DUMPSARENA

Information Systems Security Management Professional (ISSMP) Exam

ISC2 ISSMP

Version Demo

Total Demo Questions: 20

Total Premium Questions: 202

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Leadership and Business Management	34
Topic 2, Systems Lifecycle Management	48
Topic 3, Risk Management	26
Topic 4, Threat Intelligence and Incident Management	22
Topic 5, Contingency Management	24
Topic 6, Law, Ethics, and Security Compliance Management	46
Topic 7, Mix Questions	2
Total	202

QUESTION NO: 1

In which of the following mechanisms does an authority, within limitations, specify what objects can be accessed by a subject?

A. Role-Based Access Control

B. Discretionary Access Control

C. Task-based Access Control

D. Mandatory Access Control

ANSWER: B

Explanation:

Discretionary Access Control is correct because it permits an authorized authority—typically the owner or creator of an object—to determine which subjects may access that object and what permissions they receive. The word “discretionary” reflects this delegated decision-making power: access to files, folders, database records, or other protected objects can be granted, changed, or revoked by the responsible authority rather than being determined solely by a centrally imposed system-wide rule. The authority’s discretion is not unlimited; organizational policy, system configuration, administrative privilege boundaries, and platform security controls constrain who may assign permissions and how they may do so. In practice, this model is commonly implemented through access control lists or permission settings that associate subjects or groups with allowed operations such as read, write, execute, modify, or delete. This directly matches the question’s description of an authority specifying the objects a subject can access within defined limitations. NIST defines discretionary access control as a means of restricting access to objects based on the identity of subjects and/or the groups to which they belong, supporting owner-directed permission assignments. See NIST CSRC: Discretionary Access Control and NIST FIPS 200.

QUESTION NO: 2

Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

A. Determining what level of classification the information requires.

B. Delegating data protection duties to a custodian while retaining accountability.

C. Reviewing the classification assignments at regular time intervals and making changes as the business needs change.

D. Running regular backups and routinely testing the validity of the backup data.

ANSWER: A B C

Explanation:

Data ownership is a business-accountability role within an information classification program. Determining what level of classification the information requires is central to that role because the owner understands the information’s business purpose, sensitivity, value, legal obligations, and consequences of unauthorized disclosure, modification, or loss. The owner also establishes the protection requirements associated with that classification and may assign operational data-handling activities to a custodian. Accordingly, delegating data protection duties to a custodian while retaining accountability is appropriate: delegation enables implementation by personnel responsible for day-to-day technical and administrative handling, but it does not transfer the owner’s ultimate accountability for appropriate protection. Reviewing the classification assignments at regular time intervals and making changes as the business needs change is also essential because information value, sensitivity, regulatory requirements, and organizational use can evolve throughout the information life cycle. NIST defines an information owner/steward as the organizational official with statutory, management, or operational authority for specified information, supporting this accountability model. See the NIST definition of information owner/steward and NIST’s Guide for Mapping Types of Information and Information Systems to Security Categories.

QUESTION NO: 3

Which of the following plans provides procedures for recovering business operations immediately following a disaster?

A. Disaster recovery plan

B. Business continuity plan

C. Continuity of operation plan

D. Business recovery plan

ANSWER: D

Explanation:

Business recovery plan is correct because it addresses the organized restoration of business operations after a disruptive event has occurred. Its procedures guide the organization through the immediate post-disaster period, including restoring prioritized business processes, coordinating personnel and resources, resuming services at an acceptable level, and transitioning from emergency response into normal operations. The plan is business-focused: it connects recovery activities to the organization's critical functions, recovery priorities, and operational objectives rather than limiting attention to technical systems alone. Effective business recovery planning also establishes decision authority, communications, resource requirements, and recovery sequencing so leaders can make timely, consistent decisions while operations are being reestablished. This makes it the appropriate plan for procedures specifically concerned with recovering business operations immediately following a disaster. NIST describes continuity planning as a coordinated capability for sustaining or recovering mission and business processes after disruption, including recovery strategies and procedures. The UK National Cyber Security Centre likewise emphasizes planning for the recovery and restoration of important business services after an incident. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and NCSC incident-management planning guidance.

QUESTION NO: 4

Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

A. They can be analyzed and measured by the risk analysis process.

B. They can be removed completely by taking proper actions.

C. They can be mitigated by reviewing and taking responsible actions based on possible risks.

D. They are considered an indicator of threats coupled with vulnerability.

ANSWER: A C D

Explanation:

Security risk is the potential for an adverse outcome when a threat can exploit a vulnerability and cause harm to an information system or organizational asset. Therefore, it is appropriately understood as an indicator arising from the relationship between threats and vulnerabilities, while also considering potential impact. Risk analysis provides the structured process for identifying risks and evaluating their likelihood and impact, using qualitative, quantitative, or hybrid measurement approaches. This analysis enables management to prioritize the risks that need treatment according to organizational risk appetite and mission requirements.

Risk can also be mitigated through responsible, risk-based actions, such as implementing administrative, technical, or physical controls that reduce the likelihood of exploitation or lessen its impact. Mitigation is part of a broader risk-treatment strategy and should be supported by ongoing monitoring because systems, threats, vulnerabilities, and business conditions change over time. In practice, controls generally reduce risk to an acceptable residual level rather than make it disappear entirely. NIST describes risk management as an ongoing process of assessing, responding to, and monitoring risk. See NIST SP 800-37 Rev. 2 and NIST SP 800-30 Rev. 1.

QUESTION NO: 5

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

A. Editor

B. Custodian

C. Owner

D. Security auditor

E. User

ANSWER: B C E

Explanation:

Custodian, **Owner**, and **User** are the core operational roles commonly assigned in an information classification program. The Owner is the business role accountable for the information asset. This role establishes the data's business value, determines its classification, approves appropriate access requirements, and ensures handling requirements reflect organizational needs, legal obligations, and risk. A Custodian implements and operates the protections selected for the information, such as storage, backups, access-control mechanisms, retention processes, and secure disposal procedures. Custodians preserve the confidentiality, integrity, and availability requirements established by the Owner. A User is an authorized individual who accesses or handles information in accordance with its assigned classification and the organization's handling rules. Users are responsible for applying required safeguards in their daily activities, including appropriate sharing, storage, and reporting of potential incidents. Clear assignment of these roles creates accountability across classification decisions, technical administration, and day-to-day information handling. NIST's guidance on mapping information types to security categories supports establishing protection requirements based on the impact of compromise; see NIST SP 800-60 Volume I. NIST also defines the accountable data-owner concept in its Computer Security Resource Center glossary.

QUESTION NO: 6

Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

A. Confidentiality

B. Integrity

C. Availability

D. Privacy

ANSWER: A B C

Explanation:

Confidentiality, integrity, and availability are the established three fundamental principles of information security, collectively called the CIA triad. Confidentiality ensures that information is accessible only to authorized people, processes, or systems, protecting it from unauthorized disclosure. Integrity preserves the accuracy, completeness, consistency, and trustworthiness of information and systems by preventing or detecting unauthorized or improper modification or destruction. Availability ensures that authorized users can reliably access information and supporting systems when needed, which requires resilient operations, appropriate capacity, maintenance, and recovery planning. Together, these principles provide a foundational framework for security management: security leaders identify risks to each principle, select proportionate safeguards, and assess whether those safeguards protect organizational information assets and business services. This framing is reflected in NIST's security objectives, which describe preserving confidentiality, integrity, and availability as the core objectives for information and information systems. ISC2 security practice similarly treats the CIA triad as a core model for establishing security requirements and evaluating controls. See NIST's confidentiality definition and NIST's availability definition.

QUESTION NO: 7

What are the purposes of audit records on an information system? Each correct answer represents a complete solution. Choose two.

A. Troubleshooting

B. Investigation

C. Upgradation

D. Backup

ANSWER: A B

Explanation:

Audit records provide a chronological, attributable record of security-relevant and operational events, such as authentication attempts, privilege use, configuration changes, access to sensitive resources, and system errors. **Troubleshooting** is a core purpose because administrators can correlate logged events, timestamps, and system conditions to identify the source of failures, unexpected behavior, performance issues, or misconfigurations. This evidence supports timely restoration of reliable system operation.

Investigation is also a core purpose because audit data enables security personnel to reconstruct events, establish what occurred and when, identify affected accounts or systems, determine the scope of a suspected incident, and preserve evidence for incident response, forensic analysis, and potential legal or disciplinary processes. To be useful for these activities, audit records must be protected against unauthorized modification or deletion and retained according to organizational requirements. NIST identifies audit and accountability as a control family intended to create, protect, retain, and review audit records, while its incident-response guidance emphasizes collecting and analyzing relevant event data during investigations. See NIST SP 800-53, Audit and Accountability and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 8

Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

A. Determining what level of classification the information requires

B. Running regular backups and routinely testing the validity of the backup data

C. Controlling access, adding and removing privileges for individual users

D. Performing data restoration from the backups when necessary

ANSWER: B C D

Explanation:

A data custodian is responsible for the operational administration and protection of information on behalf of the data owner. This role translates the owner's requirements into day-to-day technical and procedural controls. "Running regular backups and routinely testing the validity of the backup data" is a core custodial duty because availability and recoverability depend on maintaining usable, verified backup copies. "Performing data restoration from the backups when necessary" is likewise an operational recovery activity normally carried out by the personnel or service responsible for maintaining the data environment. "Controlling access, adding and removing privileges for individual users" is also a custodian responsibility when implementing approved access rules: custodians administer access mechanisms and ensure that permissions are applied, changed, and revoked in accordance with authorization decisions and established procedures. These activities support the confidentiality, integrity, and availability objectives assigned to the information. NIST describes information-system security responsibilities as including the implementation and operation of controls, while its contingency-planning guidance emphasizes backup, restoration, and recovery capabilities. See NIST SP 800-12 Rev. 1 and NIST SP 800-34 Rev. 1.

QUESTION NO: 9

Which of the following is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems?

A. IDS

B. OPSEC

C. HIDS

D. NIDS

ANSWER: B

Explanation:

OPSEC (operations security) is the correct answer. OPSEC is a systematic process for protecting sensitive or critical information associated with friendly activities, capabilities, intentions, and vulnerabilities from adversary collection and exploitation. A central part of the process is identifying critical information and analyzing whether observable indicators created by friendly actions could be detected, collected, and interpreted by an adversary's intelligence systems. This allows security leaders to identify exposure before it can be used to undermine a mission, compromise operations, or enable a targeted attack.

In practice, OPSEC follows a structured approach: identify critical information, analyze threats, analyze vulnerabilities, assess risk, and apply countermeasures. For information-security management, this concept extends beyond military operations: public communications, system behavior, personnel activity, procurement information, and physical or technical emissions can all reveal useful indicators to an attacker. Effective OPSEC therefore helps management make informed decisions about reducing unnecessary observability while preserving mission effectiveness. The U.S. Department of Defense defines OPSEC and its process in DoD Directive 5205.02E. Additional operational-security guidance is available from CISA.

QUESTION NO: 10

Electronic communication technology refers to technology devices, such as computers and cell phones, used to facilitate communication. Which of the following is/are a type of electronic communication? Each correct answer represents a complete solution. Choose all that apply.

A. Internet telephony

B. Instant messaging

C. Electronic mail

D. Post-it note

E. Blogs

F. Internet teleconferencing

ANSWER: A B C E F

Explanation:

Internet telephony, instant messaging, electronic mail, blogs, and Internet teleconferencing are all forms of electronic communication because they create, transmit, receive, or publish information through electronic systems and communications networks. Internet telephony carries voice communications through Internet Protocol networks. Instant messaging enables near-real-time exchanges of text and other content between users. Electronic mail transmits digital messages between electronic mail systems and recipients. Blogs are electronic publishing and communication platforms through which an author or organization distributes posts to an online audience, often supporting comments and other interaction. Internet teleconferencing uses networked audio, video, and collaboration capabilities to enable communication among geographically separated participants. From a security-management perspective, these channels can carry business

records, sensitive information, or regulated data; consequently, governance should define acceptable use, retention, monitoring, access control, and protection requirements appropriate to each channel. NIST's glossary describes electronic mail as a system for creating, transmitting, receiving, and storing messages, while its collaboration-security guidance addresses risks and controls for online communication and collaboration tools. See the NIST glossary entry for electronic mail and NIST security considerations for collaboration tools.

QUESTION NO: 11

Which of the following processes is used by remote users to make a secure connection to internal resources after establishing an Internet connection?

A. Packet filtering

B. Tunneling

C. Packet sniffing

D. Spoofing

ANSWER: B

Explanation:

Tunneling is the process used to provide remote users with a secure connection to internal organizational resources over an already-established Internet connection. In a virtual private network, tunneling encapsulates private-network traffic within packets that can traverse the public Internet. The tunnel protects the confidentiality and integrity of traffic in transit through cryptographic controls and authenticates the remote user or device before access to protected internal resources is allowed. Common remote-access VPN technologies use protocols such as IPsec or TLS-based VPNs to establish this protected logical path between a remote endpoint and the organization's VPN gateway. From a security-management perspective, tunneling enables the organization to extend controlled access to authorized remote personnel without exposing internal traffic directly to the Internet. The tunnel endpoint can also enforce centralized policy, including multifactor authentication, authorization restrictions, network segmentation, and session logging. This is the essential mechanism behind secure remote access: the user first obtains ordinary Internet connectivity and then establishes an encrypted, authenticated tunnel into the organization's environment. NIST describes VPNs as creating protected communications over shared or public networks, while CISA identifies VPNs as a means to securely connect remote users to organizational networks. See NIST SP 800-77 Revision 1 and CISA: Understanding VPNs.

QUESTION NO: 12

Which of the following is a name, symbol, or slogan with which a product is identified?

A. Copyright

B. Trademark

C. Trade secret

D. Patent

ANSWER: B

Explanation:

Trademark is correct because a trademark is a form of intellectual-property protection for a source identifier: a word, name, phrase, symbol, design, or combination of these elements that identifies the source of goods or services and distinguishes them from those of other providers. In the question's terms, a product name, its logo or symbol, and a slogan associated with the product can all function as trademarks when they identify the product's commercial origin. This protection is important to security and business managers because trademarks are valuable organizational assets that can be misused through impersonation, counterfeit products, fraudulent domains, and brand spoofing. Appropriate governance includes maintaining an inventory of marks, monitoring unauthorized use, and coordinating legal, marketing, and security responses to brand

abuse. In the United States, the U.S. Patent and Trademark Office explains that trademarks protect words, phrases, symbols, and designs that identify and distinguish the source of goods or services. The International Trademark Association likewise describes trademarks as indicators of source that help consumers recognize goods and services in the marketplace. See the USPTO trademark overview and the International Trademark Association definition.

QUESTION NO: 13

Fill in the blank with an appropriate phrase._____ An is an intensive application of the OPSEC process to an existing operation or activity by a multidiscipline team of experts.

A. OPSEC assessment

ANSWER: A

Explanation:

OPSEC assessment is the appropriate phrase. In operations security terminology, an assessment is a structured, intensive application of the OPSEC process to an operation or activity that already exists. It is performed by a multidisciplinary team so that the activity can be examined from several relevant operational, technical, intelligence, security, and adversary-perspective viewpoints. The team identifies critical information associated with the activity, considers indicators that may reveal that information, evaluates threats and vulnerabilities, and develops practical measures to reduce unacceptable disclosure risk. Because it examines an established activity in depth, an OPSEC assessment supports management decisions about whether current protections adequately prevent an adversary from deriving sensitive information from observable actions or other indicators. This terminology and approach align with the Department of Defense OPSEC program, which directs the use of the OPSEC process to identify and protect critical information and manage risks to operations. See DoD Instruction 5205.02, DoD Operations Security Program and the Office of the Director of National Intelligence analytic standards guidance for authoritative context on disciplined, multidisciplinary analysis.

QUESTION NO: 14

Which of the following policies helps reduce the potential damage from the actions of one person?

A. CSA

B. Risk assessment

C. Separation of duties

D. Internal audit

ANSWER: C

Explanation:

Separation of duties is correct because it is a foundational administrative control that divides sensitive activities, authority, and access among multiple individuals. Rather than permitting one person to initiate, authorize, execute, and conceal a consequential action, the policy assigns distinct parts of that process to different people. This reduces the potential impact of an individual's error, misuse of privilege, fraud, or malicious action, since completing a harmful transaction or change ordinarily requires another person's independent involvement or approval. For example, one employee may request a payment, another may approve it, and a separate person may reconcile the resulting records. Effective separation of duties is based on identifying incompatible duties during business-process and access-control design, then enforcing those restrictions through defined roles, workflow approvals, and periodic access reviews. NIST identifies separation of duties as an access-control principle intended to reduce the risk of malevolent activity without collusion, and the control can be implemented through distinct authorizations and system roles. This directly addresses the question's focus on limiting damage attributable to one person's actions. See NIST CSRC: Separation of Duties and NIST SP 800-53 Rev. 5, AC-5 Separation of Duties.

QUESTION NO: 15

Which of the following Acts enacted in United States amends Civil Rights Act of 1964, providing technical changes affecting the length of time allowed to challenge unlawful seniority provisions, to sue the federal government for discrimination and to bring age discrimination claims?

A. PROTECT Act

B. Sexual Predators Act

C. Civil Rights Act of 1991

D. The USA Patriot Act of 2001

ANSWER: C

Explanation:

The Civil Rights Act of 1991 is correct because it amended core federal employment-discrimination laws, including provisions associated with Title VII of the Civil Rights Act of 1964 and the Age Discrimination in Employment Act. Congress enacted it in response to several Supreme Court decisions and expressly included amendments affecting employment-discrimination litigation. Among its technical and substantive changes, the Act addressed when an unlawful employment practice occurs for purposes of challenging discriminatory seniority systems, thereby clarifying the time in which a claim may be raised. It also expanded available remedies and strengthened enforcement mechanisms for intentional discrimination. The Act further amended the federal-sector provisions of the Age Discrimination in Employment Act, supporting discrimination claims involving federal employment. These changes are why this statute is the appropriate answer: it directly fits the question's combined references to seniority provisions, federal-government discrimination claims, and age-discrimination claims. The official enrolled law is Public Law 102-166, enacted on November 21, 1991. The Equal Employment Opportunity Commission also identifies the Civil Rights Act of 1991 as a major statute governing workplace discrimination and remedies. See Public Law 102-166 and the EEOC Title VII reference.

QUESTION NO: 16

Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

A. Programming and training

B. Evaluation and acceptance

C. Definition

D. Initiation

ANSWER: B

Explanation:

Evaluation and acceptance is the correct SDLC phase because it is the point at which the completed system is formally assessed against the requirements and acceptance criteria established for the project. This includes validating that the system functions as intended, that data processing and conversions are accurate and complete, and that the delivered solution satisfies documented user and business requirements. It also provides the appropriate opportunity to confirm that required security, privacy, operational, and internal control requirements have been implemented and operate as expected before the system receives approval for production use.

From an audit perspective, this phase produces evidence such as test plans and results, user acceptance testing records, control test results, defect-resolution records, and formal business-owner acceptance. These artifacts allow an auditor to determine whether validation was performed, whether identified issues were addressed or formally accepted, and whether the accountable stakeholders authorized implementation. NIST's system development guidance identifies testing, evaluation, and authorization activities as essential before a system is deployed, while NIST's control-assessment guidance emphasizes assessing implemented controls and documenting the resulting evidence. See NIST SP 800-64 Rev. 2 and NIST SP 800-53A Rev. 5.

QUESTION NO: 17

Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

A. Encouraging others to harass the victim

B. False accusations

C. Attempts to gather information about the victim

D. False victimization

ANSWER: B

Explanation:

False accusations is correct because this form of cyberstalking uses knowingly untrue or misleading claims to injure a target's reputation, credibility, relationships, or standing in a community. The stalker may publish allegations through websites, blogs, social-media profiles, review sites, discussion forums, or impersonating pages designed to appear credible. Establishing dedicated online pages is especially consistent with this conduct: it gives the perpetrator a persistent channel for distributing defamatory content, making it searchable, and encouraging third parties to distrust, isolate, or mistreat the victim.

The reputational harm is not limited to a single offensive communication. False accusations can create an ongoing digital record that is repeatedly shared, indexed, copied, or amplified by others, increasing both the victim's exposure and the difficulty of restoring their reputation. This behavior reflects the broader cyberstalking pattern of using electronic communications and online platforms to cause fear, distress, and harm. The FBI identifies cyberstalking as repeated online conduct that can include harassment, threats, and other misuse of digital channels, while NIST recognizes cyberstalking as using electronic communications to stalk or harass an individual. See the FBI's cyberstalking safety guidance and the NIST Cyberstalking Glossary entry.

QUESTION NO: 18

The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement? Each correct answer represents a complete solution. Choose all that apply.

A. Information dissemination policy

B. Electronic monitoring statement

C. Additional personnel security controls

D. Incident response plan

ANSWER: A B C D

Explanation:

Information dissemination policy, Electronic monitoring statement, Additional personnel security controls, and Incident response plan are all appropriate areas to review during post-incident improvement activities. Once containment, evidence transfer, and immediate response responsibilities are complete, the organization should conduct a lessons-learned review to determine what changes will reduce the likelihood, impact, or handling time of future incidents. This review is not limited to technical controls; it also examines governance, personnel practices, communications, monitoring authority, and documented response procedures.

An information dissemination policy should be refined where the incident exposed delays, inappropriate disclosure, unclear escalation paths, or ineffective communication with internal and external stakeholders. An electronic monitoring statement establishes employee and user notice of organizational monitoring, supporting lawful and transparent collection of security-relevant data. Additional personnel security controls may be identified when the event reveals gaps in screening, training, access governance, separation of duties, or insider-threat safeguards. The incident response plan itself must be updated to

incorporate lessons learned, including revised roles, contact information, workflows, playbooks, evidence-handling procedures, and reporting requirements. NIST identifies lessons learned as a core incident-response activity and recommends using findings to improve policies, plans, procedures, and controls. See NIST SP 800-61 Rev. 2 and CISA information sharing guidance.

QUESTION NO: 19

Which of the following issues are addressed by the change control phase in the maintenance phase of the life cycle models? Each correct answer represents a complete solution. Choose all that apply.

A. Performing quality control

B. Recreating and analyzing the problem

C. Developing the changes and corresponding tests

D. Establishing the priorities of requests

ANSWER: A B C

Explanation:

Change control during system maintenance governs the technical evaluation, implementation, verification, and acceptance of authorized modifications to an operational system. **Recreating and analyzing the problem** is a core activity because the change must be based on a confirmed defect, requirement, or operational need, with sufficient analysis to identify the affected components and the appropriate remediation. **Developing the changes and corresponding tests** is also part of controlled maintenance: the approved modification is built using established development practices, and test cases are prepared to demonstrate that the change meets its intended purpose while preserving required functionality and security properties.

Performing quality control is addressed through review, validation, testing, and acceptance activities before a changed configuration is released into production. These controls provide evidence that the implemented change conforms to documented requirements and has been evaluated for defects and unintended operational or security effects. This reflects the ISSMP emphasis on managing secure system life-cycle processes and maintaining governance over changes to production systems. NIST configuration-management guidance likewise identifies impact analysis, implementation, testing, review, and approval as essential configuration-control activities. See the ISC2 ISSMP Exam Outline and NIST SP 800-128, Guide for Security-Focused Configuration Management.

QUESTION NO: 20

Which of the following are examples of administrative controls that involve all levels of employees within an organization and determine which users have access to what resources and information? Each correct answer represents a complete solution. Choose three.

A. Employee registration and accounting

B. Disaster preparedness and recovery plans

C. Network authentication

D. Training and awareness

E. Encryption

ANSWER: A B D

Explanation:

Administrative controls, also called management controls, are the governance, personnel, process, and planning measures through which leadership directs security and employees carry out security responsibilities. **Employee registration and accounting** is an administrative control because organizations use defined personnel and account-management processes

to establish accountability, manage user identities throughout employment, and ensure that access responsibilities are assigned and reviewed. **Disaster preparedness and recovery plans** are administrative controls because they document management-approved responsibilities, recovery priorities, communication arrangements, and procedures for maintaining or restoring operations following disruption. These plans require participation across business and technical functions, rather than functioning as a technical safeguard alone. **Training and awareness** is also administrative because it establishes the workforce knowledge and behavior needed to follow security policy, recognize responsibilities, handle information appropriately, and report security concerns. NIST identifies awareness and training as a management control family and includes contingency planning among organizational control requirements. Its personnel-security guidance also addresses account access and personnel actions as managed lifecycle processes. See NIST SP 800-53 Rev. 5 and NIST SP 800-50.