ISC2

Domain 5 Key Takeaways

Overall, security professionals reviewing CISSP Domain 5 need to understand the principles of identity and access management and the different tools and techniques that can be utilized to manage user accounts and control access to information and systems. This includes understanding user authentication and authorization mechanisms, managing privileged accounts, and implementing SSO and FIM. Additionally, access control monitoring and logging are critical for detecting and preventing unauthorized access and providing an audit trail for forensic analysis.

1. Identity and access management involves managing the lifecycle of user accounts, from creation to deletion.

2. Identification, authentication, and authorization are the three key components of access control.

3. User authentication mechanisms include passwords, tokens, biometrics, and multifactor authentication.

4. Authorization mechanisms include access control lists, role-based access control, and mandatory access control.

5. Identity and access management also involves managing privileged accounts, such as administrator accounts, which require special attention to ensure that they are not misused.

6. Single sign-on (SSO) and federated identity management (FIM) can be used to simplify access control and reduce the number of accounts and passwords that users must manage.

7. Access control monitoring and logging are essential to detect and prevent unauthorized access and to provide an audit trail for forensic analysis.

Manage the Identity and Access Provisioning Lifecycle

- In organizations, every identity should be associated with an individual, allowing each person in the organization to have the exact permission they need to perform their duties—no more and no less.

- A variety of definitions of access control are in use throughout the information security community worldwide. A useful starting point can be found in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000:2016(E), which defines access control as a "means to ensure that access to assets is authorized and restricted based on business and security requirements."

- Identities are labels and data constructs that all subjects and objects in a system must have that provide a clear and unambiguous way to refer to them.

- It is important to realize that while every identity starts its lifecycle at the provisioning stage and ends when it is disabled and deprovisioned, the ebb and flow of activities across the days and months will differ. A pattern of inappropriate or suspicious activity by one user may trigger frequent and urgent reviews to determine whether corrective action is called for, while another user's may not require it so frequently. Some users will not as frequently change their role or function as others will within the organization (i.e., the duties and responsibilities they are assigned). Some users may initiate more self-service identity and privilege changes than others.

- Each change in employment status, assigned jobs and duties or responsibilities should trigger an associated permissions review. This will help prevent privilege creep.

- It is imperative that permissions access reviews are conducted on an ongoing basis so that any suspicious activities are identified in a timely manner. Scheduled and regular permissions access reviews can reveal vulnerabilities that might require the need for revocation, disablement or deletion of specific permissions, or in some cases an entire account.

- Legal and regulatory compliance regimes may dictate both minimum and maximum retention periods for data pertaining to individual persons. Investigation and analysis of ongoing events, after a person's identity has been disabled and they have left the organization, may also reveal a need to delve into the archives.

Implement and Manage Authorization Mechanisms

- The access control (AC) models addressed in this domain are Discretionary Access Control (DAC,) Mandatory Access Control (MAC)**,** nondiscretionary access control (NDAC), role-based access control (RBAC), rule-based access control (RuBAC), and attribute-based access control (ABAC). NIST SP 800-192 also provides the definition for each of the types of AC.

Control Access to Assets

- The management of information related to physical and logical access is accomplished by three primary methods: centralized, decentralized, and hybrid.

- Before selection and implementation of the logical AC type, the data owner needs to classify and categorize their information. Each of these complementary processes identifies the type of protection—Confidentiality, Integrity, Availability, Non-Repudiation, Authenticity, Privacy, and Safety (IANA+PS)—that systems designers and security professionals must provide, and to what extent, to meet the organization's overall information risk management needs.

- Because of the sheer volume of remote users, many systems environments require a more complex and nuanced logical AC system than they need for controlling physical access.

- Much of the art and science of physical AC systems is inextricably bound up with the design and construction of physical environments. This is covered in Domain 3 and Domain 7.

Manage Identification and Authentication of People, Devices, and Services

- Increasing numbers of systems have made maintaining separate identity stores expensive and error prone. Thus, organizations began seeking mechanisms to simplify the maintenance of credentials, to reduce the burden on users to manage multiple credentials, and to standardize the identity services within their various environments. A few well-known examples of such repositories are Kerberos, Remote Authentication Dial-in User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), Open Authorization (OAuth)/OAuth2.0, Security Assertion Markup Language (SAML), OpenID, OpenID Connect, Fast ID Online (FIDO), FIDO Universal 2nd Factor (U2F), FIDO Universal Authentication Framework (UAF), FIDO2, and Web Authentication (WebAuthn).

- Implementing Identity and Access Management (IAM) does not reduce an organizations' responsibility to ensure their processes are handled as desired and to uphold the relevant controls to detect and lessen chances of noncompliance.

- FIM enables the process of creating a trust relationship between different security domains. These trust domains then provide access (verification) by using common digital identities that consist of three components: the client or principal, the service provider (SP) or relying party (RP), and the identity provider (IdP).

- There are a range of devices (systems or components, if logical) associated with logical and physical AC that include but are not limited to access tokens (hardware and software), keys and cards. The objective of using AC devices is to add an additional layer of protection for data access. Devices can be used with other identification methods, providing multifactor authentication (MFA).

- The Digital Identity Guidelines of NIST SP 800-63-3 contain recommendations to support, among other items, requirements for identity proofing and registration.

- No matter what technologies, processes or procedures are used, there will be errors. Noise, sensor degradation or failure, miscalibration, and misuse can cause false readings. Error rates apply equally to any kind of event detection approach, technology, or system.

- Just-in-time identity provides on-demand, real-time (or near real-time) creation and provisioning of human and nonhuman user identities; their privilege escalation and de-escalation; and then deprovisioning, suspension, or termination of that identity in each system.

Implement Authentication Systems

- While we commonly consider session management as a requirement for managing and controlling access with online resources, it is not limited to this area alone. Session management is the process of tracking and securing multiple requests to any service coming from the same subject. An organization must track all the session IDs and be prepared to forcibly terminate sessions (connected user or systems) when a period of inactivity is reached or when anomalies within a session occur.

- There are several prominent methods for authentication in use today, ranging from a simple username/password pair to MFA to the most complex of modern centralized methods. Some of these methods, such as RADIUS, may seem like legacy systems, but they are still active in the marketplace. Infrastructures that are substantially based on Linux or Unix often use a combination of Kerberos and LDAP. Microsoft-centric infrastructures almost invariably use Microsoft's Active Directory. All these products and systems, to a greater or lesser degree, are platform- and OS-agnostic, supporting almost any device or network system that can work with their respective protocols. Almost all of them use the X.500 Directory Access Protocol, or variations of it.

- As an organization considers outsourcing or offboarding various aspects of its information security needs, it is increasingly important to keep focused. The ultimate burden of due care and due diligence stays with an organization regardless of its outsourcing, offboarding, or vendor relationships.

- Security professionals must be aware that vendors of these services may not be precise when it comes to what they name or how they describe their security, identity management, and AC services and capabilities.