ISC2 Certified in Cybersecurity

Domain 3:
Access Controls Concepts

Practice Slide

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

Question 1

The new Research and Development (R&D) department policy mandates that any researcher who creates a new proprietary design file is automatically designated as the file's owner and is granted the sole authority to grant read, write, or delete permissions to any other colleague, regardless of their departmental role.

Which Access Control Model is being implemented based on this design?

A. Mandatory Access Control (MAC)
B. Role-Based Access Control (RBAC)
C. Discretionary Access Control (DAC)
D. Attribute-Based Access Control (ABAC)

Answer 1

C. Discretionary Access Control (DAC)

Detailed Explanation (Correct Answer)

The scenario illustrates **Discretionary Access Control (DAC)**. In a DAC model, the **owner of the object (resource)**—in this case, the researcher who created the proprietary design file—has the **discretion** to assign permissions to other subjects. The R&D policy directly states the researcher/owner has the *sole authority* to grant permissions, which is the defining characteristic of DAC. This model focuses on user identity and owner control over specific resources.

Answer 1 (Incorrect Options)

A. Mandatory Access Control (MAC) is incorrect. MAC enforces access decisions based on **predefined security labels or classifications** assigned by a central authority or the system, not the resource owner. The user has no control over permissions in MAC.

B. Role-Based Access Control (RBAC) is incorrect. RBAC grants permissions based on a user's **role** (e.g., "Researcher," "Engineer") within the organization, which is centrally managed by an administrator, not the individual file owner.

D. Attribute-Based Access Control (ABAC) is incorrect. ABAC uses **intricate rules** based on various attributes (user, resource, environment) to determine access. While it's an advanced model, the scenario specifies that access is dictated solely by the owner's discretion, which is DAC.

Question 2

A financial institution employs two separate administrators for processing fund transfers: Administrator A initiates the transfer request in System X, and Administrator B must independently approve the final transaction in System Y. Neither administrator has the privileges to perform both actions.

What fundamental access control principle is this organization primarily enforcing to maintain data integrity and prevent fraud?

A. Principle of Least Privilege
B. Two-person control
C. Separation of Duties (SoD)
D. Need to Know

Answer 2

C. Separation of Duties (SoD)

Detailed Explanation (Correct Answer)

The principle being enforced is **Separation of Duties (SoD)** (also called Segregation of Duties). SoD involves dividing tasks and responsibilities among multiple individuals or roles to prevent any single person from having the ability to perform all aspects of a critical or sensitive function. In this case, dividing the critical task of a financial transfer into initiation (Admin A) and approval (Admin B) reduces the risk of error or fraud, specifically targeting the maintenance of **Data Integrity**.

Answer 2 (Incorrect Options)

A. Principle of Least Privilege is incorrect. While both administrators operate under least privilege (they only have the minimum access needed for their job), Least Privilege focuses on restricting the scope of access for a single user. SoD focuses on dividing a high-risk *task* across *multiple* users.

B. Two-person control is incorrect. Two-person control is a **specific example** of SoD (requiring two individuals to perform a sensitive process). While the concept applies, **Separation of Duties** is the broader *fundamental access control principle* being applied to prevent errors or fraud.

D. Need to Know is incorrect. The Need to Know principle is closely related to Least Privilege and pertains to the disclosure of information—only providing access to information that is specifically required for the job. While applicable, it is not the primary mechanism described here for enforcing the transactional integrity of the fund transfer process.

Question 3

A security team is debating the door configuration for the main entry/exit to a restricted server room, which houses high-value assets and is staffed 24/7. In the event of a total power failure (e.g., due to a fire), the local safety regulations require that personnel must be able to quickly evacuate.

Which configuration is the most appropriate for the door-locking mechanism in this specific scenario?

A. The door should be configured to fail-secure.
B. The door should be configured to fail-open.
C. The door should maintain its current state (locked or unlocked).
D. The door should switch to a biometric access mechanism.

Answer 3

B. The door should be configured to fail-open.

Detailed Explanation (Correct Answer)

The most appropriate configuration is **fail-open**. This means that if the power fails, the door-locking mechanism automatically releases, allowing free egress. Although server rooms contain high-value assets (implying a preference for fail-secure to maintain confidentiality), life safety regulations require that personnel—especially in a room that is staffed 24/7 and serves as the *only* entry/exit—must be able to evacuate quickly in an emergency like a fire. **Life safety takes precedence over asset security**.

Answer 3 (Incorrect Options)

A. The door should be configured to fail-secure is incorrect. Fail-secure means the door remains locked if power is lost, protecting the assets. However, this configuration would trap the personnel inside the server room in case of a fire or power outage, violating safety regulations and potentially endangering lives.

C. The door should maintain its current state (locked or unlocked) is incorrect. Relying on the current state during a catastrophic failure (like a fire leading to a power loss) is unreliable and does not guarantee the necessary action (opening) for immediate evacuation.

D. The door should switch to a biometric access mechanism is incorrect. Biometric mechanisms require power to function, meaning they would also fail in a total power outage scenario. This solution is technically infeasible for resolving the core problem described in the scenario.

Question 4

A high-security data center entrance is equipped with two sequential doors, where the first door must fully close and lock before the second door can be unlocked. This design is reinforced by a detection system that checks if more than one person attempts to pass between the two doors simultaneously.

Which physical security measure does this configuration primarily employ, and what is its main objective?

A. Bollard; To prevent unauthorized vehicle entry.
B. Turnstile; To restrict access based on time of day.
C. Mantrap; To prevent tailgating.
D. Biometric Lock; To enforce the two-person rule.

Answer 4

C. Mantrap; To prevent tailgating.

Detailed Explanation (Correct Answer)

The described configuration is a **mantrap**. A mantrap is a physical barrier system involving two sequential doors designed to control access to highly restricted areas. Their **primary objective is preventing tailgating** (or "piggybacking"), where an unauthorized individual follows closely behind an authorized person to gain entry without proper credentials. The system ensures only one person enters per authorization event.

Answer 4 (Incorrect Options)

A. Bollard; To prevent unauthorized vehicle entry is incorrect. **Bollards** are pillars or spheres used to prevent unauthorized vehicle access, typically outside a building. The scenario involves controlling human entry through sequential doors, not vehicle traffic.

B. Turnstile; To restrict access based on time of day is incorrect. **Turnstiles** are simple rotating physical barriers often used for one-way traffic. While they restrict access, they are less secure and easier to jump over. The configuration described (two sequential doors) is a mantrap.

D. Biometric Lock; To enforce the two-person rule is incorrect. While the system detects multiple people, the mechanism described is a mantrap. The **two-person rule** (specifically, **two-person integrity** in a physical context) requires two authorized individuals to *simultaneously* present credentials for access. The mantrap prevents unauthorized access after the first authorized person enters.

Question 5

In a military installation, access to intelligence documents is strictly based on whether the accessing individual possesses the required "Top Secret" security clearance label, and whether the document itself carries the corresponding "Top Secret" classification label. Access cannot be modified by the document owner or system administrator.

Which Access Control Model does this environment rely on, and what is its primary shortcoming?

A. Discretionary Access Control (DAC); Users might grant too much access.
B. Role-Based Access Control (RBAC); Roles may become complex to manage.
C. Mandatory Access Control (MAC); It can be too rigid and inflexible.
D. Attribute-Based Access Control (ABAC); It is computationally expensive.

Answer 5

C. Mandatory Access Control (MAC); It can be too rigid and inflexible.

Detailed Explanation (Correct Answer)

The system relies on **Mandatory Access Control (MAC)**, where access is determined by security classifications (labels) enforced by the system. MAC is characterized by its strict, predefined rules that cannot be overwritten by the user or resource owner. The primary shortcoming of MAC is that **it can be too rigid and inflexible**. This rigidity makes it difficult to adjust or customize access quickly to accommodate dynamic environments or evolving user needs, often hindering collaboration.

Answer 5 (Incorrect Options)

A. Discretionary Access Control (DAC); Users might grant too much access is incorrect. The scenario describes MAC, not DAC. DAC's shortcoming is indeed that owners may grant excessive privileges, leading to "privilege creep".

B. Role-Based Access Control (RBAC); Roles may become complex to manage is incorrect. The scenario describes MAC, not RBAC. RBAC uses roles based on job functions. A potential drawback of RBAC is role proliferation, but the model itself is designed to simplify management compared to DAC.

D. Attribute-Based Access Control (ABAC); It is computationally expensive is incorrect. The scenario describes MAC, not ABAC. While ABAC (access based on attributes) can be complex and computationally intensive, that is not the primary drawback of the MAC model described here.

Question 6

A newly hired Data Analyst requires access to the company's customer relationship management (CRM) database to run weekly sales reports. However, the analyst's role does not involve modifying, deleting, or exporting raw customer records. The security administrator configures the analyst's account with 'Read Only' permissions for the reporting tool interface.

Which security principle is the administrator most strictly adhering to in this provisioning scenario?

A. Need to Know
B. Separation of Duties
C. Principle of Least Privilege
D. Defense in Depth

Answer 6

C. Principle of Least Privilege

Detailed Explanation (Correct Answer)

The security administrator is strictly adhering to the **Principle of Least Privilege**. This principle dictates that a subject (the analyst) should only be granted the **minimum level of access or permissions necessary** to perform their job functions. By granting only 'Read Only' access, the administrator prevents the analyst from executing any actions (modification, deletion, or export) that are outside the scope of running reports.

Answer 6 (Incorrect Options)

A. Need to Know is incorrect. While related, the Need to Know principle pertains more specifically to the **disclosure of information**. In this context, both Least Privilege (restricting permissions) and Need to Know (restricting data sets) apply, but restricting the *level of privilege* (Read Only) is the most direct application of Least Privilege.

B. Separation of Duties is incorrect. SoD focuses on distributing tasks among multiple individuals to prevent fraud or error. The scenario involves setting the access level for a *single* user performing *one* role, which does not require task division.

D. Defense in Depth is incorrect. Defense in Depth is an information security strategy that involves deploying **multiple layers of security measures** to protect information systems. While this action is part of an overall security strategy, it is an instance of a single access control principle, not the overarching multi-layered strategy itself.

Question 7

An organization is reviewing its physical security measures by utilizing the Crime Prevention Through Environmental Design (CPTED) philosophy. The team proposes implementing the following concepts: using well-placed lighting, clearly marking property lines with fences, and requiring keycard entry at all doors.

Which of the following is NOT one of the primary goals of the CPTED philosophy being utilized in this review?

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

Answer 7

C. Natural Detection

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 Detection** is not one of the CPTED goals. CPTED focuses on using architectural and landscaping design to deter crime and control access *proactively*.

Answer 7 (Incorrect Options)

A. Natural Access Control is incorrect. This is a core CPTED goal, achieved in the scenario by requiring **keycard entry** (restricting entry flow).

B. Natural Surveillance is incorrect. This is a core CPTED goal, achieved in the scenario by using **well-placed lighting** (increasing visibility).

D. Natural Territorial Reinforcement is incorrect. This is a core CPTED goal, achieved in the scenario by **clearly marking property lines with fences** (establishing ownership and boundaries).

Question 8

A security guard stops an individual attempting to enter a secure perimeter fence line. The individual states they are a terminated employee whose access card expired last week but insists they need to retrieve personal items from their former locker. The guard confirms the access card is expired.

How should the guard classify the individual according to standard Access Control Concepts?

A. Authorized Personnel (Visitor Status)
B. Unauthorized Personnel
C. Authorized Personnel (Expired Credentials)
D. Incident Responder

Answer 8

B. Unauthorized Personnel

Detailed Explanation (Correct Answer)

The individual should be classified as **Unauthorized Personnel**. Unauthorized personnel are individuals who do not possess the legitimate authority or permission to access certain areas or information within an organization. The fact that the employee was **terminated** and their access card is **expired** confirms they no longer have the right to access the premises or resources.

Answer 8 (Incorrect Options)

A. Authorized Personnel (Visitor Status) is incorrect. A visitor is considered authorized only if they have been provided a **valid visitor pass**. This individual has an expired employee badge and no valid visitor authorization.

C. Authorized Personnel (Expired Credentials) is incorrect. The expiration of the access card and the termination status mean they are no longer authorized to be on the premises. Current, active credentials are required for authorization.

D. Incident Responder is incorrect. An Incident Responder is a role defined for managing and mitigating security incidents. This term does not describe the individual attempting entry.

Question 9

The IT department is tasked with hardening the database server. A senior engineer creates a list of specific users and groups permitted to connect to the database application from the application server, along with their assigned permissions (Read/Write).

Which technical access control mechanism is the engineer implementing?

A. Acceptable Use Policy (AUP)
B. Intrusion Detection System (IDS)
C. Access Control List (ACL)
D. Security Awareness Training

Answer 9

C. Access Control List (ACL)

Detailed Explanation (Correct Answer)

The engineer is implementing an **Access Control List (ACL)**. An ACL is a **technical control** used to define who can access specific resources (the database application) and what permissions they have (Read/Write). ACLs are lists of permissions attached to an object that specify which subjects (users or system processes) are granted or denied access.

Answer 9 (Incorrect Options)

A. Acceptable Use Policy (AUP) is incorrect. An AUP is an **administrative control** that outlines acceptable behaviors when using IT resources. It does not technically enforce the permissions list described.

B. Intrusion Detection System (IDS) is incorrect. An IDS is a **detective control** designed to monitor network or system activity for malicious behavior and generate alerts. It is not used to define or enforce specific access permissions.

D. Security Awareness Training is incorrect. This is an **administrative control** (specifically, an operational control) focused on educating employees about security practices. It is not a technical enforcement mechanism.

Question 10

A collaborative design firm utilizes a Discretionary Access Control (DAC) model where project managers (resource owners) frequently grant broad 'Full Control' permissions to various external vendors to expedite work sharing. This often results in vendors retaining excessive access long after their specific project tasks are complete.

Which inherent limitation of DAC is best exemplified by this ongoing situation?

A. Rigid enforcement rules hindering necessary resource sharing.
B. Reliance on centralized security labels enforced by the system.
C. High administrative overhead for access provisioning.
D. The risk of users having too much access to resources.

Answer 10

D. The risk of users having too much access to resources.

Detailed Explanation (Correct Answer)

The scenario highlights the intrinsic flaw of **Discretionary Access Control (DAC)**: access decisions are decentralized and rely on the discretion of the resource owner. When owners prioritize convenience (expediting work) by granting **broad, excessive permissions** ("Full Control") that persist past necessity, it directly creates the high risk of **privilege creep**—users retaining access they no longer require. This is the most common limitation of DAC.

Answer 10 (Incorrect Options)

A. Rigid enforcement rules hindering necessary resource sharing is incorrect. This statement describes a primary shortcoming of **Mandatory Access Control (MAC)**, which is designed to be rigid. DAC is known for its *flexibility*.

B. Reliance on centralized security labels enforced by the system is incorrect. This is the defining characteristic of **Mandatory Access Control (MAC)**. DAC is characterized by *decentralized* control by the resource owner.

C. High administrative overhead for access provisioning is incorrect. While DAC can involve managing many individual permissions, **Role-Based Access Control (RBAC)** is often implemented specifically to *reduce* administrative overhead by grouping users into roles. DAC's main flaw is the **quality** of the access granted (too much), not necessarily just the quantity of administrative work.

Question 11

An organization uses Role-Based Access Control (RBAC) to manage access. A temporary contractor is hired for a 60-day project that requires access to sensitive HR data. The security team creates a new role, "Temp-HR-Auditor," with specific, time-limited permissions to the necessary data tables.

Which core characteristic of RBAC simplifies the secure provisioning and management for this temporary user?

A. Access is granted based on the user's discretion.
B. Access is inherited from centralized security classification labels.
C. Permissions are assigned to the role, not the individual user.
D. Access decisions are derived from real-time environmental attributes.

Answer 11

C. Permissions are assigned to the role, not the individual user.

Detailed Explanation (Correct Answer)

The core characteristic of **Role-Based Access Control (RBAC)** that simplifies this process is that **permissions are assigned to the role**, and users are then assigned to that role. By defining a specific "Temp-HR-Auditor" role with pre-configured, limited, and time-bound permissions, the administrator can efficiently assign access to the contractor and easily **revoke** that access simply by deleting the user's assignment to the role when the contract ends. This simplifies management and enhances security.

Answer 11 (Incorrect Options)

A. Access is granted based on the user's discretion is incorrect. This describes **Discretionary Access Control (DAC)**.

B. Access is inherited from centralized security classification labels is incorrect. This describes **Mandatory Access Control (MAC)**.

D. Access decisions are derived from real-time environmental attributes is incorrect. This describes **Attribute-Based Access Control (ABAC)**, which uses dynamic context (like time or location) for access decisions. RBAC is based on the static definition of the user's role/job function.

Question 12

A security manager is assessing various physical controls implemented across the corporate campus. The manager notes that perimeter fencing, card readers at every office door, and reinforced glass on ground-floor windows are currently deployed.

Which category of security controls do these three examples primarily represent based on their function?

A. Detective Controls
B. Corrective Controls
C. Deterrent Controls
D. Preventive Controls

Answer 12

D. Preventive Controls

Detailed Explanation (Correct Answer)

All three examples (perimeter fencing, card readers/locks, reinforced glass) are fundamentally **Preventive Controls**. Preventive controls are implemented to **prevent or stop an adverse event or incident** from happening in the first place. Fencing creates a physical barrier to unauthorized access, and card readers (locks) stop unauthorized entry until verified, serving as proactive security measures.

Answer 12 (Incorrect Options)

A. Detective Controls is incorrect. Detective controls aim to **detect and alert** to unauthorized actions after they occur, such as CCTV cameras, motion sensors, or intrusion detection systems (IDS).

B. Corrective Controls is incorrect. Corrective controls are implemented to **correct or mitigate the effects** of a detected incident. Examples include restoring a backup or applying a software patch.

C. Deterrent Controls is incorrect. Deterrent controls aim to **discourage potential attackers** (e.g., security lighting or warning signs). While physical barriers also deter, their *primary function* is to physically prevent entry, making "Preventive" the best functional classification.

Question 13

A highly sensitive server rack containing encryption keys is secured by a combination lock. Organizational policy dictates that two authorized custodians must simultaneously input their respective segments of the combination code to physically unlock the cage.

This practice is the textbook definition of which access control concept?

A. Principle of Least Privilege
B. Two-person integrity
C. Segregation of Duties
D. Dual-factor authentication

Answer 13

B. Two-person integrity

Detailed Explanation (Correct Answer)

The scenario describes **Two-person integrity**. This is a specific application of the broader two-person rule that focuses on **physical access**. It requires **two authorized individuals** to simultaneously present credentials or input required information to gain physical access to a sensitive location (the server rack/cage). This ensures that neither individual can access the resource alone.

Answer 13 (Incorrect Options)

A. Principle of Least Privilege is incorrect. Least Privilege dictates that users have the minimum permissions required for their job. While the custodians likely operate under Least Privilege, this concept does not specifically mandate joint, simultaneous access.

C. Segregation of Duties (SoD) is incorrect. SoD is the broader **organizational principle** of dividing critical tasks to prevent fraud. While Two-person integrity *supports* SoD, the textbook concept for requiring joint physical access to a location is Two-person integrity.

D. Dual-factor authentication is incorrect. Dual-factor authentication uses two *different types* of authentication factors (e.g., something you know + something you have). The scenario involves two separate *people* providing their necessary credentials (something they know) to meet a two-person requirement.

Question 14

A new internal security policy requires that the staff member responsible for updating the operating system on critical production servers (Patch Engineer) cannot also be the staff member who manages the server's local administrative user accounts (Account Manager).

Which access control principle does this policy primarily enforce?

A. Defense in Depth
B. Principle of Least Privilege
C. Job Rotation
D. Segregation of Duties

Answer 14

D. Segregation of Duties

Detailed Explanation (Correct Answer)

This policy enforces **Segregation of Duties (SoD)** (or Separation of Duties). SoD requires dividing critical responsibilities among different individuals. By preventing the Patch Engineer (who controls system modification) from also being the Account Manager (who controls who has privileges on the system), the organization creates a necessary check and balance. This prevents a single individual from performing a malicious patch (or installing a rootkit) and then also covering their tracks by manipulating the audit trail through account management functions.

Answer 14 (Incorrect Options)

A. Defense in Depth is incorrect. Defense in Depth is the strategy of using multiple layers of security. SoD is just one component or principle within a larger defense-in-depth strategy.

B. Principle of Least Privilege is incorrect. Least Privilege focuses on giving an individual the minimum permissions needed to perform *their* single task. SoD focuses on distributing *tasks* among *multiple* individuals.

C. Job Rotation is incorrect. Job Rotation is a practice where employees periodically switch roles. While it can help detect fraud over time, it is an **administrative practice** aimed at providing cross-training and detection. SoD is a foundational **access control principle** enforced through system configuration to prevent concurrent conflicts of interest.

Question 15

During a site assessment for a secured facility, the security team identifies a high risk of unauthorized entry via vehicle intrusion, specifically targeting the main pedestrian entrance during peak traffic hours.

Which physical security control would be the BEST option to mitigate this specific risk?

A. Perimeter Fencing
B. Bollards
C. Man-trap
D. Security Lighting

Answer 15

B. Bollards

Detailed Explanation (Correct Answer)

Bollards are the **best option** to mitigate the specific risk of vehicle intrusion. Bollards are strong, rigid physical controls (pillars or spheres made of hard material) intentionally positioned to prevent vehicles from driving through pedestrian areas or building entrances. They act as a powerful preventive control against unauthorized vehicular access.

Answer 15 (Incorrect Options)

A. Perimeter Fencing is incorrect. Fencing defines the boundary of a property and deters general unauthorized access. While some specialized fences can stop vehicles, typical perimeter fencing is designed to stop people, not a high-speed vehicle targeting a building entrance.

C. Man-trap is incorrect. A mantrap (sequential dual doors) is designed to control **pedestrian** flow and prevent tailgating. It provides no defense against a vehicle intrusion.

D. Security Lighting is incorrect. Security lighting is a **deterrent control** (part of CPTED). It increases visibility but does nothing to physically stop a vehicle from crashing through the entrance.

Question 16

A manager terminates an employee and immediately requests the system administrator to check the employee’s account access across all organizational systems to ensure all privileges have been revoked and no unnecessary rights remain.

Which logical access control process step is the manager initiating, and what is its goal?

A. Provisioning; Setting up initial access rights.
B. Account Review; Verifying privileges align with responsibilities.
C. Authorization; Granting permissions based on role.
D. Account Revocation; Disabling or deleting the account.

Answer 16

B. Account Review; Verifying privileges align with responsibilities.

Detailed Explanation (Correct Answer)

The manager is initiating an **Account Review** (or privilege review). This process involves periodically assessing and validating the access privileges assigned to employees based on their roles and responsibilities. In this termination scenario, the review ensures that the principle of least privilege is maintained by verifying that **all privileges are removed** (or aligned with the user's current status, which is inactive). Account reviews are critical to preventing **privilege creep**.

Answer 16 (Incorrect Options)

A. Provisioning; Setting up initial access rights is incorrect. Provisioning is the process of setting up initial access when a new user joins or changes roles. This is a *post-termination* cleanup activity.

C. Authorization; Granting permissions based on role is incorrect. Authorization is the step where the system grants permission for a requested action. The manager is initiating an *audit* of existing authorizations.

D. Account Revocation; Disabling or deleting the account is incorrect. Revocation is the *action* of removing access rights. The manager is initiating the *review process* to confirm the revocation of all associated privileges. Revocation is the outcome, Review is the process described.

Question 17

The IT department manages a highly flexible project repository where the creator of any document can instantaneously share, revoke, or change access permissions for any other internal user, simply by clicking a button next to the document. The system prioritizes immediate user convenience over strict centralized control.

Which access control model is the IT department implicitly supporting with this system architecture?

A. Mandatory Access Control (MAC)
B. Role-Based Access Control (RBAC)
C. Rule-Based Access Control (RuBAC)
D. Discretionary Access Control (DAC)

Answer 17

D. Discretionary Access Control (DAC)

Detailed Explanation (Correct Answer)

The system architecture implicitly supports **Discretionary Access Control (DAC)**. DAC grants the **owner or creator** of a resource the **discretion** to grant or deny access to other users. The "immediate user convenience" and the ability of the creator to *instantaneously* manage permissions are hallmarks of DAC systems. This model is typically found in environments where flexibility and resource sharing are prioritized over stringent security classifications.

Answer 17 (Incorrect Options)

A. Mandatory Access Control (MAC) is incorrect. MAC prohibits the resource owner from modifying access; decisions are based on central classification labels enforced by the system.

B. Role-Based Access Control (RBAC) is incorrect. RBAC permissions are centrally administered based on predefined organizational roles. Access changes are not determined by the individual user's *discretion* over the file.

C. Rule-Based Access Control (RuBAC) is incorrect. Rule-Based Access Control uses specific, predefined conditions (often related to attributes or policies) to grant access. While any DAC system uses rules, the core mechanism here is the **discretionary authority of the owner**, making DAC the most specific answer.

Question 18

A security team discovers that several employee accounts were compromised after attackers successfully used stolen login credentials harvested through a phishing campaign. The team decides to implement a defense mechanism specifically to neutralize the effectiveness of such stolen passwords in the future.

Which access control mechanism is the most effective preventative control against the use of stolen credentials?

A. Implementing an Access Control List (ACL).
B. Deploying biometric scanners.
C. Enforcing Multi-Factor Authentication (MFA).
D. Installing an Intrusion Detection System (IDS).

Answer 18

C. Enforcing Multi-Factor Authentication (MFA).

Detailed Explanation (Correct Answer)

Multi-Factor Authentication (MFA) is the most effective preventative control against the use of stolen credentials. MFA requires a user to provide two or more different authentication factors (e.g., something you know and something you have). If an attacker steals only the password (something you know), they still lack the second factor (e.g., the code from a mobile device), significantly reducing the risk of account compromise.

Answer 18 (Incorrect Options)

A. Implementing an Access Control List (ACL) is incorrect. An ACL is a list defining who can access what resource. While important for authorization, an ACL cannot prevent a successful login attempt by someone using legitimate (but stolen) credentials.

B. Deploying biometric scanners is incorrect. Biometric authentication (something you are) is a form of authentication factor. While strong, replacing passwords with biometrics (Single-Factor) still relies on one unique factor. MFA (combining factors) provides a higher degree of defense than a single biometric factor alone.

D. Installing an Intrusion Detection System (IDS) is incorrect. An IDS is a **detective control** that alerts administrators *after* suspicious activity occurs. MFA is a **preventive control** designed to stop the unauthorized access attempt from succeeding in the first place.

Question 19

The Chief Information Security Officer (CISO) establishes a new mandate stating that no member of the procurement department is allowed to authorize payments to vendors they initially onboarded into the financial system.

This mandate is a direct application of which access control principle?

A. Principle of Least Privilege
B. Mandatory Access Control
C. Segregation of Duties
D. Need to Know

Answer 19

C. Segregation of Duties

Detailed Explanation (Correct Answer)

The mandate is a direct application of **Segregation of Duties (SoD)** (or Separation of Duties). This principle involves dividing high-risk tasks, such as creating a new vendor and then authorizing payments to that vendor, between two or more individuals. This separation prevents a single person from potentially creating a fraudulent vendor account and embezzling funds, thereby enforcing checks and balances and mitigating the risk of fraud or error.

Answer 19 (Incorrect Options)

A. Principle of Least Privilege is incorrect. Least Privilege is about limiting the *scope* of access (permissions) for a single user to the minimum necessary. SoD is about dividing a high-risk *task* itself among multiple individuals.

B. Mandatory Access Control (MAC) is incorrect. MAC is an access model based on rigid security classification labels applied by the system. This scenario involves an administrative decision based on job function, not a system-level classification scheme.

D. Need to Know is incorrect. Need to Know limits a user's access to information they specifically require to perform their task. While related, the core mandate here is separating high-risk *functions*, not just restricting data visibility.

Question 20

A small office implements a security measure that requires all personnel to wear photo identification badges at all times while inside the premises, and the front lobby desk is staffed by a dedicated guard responsible for visually inspecting these badges upon entry.

This combined security measure is an example of which two control types?

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

Answer 20

C. Administrative and Physical

Detailed Explanation (Correct Answer)

This combined security measure is an example of **Administrative and Physical controls**.

1. **Administrative Control:** The requirement to **wear photo identification badges at all times** is a policy or procedure set by management. This defines the rules for behavior and conduct.
2. **Physical Control:** The **photo identification badges** themselves, along with the **dedicated guard** visually inspecting them, are tangible measures designed to restrict access to the physical facilities.

Answer 20 (Incorrect Options)

A. Technical and Logical is incorrect. Technical controls involve the use of technology like firewalls or encryption. Logical controls are digital access controls like ACLs or RBAC. This scenario is focused entirely on the physical premise and manual procedures.

B. Administrative and Technical is incorrect. As stated above, there is no technical control (e.g., encryption, firewall, software enforcement) mentioned in the scenario; it involves manual inspection and physical items.

D. Detective and Corrective is incorrect. These terms describe the *function* of controls, not the *type*. Furthermore, the function described (restricting entry based on rules) is **Preventive/Deterrent**, not primarily Detective (like a CCTV camera) or Corrective (like restoring a backup).