Identity Management and Access Control

Context and Strategic Importance The principle of **"Least Privilege"**—ensuring that every user and every system has only the minimum level of access they need—is the single most important rule of security. Identity Management and Access Control are the mechanisms for enforcing this principle. In a world of remote work and cloud-based systems, your "identity" is the new security perimeter.

Control Deconstruction Enforcing strict access control requires the implementation of "Multi-Factor Authentication" (MFA) and "Role-Based Access Control" (RBAC).

- **Identity Management:** Managing the entire lifecycle of a user's identity, from onboarding to offboarding.
- **Access Control:** Defining exactly what each user can do with their identity.
- **Just-In-Time Access:** Providing administrative privileges only when they are needed and only for a limited time. The logic of access control is "risk reduction," ensuring that even if an account is compromised, the damage is limited.

Securing the Truth Robust access control prevents "unauthorized data modification," maintaining the structural integrity of the system. By ensuring that only authorized users can change data, the organization maintains its "Single Source of Truth." This prevents the data corruption that occurs when users (maliciously or accidentally) modify information they should not have access to.

Strategic Look-Ahead Achieving security maturity through identity management leads to a "significant reduction in internal threats" within 12 months. The risk of a major data breach caused by a compromised account is dramatically reduced. Neglecting these controls leaves the organization vulnerable to a wide range of security risks, including ransomware and corporate espionage.

Executive Directive Leadership is to mandate "Multi-Factor Authentication" (MFA) for every user, without exception. The IT team is to conduct a "Privilege Review" and revoke all administrative rights that are not strictly necessary for a user's job function.

Transition Specific access controls are part of the broader framework of Policy, Compliance, and International Standards.