:

Password encryption is the capability most typically associated with commercially available access-control software because such products must manage the identification and authentication information used to make authorization decisions. Whether implemented in an operating system, directory service, identity provider, or dedicated access-management product, the software needs a protected method for storing and validating password verifiers. This protects authentication secrets if the credential store is accessed or copied by an unauthorized party and supports the reliable enforcement of access-control rules.

In modern terminology, password protection should normally use a salted, computationally expensive one-way password-hashing function rather than reversible encryption. Nevertheless, "password encryption" is commonly used in exam-oriented access-control terminology to describe secure handling of password data by the access-control package. NIST states that verifiers should store passwords in a form resistant to offline guessing, using salted password hashing and an appropriate work factor. This capability is therefore a fundamental and expected feature of software responsible for authenticating users before granting controlled access. See NIST SP 800-63B, Digital Identity Guidelines: Authentication and Authenticator Management and the OWASP Password Storage Cheat Sheet.

QUESTION NO: 97

An attack utilizing social engineering and a malicious Uniform Resource Locator (URL) link to take advantage of a victim's existing browser session with a web application is an example of which of the following types of attack?

A. Clickjacking.

B. Cross-site request forgery (CSRF).

C. Cross-Site Scripting (XSS).

D. Injection.

ANSWER: B

Explanation:

Cross-site request forgery (CSRF) is the attack described because it exploits the trust a web application places in a user's already authenticated browser session. An attacker typically uses a social-engineering lure, such as a link in an email, message, or web page, to cause the victim's browser to issue a request to a target application while the victim remains signed in. The browser may automatically attach the session cookie or other ambient authentication information associated with the target site. If the application does not adequately verify that the request was intentionally initiated from its own trusted context, it can process the attacker-selected request with the victim's privileges. CSRF is therefore commonly associated with unauthorized state-changing actions, such as changing account settings, adding a payment recipient, or submitting a transaction. Effective defenses include unpredictable anti-CSRF tokens that the attacker cannot obtain, appropriate use of SameSite cookie attributes, and origin or referer validation for sensitive requests. These controls help the application distinguish legitimate user-initiated requests from requests induced through an external attacker-controlled site or URL. OWASP describes CSRF as forcing an authenticated end user to execute unwanted actions on a web application, which directly matches the scenario. See OWASP: Cross-Site Request Forgery and MDN: CSRF prevention.

QUESTION NO: 98

Which step of the Risk Management Framework (RMF) identifies the initial set of baseline security controls?

A. Selection.

B. Monitoring.

C. Implementation.

D. Assessment.

ANSWER: A

Explanation:

Selection is the RMF step that establishes the initial set of baseline security controls. Under NIST SP 800-37 Rev. 2, the Select step follows system categorization, which determines the potential impact level associated with loss of confidentiality, integrity, or availability. That impact information provides the basis for choosing an initial control baseline. The organization then tailors and supplements the baseline as necessary to address its specific risk environment, technologies, mission needs, laws, policies, and inherited common controls. The resulting control set is documented in the system security plan and serves as the planned safeguards that will subsequently be implemented and assessed. This makes Selection the point at which the starting security-control set is identified; it is not merely a later operational activity. NIST describes the Select step as selecting, tailoring, and documenting the controls needed to protect the system and its information. The detailed control catalog and baseline-selection structure are provided in NIST SP 800-53. See NIST SP 800-37 Rev. 2 and NIST SP 800-53 Rev. 5.

QUESTION NO: 99

Which of the following is NOT a critical security aspect of Operations Controls?

A. Controls over hardware.

B. Data media used.

C. Operators using resources.

D. Environmental controls.

ANSWER: D

Explanation:

Environmental controls is the correct answer because it is generally categorized as a physical and environmental protection function rather than an operations control. Operations controls concern the secure, dependable day-to-day operation of information systems. They establish repeatable processes for running workloads, administering systems, managing operational hardware, controlling privileged activities, monitoring processing, and handling the media on which organizational data resides. These measures help ensure that people and technology perform authorized operational tasks consistently, preserving the confidentiality, integrity, and availability of information throughout routine processing.

Environmental safeguards certainly remain essential to the organization's overall security posture and availability objectives. However, protections such as heating, ventilation, air conditioning, fire detection and suppression, electrical power protection, and water detection are designed primarily to protect facilities and equipment from environmental hazards. NIST separates these concerns in its Physical and Environmental Protection control family, while operational procedures and system operations are addressed through distinct operational and system-management controls. This distinction is consistent with CISSP's treatment of security as a set of related but separately managed control domains. See the ISC2 CISSP Exam Outline and NIST's SP 800-53 Physical and Environmental Protection controls.

QUESTION NO: 100

Which of the following departments initiates the request, approval, and provisioning business process?

A. Operations.

B. Security.

C. Human resources (HR).

D. Information technology (IT).

ANSWER: C

Explanation:

Human resources (HR) is correct because it commonly serves as the authoritative business source for workforce identity lifecycle events. When a person is hired, transferred, changes roles, takes leave, or leaves the organization, HR creates or updates the underlying employment record. That business event is the trigger for identity and access management workflows that request appropriate access, obtain required approvals, and provision accounts, roles, and entitlements according to the individual's job responsibilities.

This approach supports timely and consistent joiner, mover, and leaver processing. Connecting provisioning to an authoritative HR record helps ensure that access decisions reflect a current employment relationship and organizational role, while also providing auditable evidence for account-management controls. The technical workflow may be automated through an identity governance and administration platform, but the initiating event remains the HR-managed personnel change. This separation also supports governance: employment and role information originates with the accountable business function, and access is subsequently granted in alignment with defined authorization processes.

NIST account-management guidance calls for managing accounts in accordance with organizational account-management requirements, including establishing, activating, modifying, disabling, and removing accounts. See NIST SP 800-53 Rev. 5, Account Management and NIST SP 800-63A, Enrollment and Identity Proofing.

QUESTION NO: 101

Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?

A.Business and functional managers.

B. IT Security practitioners.

C. System and information owners.

D. Chief information officer.

Answer: C

Explanation:

A. IT Security practitioners.

B. System and information owners.

C. Chief information officer.

D. Business and functional managers.

ANSWER: B

Explanation:

System and information owners are responsible for ensuring that proper controls are in place to preserve the confidentiality, integrity, and availability of the information and systems for which they are accountable. Ownership is fundamentally an accountability role: the owner establishes the business and security requirements for an asset, including its classification, acceptable use, access requirements, retention needs, and acceptable level of risk. The owner must ensure that safeguards selected for the system or information are appropriate to those requirements and must formally accept any residual risk that remains after controls are applied.

This responsibility does not require the owner personally to configure or operate every technical safeguard. Control implementation and ongoing operational work can be delegated to security personnel, administrators, engineers, and other support roles. However, delegation of work does not transfer accountability for ensuring that the protection requirements are defined, addressed, and authorized. This distinction between accountable ownership and operational responsibility is central to sound security governance and risk management.

NIST identifies the system owner as the official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The RMF also defines owner responsibilities within the system life cycle: NIST CSRC System Owner glossary definition and NIST SP 800-37 Rev. 2, Risk Management Framework.

QUESTION NO: 102

In the physical security context, a security door equipped with an electronic lock configured to ignore the unlock signals sent from the building emergency access control system in the event of an issue (fire, intrusion, power failure) would be in which of the following configuration?

A. Fail Soft.

B. Fail Open.

C. Fail Safe.

D. Fail Secure.

ANSWER: D

Explanation:

Fail Secure. is the correct configuration because it describes an electronic locking arrangement that retains its locked state when normal control, communications, or power conditions are disrupted. In the scenario, the door is specifically configured not to act on emergency-system unlock signals during abnormal events. Its resulting state is therefore secured rather than released, which is the defining operational result of a fail-secure, or fail-locked, configuration.

In physical security design, fail-secure locking is used where preventing unauthorized entry and protecting assets must continue through a system failure. The designation concerns the state the locking mechanism assumes upon failure; it does not by itself eliminate the requirement to provide safe egress for people. A properly engineered facility can pair a fail-secure access-control lock with independent, code-compliant egress provisions, such as mechanical exit hardware, so occupants can leave without depending on the access-control system. This reflects the security architecture principle of ensuring that

access enforcement continues to protect protected spaces while life-safety controls are addressed separately and appropriately.

NIST identifies physical access control as a control area requiring enforcement of authorized physical access in NIST SP 800-53 Rev. 5. Requirements affecting door locking and egress are addressed through applicable building and fire codes, including resources published by the National Fire Protection Association.

QUESTION NO: 103

A recent security audit is reporting several unsuccessful login attempts being repeated at specific times during the day on an Internet facing authentication server. No alerts have been generated by the security information and event management (SIEM) system. What PRIMARY action should be taken to improve SIEM performance?

A. Implement role-based system monitoring

B. Audit firewall logs to identify the source of login attempts

C. Enhance logging detail

D. Confirm alarm thresholds

ANSWER: D

Explanation:

Confirm alarm thresholds is the primary action because the authentication server is already recording the unsuccessful login attempts, and the audit has identified a repeated, time-related pattern. This demonstrates that relevant event data exists, but the SIEM is not producing an alert from it. SIEM alerting depends on correlation rules and their configured conditions, including the number of failures, the time window in which they occur, source or target context, and severity thresholds. Reviewing and tuning these thresholds determines whether the observed activity should meet the organization's defined criteria for an alert—for example, repeated failures against an Internet-facing service within a specified interval. Effective threshold tuning balances timely detection of password attacks and other suspicious authentication activity with the need to limit excessive, low-value alerts. It should be based on a baseline of normal activity, the criticality and exposure of the authentication service, and the organization's risk tolerance. This action directly addresses the gap between available security events and the SIEM's alert-generation behavior. NIST's guidance on log management emphasizes defining monitoring requirements and using log analysis to identify security-relevant events, while CISA identifies repeated failed authentication attempts as a useful detection signal for brute-force activity. See NIST SP 800-92, Guide to Computer Security Log Management and CISA guidance on brute-force attacks.

QUESTION NO: 104

An organization that has achieved a Capability Maturity Model Integration (CMMI) level of 4 has done which of the following?

A. Achieved optimized process performance.

B. Achieved predictable process performance

C. Addressed the causes of common process variance

D. Addressed continuous innovative process improvement.

ANSWER: B

Explanation:

Achieved predictable process performance is correct. CMMI Maturity Level 4 is the *Quantitatively Managed* maturity level. At this stage, the organization manages selected processes using quantitative techniques, including measurement, statistical analysis, process-performance baselines, and performance models. These practices enable the organization to understand normal process variation, establish measurable performance objectives, and control work so that results can be predicted within defined limits.

Predictability is the essential outcome of quantitative management. Rather than merely ensuring that processes are documented and consistently deployed, the organization uses objective data to determine whether process behavior is stable and capable of meeting business and quality objectives. Management can therefore make more reliable projections about cost, schedule, quality, and other performance results. This maturity level demonstrates that process performance is understood and controlled quantitatively, creating a sound basis for dependable delivery and informed risk-based decisions.

ISACA's CMMI overview describes maturity levels and the progression toward quantitatively managed processes: ISACA CMMI. The Software Engineering Institute's CMMI material also describes the Level 4 quantitative-management focus: SEI CMMI resource.

QUESTION NO: 105

What is the PRIMARY reason for criminal law being difficult to enforce when dealing with cybercrime?

A. Jurisdiction is hard to define.

B. Law enforcement agencies are understaffed.

C. Extradition treaties are rarely enforced.

D. Numerous language barriers exist.

ANSWER: A

Explanation:

Jurisdiction is hard to define. is the primary reason because cybercrime routinely occurs across multiple legal territories at the same time. An offender may operate from one country, compromise systems located in another, route communications through infrastructure in several additional countries, and harm victims worldwide. Criminal-law enforcement is fundamentally tied to territorial sovereignty, so investigators and prosecutors must establish which jurisdiction has authority to investigate, collect evidence, charge the offender, and conduct a trial. They may also need to determine which nation's substantive laws apply to conduct whose relevant elements occurred in different locations.

This challenge has practical consequences for a case from its earliest stages. Electronic evidence, such as subscriber records, cloud data, and network logs, may be held by foreign providers or physically stored abroad. Obtaining it lawfully can require formal cross-border cooperation, including mutual legal-assistance processes, while respecting each country's procedural requirements and privacy protections. A prosecution also depends on whether the suspected offender can be located, arrested, and lawfully transferred to the prosecuting jurisdiction. These boundaries make enforcement difficult even when the underlying criminal conduct is clear. INTERPOL describes cybercrime as inherently transnational and emphasizes international cooperation in responding to it: INTERPOL Cybercrime. The U.S. Department of Justice also outlines the international evidence and extradition assistance needed in cross-border cases: DOJ Office of International Affairs.

QUESTION NO: 106

Which of the following is a network intrusion detection technique?

A. Statistical anomaly

B. Perimeter intrusion

C. Port scanning

D. Network spoofing

ANSWER: A

Explanation:

Statistical anomaly is a network intrusion detection technique because it establishes a profile or baseline representing expected network behavior, then analyzes current traffic and events for statistically meaningful deviations from that baseline. Examples of baseline characteristics can include normal connection volumes, protocol usage, packet sizes, session

durations, source and destination patterns, and traffic rates at particular times. Activity that exceeds a configured threshold or substantially differs from the learned profile can trigger an alert for investigation. This approach is especially valuable because it can identify previously unseen attacks or suspicious behavior that may not match a known attack signature. Effective use requires a representative baseline and ongoing tuning as legitimate network behavior changes; otherwise, routine operational changes may appear anomalous. NIST describes anomaly-based intrusion detection as comparing observed activity against normal profiles to identify significant deviations, including for network-based monitoring. This is consistent with the CISSP emphasis on selecting and operating detection controls that identify potentially malicious activity while supporting monitoring and incident response. See NIST's Guide to Intrusion Detection and Prevention Systems and ISC2's CISSP Certification Exam Outline.

QUESTION NO: 107

Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?

A. identification of data location.

B. integration with organizational directory services for authentication.

C. accommodation of hybrid deployment models.

D. tokenization of data.

ANSWER: A

Explanation:

Identification of data location must be included in the cloud contract because electronic discovery requires the organization to identify, preserve, collect, review, and produce relevant electronically stored information in a defensible manner. In a cloud service, a customer's information may be stored, replicated, backed up, or processed across multiple physical facilities, regions, and legal jurisdictions. The organization therefore needs contractual assurance that it can determine where its data and relevant copies reside when a legal hold, investigation, regulatory inquiry, or litigation request occurs.

Clear data-location provisions also support obligations concerning data residency, jurisdiction, cross-border transfer, and access to records held by a cloud provider or its subprocessors. The contract should establish the provider's responsibility to supply location information and reasonably assist with preservation and collection of the customer's electronically stored information, including relevant metadata and backup or replica data where applicable. This enables timely legal-hold actions and helps establish a documented, repeatable collection process. NIST highlights the importance of understanding cloud data location, jurisdiction, and contractual provisions in cloud adoption and governance guidance. See NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing and NIST SP 800-146, Cloud Computing Synopsis and Recommendations.

QUESTION NO: 108

Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?

A. Masquerading, salami, malware, polymorphism

B. Brute force, dictionary, phishing, keylogger

C. Zeus, netbus, rabbit, turtle

D. Token, biometrics, IDS, DLP

ANSWER: B

Explanation:

Brute force, dictionary, phishing, keylogger is the correct list because each is a commonly recognized method for obtaining, guessing, or capturing passwords and other authentication secrets. A brute-force attack systematically attempts candidate

passwords until one succeeds; a dictionary attack makes this process more efficient by trying likely words, common passwords, and known variations. Phishing is a credential-harvesting technique in which an attacker impersonates a trusted party or service to persuade a user to disclose a password. A keylogger captures user keystrokes, potentially including passwords entered into authentication prompts. These threats illustrate why passwords alone are not sufficient for many risk scenarios. MFA adds one or more independent authentication factors, so possession or discovery of a password does not by itself grant access. The effectiveness of MFA depends on the factors being distinct and on using phishing-resistant implementations where the threat model warrants them. NIST's digital identity guidance describes password attacks such as online guessing and stresses protections including rate limiting, while CISA explains how phishing-resistant MFA helps mitigate credential theft. See NIST SP 800-63B: Digital Identity Guidelines and CISA: Implementing Phishing-Resistant MFA.

QUESTION NO: 109

An effective information security strategy is PRIMARILY based upon which of the following?

A. Risk management practices.

B. Security budget constraints.

C. Security control implementation.

D. Industry and regulatory standards.

ANSWER: A

Explanation:

Risk management practices are the foundation of an effective information security strategy because they connect security decisions directly to organizational objectives, critical assets, relevant threats, vulnerabilities, and leadership's risk appetite. A risk-based approach enables governance stakeholders to identify and assess risks, determine whether the resulting level of risk is acceptable, and select an appropriate treatment decision, such as mitigating, transferring, avoiding, or accepting the risk. Security investments and control priorities can then be justified according to the potential business impact and likelihood of adverse events. This helps ensure that limited resources are directed toward the risks that matter most rather than toward controls selected solely because they are technically appealing or customary. Risk management is also continuous: changes in the business, technology, legal environment, threat landscape, or organizational objectives can trigger reassessment and adjustment of the strategy. The NIST Risk Management Framework describes risk management as an organization-wide process that integrates security and privacy activities into system development and operation, supporting ongoing risk-informed decisions. ISO 31000 likewise establishes principles and guidance for integrating risk management into governance, planning, management, reporting, policies, values, and culture. See NIST SP 800-37 Rev. 2 and ISO 31000 risk management guidance.

QUESTION NO: 110

An organization is planning a penetration test that simulates the malicious actions of a former network administrator. What kind of penetration

test is needed?

A. Functional test

B. Unit test

C. Grey box

D. White box

ANSWER: C

Explanation:

Grey box is the appropriate test because it models an attacker who possesses meaningful but incomplete knowledge of the target environment. A former network administrator is likely to retain knowledge of network topology, administrative processes, naming conventions, technologies in use, asset locations, and potentially historical weaknesses. At the same time, that person would not necessarily retain current credentials, complete source code, current configuration details, or knowledge of changes made after departure. This creates the realistic partial-knowledge position represented by a grey-box assessment.

Using this approach, the assessment team can be supplied with carefully scoped insider-relevant information while still being required to discover and validate current attack paths. That allows the organization to assess whether privileged historical knowledge, combined with externally available information and ordinary user-level access where applicable, could enable compromise. NIST describes testing perspectives in terms of the assessor's prior knowledge and access, and recognizes that partial knowledge provides a useful model for realistic threat scenarios. OWASP likewise characterizes grey-box testing as testing with limited knowledge of an application's internal workings. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and OWASP Gray Box Testing.

QUESTION NO: 111

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organizationâ€™s network. A plan will be necessary to address these concerns.

What is the BEST reason for the organization to pursue a plan to mitigate client-based attacks?

A. Client privilege administration is inherently weaker than server privilege administration.

B. Client hardening and management is easier on clients than on servers.

C. Client-based attacks are more common and easier to exploit than server and network based attacks.

D. Client-based attacks have higher financial impact.

ANSWER: C

Explanation:

Client-based attacks are more common and easier to exploit than server and network based attacks. Client endpoints—including user workstations, browsers, email clients, document readers, and collaboration software—are a broad and routinely exposed attack surface. They process untrusted content, access web resources, receive messages and attachments, and depend on users making security-sensitive decisions. Attackers can therefore use techniques such as phishing, malicious documents, drive-by downloads, exploit kits, and malicious browser content to gain an initial foothold or steal credentials. A mitigation plan is justified because protecting clients requires coordinated controls: timely patching, secure configuration baselines, endpoint detection and response, least privilege, application control, email and web protections, and user awareness. These controls reduce both the likelihood that a client compromise succeeds and the opportunity for an attacker to use a compromised endpoint to access organizational resources. This risk-driven focus aligns with the CISSP expectation that security programs identify relevant threats and select safeguards proportionate to exposure and business risk. The ISC2 CISSP Exam Outline includes endpoint security and security operations concepts relevant to managing this attack surface. CISA also describes phishing as a frequent method used to compromise users and systems in its phishing guidance.

QUESTION NO: 112

Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

A. Data on the device cannot be restored from backup.

B. Data on the device cannot be backed up.

C. Data in transit has been compromised when the user has authenticated to the device.

D. Data at rest has been compromised when the user has authenticated to the device.

ANSWER: D

Explanation:

Data at rest has been compromised when the user has authenticated to the device. Full-disk encryption protects the confidentiality of information stored on a device's drive by encrypting the storage volume, primarily mitigating threats involving loss, theft, or offline access to the device or its removed storage media. However, FDE is generally transparent after successful pre-boot or operating-system authentication. The system obtains the cryptographic key and can read and write the disk's contents in plaintext as needed during the authenticated session. Consequently, if an attacker compromises an active, unlocked endpoint through malware, an interactive session, remote access, or physical access to an unattended unlocked device, the attacker may access information that is normally protected as data at rest. This is a limitation of FDE rather than a failure of its intended offline-data protection function. Security programs should therefore layer FDE with endpoint hardening, strong authentication, timely screen locking, least privilege, anti-malware or EDR capabilities, and, where warranted, additional application- or file-level protections for especially sensitive information. NIST describes storage encryption as a control for protecting data stored on end-user devices, while Microsoft notes that BitLocker's protection is designed to address offline attacks and must be complemented by other safeguards for an operating system that is already running. See NIST SP 800-111 and Microsoft BitLocker documentation.

QUESTION NO: 113

Which of the following is security control volatility?

A. A reference to the impact of the security control.

B. A reference to the likelihood of change in the security control.

C. A reference to how unpredictable the security control is.

D. A reference to the stability of the security control.

ANSWER: B

Explanation:

Security control volatility is the likelihood that a security control will change over time. A volatile control may be modified, reconfigured, replaced, or affected by frequent changes in technology, business processes, threats, suppliers, or operational requirements. For example, a cloud configuration managed through infrastructure as code may change often as deployments, software releases, permissions, and security policies evolve. Understanding this characteristic helps security teams establish an appropriate frequency for monitoring, reassessment, and control testing. Controls that are likely to change require continuing assurance that they remain correctly implemented and continue to meet their intended security objectives after each relevant change. This aligns with the CISSP emphasis on maintaining security throughout changing environments, including through continuous monitoring and ongoing assessment of control effectiveness. NIST's Risk Management Framework likewise treats monitoring changes to systems, environments of operation, and controls as essential to maintaining an accurate authorization and risk posture. See the ISC2 CISSP Certification Exam Outline and NIST SP 800-37 Rev. 2, Risk Management Framework.

QUESTION NO: 114

Which of the following is a responsibility of the information owner?

A. Ensure that users and personnel complete the required security training to access the Information System(IS)

B. Defining proper access to the Information System (IS), including privileges or access rights

C. Managing identification, implementation, and assessment of common security controls

D. Ensuring the Information System (IS) is operated according to agreed upon security requirements

ANSWER: B

Explanation:

Defining proper access to the Information System (IS), including privileges or access rights is a core responsibility of the information owner. The owner is the business role accountable for information or data within its area of responsibility and determines how that information must be classified, handled, protected, and made available. An essential component of this accountability is establishing access requirements: deciding which roles or individuals have a legitimate business need to access the information, the level of access they require, and the circumstances under which access is authorized. The information owner therefore approves access rules and typically participates in periodic access reviews to confirm that permissions remain appropriate as job duties, risk, and business requirements change. Technical teams may implement these decisions through identity and access management systems, but the business authority for defining the required access rests with the information owner. This division supports accountability by ensuring that access to valuable information is governed by its business value, sensitivity, and approved use. NIST describes system and information owners as organizational officials with responsibility for information and emphasizes their role in establishing security and privacy requirements. See NIST SP 800-37 Rev. 2 and NIST SP 800-53 Rev. 5.

QUESTION NO: 115

Which of the following models does NOT include data integrity or conflict of interest?

A. Biba.

B. Clark-Wilson

C. Bell-LaPadula

D. Brewer-Nash.

ANSWER: C

Explanation:

Bell-LaPadula is correct because it is a mandatory access control model designed specifically to preserve *confidentiality* of classified information. It represents subjects and objects with security labels and controls information flow according to those labels. Its simple-security property, commonly summarized as “no read up,” prevents a subject from reading information at a classification above its authorization. Its star property, commonly summarized as “no write down,” prevents information from being written to a lower classification, where it could be disclosed to less-authorized subjects. Together, these rules address unauthorized disclosure across classification levels.

The model’s purpose is therefore protection of secrecy, rather than ensuring that data is accurate, complete, and modified only through authorized processes. It also does not use conflict-of-interest restrictions intended to separate a user’s access to competing organizations’ sensitive information. In CISSP terminology, Bell-LaPadula is the classic confidentiality model, making it the appropriate selection when the question asks for the model that does not include data-integrity or conflict-of-interest objectives. NIST describes Bell-LaPadula as a formal state-transition model of computer security policy focused on access control and security levels. See the NIST CSRC Bell-LaPadula Model glossary entry and the NIST CSRC mandatory access control glossary entry.

QUESTION NO: 116

What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

A. Information security practitioner

B. Media librarian

C. Computer operator

D. Network administrator

ANSWER: B

Explanation:

Media librarian is the operations role responsible for controlling and safeguarding removable and backup media throughout its lifecycle. This role maintains the media inventory and associated records, oversees secure storage and environmental protection, controls access and checkout procedures, and verifies that media can be reliably read and restored. These responsibilities directly support the protection of the enterprise from corrupted, damaged, or contaminated media, which could otherwise undermine data integrity and recovery capability. In operational practice, the media librarian ensures that media are appropriately labeled, tracked, transported, retained, tested, and handled according to established procedures. The role also helps maintain the availability of known-good backup media by supporting rotation, validation, and secure archival processes. This is consistent with the CISSP Security Operations domain's focus on secure management of physical and logical assets, including media handling and recovery operations. ISC2's current CISSP exam outline identifies Security Operations as a tested domain and includes operational security activities relevant to protecting organizational assets: ISC2 CISSP Exam Outline. Guidance on protecting the confidentiality and integrity of media during storage and transport is also provided by NIST SP 800-53, Media Protection controls.

QUESTION NO: 117

An organization has been collecting a large amount of redundant and unusable data and lling up the storage area network (SAN). Management

has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

A. Compression

B. Caching

C. Replication

D. Deduplication

ANSWER: D

Explanation:

Deduplication is the best technical solution because the stated storage issue is the accumulation of redundant data in the SAN. Deduplication detects identical data segments, blocks, or files and retains one unique instance, replacing additional instances with metadata references to that stored instance. This directly reduces the physical storage capacity required for repeated data while preserving logical access to each copy for authorized users and applications. It is particularly effective for common enterprise workloads that create repeated content over time, including backup sets, virtual-machine images, software distributions, email attachments, and copied documents. As an ongoing storage-efficiency capability, deduplication can operate inline as information is written or as a post-process activity after it has been stored, depending on the platform and workload requirements. Reducing duplicate content extends usable SAN capacity and can defer the expense and operational effort of provisioning additional storage. NIST identifies data deduplication as a storage-reduction technique that eliminates duplicate data objects or blocks, and NetApp describes its use of shared blocks to reduce consumed capacity. See NIST's definition of data deduplication and NetApp's overview of data deduplication.

QUESTION NO: 118

In systems security engineering, what does the security principle of modularity provide?

A. Minimal access to perform a function.

B. Documentation of functions.

C. Isolated functions and data.

D. Secure distribution of programs and data.

ANSWER: C

Explanation:

Modularity provides *isolated functions and data*. In systems security engineering, modular design decomposes a system into distinct components with defined responsibilities and controlled interfaces. Each module encapsulates its implementation and data, exposing only the functionality required by other components. This limits unnecessary dependencies and information flows, reduces overall system complexity, and makes it more practical to analyze, test, and enforce security properties at component boundaries. Isolation also helps contain the effect of a fault, design defect, or compromise, rather than allowing it to propagate freely throughout the system. A modular architecture supports secure maintenance and evolution because a component can be reviewed, modified, or replaced with less impact on unrelated functions, provided its interface and required security properties remain intact. NIST describes modularity as the extent to which a system is composed of discrete components such that changes to one component have minimal impact on others. This characteristic supports the development of trustworthy, maintainable systems and aligns with security-engineering practices for managing complexity and limiting exposure. See the NIST definition of modularity and NIST's Systems Security Engineering guidance in SP 800-160 Volume 1.

QUESTION NO: 119

An organization regularly conducts its own penetration tests. Which of the following scenarios MUST be covered for the test to be effective?

A. Third-party vendor with access to the system

B. System administrator access compromised

C. Internal attacker with access to the system

D. Internal user accidentally accessing data

ANSWER: C

Explanation:

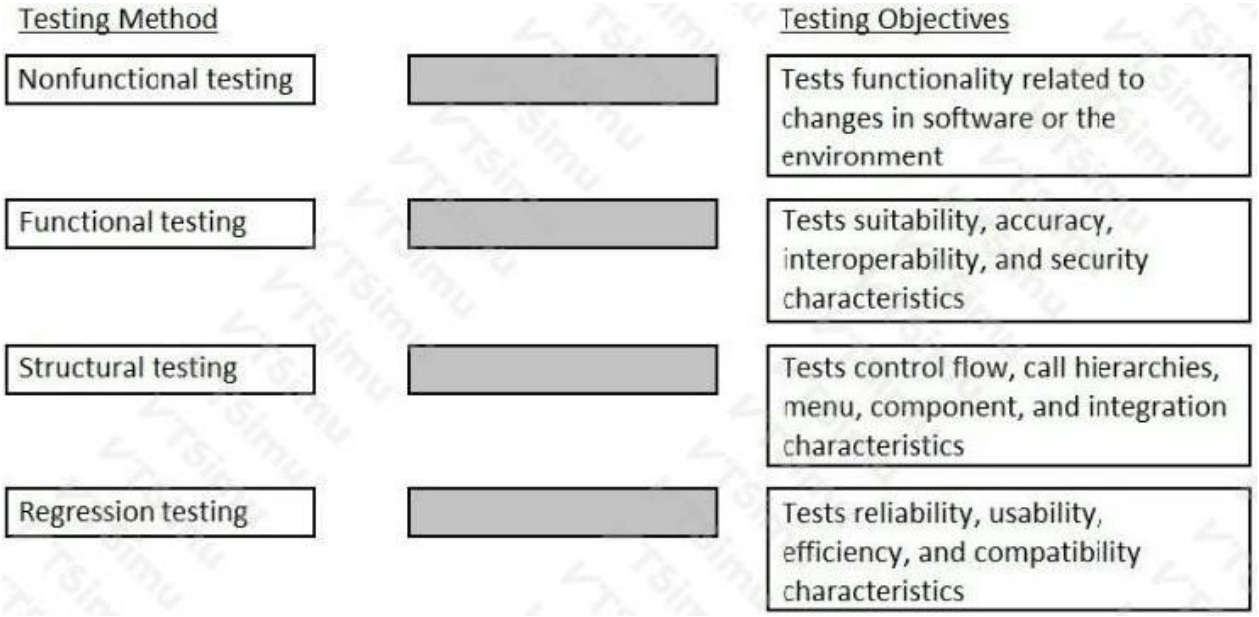
Internal attacker with access to the system is the required scenario because an effective penetration test must evaluate the organization's exposure from an assumed-breach or insider perspective, not solely from an unauthenticated external perspective. People who already possess legitimate access—including employees, contractors, and others operating within the trust boundary—may be able to misuse authorized privileges, discover excessive permissions, move laterally, access sensitive resources, or escalate privileges. Testing this scenario validates whether segmentation, least privilege, authorization controls, monitoring, and privileged-access restrictions actually limit the damage that an attacker can cause after gaining an initial foothold.

ISC2's CISSP approach is risk-driven: testing scope and objectives should reflect realistic threats, attack paths, and the organization's environment. An internal attacker scenario is fundamental because it tests the consequences of access within the environment, which is a core condition that security architecture and access-control mechanisms are intended to manage. NIST similarly identifies insider threats as threats involving individuals with authorized access who may use that access in a way that harms the organization. Including this scenario provides a meaningful assessment of defenses against misuse of trusted access and supports remediation based on demonstrated risk. See NIST guidance on insider threats and NIST Cybersecurity Framework 2.0.

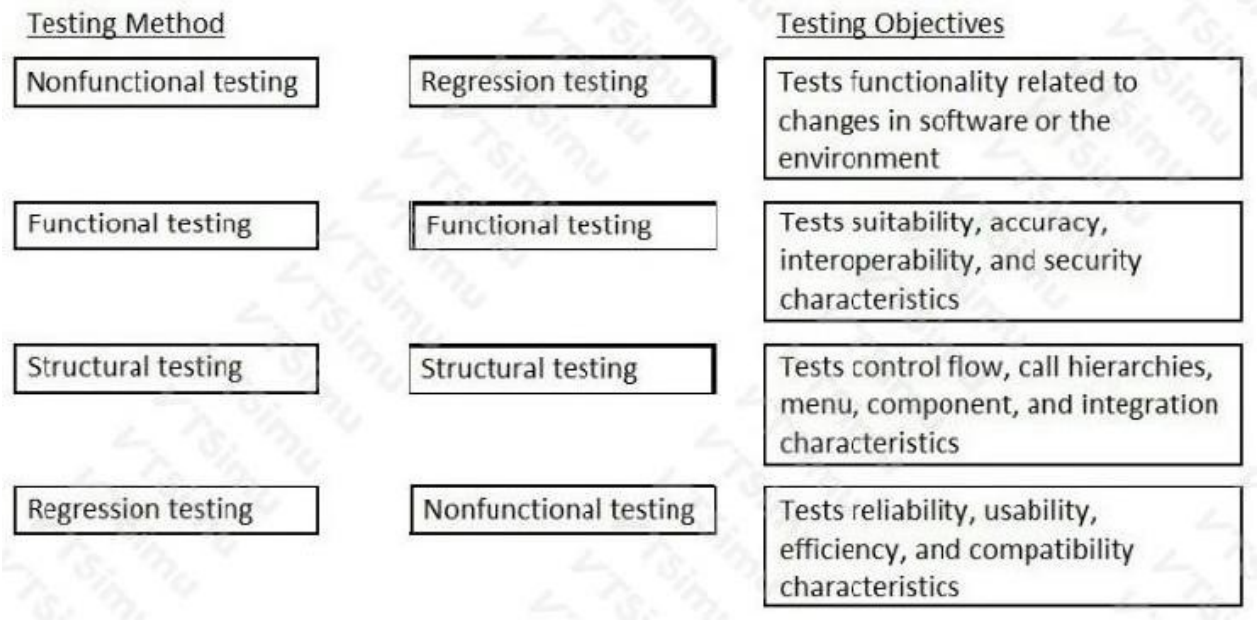
QUESTION NO: 120 - (DRAG DROP)

DRAG DROP -

Match the following generic software testing methods with their major focus and objective. Drag each testing method next to its corresponding set of testing objectives.



ANSWER:



Explanation:

The completed mapping correctly connects each generic testing method to the assurance objective it is designed to address. Regression testing is used after a software modification, patch, configuration update, or environmental change to confirm that previously established behavior remains intact. Its purpose is to identify unintended effects introduced by change, so it properly corresponds to testing functionality related to changes in the software or its environment. NIST defines regression testing as re-running functional and nonfunctional tests to ensure that previously developed and tested software still performs after a change. See the NIST CSRC definition of regression testing.

Functional testing verifies that the system provides required capabilities correctly. Suitability, accuracy, interoperability, and security are characteristics of whether the implemented functions satisfy defined requirements. This includes making sure security-relevant functions, such as authentication, authorization, and protected data handling, behave as specified.

Structural testing examines the internal organization and construction of software. Control flow, call hierarchies, components, menus, and integration paths are all internal structural concerns. This approach supports confidence that code paths, module interactions, and implementation structure operate as intended, rather than assessing only externally visible outcomes.

Nonfunctional testing evaluates the quality characteristics that describe how well a system operates. Reliability, usability, efficiency, and compatibility are system-quality attributes that apply across functions and help determine whether a system is

dependable, practical to use, performant within expected constraints, and able to operate with its required platforms or interfaces. These quality concepts are represented in the ISO/IEC 25010 software product quality model. Together, the four mappings provide complementary coverage of changed behavior, required functions, internal structure, and operational quality.

QUESTION NO: 121

Which is the PRIMARY mechanism for providing the workforce with the information needed to protect an agency's vital information resources?

A. Implementation of access provisioning process for coordinating the creation of user accounts.

B. Incorporating security awareness and training as part of the overall information security program.

C. An information technology (IT) security policy to preserve the confidentiality, integrity, and availability of systems.

D. Execution of periodic security and privacy assessments to the organization.

ANSWER: B

Explanation:

Incorporating security awareness and training as part of the overall information security program is the primary mechanism because it directly delivers the knowledge, skills, and behavioral expectations personnel need to safeguard information resources in their daily work. A policy establishes management's security direction and requirements, but awareness and training ensure that workforce members receive, understand, and can apply those requirements. This includes recognizing phishing and social-engineering attempts, handling sensitive information appropriately, using authentication securely, reporting suspected incidents, and following organization-specific procedures.

Effective awareness and training is continuous rather than a one-time event. It begins during onboarding, is refreshed periodically, and is tailored for particular roles, especially those with administrative, privileged, development, or incident-response responsibilities. It also supports a security-conscious culture by making every member of the workforce accountable for protecting organizational assets. NIST identifies awareness and training as a foundational element of an information security program and specifies that organizations provide basic security awareness training to system users and role-based security training where applicable. This makes security awareness and training the most direct and scalable means of equipping the workforce to protect vital agency resources. See NIST SP 800-50, Building an Information Technology Security Awareness and Training Program and NIST SP 800-53 Rev. 5, Awareness and Training controls.

QUESTION NO: 122

A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected.

What is the MOST probable security feature of Java preventing the program from operating as intended?

A. Least privilege.

B. Privilege escalation.

C. Defense in depth.

D. Privilege bracketing.

ANSWER: A

Explanation:

Least privilege is correct because Java's security architecture has historically restricted code to only the permissions explicitly granted to it. A program running on computer C that must access a file associated with computer A and then establish communications with computer B requires distinct permissions for the relevant file operations and network connections. In a restricted Java execution environment, the runtime's policy and permission checks can deny these

operations unless the code has been specifically authorized. This reflects the least-privilege principle: software should receive only the minimum access necessary for its authorized purpose, rather than unrestricted access to files and arbitrary network destinations. Java implemented this approach through mechanisms such as permission policy files, stack inspection, and security-manager checks in legacy controlled environments. Although the Security Manager has been deprecated and is being removed from modern Java, the scenario describes the classic Java security model commonly tested in CISSP material. For the application to operate legitimately, its deployment design must provide narrowly scoped, approved access to the required file and network resources, ideally through an authenticated service interface rather than broad host-level permissions. See Oracle's Java permissions documentation and NIST's definition of least privilege.

QUESTION NO: 123

Multi-threaded applications are more at risk than single-threaded applications to

A. race conditions.

B. virus infection.

C. packet sniffing.

D. database injection.

ANSWER: A

Explanation:

Multi-threaded applications are more at risk of **race conditions.** A race condition occurs when multiple threads concurrently access or modify shared data or another shared resource and the program's outcome depends on the unpredictable timing or sequence in which those threads execute. Because a single-threaded application executes one instruction flow at a time, it does not have the same inherent concurrent access risk. In a multi-threaded design, developers must deliberately control access to shared state with appropriate synchronization mechanisms, such as locks, mutexes, semaphores, atomic operations, or carefully designed message passing.

From a security perspective, race conditions can become time-of-check to time-of-use vulnerabilities, where an attacker exploits the small interval between validation of a resource and its subsequent use. The resulting behavior can undermine integrity controls, cause inconsistent application state, expose or overwrite data, or enable unauthorized actions when security-relevant operations are not performed atomically. Secure concurrency design therefore requires identifying shared resources, minimizing mutable shared state, and ensuring that critical operations are synchronized and atomic where necessary. OWASP discusses race conditions as a weakness arising from concurrent execution and emphasizes controlling the sequence of security-sensitive operations. See the OWASP Race Conditions resource and the MITRE CWE-362: Race Condition entry.

QUESTION NO: 124

What is the best way for mutual authentication of devices belonging to the same organization?

A. Token

B. Certificates

C. User ID and passwords

D. Biometric

ANSWER: B

Explanation:

Certificates are the best choice for mutual authentication between devices in the same organization because they provide each endpoint with a cryptographically verifiable identity. In a well-managed public key infrastructure, the organization issues device certificates through its trusted certificate authority and configures each device to trust the issuing authority. During a

mutually authenticated protocol exchange, such as mutual TLS, each device presents its certificate and proves possession of the associated private key. Each peer can then validate the certificate chain, issuer, validity period, and identity information before establishing a protected session.

This approach scales effectively for device-to-device communications because certificate issuance, renewal, revocation, trust anchors, and authorization attributes can be centrally governed. It also supports strong authentication without transmitting reusable shared secrets and allows encryption and integrity protections to be negotiated as part of the secure channel. The TLS specification describes certificate-based authentication and the use of a CertificateRequest message when the server requests client authentication. NIST's guidance also identifies certificate-based authentication as an authentication mechanism based on public-key cryptography. See RFC 8446: The Transport Layer Security Protocol Version 1.3 and NIST SP 800-63B, Digital Identity Guidelines.

QUESTION NO: 125

Which of the following is a unique feature of attribute-based access control (ABAC)?

A. A user is granted access to a system at a particular time of day.

B. A user is granted access to a system based on username and password.

C. A user is granted access to a system based on group affinity.

D. A user is granted access to a system with biometric authentication.

ANSWER: A

Explanation:

"A user is granted access to a system at a particular time of day." is the best answer because ABAC evaluates authorization policies against attributes associated with the subject, object, requested action, and environment. Time is an environmental attribute: it describes the context in which the access request occurs rather than being a permanent characteristic of the user or resource. An ABAC policy can therefore permit a user to perform a specified action on a resource only during an approved time window, such as normal business hours, and deny the identical request outside that window. This demonstrates ABAC's central capability: making fine-grained, dynamic decisions from multiple policy-relevant attributes at the time a request is evaluated. The applicable policy may also incorporate attributes such as resource classification, user department, device state, network location, and purpose of use, but the time-based condition directly illustrates environmental context driving authorization. NIST defines ABAC as a logical access-control methodology in which authorization is determined by evaluating attributes and rules; its ABAC guidance explicitly identifies environmental attributes as relevant inputs to policy decisions. See NIST's Attribute Based Access Control project and NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations.

QUESTION NO: 126

Which of the following is the MOST common use of the Online Certificate Status Protocol (OCSP)?

A. To verify the validity of an
X.509 digital certificate

B. To obtain the expiration date of an
X.509 digital certificate

C. To obtain the revocation status of an
X.509 digital certificate

D. To obtain the author name of an
X.509 digital certificate

ANSWER: C

Explanation:

The most common use of the Online Certificate Status Protocol (OCSP) is to obtain the revocation status of an X.509 digital certificate. A certificate may remain within the dates specified in its validity period but no longer be trustworthy—for example, if its private key has been compromised or the certificate was incorrectly issued. OCSP lets a relying party ask an OCSP responder, generally operated by the issuing certificate authority or its delegate, for the current status of a particular certificate. The responder returns a signed status indicating that the certificate is good, revoked, or unknown. This supports timely revocation checking without requiring the client to download and search a potentially large certificate revocation list. OCSP is therefore commonly used in public key infrastructure and TLS deployments. Servers can also use OCSP stapling, in which the server obtains a recent signed OCSP response and provides it during the TLS handshake, reducing client queries to the responder. RFC 6960 defines OCSP specifically as a protocol for determining the revocation status of an identified certificate. See RFC 6960 and Microsoft's Certificate Revocation documentation.

QUESTION NO: 127

Attack trees are MOST useful for which of the following?

A. Determining system security scopes

B. Generating attack libraries

C. Enumerating threats

D. Evaluating Denial of Service (DoS) attacks

ANSWER: C

Explanation:

Enumerating threats is correct because an attack tree is a structured threat-modeling technique that begins with an attacker's objective and decomposes it into progressively more specific subgoals, attack paths, and required conditions. This systematic decomposition helps a security team identify the different ways an adversary could compromise an asset, violate a security objective, or exploit a system feature. The resulting tree makes potential threats visible in a form that supports later analysis of likelihood, cost, required skills, controls, and residual risk.

Attack trees are particularly valuable early in design and risk assessment because they encourage analysts to consider both direct and indirect paths to an attacker goal rather than focusing only on familiar attack scenarios. A single tree can represent alternative routes using logical relationships, such as paths where any one action is sufficient or where several actions must be combined. That organized enumeration gives stakeholders a more complete threat landscape and provides useful input to security requirements, architectural decisions, and control selection. OWASP describes attack trees as a way to model threats by representing an attacker goal and the possible means of achieving it; Carnegie Mellon's SEI similarly presents attack trees as a method for analyzing attack possibilities and their structure. See the OWASP Threat Modeling guidance and the SEI Attack Trees resource.

QUESTION NO: 128

Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?

A. Personnel turnover.

B. Large plans can take a lot of work to maintain.

C. Continuous auditing makes a Disaster Recovery plan irrelevant

D. Infrastructure and environment changes.

ANSWER: C

Explanation:

Continuous auditing makes a Disaster Recovery plan irrelevant is the statement that is not true. Continuous auditing provides ongoing assessment evidence about controls, configurations, compliance, and operational conditions. This

information can be valuable for disaster recovery governance because it may identify system changes, control gaps, or process issues that should prompt a review of recovery documentation and procedures. It does not, however, provide the capabilities required to recover services after a disruptive event.

A disaster recovery plan remains necessary to establish recovery priorities, assigned responsibilities, communications and escalation procedures, alternate processing arrangements, backup restoration methods, and recovery time and recovery point objectives. These elements must be coordinated and exercised so that personnel can execute recovery activities effectively during an actual incident. NIST contingency-planning guidance specifically treats plan maintenance and testing as continuing lifecycle activities, including revising plans when systems, personnel, dependencies, or business requirements change. Audit activity can support that lifecycle, but it cannot substitute for a tested, actionable recovery plan. ISC2's resilience and business-continuity concepts likewise require organizations to maintain recovery capability despite monitoring or assurance activities. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and Ready.gov guidance for business continuity implementation.

QUESTION NO: 129

Which of the following is NOT an example of a detective control?

A. System Monitor.

B. IDS.

C. Motion detector.

D. Backup data restore.

ANSWER: D

Explanation:

Backup data restore is the correct answer because restoring data is a corrective and recovery activity, not a detective control. Detective controls identify or reveal security events, policy violations, failures, or other conditions requiring attention. Their purpose is to provide visibility through activities such as monitoring, logging, alerting, review, and detection so that personnel or automated processes can initiate an appropriate response. By contrast, a backup restoration occurs after data has been lost, corrupted, encrypted, deleted, or otherwise made unavailable. Its purpose is to remediate the effect of that incident and return data or services to an acceptable, known-good state. In a CISSP context, this supports resilience, business continuity, and disaster recovery by helping preserve or reestablish availability and integrity. NIST similarly distinguishes the Detect function, which focuses on timely discovery of cybersecurity events, from the Recover function, which focuses on restoring capabilities or services impaired by an incident. Backup restoration therefore belongs to the recovery and corrective side of security control operation, even when it is initiated as part of a broader incident-response process. See the NIST Cybersecurity Framework for the Detect and Recover functions and NIST SP 800-34 Rev. 1 for contingency-planning and system-recovery guidance.

QUESTION NO: 130

What is the BEST way to encrypt web application communications?

A. Secure Hash Algorithm 1 (SHA-1).

B. Secure Sockets Layer (SSL).

C. Cipher Block Chaining Message Authentication Code (CBC-MAC)

D. Transport Layer Security (TLS).

ANSWER: D

Explanation:

Transport Layer Security (TLS) is the appropriate standard for encrypting communications between a web application and its clients. When HTTP is delivered over TLS, it is known as HTTPS. TLS protects data in transit by establishing an authenticated, encrypted channel before application data such as credentials, session identifiers, payment information, API requests, and responses are exchanged. Its authentication capabilities let a client validate the web server's identity through a certificate and hostname validation, reducing the risk that users send sensitive data to an impersonating endpoint. TLS also provides integrity protection, enabling endpoints to detect unauthorized modification of data while it traverses a network.

For a secure deployment, organizations should use currently supported TLS versions—normally TLS 1.3, with TLS 1.2 where interoperability requires it—and configure strong cipher suites and certificate lifecycle management. TLS is designed specifically for protecting network transport and is the foundation of modern secure web communications. NIST provides implementation and configuration guidance in SP 800-52 Rev. 2. The IETF's current TLS 1.3 specification is available in RFC 8446.

QUESTION NO: 131

Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?

A. Interface with the Public Key Infrastructure (PKI)

B. Improve the quality of security software

C. Prevent Denial of Service (DoS) attacks

D. Establish a secure initial state

ANSWER: D

Explanation:

Including a Trusted Platform Module (TPM) in a computer system's design helps establish a secure initial state. A TPM is a dedicated hardware security component that can securely generate, protect, and use cryptographic keys while maintaining protected records of integrity measurements. During the boot process, the platform can measure critical components, such as firmware, boot loaders, and operating-system startup components, before they execute. These measurements are stored in TPM Platform Configuration Registers, creating evidence of the system's startup state.

This capability supports measured boot and, where platform policy permits, trusted boot decisions. The resulting measurements can be evaluated locally or supplied to a relying party through remote attestation, enabling verification that a device began operation from an expected, known-good configuration. Establishing this trustworthy starting point is fundamental because security controls loaded later depend on the integrity of the platform and software that loaded them. TPM-supported protection can also underpin functions such as device encryption key protection and platform identity, but its core architectural contribution in this context is providing a hardware root of trust for the system's initial state. See the Trusted Computing Group TPM specifications and Microsoft's Trusted Platform Module overview.

QUESTION NO: 132

Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

A. Forensic disk imaging

B. Live response

C. Memory collection

D. Malware analysis

ANSWER: B

Explanation:

Live response is the appropriate technique because it enables an investigator to collect and assess evidence while the potentially compromised system remains operational. When a rootkit is suspected, time matters: the system's current runtime state can contain active processes, network sessions, loaded drivers or modules, command history, logged-on users, and other volatile indicators that support immediate triage and containment decisions. A live response can include targeted acquisition of volatile data, including RAM, but it is broader than memory collection alone because it supports rapid examination of the running host and collection of several high-value evidence sources in a prioritized manner.

This approach follows the forensic principle of considering volatility and operational needs during incident response. The response team should use trusted collection tools, document every action, preserve timestamps and command output, and maintain chain-of-custody records. These practices help ensure that the rapidly collected information remains useful for both technical investigation and any subsequent evidentiary process. NIST describes collecting volatile data from live systems as part of integrating forensic techniques into incident response, while CISA emphasizes timely evidence gathering and documentation during incident handling. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and CISA Incident Handler's Handbook.

QUESTION NO: 133

A security practitioner has been asked to model best practices for disaster recovery (DR) and business continuity. The practitioner has decided that a formal committee is needed to establish a business continuity policy. Which of the following BEST describes this stage of business continuity development?

A. Developing and Implementing business continuity plans (BCP).

B. Project Initiation and Management.

C. Risk Evaluation and Control.

D. Business impact analysis (BIA).

ANSWER: B

Explanation:

Project Initiation and Management is the appropriate stage because business continuity must first be established as an authorized, governed organizational program. At this point, senior management sponsorship is obtained, program scope and objectives are defined, responsibilities are assigned, and a cross-functional business continuity committee or steering group is created. That committee provides the authority and representation needed to establish the business continuity policy, set direction, approve priorities, allocate resources, and coordinate participation across business units. A policy is a management-level statement of commitment and expectations; therefore, its creation belongs at the beginning of the lifecycle, before the organization performs detailed impact analysis, evaluates risks, or develops recovery procedures. Effective initiation and management also establishes the ongoing governance needed to maintain, test, review, and improve continuity capabilities as business conditions change. ISO 22301 emphasizes leadership commitment, establishment of a business continuity policy, and assignment of organizational roles as foundational elements of a business continuity management system. The U.S. Federal Emergency Management Agency likewise identifies program management and organizational coordination as essential foundations for continuity planning. See ISO 22301:2019—Business continuity management systems and Ready.gov—Business continuity planning.

QUESTION NO: 134

Which of the following is the MOST effective method of mitigating data theft from an active user workstation?

A. Implement full-disk encryption

B. Enable multifactor authentication

C. Deploy file integrity checkers

D. Disable use of portable devices

ANSWER: D

Explanation:

Disabling use of portable devices is the most effective choice because it directly removes a common and readily available path for copying data from a workstation that is already active and accessible to a user. Removable media, such as USB flash drives and external storage devices, can transfer substantial volumes of sensitive information quickly, often without requiring network connectivity. Enforcing technical controls that block or tightly restrict portable-storage use reduces the opportunity for unauthorized local data removal at the endpoint—the threat described in the question. This is an endpoint and media-control measure: it addresses the data-exfiltration channel itself rather than merely protecting data at rest or strengthening the initial authentication process. CISSP candidates should connect this control to security operations practices for managing endpoint devices and preventing unauthorized data movement. NIST SP 800-53's Media Use control calls for restricting the use of removable media on information systems, including prohibiting use where appropriate and enforcing organizationally defined restrictions. See NIST SP 800-53 Rev. 5 and ISC2's CISSP Exam Outline.

QUESTION NO: 135

An attack that involves a fraudster tricking a user into making inappropriate security decisions is known as:

A. Spoofing

B. Surveillance

C. Social Engineering

D. Man-in-the-Middle.

ANSWER: C

Explanation:

Social Engineering is correct because it is the deliberate use of deception and psychological manipulation to cause a person to make a decision or take an action that undermines security. Rather than directly exploiting a technical vulnerability, the attacker targets the human element—such as trust, fear, urgency, curiosity, or willingness to help—to bypass controls. For example, a fraudster might impersonate a help-desk employee and persuade a user to disclose a password, create a convincing pretext to obtain sensitive information, or pressure an employee into approving a malicious request. The defining feature is that the victim is manipulated into making an inappropriate security decision that benefits the attacker. Social engineering can be delivered through email, phone calls, text messages, social media, or in-person interactions, and it frequently serves as an initial access technique for broader compromise. Security awareness training, verification procedures, and reporting suspicious requests are important safeguards because they help users recognize and resist manipulative tactics. CISA describes social engineering as tactics used to deceive users into revealing sensitive information or performing harmful actions; see CISA guidance on social engineering and phishing. For additional terminology and examples, consult the OWASP Social Engineering overview.

QUESTION NO: 136

Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

A. Install mantraps at the building entrances

B. Enclose the personnel entry area with polycarbonate plastic

C. Supply a duress alarm for personnel exposed to the public

D. Hire a guard to protect the public area

ANSWER: C

Explanation:

Supply a duress alarm for personnel exposed to the public is the most cost-effective reactive physical-security control. A reactive control is intended to initiate a response once a threat, emergency, or attack is occurring, rather than to stop the event before it begins. A duress alarm gives an employee a rapid, discreet way to summon assistance when confronted with violence, a robbery, harassment, or another immediate safety concern. Depending on the implementation, activation can notify an onsite security team, a monitoring center, or law enforcement and can provide the alarm location so responders can act quickly.

This approach directly protects personnel working in areas where interaction with the public creates an elevated potential for confrontation, while generally requiring limited equipment, installation, and operating expense. It can be implemented as a fixed panic button, wearable device, wireless pendant, or integrated alarm feature. Its value comes from improving notification and response time without requiring continuous staffing or extensive facility modification. NIST physical and environmental protection guidance recognizes the use of emergency mechanisms and alarms to support personnel safety and response activities. See NIST SP 800-53 Rev. 5 and the OSHA workplace violence resources for guidance on emergency response and workplace safety planning.

QUESTION NO: 137

When reviewing the security logs, the password shown for an administrative login event was ' OR ' '1'='1' --. This is an example of which of the following kinds of attack?

A. Structured Query Language (SQL) Injection.

B. Brute Force Attack.

C. Rainbow Table Attack.

D. Cross-Site Scripting (XSS).

ANSWER: A

Explanation:

Structured Query Language (SQL) Injection is correct because `' OR ' '1'='1' --` is a recognizable SQL injection payload intended to alter the logic of a database query used in authentication. Vulnerable applications may construct a query by directly concatenating the supplied username and password into SQL. The injected `OR` expression creates a condition that evaluates as true, while `--`, a comment marker in commonly used SQL dialects, can comment out the remainder of the intended query. The resulting query may therefore bypass an authentication check if the application does not safely separate untrusted input from SQL code. This is an injection vulnerability and a secure-coding issue, rather than simply an attempted password guess. Effective prevention relies primarily on parameterized queries or prepared statements, which ensure input is treated as data rather than executable query syntax. Input validation and using database accounts with only the privileges required by the application provide important additional layers of defense. OWASP identifies SQL injection as the insertion of malicious SQL statements into an entry field for execution and recommends parameterized interfaces as a primary defense. See the OWASP SQL Injection overview and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 138

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will be the PRIMARY security concern as staff is released from the organization?

A. Inadequate IT support

B. Loss of data and separation of duties

C. Undocumented security controls

D. Additional responsibilities for remaining staff

ANSWER: B

Explanation:

Loss of data and separation of duties is the primary concern because staff reductions directly affect both the control of privileged access and the ability to maintain effective independent oversight of logical-access administration. Departing personnel may retain knowledge of systems, credentials, administrative procedures, or access paths that must be promptly identified and removed during the offboarding process. If those accounts, tokens, keys, remote-access methods, or shared administrative credentials are not addressed, organizational data is exposed to unauthorized disclosure, alteration, destruction, or unavailability.

At the same time, the scenario specifically states that security work is integrated into IT operations rather than performed by separate roles. With fewer people, remaining staff may be required to request, approve, provision, review, and potentially audit access within the same operational function. This erodes separation of duties and increases the risk that inappropriate or excessive access can be created or retained without independent detection. Separation of duties is a foundational access-control principle intended to prevent a single individual from controlling conflicting steps in a sensitive process. CISSP's Security Operations domain includes personnel security and access-control administration concerns, while NIST control AC-5 formally addresses separation of duties for organizational systems. See the ISC2 CISSP Exam Outline and NIST SP 800-53 AC-5.

QUESTION NO: 139

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) only provides which of the following?

A. Mutual authentication.

B. Server authentication.

C. User authentication.

D. Streaming ciphertext data.

ANSWER: C

Explanation:

User authentication. EAP-MD5 is an EAP method that performs one-way, client-to-network authentication through an MD5 challenge-response exchange. The authenticator sends a challenge, and the supplicant responds with an MD5 hash calculated from the challenge and its shared secret. Successful validation demonstrates that the user or client possesses the secret without transmitting the secret itself in cleartext. This is the authentication service EAP-MD5 supplies: verification of the supplicant to the network.

For EAP methods used with IEEE 802.1X, suitable methods generally need to produce keying material for subsequent protection of the connection. RFC 3748 explicitly notes that EAP-MD5 does not support key derivation and therefore cannot be used where dynamic keying is required, such as wireless LAN authentication methods that protect traffic after access is granted. It also does not authenticate the network to the client. Consequently, EAP-MD5 is an older authentication-only method rather than a modern mutual-authentication and key-establishment solution. See RFC 3748, section 5.4 for the EAP-MD5 method and its lack of key derivation, and RFC 1994 for the underlying MD5 challenge-response approach.

QUESTION NO: 140

A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

A. Transport.

B. Data link.

C. Network.

D. Application.

ANSWER: D

Explanation:

Application. A proxy firewall, also called an application-level gateway, operates primarily at OSI Layer 7 because it understands and mediates specific application protocols rather than merely forwarding packets based on network addresses or transport ports. It acts as an intermediary: the client connects to the proxy, the proxy evaluates the request according to the relevant protocol and security policy, and the proxy establishes a distinct connection to the requested service when the request is permitted. For example, an HTTP proxy can interpret HTTP requests and apply controls based on application-aware attributes such as requested URLs, methods, headers, content types, and protocol conformance. This application awareness allows the firewall to perform detailed inspection and enforce policies that depend on the meaning of the traffic, which is the defining feature of a proxy firewall. NIST describes application-proxy gateways as firewalls that relay application traffic and can perform application-specific security functions. ISC2 candidates should associate proxy or application gateway terminology with Layer 7, even though the device necessarily uses lower-layer networking and transport services to communicate. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and Cloudflare's proxy firewall overview.

QUESTION NO: 141

Which stage in the identity management (IdM) lifecycle constitutes the GREATEST risk for an enterprise if performed incorrectly?

A. Propagating

B. Deprovisioning

C. Provisioning

D. Maintaining.

ANSWER: B

Explanation:

Deprovisioning constitutes the greatest enterprise risk if it is performed incorrectly because this lifecycle stage ensures that access is revoked as soon as a user no longer has a legitimate business need for it. When an employee leaves, a contractor's engagement ends, or a user changes roles, incomplete or delayed deprovisioning can leave accounts, group memberships, privileged roles, VPN access, API keys, active sessions, and SaaS entitlements available for misuse. Such residual access may be used by a former user or exploited by an attacker who obtains the still-valid credentials. Effective deprovisioning must therefore be prompt, comprehensive, and verifiable across the identity provider, directories, applications, cloud platforms, and privileged-access systems. It should disable or remove accounts as appropriate, revoke tokens and sessions, remove entitlements and credentials, and retain appropriate audit evidence. This directly supports least privilege and account-management controls. NIST SP 800-53 control AC-2 requires organizations to manage information-system accounts, including disabling accounts within defined time periods when users no longer need access. NIST's digital identity guidance also emphasizes lifecycle management of authenticators and associated credentials. See NIST SP 800-53 Rev. 5, AC-2 Account Management and NIST SP 800-63B, Digital Identity Guidelines.

QUESTION NO: 142

Which of the following is a characteristic of an internal audit?

A. An internal audit is typically shorter in duration than an external audit.

B. The internal audit schedule is published to the organization well in advance.

C. The internal auditor reports to the Information Technology (IT) department

D. Management is responsible for reading and acting upon the internal audit results

ANSWER: D

Explanation:

Management is responsible for reading and acting upon the internal audit results because internal audit provides independent, objective assurance and advice, but it does not assume management's ownership of risks, controls, or remediation. Internal auditors communicate findings, conclusions, and recommendations to the appropriate stakeholders. Management then evaluates the reported issues, determines the appropriate corrective actions, assigns accountable owners, and supplies action plans and target dates. Internal audit may subsequently follow up to assess whether management's actions have been implemented and whether they adequately address the underlying risk; this follow-up preserves internal audit's independent assurance role rather than transferring responsibility for remediation to the auditors.

This division of responsibilities is central to sound governance. Operational management owns and manages risk and controls, while internal audit evaluates and reports on the effectiveness of governance, risk management, and control processes. Escalation to the audit committee or board may be appropriate for significant findings, overdue remediation, or management acceptance of risk, but management remains accountable for responding to audit results within its area of responsibility. The Institute of Internal Auditors' Global Internal Audit Standards describe the communication of engagement results and management action plans, and its Three Lines Model distinguishes management's risk-management role from internal audit's independent assurance role. See the IIA Global Internal Audit Standards and the IIA overview of the Standards.

QUESTION NO: 143

A software developer wishes to write code that will execute safely and only as intended. Which of the following programming language types is MOST likely to achieve this goal?

A. Weakly typed.

B. Dynamically typed.

C. Strongly typed.

D. Statically typed.

ANSWER: C

Explanation:

Strongly typed. is the best answer because a strong type system rigorously enforces the rules governing data types and the operations permitted on them. When code attempts to use a value in a manner incompatible with its declared or inferred type, the language implementation requires an explicit, valid conversion or reports an error. This makes program behavior more predictable and helps developers detect defects before they can produce unintended execution paths.

For secure software development, strong typing reduces the likelihood of type confusion, accidental interpretation of data in an unintended form, and logic errors resulting from ambiguous or implicit conversions. It also makes assumptions about data more visible in the source code, improving reviewability, maintainability, and assurance that code processes values according to the developer's intent. These controls complement—not replace—secure design, validation of untrusted input, error handling, and testing. The CERT Secure Coding standard emphasizes practices that prevent unexpected behavior and vulnerabilities in software, while the SEI discusses how type-related weaknesses can affect software security. See the SEI CERT Coding Standards and the MITRE CWE entry for access of resource using incompatible type.

QUESTION NO: 144

Which of the following is NOT a two-factor authentication mechanism?

A. Something you have and something you know.

B. Something you do and a password.

C. A smartcard and something you are.

D. Something you know and a password.

ANSWER: D

Explanation:

Something you know and a password is not a two-factor authentication mechanism because both elements are knowledge-based authenticators. A password is itself “something you know,” so pairing it with another secret that the user knows—such as a PIN, passphrase, or answers to security questions—does not introduce an authenticator from a distinct factor category. It is therefore still single-factor authentication, even if multiple prompts or credentials are required. Two-factor authentication requires authenticators from two different categories, commonly knowledge, possession, and inherence. The security value comes from the independence of those categories: compromise of a memorized secret alone should not be sufficient for authentication when a separate authenticator, such as a cryptographic device or biometric characteristic, is also required. NIST describes multifactor authentication as use of more than one distinct authentication factor and discusses the categorization of memorized secrets, physical authenticators, and biometrics. This distinction is important when designing access controls because simply increasing the number of passwords does not provide the risk reduction expected from genuine multi-factor authentication. See NIST SP 800-63B: Digital Identity Guidelines and CISA: Turn On MFA.

QUESTION NO: 145

A bank failed to meet service-level agreements (SLA) with customers after suffering from a database failure of the transaction processing system (TPS) that resulted in delayed financial deposits. A regulatory agency overseeing the bank would like to determine if the cause of the delay was a material weakness. Which of the following documents is MOST relevant for the regulatory agency to review?

A. Business continuity plan (BCP).

B. Business impact analysis (BIA)

C. Continuity of Operations Plan (COOP)

D. Enterprise resource planning (ERP).

ANSWER: B

Explanation:

Business impact analysis (BIA) is the most relevant document because it formally evaluates how interruption of a business process or supporting system affects the organization. For the bank’s transaction processing system and database, the BIA should identify the process criticality, the consequences of delayed deposits, relevant legal and regulatory obligations, customer-service commitments such as SLAs, and the financial and reputational effects of an outage. It also establishes recovery requirements, commonly including recovery time objectives, recovery point objectives, and maximum tolerable downtime. A regulator can use this documented analysis to determine whether management recognized the transaction-processing environment as sufficiently critical, whether its defined recovery requirements were appropriate for the bank’s obligations, and whether the observed delay exceeded the organization’s stated tolerance. Those findings directly support an assessment of whether the failure reflects a material weakness in continuity planning, risk management, or internal controls. The BIA is a foundational input to continuity and recovery planning because it translates business impact into prioritized resilience requirements. NIST describes the BIA as determining the impact of system disruptions and identifying recovery priorities in NIST SP 800-34 Rev. 1. The FFIEC also addresses business impact analysis as a key component of financial-institution business continuity management in its Business Continuity Management Handbook.

QUESTION NO: 146

A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes.

What is the BEST design approach to securing this environment?

A. Use reverse proxies to create a secondary "shadow" environment for critical systems.

B. Place firewalls around critical devices, isolating them from the rest of the environment.

C. Layer multiple detective and preventative technologies at the environment perimeter.

D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

ANSWER: C

Explanation:

Layer multiple detective and preventative technologies at the environment perimeter is the best approach because it applies defense in depth at the principal trust boundaries while retaining the extensive intersite connectivity required by the business. A WAN that carries information with different sensitivity levels needs consistent enforcement points where traffic entering, leaving, and traversing organizational network boundaries can be authenticated, authorized, encrypted, filtered, inspected, and logged. Preventative technologies can enforce approved communications and reduce exposure, while detective technologies provide the visibility necessary to identify suspicious activity, policy violations, and control failures. Combining these control types avoids dependence on any one safeguard and supports timely detection and response when a preventive control is bypassed or misconfigured. This approach also permits controls to be managed consistently across a distributed environment and supports risk-based policy enforcement without unnecessarily disrupting legitimate business workflows. NIST defines defense in depth as using multiple layers of security controls so that the failure of one control does not leave the system unprotected. NIST firewall guidance likewise emphasizes firewalls and firewall policy as key mechanisms for controlling traffic between networks with differing trust levels. See the NIST definition of defense in depth and NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy.

QUESTION NO: 147

Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

A. Transparent Database Encryption (TDE)

B. Column level database encryption

C. Volume encryption

D. Data tokenization

ANSWER: D

Explanation:

Data tokenization protects personally identifiable information through substitution: the original sensitive value is removed from the operational dataset and replaced with a token, a surrogate value that has no inherent or exploitable relationship to the original data. For example, an account number may be replaced by a randomly generated token while applications continue to use that token for ordinary processing. The mapping between the token and the original PII is maintained separately in a protected token vault or tokenization system, with access restricted to authorized systems and personnel. This reduces exposure because databases, logs, analytics platforms, and business workflows can often operate on tokens rather than the actual sensitive identifiers. Unlike a reversible cryptographic transformation, tokenization is fundamentally a full replacement of the data element; recovering the original value requires access to the secured mapping service or vault. This makes tokenization especially useful for minimizing the number of systems that store or process raw PII and for reducing the scope of sensitive-data protection obligations. NIST describes tokenization as replacing a sensitive data element with a non-sensitive equivalent, while retaining the ability to retrieve the original value through a controlled process. See NIST's tokenization definition and PCI SSC's tokenization guidance.

QUESTION NO: 148

Which dynamic routing protocol is BEST suited for a dispersed campus network utilizing Internet Protocol version 6 (IPv6) addresses?

A. Open Shortest Path First (OSPF) version 3

B. Enhanced Interior Gateway Routing Protocol (EIGRP)

C. Border Gateway Protocol (BGP) version 4

D. Routing Information Protocol (RIP) version 2

ANSWER: A

Explanation:

Open Shortest Path First (OSPF) version 3 is the best fit because it is an open-standard interior gateway protocol specifically defined for IPv6 routing. A dispersed campus is normally administered as one organization's internal network, where a scalable IGP with fast convergence and a hierarchical design is appropriate. OSPFv3 uses link-state information and the Shortest Path First algorithm to calculate routes, enabling routers to react efficiently when an internal path or link changes. Its area-based architecture also supports logical segmentation as a campus grows across buildings, distribution layers, and multiple routed network segments.

OSPFv3 was specified initially for IPv6 in RFC 5340 and was later updated by RFC 5838 to support address families more flexibly. In IPv6 operation, OSPFv3 forms neighbor adjacencies using IPv6 link-local addresses, while IPv6 prefixes are advertised through link-state advertisements. These characteristics make it a mature, interoperable choice for enterprise IPv6 routing. The protocol's standards-based design and support for multi-area deployment provide the scale, resilience, and rapid internal route convergence expected in a dispersed campus environment. See RFC 5340: OSPF for IPv6 and RFC 5838: Support of Address Families for OSPFv3.

QUESTION NO: 149

A business continuity plan is an example of which of the following?

A. Corrective control.

B. Detective control.

C. Preventive control.

D. Compensating control.

ANSWER: A

Explanation:

A business continuity plan is a **corrective control** because its primary purpose is to enable an organization to continue or restore critical business operations after a disruption. It documents the actions, assigned responsibilities, communications processes, recovery priorities, alternate facilities or work arrangements, and resources needed to sustain essential functions at an acceptable level. Although the plan is developed before an incident, its operational value is realized when a disruptive event has occurred or is occurring and the organization must mitigate business impact and recover services.

In CISSP-aligned security practice, corrective controls reduce the effects of an incident and support return to an acceptable operational state. Business continuity planning is therefore part of organizational resilience: it connects business-impact analysis, recovery strategies, plan implementation, testing, maintenance, and ongoing improvement so that mission-essential processes can be resumed within defined recovery objectives. NIST contingency-planning guidance similarly describes continuity and recovery planning as a structured means of restoring information-system operations and supporting organizational missions following disruption. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and Ready.gov Business Continuity Planning.

QUESTION NO: 150

An employee's home address should be categorized according to which of the following references?

A. The consent form terms and conditions signed by employees.

B. An organization security plan for human resources.

C. Existing employee data classifications.

D. The organization's data classification model.

ANSWER: D

Explanation:

The organization's data classification model is the appropriate reference because it is the formal, organization-wide framework used to assign information categories and corresponding handling requirements. An employee's home address is personally identifiable information because it can identify or help locate a specific individual. The data owner or responsible business function applies the established classification scheme by considering the information's sensitivity, applicable legal or contractual obligations, and the potential impact if confidentiality is compromised. The resulting classification drives consistent requirements for access control, storage, transmission, retention, and secure disposal throughout the information life cycle.

Although the precise label differs by organization, a home address will commonly receive a nonpublic or sensitive classification under the enterprise model. Using the organization's defined model ensures that personnel apply the same protection expectations to equivalent employee data, rather than creating separate informal labels for individual systems or departments. NIST describes PII as information that can distinguish or trace an individual's identity and explains that safeguarding requirements should be based on the context and potential impact of disclosure. See NIST SP 800-122, Guide to Protecting the Confidentiality of PII and NIST Privacy Framework.

QUESTION NO: 151

What is the MOST important factor in establishing an effective Information Security Awareness Program?

A. Obtain management buy-in.

B. Conduct an annual security awareness event.

C. Mandate security training.

D. Hang information security posters on the walls,

ANSWER: A

Explanation:

Obtain management buy-in is the most important factor because an information security awareness program needs visible executive sponsorship, organizational authority, and sustained resources to become part of the organization's culture rather than a one-time compliance activity. Senior management support establishes that secure behavior is a business priority, enables the assignment of program ownership and responsibilities, and provides the budget, time, tools, and communication channels needed to reach personnel effectively. It also gives the program the authority to align awareness content with enterprise risk, security policies, regulatory obligations, and strategic objectives. When leaders actively support and model the expected behaviors, personnel are more likely to understand that security responsibilities apply to their daily work and that participation is expected across the organization. ISC2's CISSP outline includes security-awareness, education, and training as part of security-program concepts within Security and Risk Management, where governance and management commitment provide the foundation for implementation. NIST likewise identifies leadership support, resource allocation, and integration with organizational goals as central elements of a mature awareness and training program. See the ISC2 CISSP Certification Exam Outline and NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.

QUESTION NO: 152

In order for application developers to detect potential vulnerabilities earlier during the Software Development Life Cycle (SDLC), which of the following safeguards should be implemented FIRST as part of a comprehensive testing framework?

A. Source code review

B. Acceptance testing

C. Threat modeling

D. Automated testing.

ANSWER: C

Explanation:

Threat modeling should be implemented first because it is a proactive security activity performed during the requirements and design stages, before implementation decisions become embedded in code. It systematically identifies assets, trust boundaries, entry points, likely threat scenarios, and required mitigations. This gives developers a risk-informed foundation for the rest of the secure development and testing process. In particular, it helps establish security requirements, influences architecture choices, and identifies the areas that need focused verification, such as authentication, authorization, sensitive-data handling, interfaces, and external dependencies. A comprehensive testing framework is more effective when its test cases, code-analysis rules, and test priorities are derived from threats relevant to the application rather than applied generically after development is underway. This is a core “shift-left” practice: addressing foreseeable security issues at design time is generally less costly and more effective than discovering them after code has been written or accepted. OWASP describes threat modeling as a structured approach for identifying, quantifying, and addressing application threats, while Microsoft positions it as an essential design-phase activity for recognizing security concerns early. See OWASP Threat Modeling and Microsoft threat modeling guidance.

QUESTION NO: 153

Which of the following is a weakness of the Data Encryption Standard (DES)?

A. Block encryption scheme.

B. Use of same key for encryption and decryption.

C. Publicly disclosed algorithm.

D. Inadequate key length.

ANSWER: D

Explanation:

Inadequate key length is a fundamental weakness of DES. Although DES keys are commonly represented with 64 bits, 8 of those bits are used for parity, leaving an effective cryptographic key length of only 56 bits. This produces a key space of 2^{56} possible keys, which was once expensive to search but is now small enough for brute-force attacks using modern specialized or distributed computing resources. An attacker who obtains DES-encrypted material can systematically test candidate keys until a meaningful plaintext is recovered, without needing to discover a flaw in the cipher’s internal operations. The limited key length, rather than the basic Feistel block-cipher construction, is why DES no longer provides adequate protection for sensitive information. NIST withdrew DES as a federal standard after determining that its 56-bit key was no longer sufficient to protect unclassified information, and modern cryptographic implementations should instead use appropriately configured, currently approved algorithms such as AES. NIST also identifies three-key Triple DES as deprecated for applying cryptographic protection because of its reduced security margin and block-size limitations. See NIST’s FIPS 46-3 publication for DES and SP 800-131A Rev. 2 transition guidance.

QUESTION NO: 154

When recovering from an outage, what is the Recovery Point Objective (RPO), in terms of data recovery?

A. The RPO is the minimum amount of data that needs to be recovered.

B. The RPO is the amount of time it takes to recover an acceptable percentage of data lost.

C. The RPO is a goal to recover a targeted percentage of data lost.

D. The RPO is the maximum amount of time for which loss of data is acceptable.

ANSWER: D

Explanation:

The RPO is the maximum amount of time for which loss of data is acceptable. It establishes the point in time to which data must be restored following an interruption, expressed as a duration before the disruption. Put another way, it defines the organization's tolerated data-loss window, rather than the duration required to restore systems or services. If a business sets an RPO of four hours, its backup, replication, and logging arrangements must support recovery to a state no more than four hours before the outage. Changes made within that four-hour window may be unrecoverable, but that loss is within the risk tolerance approved by the business. RPO is determined through business impact analysis and reflects the value, volatility, and operational importance of the data. Critical transactional data may require a very short RPO and therefore near-continuous replication or frequent transaction-log backups; less critical data may support a longer interval. This metric helps security and continuity teams select and validate data-protection capabilities that meet documented recovery requirements. NIST defines recovery objectives as targets for restoring capabilities after a disruption, while Microsoft's disaster-recovery guidance clearly distinguishes RPO as the acceptable amount of data loss measured in time. See NIST CSRC: Recovery Point Objective and Microsoft Learn: RTO and RPO concepts.

QUESTION NO: 155

Which of the fallowing statements is MOST accurate regarding information assets?

A. International Organization for Standardization (ISO) 27001 compliance specifies which information assets must be included in asset inventory.

B. Information assets include any information that is valuable to the organization.

C. Building an information assets register is a resource-intensive job.

D. Information assets inventory is not required for risk assessment.

ANSWER: B

Explanation:

"Information assets include any information that is valuable to the organization" is the most accurate statement because information itself has business value and therefore requires appropriate governance and protection. Such assets can include customer and employee records, financial information, business plans, operational data, intellectual property, source code, research results, and trade secrets. Their value may arise from their importance to business operations, their confidentiality, legal or contractual obligations, their contribution to decision-making, or the competitive advantage they provide. Effective information security begins with knowing what information the organization owns or handles and understanding its value, sensitivity, ownership, location, and required level of protection. This understanding supports classification, risk assessment, control selection, and accountable management throughout the information lifecycle. ISO/IEC 27001 frames information security management around preserving the confidentiality, integrity, and availability of information through risk-based processes; an organization must determine the information and other assets relevant to its information security management system and manage associated risks. ISO's overview of the standard is available at ISO/IEC 27001. NIST likewise describes information and information systems as organizational assets that must be protected in a manner commensurate with risk, as outlined in FIPS Publication 199.

QUESTION NO: 156

When conducting a third-party risk assessment of a new supplier, which of the following reports should be reviewed to confirm the operating effectiveness of the security, availability, confidentiality, and privacy trust principles?

A. Service Organization Control (SOC) 1, Type 2.

B. Service Organization Control (SOC) 2, Type 2.

C. International Organization for Standardization (ISO) 27001.

D. International Organization for Standardization (ISO) 27002.

ANSWER: B

Explanation:

Service Organization Control (SOC) 2, Type 2 is the appropriate report because it provides independent assurance against the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria. Those criteria address security, availability, processing integrity, confidentiality, and privacy. The question specifically asks for confirmation of *operating effectiveness*, which is the defining value of a Type 2 examination: the service auditor evaluates whether the described controls were suitably designed and operated effectively throughout a specified examination period, rather than only as of a single date.

For third-party risk assessment, this makes a SOC 2 Type 2 report a useful source of evidence that a supplier has consistently performed relevant controls, such as logical access management, monitoring, incident response, change management, and protection of confidential or personal information. The report also identifies the system scope, applicable Trust Services Criteria, auditor's opinion, control tests performed, and test results. A reviewer can therefore assess whether the report's coverage and period align with the organization's supplier-risk requirements and determine whether any exceptions require follow-up or compensating measures.

The AICPA describes SOC 2 examinations and the Trust Services Criteria in its SOC suite of services and SOC 2 report overview.