ISC2 Certified in Cybersecurity

Domain 3:
Access Controls Concepts

Practice Slide (Objective 3.1)

This Slide is a part of Cyber Security for All Project
[https://github.com/CS4A/]

Question 1

A new corporate security mandate requires the implementation of Crime Prevention Through Environmental Design (CPTED) principles for all external building perimeters. The project includes installing numerous floodlights across walkways and deploying high-definition closed-circuit television (CCTV) cameras covering all parking areas.

Which CPTED goal are these two controls primarily supporting?

A. Natural Access Control
B. Natural Territorial Reinforcement
C. Natural Surveillance
D. Natural Detection

Answer 1

C. Natural Surveillance

Detailed Explanation (Correct Answer)

The three established goals of the Crime Prevention Through Environmental Design (CPTED) philosophy are **Natural Surveillance**, Natural Access Control, and Natural Territorial Reinforcement. **Natural Surveillance** involves designing spaces to maximize visibility and observation, making it easier for people to monitor their surroundings. Both **floodlights** (increasing visibility) and **CCTV cameras** (monitoring and recording activity) are core components used to achieve this goal, making it easier to see and monitor threats.

Answer 1 (Incorrect Options)

A. Natural Access Control is incorrect. This principle focuses on regulating and controlling entry to spaces to prevent unauthorized individuals from gaining access, typically achieved using physical barriers like keycard systems, locks, or gates.

B. Natural Territorial Reinforcement is incorrect. This focuses on creating clear boundaries and a sense of ownership, often using physical elements like fences, signs, or landscaping to discourage criminal activity.

D. Natural Detection is incorrect. While it sounds plausible as a security function, **Natural Detection** is not one of the three established goals of the CPTED philosophy listed in the source material.

Question 2

The organization maintains a small server room accessible only by authorized IT personnel during business hours. The server room has a single entry door equipped with an electronic lock connected to the facility's main power supply. Due to safety regulations and the low occupancy, the risk management team decides that the absolute protection of the assets housed inside is the highest priority during a power failure.

Which configuration should be implemented for the electronic lock?

A. The door should be configured to fail-open (fail-safe).
B. The door should be configured to fail-secure (fail-closed).
C. The door should maintain its last state (locked or unlocked).
D. The door should switch to battery-powered biometric authentication.

Answer 2

B. The door should be configured to fail-secure (fail-closed).

Detailed Explanation (Correct Answer)

The door should be configured to **fail-secure** (also known as fail-closed). Fail-secure configuration means that in the event of a power failure, the electronic lock automatically engages, keeping the door locked. Since the scenario states that the server room has **low occupancy** and the team prioritizes the **absolute protection of the assets** (which is typically the goal of security controls), maintaining the security barrier to prevent theft or unauthorized access takes precedence over ensuring immediate human egress.

Answer 2 (Incorrect Options)

A. The door should be configured to fail-open (fail-safe) is incorrect. Fail-open ensures the preservation of human life by unlocking the door during a power failure. While required for high-traffic or essential egress points, the scenario prioritizes asset protection for a low-occupancy room.

C. The door should maintain its last state (locked or unlocked) is incorrect. This introduces unacceptable risk, as the system would not guarantee the required security (locking) or safety (opening) when power is lost.

D. The door should switch to battery-powered biometric authentication is incorrect. This configuration still requires the active function of the locking mechanism and electronics, which is a complexity that should be avoided during a total power failure emergency when rapid, guaranteed state change is needed.

Question 3

A pharmaceutical research company stores all proprietary chemical formulas on high-capacity media tapes in a secure, climate-controlled vault. The policy requires two authorized media custodians to present their separate magnetic access cards simultaneously to the door reader before the vault physically unlocks.

Which specific physical access control mechanism is being enforced?

A. Segregation of Duties (SoD)
B. Two-person control
C. Principle of Least Privilege
D. Two-person integrity

Answer 3

D. Two-person integrity

Detailed Explanation (Correct Answer)

The specific mechanism being enforced is **Two-person integrity**. Two-person integrity requires that **two authorized individuals** be physically present and provide their respective credentials **simultaneously** to gain physical access to a sensitive area, such as the media vault storing valuable information. This is used to increase security for access to valuable items or highly restricted facilities.

Answer 3 (Incorrect Options)

A. Segregation of Duties (SoD) is incorrect. SoD is a **general organizational principle** that requires dividing critical tasks among multiple individuals to prevent fraud or error. While two-person integrity supports SoD, the mechanism described for physical access to a facility is specifically **Two-person integrity**.

B. Two-person control is incorrect. Two-person control is a specific example of the two-person rule used to require two people to perform a **sensitive process or function** (e.g., initiating a large fund transfer), rather than gaining physical access to a facility.

C. Principle of Least Privilege is incorrect. Least Privilege dictates granting users the minimum access necessary for their job. While the custodians likely operate under this principle, it does not mandate the **joint, simultaneous access** requirement described in the scenario.

Question 4

A security manager is developing plans to protect a new data center campus from targeted threats. Recent risk assessments indicate a high likelihood of a vehicle-borne improvised explosive device (VBIED) attack targeting the main pedestrian entrance.

Which single physical control offers the BEST specific mitigation against this identified threat?

A. Perimeter Fencing
B. Mantrap installation
C. High-density Bollards
D. Comprehensive CCTV coverage

Answer 4

C. High-density Bollards

Detailed Explanation (Correct Answer)

Bollards are the best choice for mitigating the risk of a vehicle-borne attack. Bollards are strong, rigid physical controls (pillars or spheres) intentionally placed to prevent vehicles from driving through restricted entrances or damaging a facility. They function as direct **preventive controls** against vehicular intrusion.

Answer 4 (Incorrect Options)

A. Perimeter Fencing is incorrect. While fencing defines the property boundary and deters general unauthorized access, typical fencing is designed to deter human intruders, not stop a vehicle targeting an entrance.

B. Mantrap installation is incorrect. A mantrap (two sequential doors) is designed to control **pedestrian** flow and prevent tailgating/piggybacking. It offers no structural defense against a vehicle.

D. Comprehensive CCTV coverage is incorrect. CCTV is a **detective control** and a form of Natural Surveillance, which monitors and records activity, but it does not physically prevent the vehicle attack itself.

Question 5

A facility access requirement mandates that all employees must present a valid, active access card to the badge reader at the turnstile before proceeding. Furthermore, the security team must review daily logs of all entry and exit attempts for anomalies.

Which category of security control is represented by the *turnstile* and *badge reader*, and which category is represented by the *daily log review*?

A. Administrative and Technical
B. Physical and Technical
C. Physical and Detective
D. Technical and Administrative

Answer 5

C. Physical and Detective

Detailed Explanation (Correct Answer)

The **turnstile and badge reader** are examples of **Physical Controls** because they are tangible barriers and mechanisms implemented to restrict access to physical areas. The turnstile physically restricts passage, and the badge reader manages the physical access mechanism. The **daily log review** is a **Detective Control** because its function is to detect and identify unauthorized actions or incidents (anomalies) *after* they have occurred by scrutinizing recorded events.

Answer 5 (Incorrect Options)

A. Administrative and Technical is incorrect. Administrative controls are policies and procedures. Technical controls are hardware/software implemented through technology (e.g., encryption, firewall). Neither description fits the turnstile/reader nor the review process fully.

B. Physical and Technical is incorrect. The turnstile/reader are physical controls, making the first part correct. However, the daily log review is an *operational process* aimed at *detection*, making **Detective** a better description of its function than **Technical**.

D. Technical and Administrative is incorrect. The turnstile/reader are physical, not technical controls. Log review is detective, not primarily administrative, though the policy requiring the review is administrative.

Question 6

A company installs a new, high-security fence around its server farm perimeter. They also implement clear signage stating, "Authorized Personnel Only. Violators will be prosecuted."

Which CPTED goal is this combination of a barrier (fence) and marking (signage) primarily aimed at reinforcing?

A. Natural Access Control
B. Natural Territorial Reinforcement
C. Natural Surveillance
D. Natural Mitigation

Answer 6

B. Natural Territorial Reinforcement

Detailed Explanation (Correct Answer)

This combination is primarily aimed at **Natural Territorial Reinforcement**. This CPTED goal involves creating clearly defined spaces and boundaries that promote a sense of ownership and responsibility. The **fence** physically defines the boundary, and the **signage** establishes the specific rules for that territory ("Authorized Personnel Only"), clearly marking the property line and establishing ownership.

Answer 6 (Incorrect Options)

A. Natural Access Control is incorrect. While the fence acts as a physical barrier, this principle typically focuses on restricting entry flow through controlled points like locks and card readers. The scenario focuses on defining the *boundary* rather than controlling the *entry point*.

C. Natural Surveillance is incorrect. Surveillance focuses on maximizing visibility, typically through lighting or cameras. Neither the fence nor the sign's primary function is to enhance visibility.

D. Natural Mitigation is incorrect. This is not one of the three recognized goals of the CPTED philosophy (Natural Surveillance, Natural Access Control, and Natural Territorial Reinforcement).

Question 7

A database administrator (DBA) was temporarily assigned to a 90-day contract and issued a temporary physical access badge to the data center. The contract expired 30 days ago, but the DBA's temporary badge has not yet been collected and remains functional. The DBA attempts to enter the data center.

How should the security guard classify the DBA based on the current access status?

A. Authorized Personnel (Expired Contractor Status)
B. Unauthorized Personnel
C. Authorized Personnel (Current Credentials)
D. Authorized Visitor

Answer 7

B. Unauthorized Personnel

Detailed Explanation (Correct Answer)

The DBA should be classified as **Unauthorized Personnel**. Authorized personnel are those specifically granted permission to access a resource. Even though the access card is currently functional, the **contract has expired**, meaning the individual no longer has the legitimate authority or permission to access the facility. The guard's decision must be based on the current authorization status, which has been revoked by the contract expiration.

Answer 7 (Incorrect Options)

A. Authorized Personnel (Expired Contractor Status) is incorrect. Once the contractor status has expired, the person is unauthorized, regardless of their historical role.

C. Authorized Personnel (Current Credentials) is incorrect. Although the card may physically work (a weakness in the revocation process), the DBA is fundamentally unauthorized because the underlying authority (the contract) has expired. Authorization is determined by legitimate right, not just functional credentials.

D. Authorized Visitor is incorrect. The DBA is attempting entry using an expired employee/contractor badge, not a valid visitor pass issued by the organization for the current time.

Question 8

The main entrance to a high-rise corporate headquarters is secured by a set of automated glass doors. In the event of a fire, the local safety code requires that the doors must be instantly and fully unlocked to allow mass rapid egress for all occupants.

Which type of physical security device/configuration is required to meet this life safety mandate?

A. A keyed lock configured to fail-secure.
B. A Smart Lock system utilizing biometric verification.
C. An electronic access control system configured to fail-open.
D. A deadbolt lock with two-person integrity enforced.

Answer 8

C. An electronic access control system configured to fail-open.

Detailed Explanation (Correct Answer)

The required mechanism is an electronic access control system configured to **fail-open** (or fail-safe). This configuration ensures that if power is lost (as often happens during a fire or emergency), the door automatically releases and remains unlocked. When human life is involved, **safety takes precedence over security**, especially at primary egress points, making the fail-open setting mandatory to ensure rapid evacuation.

Answer 8 (Incorrect Options)

A. A keyed lock configured to fail-secure is incorrect. Fail-secure means the door locks upon power loss, trapping occupants, which violates life safety mandates for rapid egress.

B. A Smart Lock system utilizing biometric verification is incorrect. Smart Locks and biometric systems typically rely on power to function. Furthermore, adding biometric verification complicates mass egress, which must be instant during an emergency.

D. A deadbolt lock with two-person integrity enforced is incorrect. A deadbolt lock requires manual unlocking, delaying mass egress. Two-person integrity is relevant for high-security storage access, not emergency exit paths for a large population.

Question 9

A government contractor installs a sophisticated entry system at the entrance to its secure communications facility. The system consists of two sequential doors, where the interlock mechanism only allows one door to open at a time, preventing unauthorized persons from slipping in immediately behind an authorized user.

What security control principle is this system primarily designed to enforce?

A. Two-person integrity
B. Segregation of Duties
C. Preventing tailgating
D. Natural Territorial Reinforcement

Answer 9

C. Preventing tailgating

Detailed Explanation (Correct Answer)

The system described is a **mantrap**, which is a physical access control method involving two interlocked doors. The **primary objective** of a mantrap is **preventing tailgating** (also known as piggybacking), which occurs when an unauthorized individual follows an authorized person into a secure area without presenting their own valid credentials. The sequential door locking mechanism physically enforces single-person entry per authorization.

Answer 9 (Incorrect Options)

A. Two-person integrity is incorrect. Two-person integrity requires *two* authorized people to be present to gain physical access. A mantrap's goal is the opposite: ensuring only *one* authorized person passes through at a time, preventing unauthorized additions (tailgating).

B. Segregation of Duties is incorrect. SoD is an organizational principle dividing critical *processes* to prevent errors or fraud. It does not relate to physical security hardware designed to control pedestrian flow.

D. Natural Territorial Reinforcement is incorrect. This is a CPTED goal focusing on establishing boundaries and ownership via design elements like fences and signs. The mantrap is a specific, active control mechanism for restricting access flow.

Question 10

A facility utilizes Closed-Circuit Television (CCTV) cameras to monitor the access points of the main entrance 24/7. An attacker is deterred from attempting a breach after noticing the prominent presence of these cameras.

While the *function* of the camera is multifaceted, which is the BEST classification of the camera based on its most immediate *impact* on the attacker's decision?

A. Preventive Control
B. Detective Control
C. Compensating Control
D. Deterrent Control

Answer 10

D. Deterrent Control

Detailed Explanation (Correct Answer)

The camera's function in this specific scenario is a **Deterrent Control**. Deterrent controls are implemented to **discourage** potential attackers from violating security policies or attempting unauthorized access. The scenario explicitly states the attacker was **deterred** by the camera's presence, meaning the psychological effect of the visible control prevented the incident from starting.

Answer 10 (Incorrect Options)

A. Preventive Control is incorrect. Preventive controls actively stop an adverse event from happening (e.g., a locked door, a fence). CCTV does not physically stop the breach.

B. Detective Control is incorrect. A detective control aims to **detect and alert** to unauthorized actions *after* they occur (e.g., logging, alarms). While CCTV recording is a prime example of a detective control, the scenario specifies that the attacker noticed the camera and *did not attack*, meaning the function was *deterrence*.

C. Compensating Control is incorrect. Compensating controls provide an alternative method of achieving a security objective when the primary control is infeasible or ineffective. This is not the function described here.

Question 11

A regional office employs a physical security system that uses a combination lock to secure the main media storage closet where sensitive backup tapes are kept. The organizational policy requires that two separate authorized administrators must input their unique, sequential segments of the combination code to open the lock.

This combination of control types exemplifies which two primary access control mechanisms?

A. Physical control and Need to Know
B. Physical control and Two-person integrity
C. Technical control and Segregation of Duties
D. Administrative control and Least Privilege

Answer 11

B. Physical control and Two-person integrity

Detailed Explanation (Correct Answer)

This scenario involves a **Physical Control** and **Two-person integrity**.

1. **Physical Control:** The **combination lock** and the **media storage closet** are tangible assets and barriers, classifying them as physical security measures.
2. **Two-person integrity:** The requirement for two authorized administrators to *jointly* supply the combination to *physically unlock* the asset storage location (the closet) is the precise definition of Two-person integrity.

Answer 11 (Incorrect Options)

A. Physical control and Need to Know is incorrect. While it involves a physical control, the Need to Know principle pertains to restricting data visibility. The policy here focuses on restricting *physical access* using a two-person requirement.

C. Technical control and Segregation of Duties is incorrect. A combination lock is a physical mechanism, not a technical control (which uses technology like software or firewalls). SoD, while related, is a broader organizational policy, whereas Two-person integrity is the specific physical mechanism applied.

D. Administrative control and Least Privilege is incorrect. While the policy requiring the two-person rule is administrative, the lock and closet are physical controls. Least Privilege is about minimum *access rights*, not mandatory joint access.

Question 12

A building manager implements several measures at the entrance of the main lobby, including mandatory sign-in sheets for all visitors and the clear posting of "No Entry" signs prohibiting access past the receptionist desk without escort.

Which core CPTED principle are these administrative/physical measures primarily designed to support?

A. Natural Surveillance
B. Natural Access Control
C. Natural Detection
D. Natural Territorial Reinforcement

Answer 12

B. Natural Access Control

Detailed Explanation (Correct Answer)

These measures primarily support **Natural Access Control**. Natural Access Control focuses on regulating and controlling entry, guiding people along desirable pathways, and limiting opportunities for unauthorized entry. The **mandatory sign-in sheets** and the **receptionist desk** are mechanisms that enforce this control by channeling visitor traffic, tracking entry, and ensuring restrictions (such as escort requirements) are met.

Answer 12 (Incorrect Options)

A. Natural Surveillance is incorrect. Surveillance focuses on increasing visibility (e.g., lighting, CCTV). These controls manage movement, not specifically visibility.

C. Natural Detection is incorrect. This is not one of the three core principles of CPTED listed in the sources.

D. Natural Territorial Reinforcement is incorrect. While the "No Entry" sign suggests territoriality, the combined system's main action is controlling and tracking who enters and where they move (access flow), making Access Control the better fit for the *combined* efforts.

Question 13

The Chief Security Officer (CSO) issues a policy requiring all personnel to display organization-issued photo identification badges while on the premises. This policy is reviewed annually and enforced by security guards.

Which classification of control *type* does the *policy itself* represent?

A. Technical Control
B. Physical Control
C. Logical Control
D. Administrative Control

Answer 13

D. Administrative Control

Detailed Explanation (Correct Answer)

The **policy itself**, which establishes rules and requirements, represents an **Administrative Control**. Administrative controls (also known as managerial controls or soft controls) are management-oriented controls that provide directives and instructions aimed at people within the organization, such as documentation, policies, procedures, and training. The policy mandates *how* security is managed, even though the badge and guard enforcing it are physical controls.

Answer 13 (Incorrect Options)

A. Technical Control is incorrect. Technical controls are implemented via technology like firewalls or encryption.

B. Physical Control is incorrect. Physical controls are the tangible measures, such as the badges or the guards. The policy that dictates the use of these tangible items is administrative.

C. Logical Control is incorrect. Logical controls are digital access controls implemented through software or hardware components (often synonymous with Technical Controls).

Question 14

A security team is determining the appropriate access control measures for a wiring closet, a facility that houses crucial network equipment and data cables. Given that unauthorized manipulation of these systems could lead to widespread network outages, the primary goal is ensuring that only authorized IT staff can enter the space.

Which of the following is the BEST initial physical control decision for this facility?

A. Install a biometric reader system.
B. Implement a robust, keyed door lock.
C. Install extensive interior CCTV surveillance.
D. Apply CPTED principles to the exterior hallway.

Answer 14

B. Implement a robust, keyed door lock.

Detailed Explanation (Correct Answer)

The most essential initial step is to implement a **robust, keyed door lock**. Wiring closets are specifically cited as sensitive facilities requiring access restriction to prevent potential disruptions. A lock is a fundamental **preventive physical control** designed to stop unauthorized access in the first place. This directly addresses the goal of ensuring only authorized IT staff can enter.

Answer 14 (Incorrect Options)

A. Install a biometric reader system is incorrect. While secure, biometrics are typically more expensive and complex than necessary for internal facilities like a wiring closet, which primarily need a reliable physical barrier (a lock).

C. Install extensive interior CCTV surveillance is incorrect. CCTV is a **detective control**. While useful, it detects and records unauthorized activity *after* a breach attempt; it does not prevent the unauthorized manipulation of the cables, which is the threat vector. Prevention is prioritized over detection in this scenario.

D. Apply CPTED principles to the exterior hallway is incorrect. CPTED principles focus on environmental design (surveillance, access flow), which is helpful, but the direct and immediate security measure required for the physical doorway itself is a lock.

Question 15

A museum uses magnetic stripe cards for employee and contractor access to sensitive artifacts storage rooms. The security team has noticed an alarming increase in successful breaches despite the organization maintaining strict key management policies.

Which inherent constraint of magnetic stripe cards is the most likely cause of these security breaches?

A. They are vulnerable to degradation from physical wear and tear.
B. They are easily copied or cloned due to static, unencrypted data storage.
C. They do not support multi-factor authentication requirements.
D. They are susceptible to timing attacks based on data processing speed.

Answer 15

B. They are easily copied or cloned due to static, unencrypted data storage.

Detailed Explanation (Correct Answer)

The primary security constraint of magnetic stripe cards is their susceptibility to being **easily copied or cloned**. Magnetic stripe cards store data in a static, unencrypted format, which makes them highly vulnerable to unauthorized duplication or counterfeiting (skimming). In a scenario where unauthorized access is increasing despite good policy, cloning the access credential is the most likely inherent weakness being exploited.

Answer 15 (Incorrect Options)

A. They are vulnerable to degradation from physical wear and tear is incorrect. While this is a practical limitation affecting *availability* (read errors), it is not the primary **security risk** leading to unauthorized *access* or breaches.

C. They do not support multi-factor authentication requirements is incorrect. While true that a magnetic stripe card is a single factor ("something you have"), this is an architectural limitation, not the specific inherent vulnerability (ease of copying) that is exploited to facilitate unauthorized breaches.

D. They are susceptible to timing attacks based on data processing speed is incorrect. Timing attacks are typically associated with exploiting cryptographic systems through variations in software execution time. Magnetic stripe cards are simple data storage mechanisms and not primary targets for this kind of advanced attack.

Question 16

A manager is tasked with determining whether to deploy expensive biometric scanners on all office doors or restrict them only to doors leading to high-value evidence storage rooms and media closets.

Which factor should the manager prioritize when making this deployment decision?

A. The organizational budget and cost-effectiveness of the scanners.
B. The recommendation of the hardware vendor regarding compatibility.
C. The sensitivity and security requirements of the areas behind the doors.
D. The total number of employees requiring access credentials.

Answer 16

C. The sensitivity and security requirements of the areas behind the doors.

Detailed Explanation (Correct Answer)

The deployment decision for high-cost security measures like biometric scanners must prioritize **the sensitivity and security requirements of the areas behind the doors**. Security controls are selected and implemented based on the results of security governance and **risk management activities**. Using a **site assessment** to evaluate specific security needs and the sensitivity of assets (evidence rooms, media closets) determines where high-level protection is most needed.

Answer 16 (Incorrect Options)

A. The organizational budget and cost-effectiveness of the scanners is incorrect. While cost is a major consideration in balancing risk management, the prioritization should first be based on *need* (asset sensitivity) before costs are analyzed to determine the correct security solution.

B. The recommendation of the hardware vendor regarding compatibility is incorrect. Vendor recommendations relate to implementation efficiency, not the fundamental security requirements for the facility itself.

D. The total number of employees requiring access credentials is incorrect. The number of users affects operational convenience but does not dictate the *risk level* or the necessity of deploying a specific high-security measure like biometrics to protect a sensitive asset.

Question 17

The physical security plan for a remote corporate warehouse requires the following combination of controls: a chain-link fence defining the perimeter, a security guard patrolling the grounds, and a system of warning signs posted every fifty feet.

Which functional classification of security control is *not* represented in this combination?

A. Deterrent Control
B. Detective Control
C. Physical Control
D. Preventive Control

Answer 17

B. Detective Control

Detailed Explanation (Correct Answer)

The combination of controls **does not include a Detective Control**.

- **Preventive/Physical:** The **fence** and the **security guard** act as physical barriers/personnel designed to stop an adverse event (unauthorized entry) from happening, classifying them as Preventive and Physical controls.
- **Deterrent:** The **warning signs** are designed to discourage attackers, classifying them as Deterrent controls.

A **Detective Control** (such as CCTV, alarms, or motion sensors) is required to detect an intrusion *after* it occurs or to monitor for anomalies, and none of the listed items perform this specific function.

Answer 17 (Incorrect Options)

A. Deterrent Control is incorrect. The **warning signs** are designed to discourage violation, fulfilling the role of a deterrent control.

C. Physical Control is incorrect. The **fence** and the **security guard** are tangible measures or personnel enforcing security, making them physical controls.

D. Preventive Control is incorrect. The **fence** and the **security guard** actively stop unauthorized entry, fulfilling the role of a preventive control.

Question 18

An organization is decommissioning a hard drive from its evidence storage room that contains highly sensitive data and plans to use the drive for unclassified testing purposes afterward. Organizational policy requires the most secure method for rendering data irreversibly unreadable while retaining the potential usability of the physical media.

Which data destruction method should the team employ?

A. Physical Destruction
B. Degaussing
C. Disk Zeroing/Overwriting
D. Encryption

Answer 18

C. Disk Zeroing/Overwriting

Detailed Explanation (Correct Answer)

The recommended method is **Disk Zeroing/Overwriting**. This process involves writing binary zeroes (or other random data) multiple times across the entire disk surface. This method is considered a secure data destruction method because it renders the original data unreadable and unrecoverable, fulfilling the irreversible erasure requirement, while **retaining the potential usability of the hard drive for future use**.

Answer 18 (Incorrect Options)

A. Physical Destruction is incorrect. Physical destruction (e.g., shredding or melting) is the **most secure** method for irreversible data erasure. However, it entirely eliminates the possibility of reusing the media, violating the stated requirement.

B. Degaussing is incorrect. Degaussing involves exposing the media to a strong magnetic field to disrupt the magnetic particles. While it renders data unreadable, it often makes the storage media (especially hard drives) unusable for its original purpose, preventing reuse.

D. Encryption is incorrect. Encryption transforms data into an unreadable format. While effective for protecting data, it is a **preventive control** that relies on key management. If the key is compromised, the data is recoverable, meaning encryption does not meet the requirement for **irreversible erasure**.

Question 19

Due to recent natural disaster threats, an organization is redesigning the egress paths within its secured facilities. The new design mandate states that any locked physical door along an emergency evacuation route must unlock and stay unlocked when the fire alarm is triggered, even if primary power is lost.

This mandate primarily enforces the principle of:

A. Fail-secure access control.
B. Natural Access Control.
C. Fail-open access control.
D. Two-person control.

Answer 19

C. Fail-open access control.

Detailed Explanation (Correct Answer)

This mandate enforces the principle of **Fail-open access control** (also known as fail-safe). This configuration ensures that during a disaster, such as a fire alarm triggering a power disruption, the physical door mechanism automatically releases and stays unlocked. This configuration is mandated for emergency evacuation routes where the **preservation of human life must be the number-one priority** over asset security.

Answer 19 (Incorrect Options)

A. Fail-secure access control is incorrect. Fail-secure means the door automatically locks if power is lost. This would trap personnel in an emergency, violating safety protocols.

B. Natural Access Control is incorrect. Natural Access Control is a CPTED principle focusing on guiding and restricting the flow of people using environmental design. The mandate concerns the fail state of the locking mechanism during a catastrophe, not the normal flow control.

D. Two-person control is incorrect. Two-person control requires two individuals to execute a sensitive *process*. It is unrelated to the failure state of a locking mechanism during an emergency.

Question 20

A server room utilizes a perimeter security alarm system consisting of vibration sensors and magnetic contacts on all windows and doors. The system is designed to notify the security guard station immediately upon detecting unauthorized entry.

Based on its function, the alarm system is classified as which primary type of security control?

A. Preventive Control
B. Compensating Control
C. Deterrent Control
D. Detective Control

Answer 20

D. Detective Control

Detailed Explanation (Correct Answer)

The alarm system is classified as a **Detective Control**. Detective controls are designed to **identify and alert** security personnel or systems to unauthorized actions or security incidents **after they have occurred**. The vibration sensors and magnetic contacts detect the unauthorized attempt (entry or tampering) and then trigger the alert function.

Answer 20 (Incorrect Options)

A. Preventive Control is incorrect. Preventive controls actively stop an adverse event from happening (e.g., a locked door, a fence). The alarm system only senses and reports the entry; it does not stop it.

B. Compensating Control is incorrect. Compensating controls provide an alternative means to meet a requirement when the primary control is not feasible. This is a core control, not a compensating one.

C. Deterrent Control is incorrect. Deterrent controls discourage attackers (e.g., warning signs, visible lighting). While the visible presence of the alarm sensors might deter, the system's primary *function* is detection and alerting.