DUMPSBOSS.

Certified in Cybersecurity

ISC2 CC

Version Demo

Total Demo Questions: 139

Total Premium Questions: 1395

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Principles	362
Topic 2, Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	246
Topic 3, Access Controls Concepts	281
Topic 4, Network Security	296
Topic 5, Security Operations	210
Total	1395

QUESTION NO: 1

An unknown person obtains unauthorized access to the company file system. This is an example of:

A. Intrusion

B. Breach

C. Exploit

D. Incident

ANSWER: B

Explanation:

Breach is correct because the unknown person has successfully obtained unauthorized access to a company information system. A breach is not merely an attempted or suspected security event; it represents a compromise in which an unauthorized party gains access to an organization's systems, information, or resources. Access to a company file system can expose the confidentiality of stored files and may also create opportunities to alter or remove information, so the organization must treat it as a confirmed compromise and initiate its incident-response process. ISC2's Certified in Cybersecurity learning materials distinguish successful unauthorized access from an attempted intrusion by recognizing the resulting compromise as a breach. The organization should preserve relevant evidence, determine the scope of files and accounts accessed, contain the unauthorized session, and assess any reporting or notification obligations. The precise impact may require investigation, but the confirmed unauthorized access itself establishes the breach condition. ISC2 discusses security incidents, access control, and organizational response responsibilities in its Certified in Cybersecurity certification overview. For widely used incident-handling guidance applicable after discovering such a compromise, see NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 2

Finance Server and Transactions Server has restored its original facility after a disaster, what should be moved in FIRST?

A. Management

B. Most critical systems

C. Most critical functions

D. Least critical functions

ANSWER: C

Explanation:

Most critical functions should be moved first during the return to the original facility, commonly called failback or reconstitution. Disaster recovery is driven by business priorities established through the business impact analysis. That analysis identifies the functions whose unavailability causes the greatest operational, financial, legal, or customer impact, as well as their recovery time objectives and dependencies. Once the primary site is ready, restoring these high-priority business functions first returns essential services to normal operations as quickly as possible while the remaining functions are transitioned in a controlled sequence.

For finance and transaction processing, the recovery team should follow the approved recovery and reconstitution plan, validate that the destination environment can securely support the necessary applications, data, connectivity, and supporting services, and then move the prioritized functions according to the established business recovery order. This approach aligns technical restoration with the organization's continuity requirements rather than simply moving assets based on convenience or organizational hierarchy. NIST explains that a business impact analysis determines the impact of disruption and helps establish recovery priorities; its contingency-planning guidance also covers reconstitution following recovery. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and NIST contingency planning resources.

QUESTION NO: 3

Which of the following scenarios best illustrates the concept of "Two-Person Integrity"?

A. A single administrator has the sole authority to grant access rights to all users.

B. Two or more individuals must collaborate to perform a critical task or make a decision.

C. Users are required to use two different passwords for accessing sensitive systems.

D. A system automatically logs off a user who has been inactive for a certain period.

ANSWER: B

Explanation:

Two-Person Integrity is best illustrated by “Two or more individuals must collaborate to perform a critical task or make a decision.” This control requires the involvement of at least two authorized people before a sensitive action can be completed. It is commonly applied to high-consequence activities, such as handling highly sensitive assets, approving major financial transactions, changing critical infrastructure, or performing actions that could create substantial organizational harm if misused. Requiring joint participation creates accountability because each person can observe, verify, and challenge the other’s actions. It also reduces the chance that one individual can act alone to commit fraud, misuse privileged access, make an unreviewed error, or bypass established procedures. In practice, the control may be implemented through dual authorization, dual custody, paired approvals, or a requirement for two people to be physically present during a protected operation. ISC2’s CC curriculum includes separation of duties as an administrative control that distributes sensitive responsibilities to limit opportunities for abuse; two-person integrity is a direct application of that principle to especially critical activities. NIST likewise identifies separation of duties as a control that prevents a single individual from being able to complete conflicting or sensitive actions independently. See ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-53 AC-5, Separation of Duties.

QUESTION NO: 4

Which of the following is unlikely to be a member of the disaster recovery team?

A. Executive management

B. Public relations

C. Billing clerk

D. IT personnel

ANSWER: C

Explanation:

Billing clerk is the correct choice because disaster recovery teams are generally composed of personnel with decision-making authority, technical recovery responsibilities, business-process ownership, and communications duties. A billing clerk’s routine role is usually focused on transaction processing and accounts-related administrative work, rather than coordinating enterprise recovery, restoring technology services, authorizing emergency expenditures, or managing stakeholder communications. Although a billing function may be important to business continuity and could provide subject-matter input when financial systems are restored, its typical clerical position would not ordinarily require standing membership on the core disaster recovery team. Team membership should be based on the recovery tasks that must be performed during an incident and on the authority needed to make timely recovery decisions. NIST guidance describes recovery planning as requiring defined recovery roles, responsibilities, and teams to restore information-system capabilities and resume operations. CISA similarly emphasizes assigning continuity and recovery responsibilities across organizational leadership, essential functions, communications, and technical operations. These principles support selecting personnel whose normal responsibilities directly align with planning, directing, communicating, or executing recovery activities. See NIST SP 800-34 Rev. 1 and CISA Business Resilience.

QUESTION NO: 5

Which of the following best describes the purpose of risk management in cybersecurity?

A. To eliminate all risks associated with information technology.

B. To identify, assess, and prioritize risks to ensure they are within acceptable levels.

C. To ensure that no cybersecurity incidents occur.

D. To transfer all risks to third parties through insurance and outsourcing.

ANSWER: B

Explanation:

Risk management exists to give an organization a structured, informed basis for handling uncertainty that could affect its information assets, operations, and objectives. The correct description is “To identify, assess, and prioritize risks to ensure they are within acceptable levels.” In practice, this includes identifying threats and vulnerabilities, analyzing the likelihood and potential business impact of adverse events, evaluating the resulting risk against the organization’s risk appetite and tolerance, and selecting appropriate treatment measures. Those measures can include reducing risk through controls, accepting a justified residual risk, transferring some financial consequences, or avoiding an activity when the risk exceeds what the organization is willing to bear.

Cybersecurity risk management is therefore a continuous business process rather than a one-time technical exercise. Conditions change as systems, threats, suppliers, regulations, and business priorities change; risks and controls must consequently be monitored and reassessed. This approach helps leadership allocate limited security resources to the risks that matter most while maintaining residual risk at a level the organization has formally determined to be acceptable. NIST describes risk management as a process for identifying, assessing, and responding to risk; its Risk Management Framework also emphasizes ongoing monitoring. See NIST: About the Risk Management Framework and ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 6

An earthquake is an example of a _____?

A. Threat agent

B. Threat

C. Vulnerability

D. Risk

ANSWER: B

Explanation:

An earthquake is correctly classified as a threat. In information security risk management, a threat is any circumstance, event, or condition with the potential to adversely affect an organization’s operations, assets, people, or information systems. Natural events—including earthquakes, floods, fires, and severe weather—can disrupt facilities, damage equipment, interrupt utilities and communications, and affect the availability of systems and data. The event itself has the potential to cause harm, which is the defining characteristic of a threat.

ISC2’s Certified in Cybersecurity material includes natural disasters among the types of threats organizations must account for when identifying and managing risk. An organization can reduce the potential impact of an earthquake through controls such as geographically resilient facilities, off-site backups, redundant systems, disaster recovery capabilities, and business continuity planning. These safeguards address the consequences of the threat, but do not change the classification of the earthquake as a threat. See ISC2’s Certified in Cybersecurity Exam Outline and NIST’s definition of threat.

QUESTION NO: 7

Often offered by third-party organizations and covering advisory or compliance objectives:

A. Standard

B. Policy

C. Procedure

D. Laws or Regulations

ANSWER: A

Explanation:

Standard is correct because standards are established specifications, practices, or benchmarks that organizations can use to achieve consistent security outcomes, demonstrate due diligence, and meet advisory or compliance objectives. In cybersecurity, standards may be created by independent standards bodies, industry groups, or other third-party organizations. Examples include ISO/IEC standards and the Center for Internet Security's CIS Controls and Benchmarks. Although many standards are voluntary by default, an organization, contract, customer requirement, or regulation may adopt or reference one, making adherence mandatory in that specific context. Standards provide a common, repeatable basis for designing, assessing, and improving an information security program. They can define security management expectations, technical configuration baselines, control objectives, or methods for evaluating conformance. ISC2's CC curriculum distinguishes standards from internal policies and procedures: standards provide established requirements or recommended criteria that support governance and security practices. ISO describes ISO/IEC 27001 as a widely recognized international standard for information security management systems, while CIS publishes community-developed security best practices and secure configuration guidance. See ISO/IEC 27001 overview and CIS Controls.

QUESTION NO: 8

Which IR phase involves identifying critical data and systems?

A. Detection and analysis

B. Preparation

C. Containment

D. Eradication

ANSWER: B

Explanation:

Preparation is the incident response phase in which an organization establishes the people, processes, technology, and information needed to respond effectively before an incident occurs. A key part of this readiness work is identifying and documenting critical systems, data, assets, business processes, and their owners. This inventory and prioritization enables the incident response team to understand what must be protected first, assess business impact quickly, and make informed decisions if those assets are affected. Preparation also includes defining incident response policies and procedures, assigning roles and responsibilities, establishing communications plans, providing training, and ensuring appropriate logging, monitoring, and response tools are available. ISC2's incident-response concepts emphasize preparedness as the foundation for a coordinated, timely response. NIST similarly describes preparation as establishing and maintaining the capability to handle incidents, including understanding organizational resources and priorities. Identifying critical data and systems before an event therefore supports accurate triage and effective protection of the organization's most important assets during an incident. See NIST SP 800-61, Computer Security Incident Handling Guide and ISC2 Certified in Cybersecurity.

QUESTION NO: 9

Token Ring operates at which OSI layer?

A. Application

B. Network

C. Transport

D. Physical

E. Data Link

ANSWER: E

Explanation:

Data Link is correct because Token Ring is a LAN access technology whose core function is controlling how devices share a network medium and exchange frames on the local network. In the OSI model, these responsibilities belong to the Data Link layer (Layer 2). Token Ring uses token passing: a control frame, called a token, circulates among participating stations, and a station transmits when it possesses that token. This is a media-access-control function, which is a central Layer 2 responsibility. Token Ring also defines frame-related behavior, addressing, and local delivery mechanisms associated with LAN communication. Although a Token Ring implementation necessarily uses physical media and signaling, the Token Ring protocol's defining access method is classified at the Data Link layer. ISC2 CC candidates should associate technologies that govern local frame transmission and access to a shared LAN medium with Layer 2. Cisco's overview of LAN switching describes the Data Link layer's role in media access and framing: Cisco: What Is a Network Switch?. The IEEE 802.5 standard identifies Token Ring as an IEEE LAN technology: IEEE 802.5 Token Ring.

QUESTION NO: 10

What role do firewalls play in access control?

A. Physical barriers that prevent unauthorized entry into secure premises

B. Devices that filter incoming network traffic based on a set of administrative security policies

C. Systems that monitor and log user activities within an information system

D. Mechanisms that encrypt data to protect its confidentiality

ANSWER: B

Explanation:

Devices that filter incoming network traffic based on a set of administrative security policies are a core technical access-control mechanism. A firewall sits at a network boundary or between network segments and evaluates traffic against configured rules. Those rules commonly use characteristics such as source and destination IP addresses, ports, protocols, connection state, application attributes, and—on next-generation firewalls—identified users. When traffic satisfies the policy, the firewall permits it; otherwise, it blocks or restricts the connection. This enforcement limits which systems, services, and network paths may be reached, applying the organization's authorized access rules to communications before they reach protected resources. Firewalls can also enforce outbound policies, helping control which internal systems may initiate connections to external destinations. In ISC2's access-control context, this is an example of a logical or technical control that supports policy enforcement and network segmentation. NIST describes firewalls as devices or programs that control network traffic flow between networks or hosts with differing security postures, based on a policy. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and the ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 11

What is the primary challenge associated with VPN use from remote locations, such as coffee shops?

A. The complete elimination of any potential cyber threats

B. Ensuring that the VPN connection does not encrypt any data

C. Protecting the path from the employee's computer to the office network from interception

D. Guaranteeing high-speed internet access at all remote locations

ANSWER: C

Explanation:

Protecting the path from the employee's computer to the office network from interception is the correct answer. Remote locations such as coffee shops commonly rely on public or otherwise untrusted Wi-Fi networks. A VPN addresses the key security challenge of sending organizational traffic across that untrusted network by creating an encrypted tunnel between the remote device and the VPN gateway. Encryption helps preserve the confidentiality of data in transit, while integrity protections help detect unauthorized modification; strong authentication also helps ensure that the user connects to the legitimate organizational VPN service. The practical objective is to prevent a person monitoring the local network, or positioned between the user and the internet, from reading or tampering with protected communications as they travel toward the office network. This remains especially important when employees access internal systems, business applications, or sensitive information away from a trusted corporate network. VPN use should be paired with sound endpoint security and user verification, but its central purpose in this scenario is protection of data traversing the remote network path. NIST describes VPNs as technologies that protect communications over public networks, and CISA provides guidance on securing telework connections and remote access. See NIST SP 800-77 Rev. 1 and CISA Telework Guidance.

QUESTION NO: 12

Which type of attack will most effectively maintain remote access and control over the victim's computer?

A. Phishing

B. Trojans

C. Cross-Site Scripting

D. Rootkits

ANSWER: D

Explanation:

Rootkits most effectively maintain remote access and control because they are designed to establish persistent, privileged access while hiding their presence from users, administrators, and security tools. A rootkit may operate in user mode, kernel mode, firmware, or the boot process, enabling it to conceal malicious processes, files, network connections, and configuration changes. This stealth makes it particularly valuable to an attacker who wants to retain control of a compromised endpoint over time. Rootkits are commonly associated with installing or protecting a backdoor or other remote-access capability, allowing the attacker to return to the system and execute actions without readily being detected. ISC2's Certified in Cybersecurity material identifies rootkits as malware intended to maintain privileged access and evade detection, aligning with the persistence and control described in the question. Because rootkits can interfere with the operating system's normal reporting and inspection mechanisms, their discovery and remediation can require trusted offline scanning, system rebuilding, or firmware-focused investigation. See ISC2's Certified in Cybersecurity Exam Outline and CISA's guidance on understanding malware for additional context on malware behavior, persistence, and defensive response.

QUESTION NO: 13

organization experiences a security event that potentially jeopardizes the confidentiality, integrity or availability of its information system. What term best describes this situation?

A. Breach

B. Event

C. Incident

D. Exploit

ANSWER: C

Explanation:

Incident is the correct term because it describes a security-related occurrence that has actually or potentially endangered the confidentiality, integrity, or availability of an information system or its data. This definition deliberately includes potential harm: the organization does not need to prove that data was exposed, modified, destroyed, or that service was interrupted before it treats the occurrence as an incident and begins its response process. Classifying the occurrence as an incident prompts appropriate activities such as triage, evidence preservation, containment, investigation, recovery, communications, and lessons learned.

NIST defines a computer security incident as a violation or imminent threat of violation of computer security policies, acceptable-use policies, or standard security practices. Its incident-handling guidance also frames the purpose of incident response around addressing events that may affect organizational operations and information security. This aligns with the ISC2 CC incident-response domain, where recognizing and appropriately responding to incidents that may affect the CIA triad is a core concept. See NIST's Computer Security Incident glossary definition and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 14

Which access

control mechanism verifies a user's identity based on a unique physical characteristic?

A. Biometric authentication.

B. Password-based authentication.

C. Token-based authentication.

D. Certificate-based authentication.

ANSWER: A

Explanation:

Biometric authentication is the access control mechanism that verifies identity by measuring and comparing an individual's unique physical or behavioral characteristics. Common biometric factors include fingerprints, facial geometry, iris or retinal patterns, voice characteristics, and hand geometry. During enrollment, the system captures a biometric sample and derives a protected reference template. At authentication, it obtains a new sample and compares it with the enrolled template to determine whether the presented user is sufficiently likely to be the authorized individual. Biometrics are categorized as something a person is, which distinguishes this mechanism from knowledge factors or possession factors. In access control, biometric verification can provide a strong way to bind an identity claim to the person presenting it, especially when implemented with suitable liveness-detection controls and secure template handling. ISC2's Certified in Cybersecurity material identifies biometrics as an authentication factor based on something you are. NIST similarly describes biometrics as automated recognition of individuals based on biological or behavioral characteristics. See ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-63B: Digital Identity Guidelines.

QUESTION NO: 15

Which is NOT a possible model for an Incident Response Team (IRT)?

A. Leveraged

B. Dedicated

C. Hybrid

D. Outsourced

ANSWER: D

Explanation:

Outsourced is the correct answer because the standard IRT organizational models taught for this context are dedicated, leveraged, and hybrid. A dedicated model assigns incident-response duties to a team whose primary responsibility is handling incidents. A leveraged model draws on personnel from other organizational functions, such as IT operations, legal, human resources, and communications, when their expertise is needed. A hybrid model combines a core incident-response capability with leveraged personnel and resources. These structures establish how the organization supplies the authority, access, communications paths, and technical skills needed to coordinate and manage an incident. External providers can certainly support an organization through services such as forensics, managed detection and response, breach counsel, or surge staffing. However, using such a provider is an external sourcing arrangement rather than one of these core IRT team models; the organization must still retain accountability for incident decisions, risk acceptance, communications, and recovery. NIST similarly describes incident-response capability structures in terms of centralized, distributed, and coordinating teams, while emphasizing defined roles and coordination within the organization. See NIST SP 800-61, Computer Security Incident Handling Guide and ISC2's Certified in Cybersecurity certification overview.

QUESTION NO: 16

Which of these is NOT a best practice in access management?

A. Trust but verify

B. Periodically assessing whether user permissions still apply

C. Giving only the right amount of permission
Requesting a justification when upgrading permission

ANSWER: A

Explanation:

"Trust but verify" is not an appropriate access-management best practice because modern identity and access management is founded on explicit verification rather than granting access based on an assumed trust relationship. A user, device, application, or session should be authenticated and authorized using current contextual information before access is provided, particularly when accessing sensitive resources or performing privileged activities. Verification should be continuous or repeated as risk, device posture, location, session behavior, or requested resource changes. This approach limits implicit trust and helps contain the effect of compromised credentials, insider misuse, and lateral movement. The Zero Trust model expresses this principle as "never trust, always verify": access decisions are evaluated per request and are constrained to the minimum scope needed for the task. NIST describes Zero Trust Architecture as removing implicit trust based on network location or asset ownership and requiring authentication and authorization before access to enterprise resources is established. This makes explicit verification, risk-aware authorization, and least-privilege access the appropriate access-management direction. See NIST SP 800-207, Zero Trust Architecture and CISA's Zero Trust Maturity Model.

QUESTION NO: 17

What is the benefit of subnetting?

A. By increasing network bandwidth

B. By improving network security

C. By reducing network congestion

D. By simplifying network management

ANSWER: C

Explanation:

By reducing network congestion is correct because subnetting divides one IP network into smaller logical networks, each with its own broadcast domain. Broadcasts are messages intended for every host on the local network segment, such as certain address-resolution and service-discovery communications. In an unsplit, flat network, every host must receive and process broadcasts from all other hosts in that network. As the number of endpoints grows, this unnecessary traffic consumes network and endpoint resources and can impair overall performance.

Subnetting establishes boundaries that keep local broadcast traffic within the relevant subnet. Traffic that must reach another subnet is handled through a Layer 3 device, such as a router or multilayer switch, rather than being broadcast indiscriminately to all connected devices. Limiting the number of hosts affected by each broadcast reduces contention and makes network behavior more predictable. This is an important networking design principle for maintaining availability and efficient communication as an environment expands.

The ISC2 Certified in Cybersecurity exam includes network segmentation and foundational network concepts within its security-principles coverage. Cisco also describes subnetting as the process of partitioning a network into smaller networks, supporting controlled traffic domains. See the ISC2 CC Certification Exam Outline and Cisco documentation on IP subnetting.

QUESTION NO: 18

Which of the following best describes the role of the incident response "Containment, Eradication, and Recovery" phase?

A. To document the incident and communicate with external stakeholders

B. To prevent the incident from occurring through proactive measures

C. To contain the incident, remove the threat, and restore normal operations

D. To focus exclusively on legal proceedings related to the incident

ANSWER: C

Explanation:

The “Containment, Eradication, and Recovery” phase is correctly described as “To contain the incident, remove the threat, and restore normal operations.” After an incident is identified and analyzed, the organization must first limit its scope and impact. Containment actions can include isolating affected systems, disabling compromised accounts, or blocking malicious network activity while preserving necessary evidence. Eradication then addresses the underlying cause and removes attacker tools, malicious code, unauthorized access mechanisms, or exploited vulnerabilities from the environment. Recovery focuses on returning systems and services to an operational state in a controlled manner, such as rebuilding systems from known-good images, restoring validated backups, applying patches, and monitoring closely for signs of recurrence. These related activities protect business operations by reducing further harm, eliminating the active threat, and safely resuming normal service delivery. ISC2’s Certified in Cybersecurity training identifies incident response as a key operational security activity, including responding to and recovering from security events. The NIST incident-handling lifecycle likewise identifies containment, eradication, and recovery as a core incident-response phase. See ISC2 CC Certification Exam Outline and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 19

What is the purpose of implementing access control mechanisms in mobile devices?

A. To authenticate users attempting to access resources.

B. To assign access rights to authenticated users.

C. To enforce security policies by controlling access to device features and data.

D. To record and monitor user activities for auditing purposes.

ANSWER: C

Explanation:

To enforce security policies by controlling access to device features and data is correct because access control is the process of enforcing authorized use of systems, resources, and information. On a mobile device, this includes restricting access to the device itself, applications, stored data, cameras, microphones, location services, enterprise resources, and other sensitive functions. Controls such as screen locks, biometric verification, application permissions, device-management policies, and role- or policy-based restrictions help ensure that access is granted only in accordance with the organization's security requirements. This supports the core security objective of protecting confidentiality and integrity by preventing unauthorized users or applications from viewing, changing, extracting, or misusing information and device capabilities. In ISC2 terminology, access control encompasses the policies, procedures, and technical mechanisms used to regulate interactions between subjects, such as users or apps, and objects, such as data or resources. Mobile-device access controls apply that principle in a portable computing environment, where loss, theft, untrusted applications, and insecure networks can increase exposure. ISC2's overview of access control concepts is available at ISC2 Certified in Cybersecurity Exam Outline. For practical mobile platform guidance on controlling application permissions and device access, see NIST SP 800-124 Rev. 2.

QUESTION NO: 20

Which layer does VLAN hopping belong to?

A. Layer 3

B. Layer 4

C. Layer 7

D. Layer 2

ANSWER: D

Explanation:

Layer 2 is correct because VLAN hopping is an attack against the data-link-layer mechanisms used to separate traffic into virtual LANs on Ethernet switches. VLANs are implemented through switch port membership and, where traffic must traverse links between switches, IEEE 802.1Q VLAN tags in Ethernet frames. A VLAN-hopping attempt seeks to bypass that intended segmentation, such as by exploiting switch trunking behavior or sending specially crafted double-tagged Ethernet frames. Since the attack concerns Ethernet frames, switching, VLAN identifiers, and trunk configuration rather than network-layer routing or application protocols, it belongs to the OSI data link layer. Defenses likewise focus on Layer 2 switch configuration: explicitly set access ports, disable automatic trunk negotiation where it is not needed, restrict permitted VLANs on trunks, and avoid using the native VLAN for ordinary user traffic. ISC2's CC material treats secure network segmentation and appropriate network-device configuration as fundamental security controls. See Cisco's discussion of VLAN security and VLAN hopping and the IEEE overview of 802.1Q bridged networks and VLAN bridging.

QUESTION NO: 21

Which of the following is a key component of risk management in cybersecurity?

A. Ignoring low-probability risks

B. Transferring all risks to another entity

C. Identifying, assessing, and prioritizing risks

D. Focusing solely on internal threats

ANSWER: C

Explanation:

Identifying, assessing, and prioritizing risks is a key component of cybersecurity risk management because an organization must first understand the threats, vulnerabilities, likelihoods, and potential business impacts that could affect its assets and operations. Identification establishes what could cause harm; assessment evaluates the nature and level of that harm; and prioritization helps decision-makers direct limited resources toward the risks requiring the most urgent or significant treatment. This process supports informed selection of risk responses, such as mitigating a risk through security controls, transferring it through contractual arrangements or insurance, avoiding an activity, or formally accepting a risk within the organization's risk tolerance.

ISC2's Certified in Cybersecurity objectives include risk identification, analysis, and treatment as fundamental risk-management concepts. Similarly, NIST describes risk management as an ongoing organizational process for identifying, assessing, responding to, and monitoring risk. Using a structured, prioritized approach ensures cybersecurity actions align with business objectives and the organization's established risk appetite. See the ISC2 CC Certification Exam Outline and NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.

QUESTION NO: 22

Which of the following is NOT a primary role within an Incident Response Team (IRT)?

A. Manager or Lead who coordinates the activities and manages communication

B. Legal advisor who dictates the technical steps for containment and eradication

C. Level 1 and Level 2 Analysts who perform monitoring, alerts, and incident investigation

D. Technical or engineering staff who may take on incident response roles as needed

ANSWER: B

Explanation:

Legal advisor who dictates the technical steps for containment and eradication is the correct answer because determining and executing technical containment, eradication, and recovery actions is an operational incident-response responsibility. These decisions require personnel with hands-on knowledge of the affected systems, evidence, attack methods, business dependencies, and available remediation controls. Incident handlers, security analysts, system administrators, engineers, and technical leads investigate the incident, scope its impact, isolate affected assets, remove malicious artifacts or attacker access, and validate that systems can safely return to operation.

Legal counsel can be an important participant in an incident-response effort, particularly where regulatory obligations, breach-notification requirements, contractual commitments, evidence preservation, privilege, law-enforcement engagement, or litigation risk are involved. However, counsel provides legal guidance and helps ensure response activities meet applicable legal and organizational requirements; counsel does not ordinarily direct the technical containment and eradication procedure. NIST's incident-handling guidance identifies containment, eradication, and recovery as core technical phases of incident response and emphasizes coordination among incident-handling personnel and relevant stakeholders. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 23

Which is a primary goal of security awareness training?

A. To bypass security controls

B. To promote the use of weak passwords

C. To ignore security policies

D. To educate on the importance of protecting information

ANSWER: D

Explanation:

Security awareness training primarily aims **to educate on the importance of protecting information**. People who use organizational systems and handle data are an essential part of an organization's security posture. Training helps them understand their responsibilities, recognize common threats such as phishing and social engineering, follow applicable security policies, and make safer decisions when handling sensitive information.

In ISC2's security-principles domain, security awareness is a key administrative safeguard because it builds a security-conscious culture and reduces risk arising from human actions. Effective awareness activities communicate the value of information assets and reinforce expected practices, including appropriate data handling, secure authentication behavior, incident reporting, and compliance with organizational procedures. The goal is not merely to distribute policies; it is to ensure personnel understand why those policies exist and how their daily behavior helps preserve confidentiality, integrity, and availability.

ISC2 describes security awareness as an important component of a strong cybersecurity program, particularly because users can identify and report suspicious activity before it becomes a larger incident. See ISC2's Certified in Cybersecurity certification information and NIST's guidance on Building an Information Technology Security Awareness and Training Program.

QUESTION NO: 24

What is the primary purpose of access controls in cybersecurity?

A. To prevent all unauthorized access attempts.

B. To ensure that all users have equal access to resources.

C. To protect information by restricting access to authorized users.

D. To monitor and log all user activities.

ANSWER: C

Explanation:

To protect information by restricting access to authorized users is correct because access control is the security process of enforcing who or what may access a resource and what actions they are permitted to perform. It supports the confidentiality, integrity, and availability of information by ensuring that access decisions are based on an established authorization policy. In practice, this means identifying a subject, authenticating its claimed identity, authorizing only the required level of access, and enforcing that decision when the subject requests a system, application, data set, or physical resource.

Access controls are commonly designed around the principle of least privilege: users receive only the permissions necessary for their assigned duties. This reduces unnecessary exposure of sensitive information and limits the potential impact of mistakes, compromised accounts, or misuse. Controls may be administrative, technical, or physical, and can include permissions, roles, multifactor authentication, access-control lists, badges, and secure entry mechanisms. ISC2's Certified in Cybersecurity material identifies access controls as a core means of protecting assets by managing and enforcing authorized access. See the ISC2 Certified in Cybersecurity Exam Outline and the NIST definition of access control.

QUESTION NO: 25

Which kind of physical access control is LESS effective at preventing unauthorized individual access to a data center?

A. Turnstiles

B. Barriers

C. Fences

D. Bollards

ANSWER: D

Explanation:

Bollards are the physical control that is less effective for preventing unauthorized individual access to a data center. Their primary purpose is vehicle security: fixed, removable, or retractable bollards establish a hardened perimeter that prevents vehicles from driving into protected areas, including by mitigating vehicle-ramming threats. They can therefore protect a facility's exterior and critical entrances from vehicle intrusion, but their spacing and design ordinarily allow pedestrians to walk between or around them. Consequently, bollards do not independently authenticate, identify, or physically stop an unauthorized person on foot from reaching a data-center entrance. In a layered physical-security design, bollards complement pedestrian-focused controls such as controlled entry points, locks, guards, and turnstiles rather than replacing them. ISC2's CC domain covering security principles includes physical security controls and the importance of selecting controls that address the relevant threat; here, the threat is unauthorized access by an individual, rather than unauthorized vehicular access. The U.S. Cybersecurity and Infrastructure Security Agency describes bollards as perimeter-security measures used to mitigate vehicle-ramming risks, while the General Services Administration's facilities guidance likewise identifies bollards as vehicle barriers. See CISA vehicle-ramming mitigation guidance and GSA physical security guidance.

QUESTION NO: 26

Which kind of physical access control is LESS effective at preventing unauthorized individual access to a data center?

A. Bollards

B. Turnstiles

C. Barriers or fences

ANSWER: A

Explanation:

Bollards are the least effective control for preventing unauthorized *individual* access because their primary security purpose is stopping or channeling vehicles. Typically constructed from steel, concrete, or similarly robust materials, bollards create a vehicle-resistant perimeter and help mitigate threats such as vehicle intrusion, ramming, or an explosive device delivered by vehicle. They may establish stand-off distance between traffic and a facility, but a person on foot can generally walk around, between, or over them unless other access controls are present. Therefore, bollards do not by themselves provide meaningful identity verification, authorization, or pedestrian entry control for a data center. Physical security requires controls that match the applicable threat and protected asset. For a pedestrian-access threat, the organization should use an integrated facility-security design that includes controlled pedestrian entry points, authentication, monitoring, and appropriate perimeter protections. This distinction between vehicle barriers and controls governing physical entry is important when selecting safeguards based on risk. ISC2 includes physical security principles within its Certified in Cybersecurity examination outline, available from ISC2. NIST also describes physical and environmental protection controls for information systems and facilities in NIST SP 800-53.

QUESTION NO: 27

What is the purpose of a Business Impact Analysis (BIA) in business continuity planning?

A. To identify critical business functions and the impact of their disruption

B. To determine the organization's annual budget for security expenditures

C. To outline the legal consequences of failing to comply with industry regulations

D. To assign specific security roles and responsibilities to team members

ANSWER: A

Explanation:

A Business Impact Analysis (BIA) is used to identify an organization's critical business functions and determine the consequences if those functions are interrupted. In business continuity planning, this analysis establishes which processes, supporting resources, systems, facilities, personnel, and third-party dependencies are most important to sustaining

organizational operations. It evaluates impacts over time, which can include financial loss, operational disruption, legal or contractual exposure, reputational harm, and effects on customers or mission delivery.

The BIA provides the factual basis for recovery priorities and continuity strategies. It helps the organization define recovery requirements such as a recovery time objective (RTO), representing the target time for restoring an activity, and a recovery point objective (RPO), representing the acceptable amount of data loss. By understanding the relative criticality of functions and the effects of downtime, leadership can allocate continuity and recovery resources appropriately. NIST describes the BIA as identifying and prioritizing information system components and supporting infrastructure according to the impact of a disruption, while ISC2 includes BIA as a key element of business continuity and disaster recovery planning. See NIST SP 800-34 Rev. 1 and ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 28

Which network security mechanism is used to establish secure connections between network devices over an untrusted network?

A. Intrusion Detection System (IDS)

B. Virtual Private Network (VPN)

C. Transport Layer Security (TLS)

D. Firewall

ANSWER: B

Explanation:

Virtual Private Network (VPN) is correct because a VPN establishes a protected logical connection across an untrusted network such as the public internet. VPN technologies protect traffic in transit by creating an encrypted tunnel between endpoints, which can be individual devices, remote-access clients and a VPN gateway, or gateways connecting two separate networks. The tunnel provides confidentiality for transmitted data and generally includes peer authentication and integrity protection, so the communicating endpoints can exchange traffic as though they were connected through a trusted private network.

This use case directly matches the question's focus on securely connecting network devices across an untrusted network. In practical enterprise deployments, site-to-site VPNs commonly use IPsec to protect traffic between network gateways, while remote-access VPNs securely connect a user device to an organizational network. ISC2's Certified in Cybersecurity outline includes VPNs among network-security concepts and emphasizes protecting communications and data in transit. NIST similarly describes IPsec VPNs as mechanisms for securing communications over IP networks. See the ISC2 Certified in Cybersecurity exam outline and NIST's Guide to IPsec VPNs.

QUESTION NO: 29

Which of the following can be used to create message digests?

A. Symmetric encryption algorithms

B. Asymmetric encryption algorithms

C. Hash functions

D. All of the above

ANSWER: C

Explanation:

Hash functions are used to create message digests: fixed-length values calculated from an input of arbitrary length. A cryptographic hash function is designed so that even a small change to the input produces a substantially different digest, making the digest useful for verifying data integrity. For example, a sender or software publisher can calculate a digest for a

message or file, and the recipient can independently calculate the digest of the received content. Matching values provide evidence that the content has not changed since the original digest was generated. Cryptographic hash functions are also foundational to integrity controls such as file checks, password-storage designs that use properly salted password-hashing schemes, digital signatures, and message-authentication mechanisms. A digest itself does not reveal the original message and is not intended to be decrypted; it is a one-way representation used for comparison and integrity-related purposes. ISC2's Certified in Cybersecurity material identifies hashing as a cryptographic mechanism that produces a fixed-length hash value, also called a message digest. See the NIST Secure Hash Standard and the ISC2 Certified in Cybersecurity exam outline.

QUESTION NO: 30

Which access control model specifies access to an object based on the subject's role in the organization?

A. ABAC

B. RBAC

C. MAC and DAC

ANSWER: B

Explanation:

RBAC is correct because it grants and manages permissions according to defined organizational roles, rather than assigning permissions individually to every user. A role represents a job function or responsibility, such as payroll administrator, network operator, or help-desk technician. Permissions to access particular objects, systems, applications, or actions are assigned to the role, and subjects receive those permissions by being assigned to the appropriate role. This approach aligns access with business duties and supports efficient administration: when someone changes jobs, administrators can adjust role membership instead of reviewing and rebuilding each individual permission assignment. RBAC also supports important security practices such as least privilege and separation of duties, since roles can be designed to provide only the access needed for a defined function and to keep incompatible responsibilities separate. ISC2 includes role-based access control among the access-control concepts candidates should understand in its Certified in Cybersecurity examination outline. NIST's RBAC project likewise describes RBAC as associating permissions with roles and assigning users to those roles. See the ISC2 CC Certification Exam Outline and NIST Role-Based Access Control project.

QUESTION NO: 31

In a DAC policy scenario, which of these tasks can only be performed by a subject granted access to information?

A. Modifying the information

B. Changing security attributes

C. Executing the information

D. Reading the information

ANSWER: B

Explanation:

Changing security attributes is correct because discretionary access control (DAC) places control over an object's permissions and related protection settings with its owner. A subject that creates an object commonly becomes its owner and can use that authority to grant, revoke, or modify access permissions for other subjects. This is the defining discretionary feature of DAC: access decisions are made at the object-owner level rather than being centrally and rigidly imposed through system-wide labels or classifications. Security attributes in this context include the access-control information associated with the object, such as permissions that specify which users or groups may access it and what actions they may perform. The authority to alter those attributes is a privileged form of access associated with ownership or explicit administrative delegation. ISC2's CC examination objectives identify DAC as an access-control model in which the data owner determines who can access an object and the permissions granted. This also illustrates an important operational characteristic of DAC:

owners must apply permissions carefully because their decisions directly affect protection of the information. See the ISC2 Certified in Cybersecurity Exam Outline and the NIST glossary for access-control terminology and concepts.

QUESTION NO: 32

Which type of software testing focuses on examining the source code for vulnerabilities and security issues?

A. Black-box testing

B. White-box testing

C. Functional testing

D. User acceptance testing

ANSWER: B

Explanation:

White-box testing is correct because it assesses an application's internal implementation with knowledge of its code, architecture, logic, and control flows. This visibility lets testers examine source code directly for security defects such as unsafe input handling, flawed authorization logic, insecure cryptographic implementation, error-handling weaknesses, and embedded secrets. In a security-development context, this work commonly includes manual secure code review and static application security testing, in which analysis tools inspect source or compiled code without needing to execute the application. Finding these weaknesses during development supports secure-by-design practices: issues can be identified and remediated before deployment, when changes are generally less costly and less likely to affect users. ISC2 emphasizes incorporating security throughout the system development life cycle, including applying secure coding practices and testing controls before release. The National Institute of Standards and Technology similarly describes static application security testing as analysis of an application's source code, bytecode, or binary code to identify security vulnerabilities. See ISC2's Certified in Cybersecurity Exam Outline and NIST's definition of static application security testing.

QUESTION NO: 33

What access control principle states that users should only be granted access to resources that are relevant to their job responsibilities?

A. Principle of Least Privilege.

B. Separation of Duties.

C. Defense in Depth.

D. Need-to-Know Principle.

ANSWER: D

Explanation:

The **Need-to-Know Principle.** is correct because it limits access to information and resources to individuals who require that specific information to perform their authorized job duties. Its purpose is to prevent unnecessary exposure of sensitive data, even when a person otherwise has an appropriate role, clearance, or general authorization within the organization. Access is therefore tied to a demonstrable business requirement: the user needs the particular information to complete a defined task or responsibility.

Need-to-know is especially important when handling confidential, proprietary, personal, or classified information. Applying it reduces the population able to view sensitive material, which lowers the likelihood and impact of accidental disclosure, inappropriate browsing, insider misuse, and compromise of accounts. Access decisions should be reviewed as job assignments, projects, and responsibilities change so that users retain access only while the business need exists.

NIST defines need-to-know as a determination that access to specific information is required to carry out official duties. See the NIST Computer Security Resource Center definition of need-to-know and ISC2's Certified in Cybersecurity exam outline.

QUESTION NO: 34

Token Ring used in which OSI Layer

A. Application

B. Network

C. Transport

D. Physical

E. Data Link

ANSWER: E

Explanation:

Data Link is correct because Token Ring is an IEEE 802.5 LAN technology whose token-passing access method is implemented by the Media Access Control sublayer of the OSI Data Link layer. At this layer, network devices use MAC addresses to identify stations on the local network and apply rules governing when a station may transmit a frame. In Token Ring, a control frame called a token circulates around the ring. A station must possess that token before it can send data, providing orderly and deterministic access to the shared network medium. This function is specifically a Data Link-layer responsibility: controlling access to the medium and framing local-network communications. ISC2 CC candidates should recognize that Layer 2 includes LAN access technologies and their MAC mechanisms, while the Physical layer supplies the signaling and media characteristics that carry the bits. Although Token Ring has physical-media components, the defining token-passing protocol is categorized at the Data Link layer. The IEEE 802.5 working group standardized Token Ring LAN operation; see the IEEE 802.5 standard listing. For a concise description of the OSI Data Link layer's role in framing and media access control, see Cloudflare's OSI model overview.

QUESTION NO: 35

Which encryption method involves using the same key for encryption and decryption?

A. Asymmetric encryption

B. Symmetric encryption

C. Hash function

D. Public key infrastructure

ANSWER: B

Explanation:

Symmetric encryption is the method that uses one shared secret key for both operations: transforming plaintext into ciphertext and transforming that ciphertext back into plaintext. Because the same key is used at each end, the parties must establish and protect that shared key before exchanging encrypted information. Symmetric cryptography is commonly used to protect large volumes of data efficiently, including data stored on disks and data transmitted during secure network sessions. Well-known symmetric algorithms include AES, which is widely used in modern security implementations. ISC2's CC curriculum distinguishes symmetric cryptography from public-key cryptography by this shared-key characteristic and emphasizes that protecting the confidentiality of the secret key is essential to maintaining the confidentiality of the protected data. NIST describes AES as a symmetric block-cipher algorithm, meaning its cryptographic operation relies on a shared secret key. See NIST's Advanced Encryption Standard (AES) and ISC2's Certified in Cybersecurity exam outline for the cryptography concepts covered in the certification.

QUESTION NO: 36

which is the short form of IPv6 address 2001:0db8:0000:0000:0000:ffff:0000:0001

A. 2001:db8::ffff:0:1

B. 2001:db8:0000:ffff:0:1

C. 2001:db80::ffff:0000:1

D. 2001:db8::ffff:0000:0001

ANSWER: A

Explanation:

`2001:db8::ffff:0:1` is the shortest valid compressed representation of the given IPv6 address. IPv6 notation permits leading zeroes within each 16-bit hexadecimal block to be omitted, so `0db8` becomes `db8`, and `0000` becomes `0` when it is written as an individual block. IPv6 also permits one contiguous sequence of one or more all-zero blocks to be compressed with a double colon. Here, the three consecutive `0000` blocks between `db8` and `ffff` are replaced by `::`. The final two blocks are shortened from `0000:0001` to `0:1`. Expanding `2001:db8::ffff:0:1` restores exactly eight 16-bit blocks: `2001:0db8:0000:0000:0000:ffff:0000:0001`. This follows the canonical IPv6 text-representation rules in RFC 5952, which recommend using `::` for the longest run of zero blocks and suppressing leading zeroes. See RFC 5952: A Recommendation for IPv6 Address Text Representation and RFC 4291: IP Version 6 Addressing Architecture.

QUESTION NO: 37

The prevention of authorized access to resources or the delaying of time-critical operations is known as:

A. ARP poisoning

B. SYN flood

C. Denial-of-Service (DoS)

D. All

ANSWER: C

Explanation:

Denial-of-Service (DoS) is correct because it describes an attack or condition that compromises availability by preventing legitimate, authorized users from accessing systems, networks, applications, or data when needed. A DoS event may completely block access to a resource or degrade its performance enough that time-sensitive work cannot be completed within required deadlines. This directly affects the availability component of the CIA triad, which requires information systems and services to be accessible and usable by authorized users in a timely manner. DoS can result from overwhelming a target with traffic or requests, exhausting finite resources such as network bandwidth, memory, processing capacity, or connection tables, or exploiting a flaw that causes a service to fail. In security operations, the essential outcome is the same: legitimate access is disrupted or delayed. ISC2 identifies availability as ensuring timely and reliable access to and use of information, making prevention of that access a clear availability-focused security incident. For additional context, see the NIST Cybersecurity Framework and CISA's guidance on denial-of-service attacks.

QUESTION NO: 38

Security controls protecting against fire, floods, and earthquakes are:

A. Physical controls

B. Logical controls

C. Administrative controls

D. Technical controls

ANSWER: A

Explanation:

Physical controls is correct because these safeguards protect the tangible environment in which information systems, people, and facilities operate. Fire, flooding, and earthquakes are environmental or natural hazards that can damage buildings, data centers, network infrastructure, servers, and stored media. Appropriate physical protections include fire detection and suppression systems, water sensors and flood barriers, raised flooring, appropriate site selection, secure facility construction, and seismic bracing for equipment. These measures reduce the likelihood that an environmental event will disrupt operations or cause loss of information assets.

ISC2's CC curriculum includes physical security as a core security-control area and recognizes environmental protections as facility safeguards. Physical security is not limited to locks and guards; it also encompasses controls that protect facilities and equipment from fire, water, power, and other environmental conditions. Selecting and maintaining these controls supports availability, resilience, and business continuity by limiting physical damage and enabling systems to remain operational or recover more effectively after an incident. See ISC2's Certified in Cybersecurity exam outline and NIST's guidance on physical and environmental protection controls.

QUESTION NO: 39

Networks are often micro segmented networks, with firewalls at nearly every connecting point

A. DMZ

B. VPN

C. VLAN

D. Zero Trust

ANSWER: D

Explanation:

Zero Trust is correct because microsegmentation is a core network-security technique used to implement a Zero Trust architecture. Rather than treating an entire internal network as inherently trusted, Zero Trust limits implicit trust and requires access decisions to be continuously evaluated using factors such as identity, device posture, workload, application, and context. Microsegmentation divides infrastructure into small, isolated security zones and applies narrowly scoped policies between workloads, users, and services. Firewalls or equivalent policy-enforcement points at many connection paths provide the practical controls needed to permit only explicitly authorized communications. This containment reduces lateral movement: if an account, endpoint, or workload is compromised, the attacker should not automatically gain broad access to other network resources. NIST describes Zero Trust as an approach that focuses on protecting resources rather than relying on network location, with no implicit trust granted based solely on network placement. Its guidance also identifies microsegmentation as a deployment approach for enforcing granular access controls. ISC2's Zero Trust concepts similarly emphasize verifying explicitly, using least-privilege access, and assuming breach. See NIST SP 800-207: Zero Trust Architecture and ISC2: What Is Zero Trust Security?.

QUESTION NO: 40

Which element of the security policy framework includes recommendations that are NOT binding?

A. Procedures

B. Guidelines

C. Standards

D. Policies

ANSWER: B

Explanation:

Guidelines are the nonbinding, advisory element of a security policy framework. They communicate recommended practices that help personnel make security-conscious decisions while allowing appropriate flexibility for differing business processes, technologies, operational contexts, and risk levels. A guideline can recommend a preferred secure approach, such as using a password manager or applying additional protections to sensitive data, without creating a mandatory compliance obligation.

ISC2 describes policies, standards, procedures, and guidelines as related governance documents that translate organizational security objectives into usable direction. Within this hierarchy, guidelines support the security program by offering practical advice and accepted methods where a strict, universal requirement may not be appropriate. Organizations can use them to promote consistent secure behavior and to help teams interpret and apply overarching security expectations in their particular environments.

This distinction is important because policy frameworks need both enforceable direction and adaptable recommendations. Nonbinding guidance enables an organization to encourage strong security practices without treating every recommended implementation detail as a mandatory rule. See ISC2's Certified in Cybersecurity certification overview and NIST's Introduction to Information Security (SP 800-12 Rev. 1) for security-program governance context.

QUESTION NO: 41

What is the primary goal of Identity and Access Management (IAM) in cybersecurity?

A. To ensure 100% security against all threats

B. To provide secure and controlled access to resources

C. To eliminate the need for user authentication

D. To monitor network traffic for performance optimization

ANSWER: B

Explanation:

Identity and Access Management (IAM) exists to provide secure, controlled access to organizational resources by ensuring that identities are established and that access decisions are made according to approved rules. In practical terms, IAM manages the identity lifecycle, verifies a user or system's identity through authentication, and authorizes only the access that identity needs. This supports the core security principle of least privilege: granting the minimum permissions required to perform an approved task, for only as long as needed.

IAM controls commonly include account provisioning and deprovisioning, password and multifactor authentication, role- or attribute-based access control, privileged-access management, periodic access reviews, and audit logging. Together, these capabilities help an organization ensure that the appropriate identities can access the appropriate resources under appropriate conditions. This is foundational to protecting the confidentiality, integrity, and availability of systems and data, particularly as organizations use cloud services, remote work, and interconnected applications. NIST describes digital identity as encompassing identity proofing, authentication, and federation in its Digital Identity Guidelines. NIST's Zero Trust Architecture further emphasizes explicit authentication and authorization before access to resources is granted.

QUESTION NO: 42

What is the primary function of access control mechanisms in identity federation systems?

A. To authenticate users attempting to access resources.

B. To assign access rights to authenticated users.

C. To enforce security policies by facilitating single sign-on (SSO) across multiple domains.

D. To record and monitor user activities for auditing purposes.

ANSWER: B

Explanation:

To assign access rights to authenticated users. is correct because access control primarily determines whether an authenticated identity is authorized to use a particular resource and what actions that identity may perform. In an identity federation architecture, a trusted identity provider supplies authentication assertions to a relying party or service provider. The target system must then apply its own access-control policy—such as roles, groups, attributes, permissions, resource ownership, time restrictions, or other authorization rules—to make an access decision. In other words, federation can make identity and authentication information portable across organizational or security domains, but access control turns that trusted identity information into an allowed or denied request for a specific resource or action.

This distinction is central to identity and access management: authentication establishes confidence in who the user is, while authorization assigns and enforces the rights available to that authenticated user. NIST defines access control as the process of granting or denying specific requests to obtain and use information-processing services, and its digital identity guidance describes federation as the use of assertions exchanged between an identity provider and relying party. See NIST's Access Control glossary definition and NIST SP 800-63C, Federation and Assertions.

QUESTION NO: 43

What is the main purpose of digital signatures?

A. Encrypt data

B. Verify sender identity and ensure message integrity

C. Prevent network access

D. Compress data

ANSWER: B

Explanation:

Digital signatures are used to verify the identity of the signer and protect the integrity of signed data. The signer creates a signature using their private key, typically over a cryptographic hash of the message. A recipient uses the corresponding public key to validate that signature. Successful validation provides assurance that the signature was produced by the holder of the associated private key and that the signed message has not changed since it was signed. This supports authentication and integrity, two fundamental security objectives. Digital signatures can also provide non-repudiation when the private key is properly controlled and the surrounding identity, certificate, and logging processes are trustworthy. They do not inherently keep the message confidential; confidentiality requires encryption. ISC2's CC curriculum includes cryptographic controls such as digital signatures as mechanisms that support data integrity, authentication, and non-repudiation. See the ISC2 Certified in Cybersecurity Exam Outline and NIST's Digital Signature glossary definition for further reference.

QUESTION NO: 44

A backup that captures the changes made since the latest full backup is an example of:

A. A differential backup

B. An incremental backup

C. A backup snapshot
A full backup

ANSWER: A

Explanation:

A differential backup captures all data that has changed since the most recent full backup. For example, after a full backup is completed on Sunday, a differential backup on Monday contains changes made since Sunday; a further differential backup on Tuesday still contains all changes made since that same Sunday full backup. This approach makes restoration relatively straightforward: recover the latest full backup first, then apply the most recent differential backup. The amount of data in each differential backup generally grows until another full backup is performed, because each differential continues to include changes made since that baseline full backup. This backup type is a common component of a recovery strategy because it balances backup time, storage use, and recovery complexity. NIST describes differential backup as a backup of files changed since the last full backup in its contingency-planning guidance. See NIST SP 800-34 Rev. 1 and the ISC2 Certified in Cybersecurity Exam Outline for related backup and recovery concepts.

QUESTION NO: 45

Which regulation addresses personal privacy?

A. HIPAA

B. GDPR

C. NIST

D. ISO

ANSWER: B

Explanation:

GDPR is correct because the General Data Protection Regulation is a legally binding European Union regulation specifically designed to protect individuals' personal data and privacy. It establishes rules for organizations that collect, use, store, share, or otherwise process personal data relating to people in the European Economic Area. Its scope can also extend to organizations outside the EU when they offer goods or services to, or monitor the behavior of, individuals in the EEA. Core GDPR requirements include a lawful basis for processing, transparency about data use, appropriate security measures, accountability, and support for data-subject rights. These rights include access to personal data, correction of inaccurate data, erasure in defined circumstances, and data portability. For an ISC2 CC question asking generally which regulation addresses personal privacy, GDPR is the clearest and most directly applicable answer because privacy and personal-data protection are its central purpose. The official legal text describes GDPR as protecting natural persons with regard to the processing of personal data and the free movement of such data. See the official GDPR text on EUR-Lex and the European Commission's data-protection overview.

QUESTION NO: 46

What is the primary purpose of conducting a vulnerability assessment?

A. To increase network bandwidth

B. To identify and prioritize security risks and weaknesses

C. To restrict employee access to information resources

D. To recover lost data from network devices

ANSWER: B

Explanation:

The primary purpose of a vulnerability assessment is **to identify and prioritize security risks and weaknesses** in systems, applications, networks, and their configurations. It is a systematic process of discovering known weaknesses, such as missing patches, insecure settings, exposed services, or outdated software, and evaluating their potential significance to the organization. The assessment results give security personnel actionable information for risk treatment: they can validate findings, rank remediation work according to factors such as severity, exposure, business criticality, and likely impact, then track the weaknesses through correction or mitigation.

This supports a proactive security program because organizations can reduce their attack surface before weaknesses are exploited. In ISC2's CC security-operations context, vulnerability management is a continuing lifecycle rather than a one-time scan: assets are assessed, findings are analyzed and prioritized, remediation is applied, and the environment is reassessed to verify the risk has been addressed. This risk-focused outcome distinguishes the assessment's core purpose from operational activities such as performance improvement, access administration, or data recovery. For further guidance, see the CISA vulnerability management resources and NIST SP 800-40 Rev. 4.

QUESTION NO: 47

What is the process of verifying a user's identity called?

A. Confidentiality

B. Authentication

C. Authorization

D. Identification

ANSWER: B

Explanation:

Authentication is the process of verifying that a user, device, service, or other entity is genuinely the identity it claims to be. In practice, this verification relies on one or more authentication factors: something the user knows, such as a password or PIN; something the user has, such as a hardware token or authenticator application; or something the user is, such as a fingerprint or other biometric characteristic. Using more than one independent factor is known as multifactor authentication and provides stronger assurance of identity. Authentication is a foundational access-control concept because a system must establish confidence in an identity before it can reliably apply permissions, record actions, or protect resources. ISC2's Certified in Cybersecurity material treats authentication as a core component of identity and access management. For an overview of digital identity and authentication assurance concepts, see the NIST Digital Identity Guidelines: Authentication and Lifecycle Management. The CISA multifactor authentication guidance also describes authentication as proving identity through multiple factors.

QUESTION NO: 48

What access control principle ensures that sensitive information is only disclosed to authorized users who have a legitimate need to know?

A. Principle of Least Privilege.

B. Separation of Duties.

C. Defense in Depth.

D. Need-to-Know Principle.

ANSWER: D

Explanation:

The Need-to-Know Principle is the correct answer because it restricts access to sensitive information to individuals who are authorized and require that specific information to perform an assigned job function or task. Authorization alone is not sufficient: the individual's current duties must create a legitimate operational requirement for the information. This principle limits unnecessary exposure of confidential data, reducing the likelihood of inappropriate disclosure, misuse, or compromise. In practice, need-to-know is commonly enforced through data classification, role- or attribute-based access controls, compartmentalization, and approval workflows that grant access only to relevant records, systems, or projects. It supports confidentiality by ensuring that access decisions consider both a person's permission level and the specific business purpose for the requested data. ISC2's Certified in Cybersecurity training identifies need-to-know as an access-control concept used to limit information access based on a valid requirement for a particular task. The principle is also consistent

with NIST guidance that access authorizations should be limited to the information and system resources necessary for authorized duties. See the ISC2 CC Certification Exam Outline and NIST CSRC definition of need to know.

QUESTION NO: 49

Which authentication factor verifies something a user knows?

A. Biometric authentication

B. Token-based authentication

C. Password-based authentication

D. Certificate-based authentication

ANSWER: C

Explanation:

Password-based authentication verifies the knowledge factor: information the user is expected to know and can present to authenticate. Common examples are a password, passphrase, PIN, or the answer to a security question. The system compares the supplied secret, usually through a protected verifier such as a salted password hash, with the enrolled authentication data. If it matches, the user has demonstrated knowledge of that secret without the secret necessarily being transmitted or stored in plaintext.

ISC2 describes authentication factors as categories including something you know, something you have, and something you are. Passwords and PINs are standard examples of the “something you know” category. In a stronger multifactor authentication design, password-based authentication can be combined with an independent possession or inherence factor to provide greater assurance that the authenticating person is the legitimate user. See ISC2’s overview of multi-factor authentication and the NIST Digital Identity Guidelines discussion of memorized secrets.

QUESTION NO: 50

Which scenario best represents defense in depth?

A. Relying only on a firewall

B. Storing all data on one server

C. Requiring only a username and password

D. None

ANSWER: D

Explanation:

“None” is correct because defense in depth is the deliberate use of multiple, complementary security controls across different layers of an environment. The listed scenarios each describe a single control or a single-point design rather than a layered strategy. A true defense-in-depth implementation would combine safeguards such as network segmentation and firewalls, strong authentication including multifactor authentication, endpoint protection, least-privilege access controls, encryption, logging and monitoring, secure backups, and documented response processes. The layers are intended to reduce the likelihood that one failed, bypassed, or misconfigured control leads directly to a compromise. For example, an attacker who passes a network boundary should still encounter identity verification, authorization restrictions, endpoint controls, and monitoring. NIST describes this concept as using multiple security controls so that the failure of one control does not leave the system unprotected. ISC2 similarly presents defense in depth as a foundational security principle that applies administrative, technical, and physical safeguards in coordinated layers. Since no listed scenario includes this combination of independent and mutually reinforcing protections, “None” accurately identifies that none represents defense in depth. See NIST’s definition of defense in depth and ISC2’s overview of the defense-in-depth strategy.

QUESTION NO: 51

What is the primary purpose of conducting a Business Impact Analysis (BIA)?

A. To document the organization's IT infrastructure and software applications.

B. To identify critical business functions and the impact of their disruption on the organization.

C. To assess the organization's compliance with industry regulations.

D. To evaluate the technical skills of the IT staff.

ANSWER: B

Explanation:

A Business Impact Analysis (BIA) primarily identifies an organization's critical business functions and determines the consequences if those functions are disrupted. It gives business continuity and disaster recovery planning a business-focused basis by establishing which processes, resources, dependencies, and services are essential to meeting organizational objectives. The analysis evaluates impacts such as financial loss, operational disruption, legal or contractual consequences, customer effects, and reputational damage over time. It also supports the identification of recovery priorities and recovery objectives, including the maximum acceptable period of disruption for a process. ISC2's CC curriculum includes business impact analysis within business continuity planning and emphasizes determining the impact of disruptive events on business operations. This information enables the organization to prioritize continuity strategies and recovery efforts according to business need rather than solely according to technical considerations. The purpose is therefore accurately expressed by *To identify critical business functions and the impact of their disruption on the organization.* See ISC2's Certified in Cybersecurity exam outline and NIST's SP 800-34 Rev. 1, Contingency Planning Guide, which describes the BIA as identifying and prioritizing information systems and components supporting critical business processes.

QUESTION NO: 52

A digital certificate is used to:

A. Increase the speed of internet connections

B. Verify the identity of a device or person online

C. Store data in a cloud environment

D. Act as a physical form of identification

ANSWER: B

Explanation:

A digital certificate is used to verify the identity of a device or person online by binding an asserted identity, such as a domain name, organization, user, or device, to a public cryptographic key. Issued and digitally signed by a trusted certificate authority within a public key infrastructure, the certificate enables a relying party to validate that the presented public key belongs to the claimed entity. This supports trusted communications and transactions, including the authentication of websites through Transport Layer Security and the verification of digital signatures. Certificate validation involves checking the issuer's signature and trust chain, the certificate's validity period, and whether the certificate is applicable to the intended identity or use. The certificate itself does not need to remain secret; its security value comes from the certificate authority's signature and from the certificate holder's control of the corresponding private key. ISC2 describes public key infrastructure as a framework that uses certificates to establish and manage trust in public keys. See the ISC2 Certified in Cybersecurity Exam Outline and the NIST Digital Identity Guidelines.

QUESTION NO: 53

Which of the following is not a true statement about a worm?

A. It can replicate itself.

B. It is a type of malware.

C. It is a type of botnet.

D. It does not require a host program to infect and deliver it to the victim system.

ANSWER: C

Explanation:

“It is a type of botnet.” is the statement that is not true. A worm is a form of malicious software designed to propagate, typically by exploiting vulnerabilities or using network connections to copy itself from one system to another. Its defining characteristic is autonomous replication and spread without needing to attach itself to a separate host application. A botnet, in contrast, is a collection of compromised devices that an attacker can remotely control as a group, often through command-and-control infrastructure. Individual malware—including a worm—may compromise devices that are later enrolled into a botnet, but that possible relationship does not make the worm itself a botnet. The terms describe different security concepts: one identifies a malware type and propagation behavior, while the other identifies an attacker-controlled network of infected systems. This distinction is important when assessing incidents because containment of a self-propagating worm focuses on stopping spread, patching exposed vulnerabilities, and isolating affected systems. See the NIST definition of a worm and the NIST definition of a botnet.

QUESTION NO: 54

What is the primary purpose of a continuity of operations plan (COOP)?

A. To prevent all business disruptions

B. To recover all lost data immediately after an incident

C. To ensure that critical business functions can continue during and after disruptions

D. To wait for external assistance before taking any action

ANSWER: C

Explanation:

A continuity of operations plan (COOP) exists to ensure that an organization can sustain its essential or critical functions when a disruption occurs and throughout the period of recovery. A COOP identifies the functions that must not stop, the personnel and resources required to perform them, alternate facilities or work arrangements, communications methods, delegated authorities, and procedures for resuming normal operations. Its focus is operational resilience: maintaining an acceptable level of service during events such as natural disasters, technology outages, loss of a facility, or other emergencies.

This purpose aligns with the business continuity concepts covered in ISC2 CC. Continuity planning is based on understanding business requirements and prioritizing activities whose interruption would cause unacceptable harm. A COOP therefore provides practical, preapproved arrangements that allow those functions to continue despite adverse conditions, rather than treating continuity as a purely technical recovery activity. The U.S. Federal Emergency Management Agency describes continuity planning as ensuring the performance of essential functions during a broad range of emergencies. See FEMA Continuity and the ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 55

Which organization defines Internet protocol standards?

A. ISO

B. NIST

C. IETF

D. GDPR

ANSWER: C

Explanation:

The Internet Engineering Task Force (IETF) is correct because it is the principal open international community responsible for developing and promoting voluntary Internet standards, including the protocols that enable interoperable Internet communications. Its work is organized through working groups that produce technical specifications, commonly published in the Request for Comments (RFC) document series. While not every RFC is an Internet Standard, the IETF's standards process defines how protocol specifications progress through review, consensus, implementation experience, and eventual designation as Internet Standards. Core Internet technologies—including IP-related protocols, TCP, DNS operational standards, HTTP specifications, TLS, and email protocols—are developed or standardized through this ecosystem. The IETF operates through open participation and "rough consensus and running code," emphasizing technically sound, implementable specifications rather than regulation or national policy. This makes it the relevant standards-development organization when identifying who defines the technical protocols used across the Internet. The IETF's own overview describes its mission and role in creating high-quality, relevant technical documents that influence how people design, use, and manage the Internet. Its standards-process documentation further explains the formal lifecycle for Internet-Drafts and RFC publications. See the IETF About page and IETF standards process.

QUESTION NO: 56

Natalia is concerned that users on her network may be storing sensitive information, such as social security numbers, on their hard drives without proper authorization or security controls. What 3rd -party security service can she implement to best detect this activity?

A. IDS - Intrusion Detection System

B. IPS - Intrusion Prevention System

C. DLP - Data Loss Prevention

D. TLS - Transport Layer Security

ANSWER: C

Explanation:

DLP - Data Loss Prevention is the appropriate service because endpoint DLP tools can discover, classify, and monitor sensitive data stored on users' local hard drives. An organization can configure DLP policies to identify patterns associated with Social Security numbers, such as defined number formats and contextual keywords, then scan endpoint storage for files containing that information. This gives Natalia visibility into data at rest that may have been saved outside approved repositories or without required protections. Endpoint DLP can also generate alerts, produce incident records for investigation, and, depending on policy and product capabilities, apply protective actions such as blocking transfers, restricting access, encrypting files, or requiring remediation. These capabilities support data handling and protection requirements by helping security teams locate sensitive information and enforce organizational policy before unauthorized exposure occurs. The National Institute of Standards and Technology describes data loss prevention as a set of capabilities for detecting and preventing unauthorized disclosure of sensitive data; its guidance includes protecting data at rest on endpoints. See NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices and NIST Privacy Framework.

QUESTION NO: 57

Which security control is designed to prevent unauthorized access to sensitive information by ensuring it is accessible only to authorized users?

A. Encryption

B. Firewall

C. Antivirus

D. Access control

ANSWER: D

Explanation:

Access control is correct because it is the set of policies, processes, and technical mechanisms used to ensure that only authorized subjects can access specified information and resources. It supports the confidentiality component of the CIA triad by identifying a user or system, authenticating its claimed identity, and authorizing only the actions and data access permitted by the applicable rules. For example, role-based access control can limit payroll records to authorized human-resources and finance personnel, while enforcing least privilege so those users receive only the permissions needed for their duties. Access control also commonly includes account provisioning and deprovisioning, permission reviews, session controls, and logging of access attempts. ISC2's Certified in Cybersecurity material treats access controls as a core means of protecting information assets and managing access according to business requirements. The National Institute of Standards and Technology similarly defines access control as limiting system access to authorized users, processes acting on behalf of authorized users, and devices. See the ISC2 Certified in Cybersecurity Exam Outline and NIST definition of access control.

QUESTION NO: 58

Which of the following is a primary goal of cybersecurity awareness training?

A. To teach employees about the company's sales strategies

B. To ensure employees understand and can identify cybersecurity threats

C. To prepare employees for roles in IT support

D. To increase the company's revenue through improved cybersecurity

ANSWER: B

Explanation:

To ensure employees understand and can identify cybersecurity threats is a primary goal of cybersecurity awareness training. People are an important part of an organization's security posture: employees routinely receive email, handle sensitive information, use organizational systems, and may encounter social-engineering attempts. Awareness training builds the knowledge needed to recognize common threats such as phishing, malicious links or attachments, unsafe password practices, and suspicious requests for information. It also teaches personnel the organization's expected security behaviors and reporting procedures so potential incidents can be identified and escalated promptly.

ISC2's Certified in Cybersecurity curriculum includes security awareness training as an administrative control that helps personnel understand their security responsibilities and make safer decisions in their daily work. Effective training is ongoing and relevant to users' roles, reinforcing the ability to identify threats and respond according to established policy. This reduces the likelihood that routine human actions will create an opportunity for a cyber incident. See the ISC2 Certified in Cybersecurity Exam Outline and the CISA Cybersecurity Awareness Program guidance.

QUESTION NO: 59

A security engineer is performing a review of an organization's datacenter security controls. They document that the datacenter lacks security cameras for monitoring the facilities. What type of control does this represent?

A. Administrative

B. Technical

C. Physical

D. Logical

ANSWER: C

Explanation:

Physical is correct because security cameras are deployed to protect and monitor the datacenter's real-world environment, including entrances, equipment areas, corridors, and other facilities. A camera is a tangible device used to observe people and events in a location, supporting facility protection, incident detection, investigation, and deterrence. Although cameras may transmit footage over a network or use digital recording systems, their primary security purpose in this context is surveillance of a physical site. Therefore, documenting their absence identifies a gap in the organization's physical security controls.

ISC2 describes physical controls as safeguards that protect facilities, equipment, and people from physical threats. Surveillance systems are commonly included among such safeguards, alongside measures such as locks, barriers, guards, lighting, and access-control mechanisms. Camera footage can also provide evidence for response and forensic activities after a suspected event, but that additional benefit does not change the control's primary classification. The review finding should consequently be tracked as a physical-security deficiency and addressed through appropriate facility surveillance design, coverage, retention, monitoring, and maintenance requirements. See ISC2's Certified in Cybersecurity examination outline and NIST's Security and Privacy Controls catalog for related physical and environmental protection guidance.

QUESTION NO: 60

Which of these is WEAKEST form of authentication we can implement?

A. Something you know

B. Something you are

C. Something you have

D. Biometric authentications

ANSWER: A

Explanation:

Something you know is the weakest authentication factor in this comparison because it relies on a memorized secret, such as a password, PIN, or answer to a security question. A knowledge-based secret can be guessed, reused across services, exposed through phishing, captured by keylogging malware, or obtained after a breach of a password database. Its effectiveness also depends heavily on users choosing unique, sufficiently long secrets and on the organization enforcing secure password storage and controls against repeated login attempts. ISC2's entry-level cybersecurity material identifies authentication factors as something you know, have, or are, and emphasizes the value of combining independent factors through multifactor authentication. A knowledge factor can still be an important component of an authentication process, particularly when protected by password-management practices and paired with another factor, but alone it provides comparatively limited assurance of the claimant's identity. NIST likewise describes memorized secrets as authentication information that must be protected and recommends controls such as rate limiting and resistance to common password attacks. See ISC2 Certified in Cybersecurity and NIST SP 800-63B: Digital Identity Guidelines.

QUESTION NO: 61

Which of these is an attack whose PRIMARY goal is to gain access to a target system through falsified identity?

A. Ransomware

B. Amplification

C. Spoofing

D. DDoS

ANSWER: C

Explanation:

Spoofing is an attack in which a threat actor falsifies or impersonates an identity, device, address, service, or communication source in order to be trusted by a target. That false identity can be used to obtain unauthorized access directly, such as when an attacker impersonates a legitimate host or user, or to induce a person or system to take an action that grants access. Common forms include IP spoofing, email spoofing, website or URL spoofing, and caller-ID spoofing. The common security principle is that the recipient or target is deceived into treating malicious activity as if it came from a legitimate and trusted source. ISC2's CC curriculum includes spoofing among common attack types and emphasizes identity, authentication, and trust as foundational security concepts. Effective defenses include strong authentication, validation of network and message sources, encryption where appropriate, and user awareness training. For additional background, see the CISA overview of spoofing and phishing and the ISC2 Certified in Cybersecurity exam outline.

QUESTION NO: 62

A measure of an organization's baseline security performance is a:

A. Security assessment

B. Security audit

C. Security benchmark

D. Security management

ANSWER: C

Explanation:

Security benchmark is correct because a benchmark is a defined point of reference used to establish and measure an organization's expected security posture or the security configuration of its systems. It provides a repeatable baseline against which actual performance, controls, and configurations can be compared. For example, a system hardening benchmark can specify required settings for an operating system, while an organizational benchmark can support measuring progress toward a defined security standard. This enables consistent evaluation over time, identification of gaps, and more meaningful reporting about whether security objectives are being met. Benchmarks are commonly developed from recognized standards, vendor guidance, and industry practices, then tailored to the organization's risk tolerance and operational requirements. The Center for Internet Security publishes widely used secure-configuration benchmarks that organizations can adopt as a baseline for many technologies. NIST also describes security control baselines as starting points for selecting controls appropriate to system impact and risk. Together, these concepts demonstrate why a security benchmark is the appropriate measure of baseline security performance. See the CIS Benchmarks and NIST SP 800-53 control baselines.

QUESTION NO: 63

Endpoint Protection Software is essentially the same as:

A. Host-based IDS/IPS (HIDS/HIPS).

B. Network-based IDS/IPS (NIDS).

C. Firewalls.

D. VPNs.

ANSWER: A

Explanation:

Host-based IDS/IPS (HIDS/HIPS). is the best answer because endpoint protection software operates directly on individual endpoints, such as workstations, servers, and mobile devices. Like a host-based intrusion detection or prevention capability, it uses an agent or local operating-system integration to observe activity occurring on that specific device. This can include monitoring processes, files, system events, application behavior, malware indicators, and attempted exploitation. When suspicious or malicious behavior is identified, the endpoint tool can alert security personnel, block execution, quarantine a file, terminate a process, or otherwise prevent the activity from succeeding.

This endpoint-level visibility and response model is the key similarity to HIDS/HIPS. Modern endpoint protection platforms commonly combine traditional anti-malware controls with behavioral detection, exploit prevention, and endpoint detection and response features, but their protective function remains centered on the individual host. ISC2's Certified in Cybersecurity outline includes security controls and operational technologies relevant to protecting systems and endpoints; see the ISC2 CC Certification Exam Outline. NIST also describes host-based protection measures, including anti-malware and host monitoring, in its guidance on malware incident prevention and handling: NIST SP 800-83 Rev. 1.

QUESTION NO: 64

Which of the following is included in an SLA document?

A. A plan to prepare the organization for the continuation of critical business functions

B. A plan to keep business operations going while recovering from a significant disruption

C. Instructions to detect, respond to, and limit the consequences of a cyber-attack

D. Instructions on data ownership and destruction

ANSWER: D

Explanation:

Instructions on data ownership and destruction are appropriately included in a service-level agreement because an SLA documents the agreed expectations, responsibilities, and service-management commitments between a service provider and its customer. Where a provider stores, processes, backs up, or otherwise manages customer information, the agreement should establish that the customer retains ownership of its data and specify how the provider will handle that data when the service ends. This includes requirements for secure return, retention periods where applicable, and secure deletion or destruction using an agreed process. Clear data-lifecycle terms provide accountability and help the customer maintain governance over information entrusted to a third party. They also establish measurable obligations that can be reviewed during vendor oversight and at contract termination. NIST's cloud-computing security guidance identifies data ownership, data handling, and data sanitization as important considerations in agreements with external service providers. ISC2's CC examination outline likewise includes security governance and third-party considerations within its security-principles domain. See NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing and the ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 65

An organization is concerned about the risk of a car driving from the parking lot through the entrance of the building. Which of the following security measures would best help address this concern?

A. Biometrics

B. RBAC

C. Badge system

D. Bollards

ANSWER: D

Explanation:

Bollards are the appropriate control because they create a strong physical vehicle barrier between the parking area and a building entrance. Properly designed, installed, and spaced bollards can stop or redirect a vehicle before it reaches doors, glazing, lobby areas, or occupied spaces. This directly mitigates the stated risk: a vehicle intentionally or accidentally driving into the entrance.

In physical security, perimeter and facility protections should address the specific threat being considered. For vehicle-incursion threats, security planners use vehicle barriers such as fixed bollards, crash-rated barriers, reinforced planters, or other engineered protective elements. The required level of protection depends on factors such as vehicle approach distance, expected vehicle speed, vehicle mass, and the consequence of impact. Where a credible hostile-vehicle or accidental-vehicle hazard exists, crash-tested bollards should be selected and installed according to their tested performance and the site layout. The U.S. General Services Administration describes vehicle barriers and their role in protecting facilities in its Vehicle Barriers guidance. The Cybersecurity and Infrastructure Security Agency also provides protective-design resources for mitigating vehicle impacts at facilities through its Vehicle Ramming Attack Mitigation guidance.

QUESTION NO: 66

What is the primary function of a Security Information and Event Management (SIEM) system?

A. To manage software installations and updates

B. To provide real-time analysis of security alerts generated by applications and network hardware

C. To physically secure server rooms and data centers

D. To train employees on cybersecurity awareness

ANSWER: B

Explanation:

A Security Information and Event Management system's primary function is to centralize security-relevant log and event data from across an environment and analyze it to identify potentially significant security activity. A SIEM collects telemetry from sources such as applications, servers, endpoints, identity systems, firewalls, and other network devices. It normalizes and correlates events that may appear unrelated when viewed separately, then applies rules, analytics, and threat intelligence to generate alerts for suspicious behavior or possible incidents. This consolidated, near-real-time visibility helps security personnel investigate events more efficiently, establish timelines, support incident response, and retain log data for monitoring and compliance needs. ISC2 describes security operations as relying on monitoring and analysis to detect and respond to threats; SIEM technology is a common platform supporting those activities. The SIEM does not itself replace the systems that generate logs or the analysts who validate and investigate alerts, but it provides the collection, correlation, and alerting capability needed to make large volumes of security events actionable. See the ISC2 Certified in Cybersecurity Exam Outline and the CISA information-sharing resources for related security monitoring and detection context.

QUESTION NO: 67

Which access control principle divides tasks and privileges among multiple individuals to prevent fraud and errors

?

A. Principle of Least Privilege.

B. Separation of Duties.

C. Defense in Depth.

D. Need-to-Know Principle.

ANSWER: B

Explanation:

Separation of Duties is correct because it distributes sensitive responsibilities across two or more individuals so that one person cannot independently complete a critical process. This control reduces the opportunity for fraud, misuse, and unintentional error by requiring oversight or participation from another authorized person. For example, within a financial process, one employee may initiate a payment request while another reviews and approves it; in an IT environment, an administrator who deploys a change may not be the same person authorized to approve that change. The principle is an important administrative access control because privileges are designed around distinct job functions and process stages, rather than giving a single account end-to-end control. ISC2's CC curriculum includes separation of duties among the fundamental access-control concepts used to protect assets and reduce risk. NIST similarly identifies separation of duties as dividing duties and privileges among individuals to reduce the risk of malevolent activity occurring without collusion. See the ISC2 Certified in Cybersecurity exam outline and NIST definition of separation of duties.

QUESTION NO: 68

Which of the following is not a secure method of data deletion?

A. Emptying the recycle bin on your computer desktop

B. Physical destruction of a hard drive

C. Zeroization

D. Overwriting

ANSWER: A

Explanation:

Emptying the recycle bin on your computer desktop is not a secure data-deletion method. When a user empties the recycle bin, the operating system typically removes the file-system references that make the file appear in normal directory listings and marks its storage space as available for reuse. The underlying data may remain on the drive until it is overwritten by subsequent activity, and recovery tools can potentially reconstruct it while those data blocks remain intact. Therefore, this action does not provide assurance that sensitive information is unrecoverable.

Secure media sanitization requires a method appropriate to the media type, data sensitivity, and intended disposition of the device. NIST describes sanitization as rendering access to target data infeasible for a given level of effort, and it identifies techniques such as clear, purge, and destroy. Organizations should define and document sanitization procedures as part of their media-handling and data-protection practices. See NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization and ISC2's Certified in Cybersecurity certification overview.

QUESTION NO: 69

Which type of attack attempts to gain information by observing the device's power consumption? (★)

A. Denials of Service

B. Side Channels

C. Cross Site Scripting

D. Trojans

ANSWER: B

Explanation:

Side Channels is correct because a side-channel attack derives sensitive information from observable effects of a system's operation rather than directly attacking its algorithms or authorized interfaces. Power analysis is a well-known side-channel technique: an attacker measures and analyzes a device's power consumption while it performs cryptographic or other sensitive operations. Variations in the power trace can correlate with instructions executed, data values processed, or secret-key-dependent operations. With appropriate measurements and statistical analysis, this leakage can enable recovery of

confidential values, including cryptographic keys. Side-channel analysis also encompasses other unintentional information emissions, such as execution timing, electromagnetic radiation, cache activity, and acoustic signals. For certification purposes, the essential connection is that observing power usage is an attempt to exploit physical or behavioral information leakage from the device. ISC2's CC domain material addresses attacks and mitigations as part of security operations and recognizes the importance of protecting systems from threats that exploit weaknesses beyond conventional network or application interfaces. NIST also describes power analysis as a side-channel attack against cryptographic modules. See NIST's definition of a side-channel attack and NIST's definition of power analysis.

QUESTION NO: 70

Software that creates and manages virtual machines (VMM) is called:

A. Hypervisor

B. Simulation

C. Emulation

D. Cloud controller

ANSWER: A

Explanation:

Hypervisor is the correct term for the software layer that creates, runs, and manages virtual machines. A hypervisor virtualizes the underlying physical hardware resources—such as processors, memory, storage, and network interfaces—so that multiple isolated guest operating systems can operate on one physical host. Each virtual machine receives virtual hardware and can run its own operating system and applications independently of the other virtual machines on that host. This isolation and controlled allocation of resources are central virtualization concepts relevant to secure and efficient infrastructure operations. Hypervisors are commonly categorized as Type 1, which run directly on the host hardware, and Type 2, which run as applications on a conventional host operating system. In either model, the hypervisor is responsible for coordinating virtual-machine access to physical resources and maintaining separation between guest environments. NIST describes virtualization as using a virtual machine monitor, also called a hypervisor, to provide and manage virtualized resources. See NIST's Hypervisor glossary entry and NIST SP 800-125, Guide to Security for Full Virtualization Technologies.

QUESTION NO: 71

Which one of the following groups is NOT normally part of an organization's cybersecurity incident response team?

A. Technical subject matter experts

B. Cybersecurity experts

C. Management

D. Law enforcement

ANSWER: D

Explanation:

Law enforcement is not normally a standing member of an organization's cybersecurity incident response team. An incident response capability is primarily an internal organizational function that brings together personnel able to make business decisions, investigate and remediate technical issues, manage communications, preserve relevant information, and coordinate recovery. Depending on the organization's size and structure, this commonly includes cybersecurity personnel, IT operations staff, technical subject matter experts, management, legal counsel, human resources, and public-relations staff.

Law enforcement is an important *external* stakeholder that the organization may contact when an incident potentially involves criminal conduct, fraud, theft, extortion, or other matters warranting a criminal investigation. The decision and

process for such notification should be defined in incident-response policies and coordinated with legal counsel and leadership. NIST describes the need to establish relationships and coordinate information sharing with external parties, including law enforcement, while treating those parties separately from the organization's incident-response team. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and ISC2's Certified in Cybersecurity certification overview.

QUESTION NO: 72

Why is identifying roles and responsibilities important in IR planning?

A. To prevent incidents

B. To ensure everyone knows their role

C. To reduce impact

D. To select containment strategy

ANSWER: B

Explanation:

To ensure everyone knows their role is correct because an incident response (IR) plan must establish who has the authority and responsibility to perform specific response activities before an incident occurs. Clear assignment of roles ensures that responders, incident handlers, management, communications staff, legal counsel, and technical specialists understand their expected actions, decision-making authority, escalation paths, and communication channels. This reduces uncertainty during a high-pressure event and enables the organization to coordinate its response efficiently. For example, the plan can identify who validates an incident, who leads technical investigation and containment, who approves major business-impacting actions, and who communicates with internal leaders or external parties. ISC2's incident-response concepts emphasize preparation, including defined policies, procedures, teams, and responsibilities, so that response activities can be executed in an organized and timely way. NIST likewise states that incident response teams need clearly defined roles and responsibilities as part of incident response preparation. Documenting these assignments also supports accountability, training, exercises, and consistent execution of the plan when different personnel are involved. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and the ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 73

The process of disguising a message or data in such a way that its true meaning is hidden refers to:

A. Encryption

B. Tokenization

C. Authentication

D. Authorization

ANSWER: A

Explanation:

Encryption is correct because it transforms readable plaintext into an unreadable form, called ciphertext, using a cryptographic algorithm and key. Its purpose is to conceal the meaning of information from parties that are not authorized to access it. A recipient with the appropriate key can decrypt the ciphertext and recover the original plaintext. Encryption is a foundational control for protecting confidentiality when data is stored, transmitted across networks, or processed in environments where unauthorized disclosure is a concern. It can be implemented with symmetric cryptography, where the same secret key is used to encrypt and decrypt, or asymmetric cryptography, where related public and private keys are used. In either case, the defining characteristic is that the underlying content is intentionally made unintelligible without the required cryptographic key. ISC2's Certified in Cybersecurity material identifies cryptography and encryption as important mechanisms for preserving confidentiality. NIST likewise defines encryption as the cryptographic transformation of data to

conceal its information content. See the NIST Privacy Framework Glossary and ISC2's Certified in Cybersecurity Exam Outline.

QUESTION NO: 74

What is the primary objective of network access controls?

A. To restrict all access to the network

B. To provide unrestricted access to network resources

C. To ensure the availability of network services

D. To regulate and manage access to network resources based on policies

ANSWER: D

Explanation:

The primary objective of network access controls is **to regulate and manage access to network resources based on policies**. These controls enforce an organization's access rules so that users, devices, and services can connect only to the systems, applications, network segments, and data for which they have appropriate authorization. Network access control mechanisms commonly evaluate identity, authentication status, device posture, role, location, and other contextual information before granting, limiting, or denying connectivity.

This policy-driven approach supports the principle of least privilege: access is limited to the minimum network resources and permissions needed for a legitimate business task. Examples include firewall rules, network segmentation, virtual private network access policies, access control lists, and Network Access Control solutions that validate a device before permitting it onto a network. Properly implemented controls reduce opportunities for unauthorized access and lateral movement while helping preserve the confidentiality and integrity of organizational resources. ISC2's Certified in Cybersecurity material identifies access controls as safeguards that enforce security policy and manage subjects' access to assets. See ISC2 Certified in Cybersecurity Exam Outline and the NIST Cybersecurity Framework.

QUESTION NO: 75

Which of the following protocols is a secure alternative to using Telnet?

A. SSH

B. HTTPS

C. SFTP

D. LDAPS

ANSWER: A

Explanation:

SSH is the secure alternative to Telnet for remote command-line access and device administration. Secure Shell establishes an encrypted connection between a client and server, protecting commands, session data, and credentials from interception or unauthorized alteration while they traverse a network. It also supports server authentication and can authenticate users using passwords, public keys, or other mechanisms. These protections address the principal security limitation of Telnet: Telnet sends its traffic, including login credentials, in plaintext. In practical security operations, administrators should use SSH when remotely managing systems, network devices, and Unix/Linux hosts, especially across untrusted or shared networks. SSH commonly uses TCP port 22, although an organization may configure a different port as part of its security architecture. The IETF SSH protocol architecture describes SSH as providing secure remote login and other secure network services over an insecure network. ISC2's Certified in Cybersecurity training similarly treats encrypted administrative protocols, including SSH, as the appropriate protection for remote management communications. See IETF RFC 4251: The Secure Shell Protocol Architecture and ISC2 Certified in Cybersecurity.

QUESTION NO: 76

Which of the following cloud models allows access to fundamental computer resources? (★)

A. IaaS

B. FaaS

C. SaaS

D. PaaS

ANSWER: A

Explanation:

IaaS is correct because it delivers the foundational computing components of a cloud environment as on-demand services. Under the National Institute of Standards and Technology cloud-computing definition, Infrastructure as a Service provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources. The customer can deploy and run software, including operating systems and applications, while the cloud provider manages the underlying physical infrastructure. This model is appropriate when an organization needs substantial flexibility to configure virtual machines, storage capacity, network connectivity, and its own software stack without purchasing or operating physical servers and data-center hardware. This division of responsibility is central to IaaS: the provider supplies and maintains the cloud infrastructure, while the customer retains responsibility for configuring and securing many of the resources it provisions, such as guest operating systems, applications, identities, and data. ISC2 learners should recognize the phrase “fundamental computing resources” as language that directly describes the IaaS service model. NIST defines these service-model characteristics in SP 800-145, The NIST Definition of Cloud Computing. For additional practical context on the shared responsibilities associated with cloud infrastructure, see the CISA cloud security guidance.

QUESTION NO: 77

What is the main limitation of Role-Based Access Control (RBAC)?

A. It lacks flexibility in assigning permissions.

B. It requires constant updates to access policies.

C. It does not provide granular control over individual user permissions.

D. It is too complex to implement.

ANSWER: C

Explanation:

Role-Based Access Control is designed to assign permissions to job-function roles and then assign users to those roles, rather than tailoring permissions independently for every person. This makes access administration consistent and scalable when people with the same responsibilities need the same access. Its principal limitation is therefore reduced granularity for individual exceptions: a user whose responsibilities differ slightly from the standard role may need permissions that do not align neatly with the role’s permission set.

In practice, an organization may address such exceptions by creating additional roles, assigning multiple roles, or granting special access. Without careful governance, these workarounds can result in users receiving permissions beyond their actual need, contrary to least privilege. This limitation becomes especially important when duties are highly individualized or change frequently. NIST describes RBAC as a model in which permissions are associated with roles and users acquire permissions through role membership, which explains why the role—not the individual user—is the normal unit of authorization. See NIST’s Role-Based Access Control project and NIST’s RBAC model documentation.

QUESTION NO: 78

Example of a technical control:

A. Security guard

B. GPS installed in a vehicle to track location

C. Door lock

D. None

ANSWER: B

Explanation:

GPS installed in a vehicle to track location is a technical control because it uses technological components—such as a receiver, communications capability, software, and a monitoring platform—to collect, transmit, process, and present location information. Technical controls, also called logical controls, are safeguards implemented through hardware, software, firmware, or electronic systems to support security objectives. In this case, location tracking can help an organization monitor the whereabouts of company assets, detect unauthorized movement, support incident investigation, and provide evidence of an asset's location at a particular time. The control operates through technology rather than relying solely on a person's actions or a purely mechanical barrier. NIST describes technical controls as safeguards primarily implemented and executed through mechanisms contained in hardware, software, or firmware. This classification aligns with the ISC2 CC distinction between administrative, physical, and technical controls: the technology itself performs or enables the security-relevant monitoring function. The GPS device may be used alongside policies and personnel procedures, but its core tracking capability remains a technical safeguard. See NIST's definition of technical control and ISC2 Certified in Cybersecurity resources.

QUESTION NO: 79

Which of the following is NOT an ethical canon of the ISC2?

A. Provide active and qualified service to principal

B. Act honorably, honestly, justly, responsibly and legally

C. Advance and protect the profession

D. Protect society, the common good, necessary public trust and confidence, and the infrastructure

ANSWER: A

Explanation:

"Provide active and qualified service to principal" is not an ISC2 Code of Ethics canon. ISC2 establishes four mandatory canons that guide the professional conduct of its members and certification holders. The service-focused canon specifically requires members to "Provide diligent and competent service to principals." This wording emphasizes the duty to perform work carefully, persistently, and with the knowledge and skill appropriate to the engagement, while recognizing that professionals may serve more than one principal. Ethical conduct is a core expectation for ISC2-certified professionals: they are expected to apply these canons when making decisions, carrying out cybersecurity responsibilities, and balancing obligations to employers, clients, the public, and the profession. The ISC2 Code of Ethics also states that members who observe violations should take appropriate action, reinforcing that the canons are actionable professional standards rather than general aspirational statements. The official text of the canons is available in the ISC2 Code of Ethics. ISC2 also describes ethics as a foundational element of certification-holder responsibilities in its member policies.

QUESTION NO: 80

What does Personally Identifiable Information (PII) pertain to?

A. Information about an individual's health status

B. Data about an individual that could be used to identify them

C. Trade secrets, research, business plans and intellectual property

D. The importance assigned to information by its owner

ANSWER: B

Explanation:

Personally Identifiable Information pertains to data that can identify a specific individual, either on its own or when combined with other reasonably available information. This includes direct identifiers, such as a person's name, government-issued identification number, biometric data, email address, or home address. It can also include indirect identifiers that may identify someone when correlated with other data. In an information-security context, PII requires appropriate classification and protection because unauthorized disclosure, alteration, or loss can affect an individual's privacy and may create legal, regulatory, financial, and reputational consequences for an organization. ISC2's CC training treats protecting sensitive information, including personal data, as a core security responsibility. The U.S. National Institute of Standards and Technology defines PII as information that can distinguish or trace an individual's identity, alone or combined with other information. Therefore, "Data about an individual that could be used to identify them" accurately describes what PII pertains to. See NIST's PII glossary definition and ISC2 Certified in Cybersecurity.

QUESTION NO: 81

Which network security mechanism encrypts data transmissions over a public network to ensure confidentiality?

A. Intrusion Detection System (IDS)

B. Virtual Private Network (VPN)

C. Network Access Control (NAC)

D. Firewall

ANSWER: B

Explanation:

Virtual Private Network (VPN) is correct because a VPN establishes an encrypted tunnel across an untrusted or public network, commonly the internet. Encryption protects the confidentiality of data while it travels between VPN endpoints, such as a remote employee's device and an organization's network, helping prevent unauthorized parties that can observe public-network traffic from reading the transmitted information. Depending on the implementation, VPNs can use protocols such as IPsec or TLS/SSL-based VPN technology to provide protected remote-access or site-to-site communications. This supports the confidentiality objective within the CIA triad by making intercepted traffic unintelligible without the appropriate cryptographic keys. VPNs are therefore a key network security mechanism for securely extending access to organizational resources over public infrastructure. ISC2's Certified in Cybersecurity material includes VPNs among technologies used to protect communications, and NIST describes IPsec as a suite of protocols that provides security services for IP communications. See ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-77 Rev. 1: Guide to IPsec VPNs.

QUESTION NO: 82

What is the process of verifying a users identity called?

A. Confidentiality

B. Authentication

C. Authorization

D. Identification

ANSWER: B

Explanation:

Authentication is the process of verifying that a user, system, service, or device is genuinely the identity it claims to be. In a typical login flow, a user first presents an identity, such as a username or account identifier, and then provides one or more authenticators to substantiate that claim. Authenticators can include something the user knows, such as a password or PIN; something the user has, such as a hardware token or mobile authenticator; or something the user is, such as a biometric characteristic. Using more than one authenticator category is commonly called multifactor authentication.

This distinction is fundamental to access control: authentication establishes identity before a system can make access decisions for that verified identity. The National Institute of Standards and Technology describes authentication as establishing confidence in a claimant's identity, including through authentication factors and authenticators. ISC2's Certified in Cybersecurity material likewise treats authentication as a core access-control concept used to verify identity. See NIST SP 800-63B: Digital Identity Guidelines—Authentication and Lifecycle Management and ISC2 Certified in Cybersecurity.

QUESTION NO: 83

Which principle ensures data is accurate and unchanged?

A. Confidentiality

B. Integrity

C. Availability

D. Accountability

ANSWER: B

Explanation:

Integrity is the information-security principle that ensures data remains accurate, complete, consistent, and protected from unauthorized or accidental alteration. In the CIA triad, integrity applies both to data stored in systems and to data while it is being processed or transmitted. Preserving integrity means an organization can rely on information for operational decisions, business processes, investigations, and compliance activities because the information has not been improperly modified, corrupted, or destroyed.

Common controls that support integrity include access controls that restrict who may modify records, input validation, change-management procedures, audit logs, version control, cryptographic hashes, and digital signatures. A hash can help detect whether content has changed, while a digital signature can provide stronger assurance that a signed item has not been altered since it was signed. ISC2 identifies integrity as a foundational security objective within the CIA triad. See ISC2's Certified in Cybersecurity overview and NIST's glossary definition of integrity.

QUESTION NO: 84

Which of these types of malware self-replicates without the need for human intervention?

A. Worm

B. Virus

C. Trojan

D. Rootkits

ANSWER: A

Explanation:

Worm is correct because a computer worm is malware that can independently copy itself and propagate across networks or between systems without requiring a user to open a file, execute an attachment, or otherwise activate it. Worms commonly identify and exploit vulnerabilities in network-facing services, weak credentials, or insecure configurations, then use the

resulting access to spread to additional reachable devices. This autonomous propagation can cause a rapid increase in infected hosts and may consume bandwidth, degrade availability, or deliver another malicious payload. The defining distinction for this question is the lack of required human intervention for replication and spread. ISC2's Certified in Cybersecurity material identifies malware as a key threat category and emphasizes understanding how malicious code can affect systems, networks, and organizational operations. The U.S. Cybersecurity and Infrastructure Security Agency also describes worms as self-replicating malware that spreads without user action. See CISA: Understanding Malware and Its Threats and ISC2 Certified in Cybersecurity.

QUESTION NO: 85

Protection against an individual falsely denying having performed a particular action

A. Authentication

B. Identification

C. Verification

D. Non repudiation

ANSWER: D

Explanation:

Nonrepudiation is the security property that provides evidence linking a person or entity to a specific action, transaction, or message so that they cannot credibly deny having performed it later. For example, a digitally signed message can provide evidence of the signer's identity, the integrity of the signed content, and the signer's intent to approve or send that content. Effective nonrepudiation commonly relies on strong identity binding through public key infrastructure, protection of private keys, trustworthy timestamps, and retained audit records. These controls establish evidence that can be independently validated after the event, which is essential for accountability in business transactions, access approvals, and electronic communications. ISC2 includes nonrepudiation among the fundamental information-security concepts and describes it as assurance that a party cannot deny the authenticity of their signature or a transaction. The NIST glossary similarly defines non-repudiation as assurance that the sender of information is provided with proof of delivery and the recipient with proof of the sender's identity, preventing denial of participation. See the ISC2 Certified in Cybersecurity Exam Outline and the NIST CSRC definition of non-repudiation.

QUESTION NO: 86

What is the BEST defense against dumpster diving attacks?

A. Anti-malware software

B. Clean desk policy

C. Data loss prevention tools

D. Shredding

ANSWER: D

Explanation:

Shredding is the best defense against dumpster diving because it directly protects the physical information source that an attacker seeks in discarded waste. Dumpster diving is a social-engineering and physical-security threat in which someone searches refuse, recycling, or unsecured disposal areas for documents and media containing sensitive information. Proper destruction makes the contents unreadable before they enter the waste stream, preventing recovery of data such as account information, personnel records, system diagrams, business plans, or authentication-related material.

For sensitive paper records, an organization should use an appropriate shredding method, such as cross-cut or micro-cut shredding, based on the data classification and any legal, contractual, or regulatory retention and disposal requirements. The

control is most effective when supported by documented media-sanitization procedures, secure collection bins, trained personnel, and a vetted destruction provider when disposal is outsourced. This reflects the principle that information must be protected throughout its lifecycle, including disposal. NIST describes media sanitization as rendering access to target data on media infeasible, while NIST physical and environmental protection controls address secure handling and disposal of information and system media. See NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization and NIST SP 800-53 Rev. 5, Physical and Environmental Protection controls.

QUESTION NO: 87

What advantage does endpoint protection software have over traditional antivirus solutions?

A. It can only detect known malware based on signatures.

B. It relies solely on user behavior to detect threats.

C. It monitors host activities to detect and prevent a wider range of malicious activities.

D. It is less resource-intensive and does not require regular updates.

ANSWER: C

Explanation:

Endpoint protection software has the advantage that it monitors host activities to detect and prevent a wider range of malicious activities. Traditional antivirus capabilities have historically focused primarily on identifying known malicious files, often through signatures. Endpoint protection platforms expand this protection by collecting and analyzing endpoint telemetry, such as process execution, command activity, file modifications, registry changes, network connections, and user or system behavior. This broader visibility allows the software to identify suspicious activity patterns, including techniques that may not match a previously known malware signature.

For example, endpoint protection can detect an unusual process spawning a command interpreter, attempts to alter security settings, or rapid file-encryption behavior associated with ransomware. It can then support preventive or response actions such as blocking execution, isolating an endpoint, terminating a process, or enabling investigation of the activity. This host-level monitoring and behavior-based detection gives security teams a more comprehensive ability to address modern endpoint threats. ISC2 describes endpoint security as protecting endpoint devices from threats through safeguards that include detection and response capabilities. See ISC2 Certified in Cybersecurity Exam Outline and CISA's malware guidance.

QUESTION NO: 88

What is the primary purpose of implementing multifactor authentication (MFA) within an organization's security strategy?

A. To increase the complexity of password policies

B. To ensure that only authorized users can access sensitive information by requiring multiple forms of verification

C. To encrypt data both at rest and in transit

D. To monitor and log all user activities within the system

ANSWER: B

Explanation:

To ensure that only authorized users can access sensitive information by requiring multiple forms of verification is correct because multifactor authentication strengthens the authentication process by requiring a user to present evidence from two or more distinct factor types before access is granted. Common factor categories include something the user knows, such as a password or PIN; something the user has, such as a hardware token, authenticator application, or smart card; and something the user is, such as a fingerprint or other biometric characteristic. Requiring more than one factor provides layered assurance of the user's identity and substantially reduces the likelihood that a compromised password alone can

lead to unauthorized access. MFA is therefore an important access-control safeguard for organizational systems, accounts, and sensitive data, particularly for remote access and privileged accounts. The ISC2 Certified in Cybersecurity curriculum identifies multifactor authentication as a means of strengthening identity and access management through more reliable user authentication. NIST similarly describes MFA as authentication based on two or more different authentication factors. See the ISC2 CC Certification Exam Outline and NIST SP 800-63B Digital Identity Guidelines.

QUESTION NO: 89

What is the purpose of a business continuity plan (BCP)?

A. To prevent all incidents from occurring.

B. To ensure business operations can continue during and after disruptions.

C. To recover all lost data immediately after an incident.

D. To provide a structured approach for responding to incidents.

ANSWER: B

Explanation:

The purpose of a business continuity plan (BCP) is **to ensure business operations can continue during and after disruptions.** Business continuity planning prepares an organization to maintain or restore its critical business functions when a disruptive event affects normal operations. Such events can include natural disasters, technology failures, cyber incidents, supply-chain interruptions, or loss of access to facilities. A BCP identifies essential processes and resources, establishes continuity strategies and recovery priorities, assigns roles and responsibilities, and documents procedures for operating at an acceptable level during a disruption.

In ISC2-aligned security practice, continuity planning supports organizational resilience by focusing on the sustained delivery of critical products and services, rather than merely responding to the initial event. The plan is informed by business impact analysis, which helps determine the consequences of outages and establish recovery objectives for key activities. It should also be tested, maintained, and updated so that personnel can execute it effectively when needed. NIST describes business continuity as the capability to continue mission or business processes following disruption, while CISA emphasizes planning to sustain essential functions and recover operations. See NIST's Business Continuity Plan glossary entry and CISA Resilience Services.

QUESTION NO: 90

A company network experiences a sudden flood of network packets that causes major slowdown in Internet traffic. What type of event is this?

A. Security incident

B. Natural disaster

C. Exploit

D. Adverse event

ANSWER: D

Explanation:

Adverse event is correct because the described packet flood has an observable negative effect on network availability and performance: Internet traffic is substantially slowed. An adverse event is an occurrence with an adverse consequence for an information system or its operations. It can include anomalous network conditions, service degradation, and availability impacts that require detection, analysis, and response. At the point described, the key confirmed fact is the harmful operational impact of unusually high packet traffic; the scenario does not establish the source, intent, or technical mechanism behind it. Security teams should treat this as an adverse event, collect relevant network and system evidence,

assess the scope and affected services, and determine whether escalation under the organization's incident-response process is warranted. This terminology supports disciplined handling of potentially significant conditions without assuming facts that have not yet been verified. NIST defines an adverse event as an event with a negative consequence and distinguishes it from a confirmed incident classification. See the NIST CSRC definition of adverse event and NIST's Computer Security Incident Handling Guide.

QUESTION NO: 91

Which access control mechanism assigns access rights based on the user's identity and specific attributes?

A. Role-Based Access Control (RBAC).

B. Mandatory Access Control (MAC).

C. Discretionary Access Control (DAC).

D. Attribute-Based Access Control (ABAC).

ANSWER: D

Explanation:

Attribute-Based Access Control (ABAC) is correct because it makes authorization decisions by evaluating attributes associated with the subject requesting access, the object or resource being requested, the intended action, and often environmental context. User identity can itself be an attribute, alongside attributes such as department, job function, clearance, employment status, location, device security posture, and time of access. Policies combine these characteristics to determine whether access should be allowed for a particular request, enabling decisions that are granular and adaptive rather than permanently tied to a single static permission assignment.

For example, an ABAC policy could permit a clinician to view a patient record only when the clinician is assigned to that patient, is working from a managed device, and access occurs during an active treatment relationship. This policy-based approach is especially useful when an organization needs to apply consistent controls across many users, resources, and changing conditions. NIST describes ABAC as a method in which authorization is determined by evaluating attributes and policies; see NIST SP 800-162: Guide to Attribute Based Access Control. ISC2's CC training outline also includes access-control concepts within its Security Principles domain: ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 92

An organization needs a network security tool that detects and acts in the event of malicious activity. Which of these tools will BEST meet their needs?

A. Firewall

B. Router

C. IDS

D. IPS

ANSWER: D

Explanation:

IPS is the best choice because an intrusion prevention system monitors network traffic for indicators of attacks or malicious behavior and can take automated action when it identifies a threat. Depending on its configuration and deployment, an IPS can block or drop malicious packets, terminate a suspicious connection, reset a session, or apply other preventive controls before the harmful activity reaches its intended target. This combination of detection and active prevention directly meets the requirement for a tool that both identifies malicious activity and acts in response to it. An IPS commonly uses signatures, protocol analysis, and behavioral or anomaly-based techniques to inspect traffic and enforce security policy in real time. ISC2 describes intrusion prevention as a control that detects malicious activity and then prevents or mitigates its effect,

making it a key technical safeguard for network defense. For additional authoritative background on intrusion detection and prevention technologies, see the NIST Guide to Intrusion Detection and Prevention Systems (IDPS) and ISC2's Certified in Cybersecurity certification overview.

QUESTION NO: 93

Which access control model grants permissions based ondata sensitivityanduser job functions?

A. DAC

B. RBAC

C. MAC

D. RuBAC

ANSWER: B

Explanation:

RBAC is correct because it assigns permissions to organizational roles that reflect users' job functions, responsibilities, and required level of access. Users receive the permissions associated with the role or roles to which they are assigned, rather than receiving permissions individually. An organization can define roles around both business duties and the sensitivity of information those duties require—for example, a payroll role authorized to access sensitive compensation records, or an executive role authorized to view confidential strategic reports. This lets the organization consistently grant access appropriate to the work being performed while applying least privilege and simplifying access administration when employees change positions. Role definitions and their permission assignments are reviewed and maintained as job responsibilities or information-handling requirements change. NIST describes RBAC as an approach in which permissions are associated with roles and users are assigned to those roles; it is intended to align access with organizational functions. ISC2 includes role-based access control among the access-control concepts assessed for Certified in Cybersecurity candidates. See the NIST Role-Based Access Control project and the ISC2 Certified in Cybersecurity exam outline.

QUESTION NO: 94

What distinguishes a "hot site" in disaster recovery planning?

A. A location without any pre-installed hardware or software, requiring significant setup time

B. A fully equipped, ready-to-use facility that can take over operations immediately

C. A partially equipped site that requires additional resources to become operational

D. A virtual space that relies exclusively on cloud resources, with no physical infrastructure

ANSWER: B

Explanation:

A fully equipped, ready-to-use facility that can take over operations immediately is the defining characteristic of a hot site. In disaster recovery planning, a hot site is maintained with the infrastructure needed to support critical business processes, such as servers, network connectivity, systems software, data access or replication capabilities, and appropriate environmental controls. Because these resources are already installed, configured, and available, the organization can transition processing to the alternate facility with very little delay after a disruption.

The purpose of using a hot site is to meet business requirements for highly time-sensitive services where prolonged outages would cause unacceptable operational, financial, legal, or reputational consequences. A hot site therefore supports a very short recovery time objective (RTO). Its readiness requires ongoing maintenance, testing, and synchronization of systems and data so that the alternate capability remains usable when needed. ISC2's disaster-recovery concepts emphasize selecting recovery capabilities that align with business continuity requirements and recovery objectives. See ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-34, Contingency Planning Guide.

QUESTION NO: 95

Which of the following best describes a honeypot?

A. A tool that increases data transfer speeds

B. A malicious software used by hackers

C. A decoy system designed to attract and trap attackers

D. A type of antivirus software

ANSWER: C

Explanation:

A decoy system designed to attract and trap attackers is the best description of a honeypot. A honeypot is an intentionally deployed resource, such as a host, service, application, account, or data set, that is made to appear useful or vulnerable to an adversary but has no legitimate production purpose. Because legitimate users should not normally interact with it, activity directed at the honeypot can provide a high-confidence indicator of suspicious reconnaissance, exploitation attempts, credential attacks, or lateral-movement activity.

Security teams use honeypots to detect unauthorized behavior, collect evidence about attacker techniques, and gain threat intelligence that can improve defensive controls. A honeypot should be isolated and carefully monitored so that an attacker who reaches it cannot use it as a pivot point into real systems. This concept aligns with ISC2's emphasis on monitoring, detection, and incident response: the decoy helps identify potentially malicious activity early and provides useful information for investigation. The National Institute of Standards and Technology describes deception technologies, including honeypots, as resources that can be used to detect and analyze adversary activity. See NIST's honeypot glossary definition and CISA's cyber-threat guidance.

QUESTION NO: 96

What goal of security is enhanced by a strong business continuity program?

A. Non-repudiation

B. Availability

C. Confidentiality

D. Integrity

ANSWER: B

Explanation:

Availability is enhanced by a strong business continuity program because business continuity planning prepares an organization to maintain or rapidly restore critical business processes and supporting technology after a disruption. The program identifies essential services, establishes recovery priorities and procedures, assigns responsibilities, and uses measures such as alternate work locations, redundant systems, backups, and tested recovery plans. These capabilities reduce downtime and help ensure that authorized users can access systems, applications, and information when they need them, including during incidents such as natural disasters, equipment failures, cyberattacks, or utility outages. Availability is a core information-security objective alongside confidentiality and integrity, and continuity planning directly supports its resilience component: sustaining operations despite adverse conditions. ISC2's Certified in Cybersecurity material includes business continuity, disaster recovery, and incident response as operational activities that protect an organization's ability to continue delivering services. NIST similarly defines contingency planning as establishing plans and procedures to recover systems and operations following a disruption. See ISC2 CC Certification Exam Outline and NIST SP 800-34 Rev. 1, Contingency Planning Guide.

QUESTION NO: 97

What role does documentation play in incident response?

A. Documentation is unnecessary and can slow down response efforts.

B. Documentation provides a record of incidents and response activities for analysis and improvement.

C. Documentation is solely the responsibility of the legal department.

D. Documentation is only required for incidents involving data breaches.

ANSWER: B

Explanation:

Documentation provides a record of incidents and response activities for analysis and improvement. Throughout an incident's lifecycle, responders should document what was observed, when events occurred, affected assets and accounts, decisions made, actions taken, evidence collected, communications, and the incident's resolution. This creates a reliable incident record that supports coordinated handling while the event is active and enables a meaningful post-incident review afterward.

Accurate records help the organization identify root causes, assess the effectiveness of containment and recovery actions, recognize recurring patterns, and improve incident-response playbooks, technical controls, training, and escalation procedures. Documentation also supports accountability and preservation of relevant evidence. Depending on organizational and regulatory requirements, incident records may be needed to demonstrate that established response processes were followed and to support required reporting or audit activities. ISC2's incident-response concepts emphasize lessons learned and continual improvement, both of which depend on retaining sufficient information about the incident and the response. NIST similarly identifies documentation as an activity that supports incident analysis, reporting, and learning from events. See NIST Special Publication 800-61, Computer Security Incident Handling Guide and ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 98

The process of verifying the actions taken by a user or system is known as:

A. Authentication

B. Authorization

C. Accounting

D. Auditing

ANSWER: D

Explanation:

Auditing is the process of examining, reviewing, and verifying records of activities performed by users and systems. It uses audit trails, event logs, and other evidence to establish what occurred, when it occurred, and which account or system performed the action. This provides accountability and supports the investigation of security events, operational errors, or potential policy violations. In an access-control context, auditing is closely associated with the ability to trace actions after access has been granted and used. Effective audit records commonly capture details such as the identity involved, date and time, source, action performed, and outcome. Organizations protect these records from unauthorized modification and review them regularly so that they can identify suspicious activity and demonstrate compliance with applicable security requirements. ISC2's Certified in Cybersecurity material includes accountability and auditability among the foundational security concepts used to monitor and assess system activity. NIST similarly describes audit and accountability controls as mechanisms for creating, protecting, retaining, and reviewing audit records. See ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-53 Audit and Accountability controls.

QUESTION NO: 99

A hacker gains unauthorized access and steals confidential data. What term best describes this?

A. Event

B. Breach

C. Intrusion

D. Exploit

ANSWER: B

Explanation:

Breach is the best description because the scenario includes both unauthorized access and the theft of confidential data. In cybersecurity and incident-response terminology, a data breach is an incident in which protected or sensitive information is accessed, disclosed, or acquired without authorization. The essential outcome in this case is the compromise of confidentiality: confidential data has been taken by an unauthorized party. ISC2's CC curriculum treats the protection of information from unauthorized disclosure as a core confidentiality objective, and an incident that exposes or removes such information constitutes a breach of that protection. The U.S. Cybersecurity and Infrastructure Security Agency similarly defines a data breach as an incident involving unauthorized access to sensitive, protected, or confidential data. This term therefore accurately captures the complete event described: not merely an attempt, a security-relevant occurrence, or unauthorized entry, but a realized compromise involving data theft. See CISA's overview of data breaches and the ISC2 Certified in Cybersecurity exam outline.

QUESTION NO: 100

The mitigation of violations of security policies and recommended practices is known as:

A. Disaster recovery

B. Incident response

C. Threat hunting

D. Incident response

ANSWER: D

Explanation:

Incident response is the correct term because it is the organized process used to address suspected or confirmed security incidents, including events that violate an organization's security policies or accepted security practices. Its purpose is to limit harm, restore affected services and systems safely, preserve relevant evidence, and ensure that the organization learns from the event. In practical terms, incident response brings together defined procedures, assigned responsibilities, communications, technical investigation, containment, eradication, recovery, and post-incident improvement activities. This makes it a core operational security capability rather than simply a technical tool or a one-time recovery activity.

For ISC2 CC candidates, the key distinction is that an incident is an event requiring coordinated handling because it may adversely affect confidentiality, integrity, availability, operations, or policy compliance. A documented incident response capability enables the organization to act consistently and promptly when such violations occur. NIST describes incident handling as including preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and ISC2's Certified in Cybersecurity certification overview.

QUESTION NO: 101

In network security, what is the function of encryption?

A. To physically secure network equipment from unauthorized access

B. To monitor network traffic for malicious activities

C. To convert data into a coded format to prevent unauthorized access

D. To increase the speed of network transmissions

ANSWER: C

Explanation:

Encryption converts readable information, known as plaintext, into an unintelligible coded form, called ciphertext, using a cryptographic algorithm and key. Its primary network-security function is protecting confidentiality: if data is intercepted while traveling across a network, an unauthorized party should not be able to understand it without the appropriate decryption key. The intended recipient uses the key to transform the ciphertext back into usable plaintext. Encryption can protect data in transit, such as information exchanged through a TLS-secured web session or VPN, and data at rest, such as files stored on a device or server. ISC2 identifies cryptography as a control used to protect the confidentiality of information, which directly supports the CIA triad. Effective encryption also depends on sound key management, because the secrecy and protection of cryptographic keys determine who can decrypt the protected data. Therefore, *To convert data into a coded format to prevent unauthorized access* accurately states encryption's fundamental purpose. See ISC2's discussion of cryptography and encryption in its Certified in Cybersecurity exam outline and NIST's overview of cryptographic mechanisms in NIST's encryption glossary entry.

QUESTION NO: 102

Which devices would be more effective in detecting an intrusion into a network?

A. HIDS

B. Firewalls

C. NIDS

D. Routers

ANSWER: C

Explanation:

NIDS is correct because a Network Intrusion Detection System is specifically designed to monitor network traffic and identify indicators of malicious activity, policy violations, or known attack patterns. It examines packets and network flows at strategically selected points, such as network boundaries or key internal segments, providing visibility into threats moving across the network. NIDS detection commonly relies on signature-based methods for known threats and anomaly-based methods for activity that deviates from established normal behavior. This makes it well suited to detecting attempts to intrude into a network, including reconnaissance, exploit traffic, command-and-control communications, and suspicious lateral movement. In the ISC2 Certified in Cybersecurity domain covering security operations, intrusion detection systems are security controls used to detect and alert on potentially unauthorized or harmful activity. A NIDS is network-focused: its sensors observe communications traversing the monitored segment and send relevant alerts to security personnel or a centralized monitoring platform for investigation and response. This capability directly addresses detection of an intrusion at the network level. For further background, see the NIST Guide to Intrusion Detection and Prevention Systems and the ISC2 Certified in Cybersecurity Exam Outline.

QUESTION NO: 103

What is the primary purpose of implementing multi-factor authentication (MFA)?

A. To increase network speed

B. To reduce employee productivity

C. To enhance security by requiring multiple forms of verification

D. To encrypt all data transmissions

ANSWER: C

Explanation:

The primary purpose of multi-factor authentication (MFA) is to enhance security by requiring multiple forms of verification. MFA requires a user to present evidence from at least two different authentication-factor categories, such as something they know (a password or PIN), something they have (a hardware security key, authenticator application, or smart card), or something they are (a biometric characteristic). This layered approach makes account compromise substantially more difficult because obtaining or guessing a password alone is not enough to authenticate. MFA is particularly valuable against common credential-based threats, including password reuse, phishing, credential stuffing, and brute-force attacks. Effective MFA implementations use factors that are independent of one another and apply MFA especially to remote access, privileged accounts, and sensitive systems. The ISC2 Certified in Cybersecurity curriculum identifies MFA as an important access-control safeguard, supporting the principle that access decisions should rely on strong identity verification rather than a single credential. For further guidance, see the CISA guidance on implementing phishing-resistant MFA and NIST SP 800-63B Digital Identity Guidelines.

QUESTION NO: 104

Who should participate in creating a BCP

A. Only members from the IT department

B. Only members from the management team

C. Members from across the organization

D. Only members from the finance department

ANSWER: C

Explanation:

Members from across the organization should participate in creating a business continuity plan (BCP). A BCP addresses how the organization will sustain or restore critical business processes following a disruption, so it must reflect operational dependencies, recovery priorities, required resources, personnel needs, communications procedures, facilities, technology, legal obligations, and customer or supplier commitments. Representatives from business units identify the processes that support their objectives and the impacts of an outage; IT contributes knowledge of systems and recovery capabilities; management provides governance, priorities, funding, and risk acceptance; and functions such as HR, legal, finance, security, facilities, and communications contribute their respective requirements. This cross-functional participation supports an accurate business impact analysis and produces practical, organization-wide recovery strategies rather than a plan limited to a single department's perspective. ISC2 describes business continuity as maintaining or rapidly resuming business functions after disruption, which inherently requires coordination among the people responsible for those functions. NIST likewise states that contingency planning involves business process owners and other stakeholders to establish recovery capabilities aligned with organizational needs. See ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-34 Rev. 1, Contingency Planning Guide.

QUESTION NO: 105

A companyâ€™s servers are down due to malware. What is the FIRST step the DR team should take?

A. Disconnect affected systems

B. Conduct risk assessment

C. Restore from backups

D. Contact law enforcement

ANSWER: A

Explanation:

Disconnect affected systems is the correct first action because a malware-caused outage must be stabilized before disaster-recovery restoration activities begin. Disconnecting, isolating, or otherwise containing the affected servers prevents the malware from spreading to additional systems, administrative workstations, backup repositories, recovery infrastructure, and network shares. It also limits an attacker's ability to continue command-and-control communications, move laterally, exfiltrate data, or alter evidence while the incident is being assessed.

Effective recovery depends on establishing a controlled environment and determining that recovery assets are clean. Once affected systems are isolated, the response team can preserve relevant evidence, identify the scope and nature of the compromise, validate backups or golden images, eradicate the malware, and then recover services in a manner that does not reintroduce the threat. This sequencing aligns incident response with disaster recovery: containment protects the organization and makes subsequent restoration reliable. NIST's incident-handling guidance identifies containment as a core activity before eradication and recovery, while CISA emphasizes isolating impacted systems during ransomware and malware incidents. See NIST SP 800-61 Rev. 2 and CISA Ransomware Guide.

QUESTION NO: 106

A company network experience a sudden flood of network packets that causes major slowdown in internet traffic. What type of event it this?

A. Security incident

B. Natural disaster

C. Exploit

D. Adverse event

ANSWER: D

Explanation:

Adverse event is correct because the described packet flood is an observable occurrence that has a negative effect on the organization's network operations: it causes a major slowdown in internet traffic. In ISC2 incident-response terminology, an adverse event is an event with potentially harmful consequences for business operations, systems, or security. The scenario establishes an operationally harmful condition but does not provide enough evidence to confirm the source, intent, exploit mechanism, or whether a specific security policy has been violated. Therefore, classifying the observed condition as an adverse event is the appropriate initial classification.

A sudden, excessive volume of packets may be consistent with a denial-of-service condition, whether accidental or malicious, and it warrants monitoring, triage, and escalation under the organization's incident-response procedures. At this point, responders should preserve relevant network telemetry, assess scope and service impact, and determine whether the adverse event meets the organization's criteria for declaration as a security incident. ISC2's CC exam outline includes incident-response concepts and the distinction between events and incidents, while NIST guidance describes the importance of detecting, analyzing, and handling adverse cybersecurity events. See the ISC2 Certified in Cybersecurity exam outline and NIST SP 800-61 Rev. 2.

QUESTION NO: 107

Which of these Access Control Systems is commonly used in the military?

A. RBAC

B. DAC

C. ABAC

D. MAC

ANSWER: D

Explanation:

MAC is commonly associated with military and government environments because it enforces centrally defined access decisions based on security labels. Under mandatory access control, an authority assigns classifications to information, such as Confidential, Secret, or Top Secret, and assigns corresponding clearances to subjects. The system evaluates those labels and clearances to determine whether access is permitted. Individual users generally cannot alter an object's classification or independently grant access to it, which supports consistent enforcement of organizational security policy.

This model is especially appropriate where information sensitivity and disclosure restrictions must be tightly controlled across a hierarchy of classification levels. A user must have an appropriate clearance and, in practical classified environments, an authorized need to know before receiving access to sensitive information. ISC2 identifies mandatory access control as a model in which the system enforces access according to rules established by a central authority. The U.S. National Institute of Standards and Technology also defines mandatory access control as restricting access based on security attributes and centrally managed policy. See NIST SP 800-192 and ISC2 Certified in Cybersecurity.

QUESTION NO: 108

Exhibit.

What is the purpose of a Security Information and Event Management (SIEM) system?

A. Encrypting files

B. Monitoring and analyzing security events

C. Blocking malicious websites

D. Managing user passwords

ANSWER: B

Explanation:

Monitoring and analyzing security events is the purpose of a Security Information and Event Management (SIEM) system. A SIEM centralizes security-relevant log and event data from sources across an organization, such as endpoints, servers, network devices, identity services, applications, and cloud platforms. It normalizes and stores this information so security personnel can search it, investigate activity, and maintain visibility across the environment.

A key SIEM capability is correlation: it connects related events from multiple sources and applies analytics or detection rules to identify patterns that may indicate a security incident. For example, a SIEM can associate authentication events, endpoint alerts, and network activity to produce a prioritized alert for investigation. This supports continuous monitoring, threat detection, incident response, forensic analysis, and reporting. NIST describes centralized logging and log analysis as important capabilities for identifying and responding to security issues; SIEM platforms operationalize these practices at scale. ISC2's security-operations concepts likewise emphasize collecting and analyzing events to detect potentially malicious activity and support response processes. See NIST SP 800-92: Guide to Computer Security Log Management and NIST Cybersecurity Framework.

QUESTION NO: 109

Which of the following best describes "tailgating" in a security context?

A. A network attack that intercepts data packets

B. An unauthorized person following an authorized person into a secured area

C. A type of malware attack

D. A method of secure software development

ANSWER: B

Explanation:

Tailgating is a physical security and social-engineering threat in which an unauthorized individual gains access to a restricted area by closely following someone who is authorized to enter. For example, an attacker may wait near a badge-controlled door and walk in while an employee opens it, perhaps carrying a box or acting as though they belong. The authorized person may hold the door open out of courtesy or may not notice that another person entered behind them. This bypasses access-control mechanisms because the unauthorized person does not present their own credential or receive separate authorization. Effective safeguards include enforcing one-person-per-badge entry, using turnstiles or mantraps where appropriate, training personnel not to allow unverified individuals through secure doors, and challenging or escorting unknown visitors. ISC2 identifies physical access controls and security awareness as important components of protecting organizational assets and facilities. See the ISC2 Certified in Cybersecurity Exam Outline and the CISA physical security guidance.

QUESTION NO: 110

Which of the following best describes the concept of "defense-in-depth"?

A. A single, strong security measure that provides complete protection

B. A strategy that relies solely on physical security controls

C. The coordination of multiple security measures to protect data

D. A cybersecurity approach that focuses only on external threats

ANSWER: C

Explanation:

Defense-in-depth is correctly described as “The coordination of multiple security measures to protect data.” It is a security strategy that deliberately combines overlapping and complementary safeguards so that the failure, bypass, or compromise of one control does not leave systems or information unprotected. These layers can include administrative measures, such as policies and awareness training; technical measures, such as multifactor authentication, network segmentation, encryption, endpoint protection, and logging; and physical protections. The purpose is not simply to deploy many tools, but to coordinate controls across people, processes, and technology to reduce the likelihood and impact of a successful attack.

For example, a protected system may require strong authentication before access is granted, limit the user’s authorization after login, encrypt sensitive data, monitor activity for suspicious behavior, and maintain recoverable backups. Each layer addresses different portions of the attack path and provides resilience if another layer is circumvented. This principle supports confidentiality, integrity, and availability by making unauthorized access more difficult to achieve and easier to detect and contain. ISC2 identifies defense in depth as the use of multiple, overlapping security controls to protect information assets. See the ISC2 overview of defense in depth and the CISA defense-in-depth resource.

QUESTION NO: 111

Representation of data at OSI Layer 3 is called a:

A. Segment

B. Packet

C. Frame

D. None of the above

ANSWER: B

Explanation:

The correct answer is **Packet**. The Open Systems Interconnection (OSI) model assigns logical addressing and routing functions to Layer 3, the Network layer. When data reaches this layer, the Network layer encapsulates the higher-layer data with a Layer 3 header, producing a protocol data unit commonly called a packet. In Internet Protocol networks, this header contains information used to move traffic between networks, including source and destination IP addresses. Routers operate primarily at this layer: they examine Layer 3 addressing and forwarding information to select a path toward the destination across interconnected networks. Understanding that a packet is the Layer 3 representation of data is fundamental because it distinguishes network-layer delivery and routing from the services performed by other OSI layers. This terminology is also reflected in the IPv4 specification, which defines the Internet Protocol datagram format and its addressing fields; in everyday networking instruction and certification contexts, an IP datagram is commonly referred to as an IP packet. See the ISC2 Certified in Cybersecurity Exam Outline for networking concepts within the certification scope and RFC 791, Internet Protocol for the IPv4 packet structure.

QUESTION NO: 112

Phishing attacks typically aim to:

A. Install malware on a target's computer

B. Steal sensitive information like passwords and credit card numbers

C. Increase network bandwidth

D. Promote cybersecurity awareness

ANSWER: B

Explanation:

Phishing attacks typically aim to steal sensitive information like passwords and credit card numbers. In a phishing campaign, an attacker impersonates a trusted person, organization, or service—often through email, text messages, social-media messages, or fraudulent websites—to persuade a recipient to disclose information or take an unsafe action. The requested data commonly includes usernames, passwords, multifactor authentication codes, financial-account details, payment-card numbers, or other personally identifiable information. Once obtained, these credentials or details can enable account takeover, financial fraud, identity theft, or unauthorized access to organizational systems.

This aligns with ISC2's treatment of phishing as a social-engineering threat: the attacker exploits human trust and urgency rather than directly defeating a technical control. The U.S. Cybersecurity and Infrastructure Security Agency similarly describes phishing as an attempt to steal sensitive information by posing as a trustworthy source. See ISC2 Certified in Cybersecurity exam outline and CISA guidance on recognizing and reporting phishing.

QUESTION NO: 113

Your organization is concerned about network security and wants to prevent unauthorized access to its resources by implementing a security model where the network has not trusted space what type of security model is this

A. Zero trust

B. Trusted computing

C. Trusted platform modelus

D. Trusted execution environment

ANSWER: A

Explanation:

Zero trust is the correct security model because it removes the assumption that a user, device, workload, or connection should be trusted merely because it is on an internal network. Instead, access decisions are made explicitly for each request based on verified identity, device condition, authorization, and relevant contextual signals. This approach supports

preventing unauthorized access by enforcing least-privilege access, continuously evaluating risk, and limiting access to only the specific resources needed for an approved task. In a zero-trust architecture, the network location is not itself a basis for trust; internal and external connections are treated as potentially untrusted until they satisfy the organization's access policy. This is particularly important for modern environments that include cloud services, remote users, mobile devices, and third-party connections, where a traditional network perimeter cannot reliably distinguish trusted activity from malicious activity. NIST defines zero trust as a cybersecurity paradigm that shifts defenses away from static, network-based perimeters toward users, assets, and resources. ISC2's CC material similarly emphasizes applying security controls and access management principles to protect organizational resources. See NIST SP 800-207, Zero Trust Architecture and ISC2 Certified in Cybersecurity exam outline.

QUESTION NO: 114

Which security control is used to verify the identity of a user or device before granting access to resources?

A. Encryption

B. Authentication

C. Authorization

D. Firewall

ANSWER: B

Explanation:

Authentication is the security process that verifies a claimed identity before a user or device is permitted to access a system, service, application, or other resource. It establishes confidence that the entity requesting access is actually the account holder, authorized device, or service it claims to be. Authentication can use one or more factors, including something the user knows (such as a password or PIN), something they have (such as a hardware token or cryptographic key), or something they are (such as a fingerprint). Multi-factor authentication combines factors to provide stronger assurance of identity.

Identity verification occurs before access decisions can be applied because the system must first know who, or what, is making the request. In practical environments, authentication may occur through login credentials, certificates, security keys, biometrics, or device-based mechanisms. ISC2 describes authentication as the process of proving an identity, a foundational concept within identity and access management. After identity is authenticated, access can be managed according to the organization's established permissions and policies. See the ISC2 overview of identity and access management and the NIST definition of authentication.

QUESTION NO: 115

What is the primary purpose of a firewall in network security?

A. To detect and remove viruses from email attachments

B. To serve as a physical barrier to unauthorized network access

C. To monitor and control incoming and outgoing network traffic based on predetermined security rules

D. To encrypt data transmissions over the internet

ANSWER: C

Explanation:

The primary purpose of a firewall is to monitor and control incoming and outgoing network traffic based on predetermined security rules. A firewall enforces an organization's network-access policy at a boundary between networks or security zones, such as between an internal network and the internet. It evaluates traffic against configured criteria—including source and destination addresses, ports, protocols, connection state, and, for more advanced firewalls, application-level

characteristics—and permits or blocks that traffic according to the policy. This filtering reduces exposure to unauthorized connections and helps limit communications to only those services and systems the organization intends to make available. Firewalls may be deployed as dedicated network appliances, software on an endpoint or server, or cloud-based controls; regardless of form, their essential function is policy-based traffic control. ISC2's Certified in Cybersecurity material identifies firewalls as a technical control used to filter network traffic and protect network boundaries. See ISC2's Certified in Cybersecurity Exam Outline and the NIST glossary definition of a firewall.

QUESTION NO: 116

A security analyst discovers that a terminated employee's account is still enabled and can access the organization's remote email service. Which of the following processes most likely failed?

A. Deprovisioning

B. Data classification

C. Tokenization

D. Network segmentation

ANSWER: A

Explanation:

Deprovisioning is correct because deprovisioning removes or disables accounts, privileges, and access when an individual no longer has a valid business need. A terminated employee should have access revoked promptly to prevent unauthorized use of active credentials and organizational systems.

Effective identity and access management includes provisioning when access is approved, periodic review to ensure access remains appropriate, and deprovisioning when a person changes roles or leaves the organization. Delayed account removal creates the risk of unauthorized access through dormant or former employee accounts. See NIST's account management definition.

QUESTION NO: 117

What is the primary function of "Logical Access Control Systems"?

A. To physically secure data centers and server rooms

B. To control an individual's ability to access computer system resources through validation mechanisms such as PINs, cards, or biometrics

C. To monitor environmental conditions within secure facilities

D. To encrypt network traffic between different segments of an information system

ANSWER: B

Explanation:

To control an individual's ability to access computer system resources through validation mechanisms such as PINs, cards, or biometrics is correct because logical access controls enforce authorization decisions for information systems and their resources. These controls first support identification and authentication by validating a user's claimed identity through one or more factors, such as something the user knows (a PIN), has (a card or token), or is (a biometric characteristic). After identity validation, the system applies access rules—commonly based on assigned roles, permissions, and the principle of least privilege—to determine which systems, applications, files, or services the individual may use and what actions they may perform. This function helps ensure that access to digital resources is limited to authorized users and appropriate business needs. ISC2's Certified in Cybersecurity training identifies logical controls as controls implemented through software, hardware, and technical mechanisms to manage access to systems and data. NIST likewise describes access

control as limiting information-system access to authorized users, processes acting on behalf of users, or devices. See ISC2 Certified in Cybersecurity Exam Outline and NIST CSRC: Access Control.

QUESTION NO: 118

Which access control model is based on a uniform set of policies enforced across all subjects and objects within an information system?

A. Discretionary Access Control (DAC)

B. Mandatory Access Control (MAC)

C. Role-Based Access Control (RBAC)

D. Attribute-Based Access Control (ABAC)

ANSWER: B

Explanation:

Mandatory Access Control (MAC) is correct because it applies centrally defined, system-wide security policies consistently to subjects, such as users or processes, and objects, such as files or databases. In a MAC implementation, an authority establishes security rules and assigns classifications or labels to resources and clearances to subjects. The system evaluates those labels and the governing policy before permitting access, rather than allowing individual resource owners to decide permissions. This centralized enforcement makes MAC especially appropriate for environments that require strong, uniform control over sensitive information, including government and military systems.

ISC2 describes mandatory access control as a model in which access decisions are governed by policy and centrally controlled rules. The model's defining characteristic is that users cannot freely alter permissions for protected objects; access is determined through the established security policy and authorization attributes. This supports consistent protection of information throughout the environment and helps preserve confidentiality when data has different sensitivity levels. For further background, see ISC2 Certified in Cybersecurity and the NIST definition of mandatory access control.

QUESTION NO: 119

What are registered port used for

A. Common protocols at the core of TCP/IP model

B. Used for web servers

C. Used for in housed or opensource applications

D. Proprietary applications from vendors and developers

ANSWER: D

Explanation:

Registered ports are used by specific applications and services that have been registered with the Internet Assigned Numbers Authority (IANA). They occupy the range from 1024 through 49151 and give software vendors, developers, and service maintainers a predictable port number for a particular service. This registration helps clients and network administrators identify the intended service and create consistent firewall, monitoring, and access-control rules. For example, IANA maintains a public registry that maps registered transport-protocol port numbers to service names and their associated organizations or contacts. The wording "Proprietary applications from vendors and developers" is the best answer because vendor-developed applications commonly use registered ports to provide a known, non-conflicting service endpoint. Registration does not make a port exclusive in a technical sense—an administrator can configure services differently—but it establishes the standardized, documented association used across networks. IANA distinguishes this registered range from the well-known system-port range and the dynamic/private range. See the IANA Service Name and Transport Protocol Port Number Registry and IANA's Assigned Numbers overview for the authoritative definitions and ranges.

QUESTION NO: 120

IDS can be described in terms of what fundamental functional components?

A. Response

B. Information sources

C. Analysis

D. All of the choices

ANSWER: D

Explanation:

All of the choices is correct because an intrusion detection system is commonly described through three core functional components: information sources, analysis, and response. Information sources provide the raw security-relevant data that the IDS monitors, such as network traffic, operating-system audit records, application logs, and host events. The analysis component processes and evaluates that data, using approaches such as signature-based detection or anomaly detection, to identify activity that may indicate an intrusion or policy violation. The response component communicates the detection result and supports incident handling, typically by generating alerts, recording events, notifying administrators, or initiating an approved response workflow. Together, these functions describe the complete detection lifecycle: collect relevant evidence, analyze it for suspicious activity, and produce a response or notification that enables action. NIST's Guide to Intrusion Detection and Prevention Systems (IDPS) discusses the monitoring, analysis, alerting, and response capabilities of IDPS technologies. ISC2 CC candidates should recognize that IDS functionality is not limited to examining traffic; it includes the data inputs, detection logic, and resulting alerting or response process. See also the NIST Cybersecurity Framework for the broader relationship between detecting cybersecurity events and supporting response activities.

QUESTION NO: 121

What role do physical access controls play in an organization's security posture?

A. They are used to encrypt data at rest.

B. They provide mechanisms to ensure data integrity.

C. They prevent unauthorized physical access to facilities and resources.

D. They manage digital identities and access rights within information systems.

ANSWER: C

Explanation:

Physical access controls are used to prevent unauthorized physical access to facilities and resources. They protect the places where people, systems, network equipment, media, and other organizational assets are located. Common examples include perimeter barriers, doors and locks, access badges, guards, visitor-management procedures, cameras, alarms, mantraps, and biometric readers. By restricting entry to authorized individuals and recording or monitoring access where appropriate, these controls reduce the opportunity for theft, tampering, sabotage, and unauthorized viewing or removal of sensitive information.

In a defense-in-depth security posture, physical security complements administrative and technical safeguards. For example, even strong logical authentication can be undermined if an unauthorized person can enter a server room, connect an unapproved device, steal storage media, or directly manipulate equipment. ISC2's Certified in Cybersecurity material includes physical controls as a fundamental category of security control used to safeguard assets and support organizational security objectives. The NIST physical and environmental protection control family likewise addresses measures for limiting physical access to systems, equipment, and operating environments. See ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-53 Physical and Environmental Protection controls.

QUESTION NO: 122

In symmetric encryption, what is a key characteristic?

A. Different keys are used for encryption and decryption.

B. The same key is used for both encryption and decryption.

C. Encryption keys are publicly available while decryption keys are private.

D. No keys are required for the encryption process.

ANSWER: B

Explanation:

The same key is used for both encryption and decryption. In symmetric-key cryptography, the communicating parties share a single secret key before protected communication begins. The sender applies that shared key to transform plaintext into ciphertext, and the intended recipient uses the same secret key to recover the original plaintext. Protecting and securely distributing this shared key is therefore central to the security of a symmetric encryption system: anyone who obtains it can generally decrypt information protected with it and create valid encrypted messages using that key.

Symmetric encryption is widely used when efficient protection of large quantities of data is needed. Common symmetric algorithms include the Advanced Encryption Standard (AES), which is used to protect data at rest and data in transit. In practical protocols, symmetric session keys may be established or exchanged using asymmetric cryptography, but the subsequent bulk-data encryption remains symmetric because the same session key performs both encryption and decryption. ISC2's CC curriculum includes cryptography concepts such as encryption methods, key management, and the distinction between symmetric and asymmetric encryption. See the NIST Advanced Encryption Standard (AES) publication and the ISC2 Certified in Cybersecurity exam outline.

QUESTION NO: 123

Which department in a company is NOT typically involved in a Disaster Recovery Plan (DRP)?

A. IT

B. Public Relations

C. Executive

D. Financial

ANSWER: D

Explanation:

Financial is the best answer in the context of the ISC2 CC disaster-recovery-plan material. A DRP is primarily an operational plan for restoring technology, systems, data, and essential business services after a disruptive event. Its development and execution therefore require substantial involvement from IT personnel, who perform recovery activities; executive leadership, who provide authority, priorities, resources, and decision-making; and public relations personnel, who help manage timely, accurate communications with customers, the public, and other stakeholders. The financial department may be consulted when a disruption has a direct financial impact, such as approving emergency expenditures, addressing insurance matters, or supporting cost assessments. However, it is not normally a core participant in the technical and communications activities that make up a DRP. This distinction reflects the DRP's focus on restoring operational capability rather than conducting routine financial functions. ISC2 identifies disaster recovery as a component of business continuity and emphasizes planning for recovery of critical information-processing capabilities. See ISC2's Certified in Cybersecurity exam outline and NIST's Contingency Planning Guide for Federal Information Systems for recovery-planning concepts and organizational responsibilities.

QUESTION NO: 124

What is the primary purpose of network access control (NAC) in network security?

A. To prevent unauthorized access to the network.

B. To encrypt data transmissions over the network.

C. To detect and respond to potential security threats.

D. To authenticate users accessing the network.

ANSWER: A

Explanation:

Network access control (NAC) primarily prevents unauthorized access to a network by applying an organization's access and security policies before a user or device is permitted to connect. NAC commonly identifies and authenticates the connecting user or endpoint, evaluates its posture against defined requirements, and then makes an authorization decision. For example, a NAC implementation can limit access for an unmanaged device, a device missing required updates, or an endpoint that does not meet the organization's security baseline. Depending on the result, NAC may deny connectivity, place the endpoint in a restricted network segment, or allow normal access. This supports the core security objective of ensuring that only authorized, policy-compliant entities gain appropriate network access. Authentication can be one component of NAC, but NAC has the broader purpose of enforcing access policy and controlling the level of network access granted. ISC2 describes access control as the process of granting or denying requests to use information-processing services, while NIST's zero trust guidance emphasizes explicit verification and limiting access based on policy and context. See the ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-207, Zero Trust Architecture.

QUESTION NO: 125

What is the purpose of implementing access control mechanisms in wireless networks?

A. To authenticate users attempting to access resources.

B. To assign access rights to authenticated users.

C. To enforce security policies by controlling access to wireless networks and devices.

D. To record and monitor user activities for auditing purposes.

ANSWER: C

Explanation:

To enforce security policies by controlling access to wireless networks and devices is correct because wireless access control applies an organization's authorization requirements to connections made over the air. Its purpose is to limit network access to approved users and managed or otherwise permitted devices, helping prevent unauthorized parties from joining the wireless environment and reaching internal resources. In practice, this may involve centrally defined policies that determine who may connect, which device characteristics are required, what network segment is available, and what resources can be used after a connection is established. Wireless controls commonly work with authentication and authorization services, such as enterprise Wi-Fi configurations using IEEE 802.1X, but the broader access-control purpose is enforcing the policy decision—not merely performing one individual authentication, permission-assignment, or logging activity. This supports the core access-control objective of ensuring that access is granted only in accordance with established organizational rules and business needs. ISC2 describes access control as the process of granting or denying requests to use information-processing services and related resources. For additional context on access control concepts, see NIST SP 800-12 Rev. 1 and NIST's guidance on securing wireless local area networks.

QUESTION NO: 126

Which of the following canons is found in the ISC2 code of ethics?

A. Protect society, the common good, and the infrastructure

B. Act honorably, honestly, safely and legally

C. Provide diligent and competent service to principals

D. Advance and promote the profession

ANSWER: C

Explanation:

“Provide diligent and competent service to principals” is an exact canon in the ISC2 Code of Ethics. In this context, principals are the people or organizations to whom the cybersecurity professional has a professional responsibility, such as an employer, client, or other authorized stakeholder. The canon establishes that credential holders must perform security work carefully, responsibly, and with the knowledge and skill appropriate to the assignment. Diligence means applying appropriate care, attention, and persistence when carrying out professional duties. Competence means recognizing the limits of one’s expertise, maintaining relevant knowledge and skills, and ensuring that work is performed to an appropriate professional standard. This ethical obligation is particularly important in cybersecurity because professional decisions can affect the confidentiality, integrity, availability, and resilience of systems and information. ISC2 presents this principle as one of the four mandatory canons that guide the conduct of its members and associates. The wording is stated directly in the official ISC2 Code of Ethics and is a key phrase candidates should recognize for the ISC2 CC examination. See the ISC2 Code of Ethics and ISC2’s Ethics Complaint Procedures.

QUESTION NO: 127

Which of these cannot be a corrective access control?

A. Patches

B. Backups

C. Bollards

D. CCTV cameras

ANSWER: C

Explanation:

Bollards are physical barriers installed to control vehicle movement and protect a facility’s perimeter, entrances, or other exposed areas. Their security purpose is to stop or discourage an unwanted action before it reaches protected people, buildings, or assets. This makes them a physical preventive or deterrent measure, rather than a corrective control.

Corrective controls are applied after a security problem, incident, or identified weakness and are intended to remediate the condition or restore secure operations. In contrast, a bollard does not repair a vulnerability, restore affected data or systems, or return an environment to a known-good state after an incident. It remains a fixed, forward-looking barrier intended to reduce the likelihood or impact of unauthorized vehicle access and similar threats.

ISC2’s CC learning materials distinguish security controls by function, including preventive, detective, corrective, deterrent, recovery, and compensating functions. Understanding the purpose of a control—not merely whether it is technical or physical—is essential when classifying it. See ISC2’s Certified in Cybersecurity exam outline and NIST’s discussion of physical and environmental protection controls in SP 800-53 Rev. 5.

QUESTION NO: 128

An employee receives an email with an attachment that appears to be an invoice from a supplier. The employee did not expect an invoice and is unsure whether the message is legitimate. What is the best action for the employee to take?

A. Open the attachment in order to inspect the invoice

B. Reply to the email and ask whether the attachment is safe

C. Verify the request through an independent communication channel

D. Forward the attachment to coworkers for their opinion

ANSWER: C

Explanation:

Verify the request through an independent communication channel is correct because an unexpected attachment may be part of a phishing or malware-delivery attempt. The employee should avoid opening the attachment and independently verify the message, such as by contacting the supplier through a known telephone number or an established business contact method. The suspicious email should also be reported according to organizational procedures.

Replying directly to the email or using contact information included in the message could communicate with the attacker rather than the genuine supplier. Opening the attachment to inspect it can execute malicious content or expose the organization to compromise. CISA recommends recognizing and reporting phishing attempts and independently verifying suspicious requests in its phishing guidance.

QUESTION NO: 129

A backup that captures the changes made since the latest full backup is an example of:

A. A backup snapshot

B. A full backup

C. A differential backup

D. An incremental backup

ANSWER: C

Explanation:

A differential backup captures all data that has changed since the most recent full backup. For example, after a full backup is completed on Sunday, each differential backup during the following days contains every change made since that Sunday full backup. The amount of data in each differential backup therefore generally grows until another full backup establishes a new baseline. During restoration, the organization needs the most recent full backup and only the latest differential backup, which can simplify recovery compared with a chain of multiple backups. This approach supports availability and resilience by providing a defined recovery process and preserving data needed to restore systems following an outage, corruption event, or other incident. Backup strategy decisions should account for recovery objectives, storage capacity, backup windows, and the operational need to restore information reliably. NIST's contingency-planning guidance describes backups as a key recovery capability and emphasizes maintaining and testing data backup and recovery procedures. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and the ISC2 Certified in Cybersecurity certification page.

QUESTION NO: 130

Which component of the incident response plan involves identifying critical data and systems?

A. Detection and Analysis

B. Preparation

C. Containment

D. Eradication

ANSWER: B

Explanation:

Preparation is correct because an organization must understand what it needs to protect before it can respond effectively to an incident. This work includes identifying critical business functions, sensitive and high-value data, essential applications, infrastructure, system owners, dependencies, and recovery priorities. That information lets the incident response team assess potential business impact, determine which assets require immediate attention, and apply appropriate escalation and recovery procedures during an event. Preparation also establishes the people, processes, communications channels, tools, policies, and documentation needed to support a coordinated response. Maintaining accurate asset inventories and data classifications is especially important because responders need reliable context to determine whether an affected system contains regulated, confidential, or mission-critical information. NIST's incident-handling guidance describes preparation as the phase in which organizations establish incident-response capabilities and supporting resources before incidents occur. ISC2's Certified in Cybersecurity material likewise emphasizes preparation and planning as foundational activities for managing cybersecurity incidents. Identifying critical data and systems in advance ensures response decisions are aligned with business priorities rather than being made without adequate context during a crisis. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and ISC2 Certified in Cybersecurity.

QUESTION NO: 131

What is the primary purpose of encryption in network security?

A. To authenticate users accessing the network

B. To prevent unauthorized access to the network

C. To ensure the confidentiality of data in transit

D. To monitor and analyze network traffic for security threats

ANSWER: C

Explanation:

To ensure the confidentiality of data in transit is correct because encryption transforms readable plaintext into ciphertext using a cryptographic algorithm and key. A party that intercepts the traffic should be unable to understand the protected information unless it possesses the appropriate decryption key. This is the fundamental security service encryption provides in network communications, protecting sensitive content such as credentials, business information, and personal data as it traverses networks that may be untrusted or subject to interception.

In practice, protocols such as TLS and IPsec apply encryption to network traffic, with modern cipher suites commonly combining encryption with separate integrity and authentication protections. However, confidentiality remains encryption's primary purpose; integrity is a distinct security objective that requires cryptographic authentication mechanisms, such as a message authentication code or authenticated-encryption mode. This distinction is important for ISC2 CC candidates because security controls should be mapped to the specific objective they provide. ISC2 identifies cryptography concepts and the protection of data as core CC knowledge areas. See the ISC2 Certified in Cybersecurity exam outline and NIST's definition of encryption.

QUESTION NO: 132

According to ISC2 Code of Ethics, to whom does Kristal ultimately report?

A. The company

B. Governments

C. ISC2

D. The users

ANSWER: D

Explanation:

The users is correct because the ISC2 Code of Ethics places the safety, welfare, and trust of people affected by cybersecurity decisions above an information-security professional's organizational loyalties. Its first canon directs members to protect society, the common good, necessary public trust and confidence, and the infrastructure. In practical terms, users and the public are the ultimate beneficiaries of security work: they depend on professionals to safeguard their information, systems, privacy, and ability to use technology safely. Kristal may have contractual, managerial, or professional obligations to an employer and to the certification body, but those responsibilities must be carried out consistently with the overriding duty to protect people and the public interest. This principle is especially important when an employer's preferred course of action could expose users to avoidable harm, conceal a material security risk, or undermine public trust. The ISC2 ethical framework therefore guides Kristal to make decisions that prioritize users' protection and confidence in the systems they rely on. See the ISC2 Code of Ethics and ISC2's policies and procedures for the governing ethical expectations.

QUESTION NO: 133

Exhibit.

IPSec works in which layer of OSI Model

A. Layer 2

B. Layer 5

C. Layer 3

D. Layer 7

ANSWER: C

Explanation:

IPSec operates at OSI Layer 3, the Network layer. It is a suite of standards that protects traffic at the Internet Protocol layer, applying security controls to IP packets independently of the applications generating the traffic. This placement allows IPSec to provide protections such as packet authentication, integrity, confidentiality, and anti-replay capability for many kinds of IP communications without requiring individual applications to implement their own security mechanisms. IPSec is therefore widely used to establish virtual private networks, including gateway-to-gateway (site-to-site) VPNs and remote-access VPNs. The Encapsulating Security Payload protocol can provide confidentiality as well as integrity and authentication, while the Authentication Header provides integrity and origin authentication for IP packets. Internet Key Exchange establishes and manages the security associations and cryptographic keys used by IPSec. ISC2 CC candidates should associate IPSec with network-layer protection because its fundamental unit of protection is the IP packet, rather than an application session or a specific transport protocol. NIST's guidance describes IPSec as a network-layer security architecture, and the IETF architecture specification defines security services for traffic at the IP layer. See NIST SP 800-77 Rev. 1 and RFC 4301: Security Architecture for the Internet Protocol.

QUESTION NO: 134

After an earthquake disrupts business operations, which document contains the reactive procedures required to return business to normal operations?

A. Business Impact Analysis

B. Business Continuity Plan

C. Disaster Recovery Plan

D. Business Impact Plan

ANSWER: C

Explanation:

The **Disaster Recovery Plan** contains the documented reactive procedures used after a disruptive event, such as an earthquake, to recover affected technology services and support the return to normal business operations. It typically establishes recovery roles, escalation and communication processes, recovery priorities, alternate processing arrangements, restoration steps for systems and data, and validation activities to confirm that recovered services operate correctly. Disaster recovery is therefore the recovery-focused component of organizational resilience: it addresses the practical restoration of IT infrastructure, applications, data, and supporting facilities following an incident that has caused an outage or degradation.

ISC2's Certified in Cybersecurity material distinguishes business continuity, which addresses sustaining or resuming critical business functions, from disaster recovery, which addresses restoring the systems and capabilities needed to operate normally after a disaster. A recovery plan should be based on organizational recovery requirements and exercised so personnel can execute it effectively under real incident conditions. The U.S. Cybersecurity and Infrastructure Security Agency likewise identifies disaster recovery planning as the process of restoring IT capabilities after a disruption. See ISC2 Certified in Cybersecurity Exam Outline and CISA Continuity and Resilience.

QUESTION NO: 135

The process of assessing the impact and likelihood of a potential security threat is known as:

A. Threat modeling

B. Password management

C. Social engineering

D. Network segmentation

E. Risk assessment

ANSWER: E

Explanation:

Risk assessment is the correct term because it evaluates potential adverse events by considering their likelihood of occurring and the magnitude of their impact. This evaluation helps an organization determine the level of risk associated with threats to its systems, information, and operations. The resulting risk information supports informed decisions about which risks require treatment, what safeguards are appropriate, and how resources should be prioritized.

This terminology aligns with the foundational risk-management concepts covered in ISC2 Certified in Cybersecurity material. NIST describes risk assessment as a process that identifies threats and vulnerabilities, determines likelihood and impact, and establishes risk. Likelihood represents the chance that a threat event will occur or succeed, while impact represents the potential harm or consequence if it does. Assessing both factors provides a consistent basis for ranking risks and selecting proportionate controls. See the ISC2 Certified in Cybersecurity Exam Outline and NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.

QUESTION NO: 136

In network security, what is the purpose of using a Demilitarized Zone (DMZ)?

A. To encrypt data transmissions

B. To serve as an external-facing network segment that adds an additional layer of security

C. To detect and prevent malware infections

D. To provide a backup for network data

ANSWER: B

Explanation:

A Demilitarized Zone (DMZ) is a separate, perimeter network segment used to host systems that must be reachable by untrusted external networks, such as public web servers, email gateways, and DNS servers. Its purpose is to create a controlled buffer between the internet and the organization's trusted internal network. Rather than allowing inbound internet traffic to reach internal systems directly, security controls such as firewalls strictly govern communication between the internet and the DMZ, as well as between the DMZ and the internal network. This layered design reduces exposure of internal resources and helps contain the impact if a public-facing system is compromised. A DMZ therefore supports network segmentation and defense in depth: services intended for public access can be made available while the internal network remains isolated behind additional access controls. ISC2 describes network segmentation as an important means of limiting access and reducing the potential scope of an incident. For further background on segmentation and perimeter protections, see the CISA guidance on defending a DMZ and the UK National Cyber Security Centre network security guidance.

QUESTION NO: 137

What access control principle ensures that access rights are separated among multiple individuals to prevent fraud and errors?

A.

Principle of Least Privilege.

B. Separation of Duties.

C. Defense in Depth.

D. Need-to-Know Principle.

Answer: B

Explanation:

Separation of Duties ensures that access rights are separated among multiple individuals to prevent fraud and errors, reducing the risk of unauthorized activities and ensuring accountability.

A. Separation of Duties.

B. Defense in Depth.

C. Need-to-Know Principle.

ANSWER: A

Explanation:

Separation of Duties is the access-control principle that divides sensitive or consequential activities among different individuals so that no single person can complete an entire high-risk process alone. For example, one employee may be authorized to create a supplier record, while another approves payments to that supplier. Requiring distinct people and permissions for these steps introduces independent oversight and makes fraudulent or erroneous actions more likely to be detected before they cause harm.

This principle supports accountability because actions can be attributed to separate roles, and it reduces the opportunity for an individual to misuse excessive authority without review. In cybersecurity and business operations, Separation of Duties is commonly implemented through role-based access controls, approval workflows, dual control, and periodic access reviews. It is particularly important for functions involving financial transactions, privileged administration, changes to production systems, and access to sensitive data.

ISC2 includes access-control concepts within its Certified in Cybersecurity curriculum, emphasizing the use of controls to manage and limit access appropriately. NIST also identifies separation of duties as a foundational control technique for preventing fraud and errors. See the ISC2 Certified in Cybersecurity Exam Outline and NIST definition of Separation of Duties.

QUESTION NO: 138

Which is related to Privacy

A. GDPR

B. FIPS

C. MOU

D. All

ANSWER: A

Explanation:

GDPR is directly related to privacy because it is the European Union's General Data Protection Regulation, a legal framework governing the processing of personal data. Privacy concerns an individual's ability to control information about themselves and the appropriate collection, use, sharing, retention, and protection of that information. GDPR establishes enforceable requirements for organizations that process personal data of people in the European Economic Area, including requirements for a lawful basis for processing, transparency through privacy notices, data minimization, purpose limitation, and appropriate security measures. It also establishes data-subject rights, such as access to personal data, correction of inaccurate data, erasure in applicable circumstances, and restrictions on certain processing activities. These requirements make GDPR a central privacy-related law and an important example of how privacy principles are translated into organizational obligations. ISC2 cybersecurity professionals should recognize that privacy responsibilities overlap with security practices, particularly when protecting the confidentiality and integrity of personal data. The official GDPR text is available through EUR-Lex, and the European Commission provides an overview of data protection in the EU.

QUESTION NO: 139

The amount of risk an organization is willing to accept in pursuit of objectives is called:

A. Risk assessment

B. Risk transfer

C. Risk appetite

D. Risk management

ANSWER: C

Explanation:

Risk appetite is the correct term for the amount and type of risk an organization is prepared to accept while pursuing its objectives. It is established by leadership and governance bodies to provide a strategic boundary for decision-making: teams can take risks that support business goals, but those risks should remain within the organization's stated appetite. This concept helps align cybersecurity and broader enterprise risk decisions with organizational priorities, resources, legal obligations, and stakeholder expectations.

For example, an organization with a low risk appetite for exposure of sensitive customer information may invest heavily in protective controls and require prompt remediation of related vulnerabilities. Its appetite can be expressed qualitatively or quantitatively and should guide the development of risk tolerances, which are more specific limits for particular objectives, processes, or metrics. ISC2's Certified in Cybersecurity material treats risk appetite as a key governance concept that informs how risks are evaluated and handled. See the ISC2 Certified in Cybersecurity Exam Outline and NIST's SP 800-39, Managing Information Security Risk for risk-management governance context.