L3 Access Control Concepts

Introduction

Types of access control, physical and logical controls and how they are combined to strengthen the overall security of an organization.

Module 1 Understand Access Control Concepts

Domain D3.1, D3.1.3, D3.1.5, D3.2, D3.2.1, D3.2.2, D3.2.5

What is Security Control?

Access control involves **limiting what objects can be available to what subjects according to what rules**.

Controls Overview

Earlier in this course we looked at security principles through foundations of risk management, governance, incident response, business continuity and disaster recovery. But in the end, security all comes down to, **"who can get access to organizational assets (buildings, data, systems, etc.) and what can they do when they get access?"**

Access controls **are not just about restricting access** to information systems and data, **but also about allowing access**. It is about granting the appropriate level of access to authorized personnel and processes and denying access to unauthorized functions or individuals.

Access is based on three elements:

- subjects: **any entity that requests access to our assets**. The entity requesting access may be a **user**, a **client**, a **process** or a **program**, for example. A subject is the initiator of a request for service; therefore, a subject is referred to as "active." A subject:
  - Is a user, a process, a procedure, a client (or a server), a program, a device such as an endpoint, workstation, smartphone or removable storage device with onboard firmware.
  - Is active: It initiates a request for access to resources or services.
  - Requests a service from an object.
  - Should have a level of clearance (permissions) that relates to its ability to successfully access services or resources.

Controls Assessments

Risk reduction depends on the effectiveness of the control. It must apply to the current situation and adapt to a changing environment.

Defense in Depth

We are looking at all access permissions including building access, access to server rooms, access to networks and applications and utilities. These are all implementations of access control and are part of **a layered defense strategy**, **also known as defense in depth**, developed by an organization.

Defense in depth describes an information security strategy that integrates people, technology and operations capabilities to establish variable barriers across multiple layers and missions of the organization. It applies multiple countermeasures in a layered fashion to fulfill security objectives. Defense in depth should be implemented to prevent or deter a cyberattack, but it cannot guarantee that an attack will not occur.

A technical example of defense in depth, in which multiple layers of technical controls are implemented, **is when a username and password are required for logging in to your account, followed by a code sent to your phone to verify your identity**. **This is a form of multi-factor authentication using methods on two layers, something you have and something you know.** The combination of the two layers is much more difficult for an adversary to obtain than either of the authentication codes individually.

Another example of multiple technical layers is when additional firewalls are used to separate untrusted networks with differing security requirements, such as the internet from trusted networks that house servers with sensitive data in the organization. When a company has information at multiple sensitivity levels, it might require the network traffic to be validated by rules on more than one firewall, with the most sensitive information being stored behind multiple firewalls.

For a non-technical example, consider the multiple layers of access required to get to the actual data in a data center. First, a lock on the door provides a physical barrier to access the data storage devices. Second, a technical access rule prevents access to the data via the network. Finally, a policy, or administrative control defines the rules that assign access to authorized individuals.

Principle of Least Privilege

The Principle of Least Privilege (NIST SP 800-179) is a standard of permitting only minimum access necessary for users or programs to fulfill their function. Users are provided access only to the systems and programs they need to perform their specific job or tasks.

To preserve the confidentiality of information and ensure that it is only available to personnel who are authorized to see it, **we use privileged access management**, **which is based on the principle of least privilege**. **That means each user is granted access only to the items they need and nothing further**.

For example, only individuals working in billing will be allowed to view consumer financial data, and even fewer individuals will have the authority to change or delete that data. This maintains confidentiality and integrity while also allowing availability by providing administrative access with an

appropriate password or sign-on that proves the user has the appropriate permissions to access that data.

Sometimes it is necessary to allow users to access the information via a temporary or limited access, for instance, for a specific time period or just within normal business hours. Or access rules can limit the fields that the individuals can have access to. One example is a healthcare environment. Some workers might have access to patient data but not their medical data. Individual doctors might have access only to data related to their own patients. In some cases, this is regulated by law, such as HIPAA in the United States, and by specific privacy laws in other countries.

Systems often monitor access to private information, and if logs indicate that someone has attempted to access a database without the proper permissions, that will automatically trigger an alarm. The security administrator will then record the incident and alert the appropriate people to take action.

The more critical information a person has access to, the greater the security should be around that access. They should definitely have multi-factor authentication, for instance.

Privileged Access Management

Privileged access management provides the first and perhaps most familiar use case. Consider a human user identity that is granted various create, read, update, and delete privileges on a database. Without privileged access management, the system's access control would have those privileges assigned to the administrative user in a static way, effectively "on" 24 hours a day, every day. Security would be dependent upon the login process to prevent misuse of that identity. Just-in-time privileged access management, by contrast, includes role-based specific subsets of privileges that only become active in real time when the identity is requesting the use of a resource or service.

Privileged Accounts

Privileged accounts are those with permissions beyond those of normal users, such as managers and administrators. Broadly speaking, these accounts have **elevated privileges** and are used by many different classes of users, including:

- Systems administrators, who have the principal responsibilities for operating systems, applications deployment and performance management.
- Help desk or IT support staff, who often need to view or manipulate endpoints, servers and applications platforms by using privileged or restricted operations.
- Security analysts, who may require rapid access to the entire IT infrastructure, systems, endpoints and data environment of the organization.

Other classes of privileged user accounts may be created on a per-client or per-project basis, to allow a member of that project or client service team to have greater control over data and applications. These few examples indicate that organizations often need to delegate the capability to manage and protect information assets to various managerial, supervisory, support or leadership people, with differing levels of authority and responsibility. This delegation, of course, should be contingent upon

trustworthiness, since misuse or abuse of these privileges could lead to harm for the organization and its stakeholders.

Typical measures used for moderating the potential for elevated risks from misuse or abuse of privileged accounts include the following:

```
* More extensive and detailed logging than regular user accounts. The record of privileged act
* More stringent access control than regular user accounts. As we will see emphasized in this
* Deeper trust verification than regular user accounts. Privileged account holders should be s
* More auditing than regular user accounts. Privileged account activity should be monitored an
```

Segregation of Duties

A core element of authorization is the **principle of segregation of duties** (also known as separation of duties). **Segregation of duties is based on the security practice that no one person should control an entire high-risk transaction from start to finish**. **Segregation of duties breaks the transaction into separate parts and requires a different person to execute each part of the transaction**. For example, an employee may submit an invoice for payment to a vendor (or for reimbursement to themselves), but it must be approved by a manager prior to payment; in another instance, almost anyone may submit a proposal for a change to a system configuration, but the request must go through technical and management review and gain approval, before it can be implemented.

These steps can prevent fraud or detect an error in the process before implementation. It could be that the same employee might be authorized to originally submit invoices regarding one set of activities, but not approve them, and yet also have approval authority but not the right to submit invoices on another. It is possible, of course, that two individuals can willfully work together to bypass the segregation of duties, so that they could jointly commit fraud. This is called collusion.

Another implementation of segregation of duties is dual control. This would apply at a bank where there are two separate combination locks on the door of the vault. Some personnel know one of the combinations and some know the other, but no one person knows both combinations. Two people must work together to open the vault; thus, the vault is under dual control.

The two-person rule is a security strategy that requires a minimum of two people to be in an area together, making it impossible for a person to be in the area alone. Many access control systems prevent an individual cardholder from entering a selected high-security area unless accompanied by at least one other person. Use of the two-person rule can help reduce insider threats to critical areas by requiring at least two individuals to be present at any time. It is also used for life safety within a security area; if one person has a medical emergency, there will be assistance present.

How Users Are Provisioned

Other situations that call for provisioning new user accounts or changing privileges include:

- **A new employee**: When a new employee is hired, the hiring manager sends a request to the security administrator to create a new user ID. This request authorizes creation of the new ID and provides instructions on appropriate access levels. Additional authorization may be required by company policy for elevated permissions.
- **Change of position**: When an employee has been promoted, their permissions and access rights might change as defined by the new role, which will dictate any added privileges and updates to access. At the same time, any access that is no longer needed in the new job will be removed.
- **Separation of employment**: When employees leave the company, depending on company policy and procedures, their accounts must be disabled after the termination date and time. It is recommended that accounts be disabled for a period before they are deleted to preserve the integrity of any audit trails or files that may be owned by the user. Since the account will no longer be used, it should be removed from any security roles or additional access profiles. This protects the company, so the separated employee is unable to access company data after separation, and it also protects them because their account cannot be used by others to access data.

Module 2: Understand Physical Access Controls

Domain D3.1, D3.1.1, D3.1.2

What Are Physical Security Controls?

Physical access controls are items you can physically touch, which include physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility. Examples of physical access controls include security guards, fences, motion detectors, locked doors/gates, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, cameras, mantraps/turnstiles, and alarms.

Physical access controls are necessary to protect the assets of a company, including its most important asset, people. When considering physical access controls, the security of the personnel always comes first, followed by securing other physical assets.

Why Have Physical Security Controls?

Physical access controls include **fences, barriers, turnstiles, locks and other features that prevent unauthorized individuals from entering a physical site**, such as a workplace. This is to protect not only physical assets such as computers from being stolen, but also to protect the health and safety of the personnel inside.

Types of Physical Access Controls

Many types of physical access control mechanisms can be deployed in an environment to control, monitor and manage access to a facility. These range from deterrents to detection mechanisms. Each

area requires unique and focused physical access controls, monitoring and prevention mechanisms.

Badge Systems and Gate Entry

Physical security controls for human traffic are often done with technologies such as turnstiles, mantraps and remotely or system-controlled door locks. For the system to identify an authorized employee, an access control system needs to have some form of enrollment station used to assign and activate an access control device. Most often, a badge is produced and issued with the employee's identifiers, with the enrollment station giving the employee specific areas that will be accessible. In high-security environments, enrollment may also include biometric characteristics. In general, an access control system compares an individual's badge against a verified database. If authenticated, the access control system sends output signals allowing authorized personnel to pass through a gate or a door to a controlled area. The systems are typically integrated with the organization's logging systems to document access activity (authorized and unauthorized)

A range of card types allow the system to be used in a variety of environments. These cards include: Bar code, Magnetic stripe, Proximity, Smart, Hybrid

Environmental Design

Crime Prevention through Environmental Design (CPTED) approaches the challenge of creating safer workspaces through passive design elements. This has great applicability for the information security community as security professionals design, operate and assess the organizational security environment. Other practices, such as standards for building construction and data centers, also affect how we implement controls over our physical environment. Security professionals should be familiar with these concepts so they can successfully advocate for functional and effective physical spaces where information is going to be created, processed and stored.

CPTED provides direction to solve the challenges of crime with organizational (people), mechanical (technology and hardware) and natural design (architectural and circulation flow) methods. By directing the flow of people, using passive techniques to signal who should and should not be in a space and providing visibility to otherwise hidden spaces, the likelihood that someone will commit a crime in that area decreases.

Biometrics

To authenticate a user's identity, biometrics uses characteristics unique to the individual seeking access. A biometric authentication solution entails two processes.

Enrollment—during the enrollment process, the user's registered biometric code is either stored in a system or on a smart card that is kept by the user. Verification—during the verification process, the user presents their biometric data to the system so that the biometric data can be compared with the stored biometric code.

Even though the biometric data may not be secret, it is personally identifiable information, and the protocol should not reveal it without the user's consent. Biometrics takes two primary forms,

physiological and behavioral.

Physiological systems measure the characteristics of a person such as a fingerprint, iris scan (the colored portion around the outside of the pupil in the eye), retinal scan (the pattern of blood vessels in the back of the eye), palm scan and venous scans that look for the flow of blood through the veins in the palm. Some biometrics devices combine processes together—such as checking for pulse and temperature on a fingerprint scanner—to detect counterfeiting.

Behavioral systems measure how a person acts by measuring voiceprints, signature dynamics and keystroke dynamics. As a person types, a keystroke dynamics system measures behavior such as the delay rate (how long a person holds down a key) and transfer rate (how rapidly a person moves between keys).

Biometric systems are considered highly accurate, but they can be expensive to implement and maintain because of the cost of purchasing equipment and registering all users. Users may also be uncomfortable with the use of biometrics, considering them to be an invasion of privacy or presenting a risk of disclosure of medical information (since retina scans can disclose medical conditions). A further drawback is the challenge of sanitization of the devices.

Monitoring

The use of physical access controls and monitoring personnel and equipment entering and leaving as well as auditing/logging all physical events are primary elements in maintaining overall organizational security.

Cameras

Cameras are normally integrated into the overall security program and centrally monitored. Cameras provide a flexible method of surveillance and monitoring. They can be a deterrent to criminal activity, can detect activities if combined with other sensors and, if recorded, can provide evidence after the activity They are often used in locations where access is difficult or there is a need for a forensic record.While cameras provide one tool for monitoring the external perimeter of facilities, other technologies augment their detection capabilities. A variety of motion sensor technologies can be effective in exterior locations. These include infrared, microwave and lasers trained on tuned receivers. Other sensors can be integrated into doors, gates and turnstiles, and strain-sensitive cables and other vibration sensors can detect if someone attempts to scale a fence. Proper integration of exterior or perimeter sensors will alert an organization to any intruders attempting to gain access across open space or attempting to breach the fence line.

Logs

In this section, we are concentrating on the use of physical logs, such as a sign-in sheet maintained by a security guard, or even a log created by an electronic system that manages physical access. Electronic systems that capture system and security logs within software will be covered in another section.

A log is a record of events that have occurred. Physical security logs are essential to support business requirements. They should capture and retain information as long as necessary for legal or business reasons. Because logs may be needed to prove compliance with regulations and assist in a forensic investigation, the logs must be protected from manipulation. Logs may also contain sensitive data about customers or users and should be protected from unauthorized disclosure.

The organization should have a policy to review logs regularly as part of their organization's security program. As part of the organization's log processes, guidelines for log retention must be established and followed. If the organizational policy states to retain standard log files for only six months, that is all the organization should have.

A log anomaly is anything out of the ordinary. Identifying log anomalies is often the first step in identifying security-related issues, both during an audit and during routine monitoring. Some anomalies will be glaringly obvious: for example, gaps in date/time stamps or account lockouts. Others will be harder to detect, such as someone trying to write data to a protected directory. Although it may seem that logging everything so you would not miss any important data is the best approach, most organizations would soon drown under the amount of data collected.

Business and legal requirements for log retention will vary among economies, countries and industries. Some businesses will have no requirements for data retention. Others are mandated by the nature of their business or by business partners to comply with certain retention data. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires that businesses retain one year of log data in support of PCI. Some federal regulations include requirements for data retention as well.

If a business has no business or legal requirements to retain log data, how long should the organization keep it? The first people to ask should be the legal department. Most legal departments have very specific guidelines for data retention, and those guidelines may drive the log retention policy.

Security Guards

Security guards are an effective physical security control. No matter what form of physical access control is used, a security guard or other monitoring system will discourage a person from masquerading as someone else or following closely on the heels of another to gain access. This helps prevent theft and abuse of equipment or information.

Alarm Systems

Alarm systems are commonly found on doors and windows in homes and office buildings. In their simplest form, they are designed to alert the appropriate personnel when a door or window is opened unexpectedly.

For example, an employee may enter a code and/or swipe a badge to open a door, and that action would not trigger an alarm. Alternatively, if that same door was opened by brute force without someone entering the correct code or using an authorized badge, an alarm would be activated.

Another alarm system is a fire alarm, which may be activated by heat or smoke at a sensor and will likely sound an audible warning to protect human lives in the vicinity. It will likely also contact local response personnel as well as the closest fire department.

Finally, another common type of alarm system is in the form of a panic button. Once activated, a panic button will alert the appropriate police or security personnel.

Module 3: Understand Logical Access Controls

Domain D3.2, D3.2.3, D3.2.4, D3.2.5

What are Logical Access Controls?

Whereas physical access controls are tangible methods or mechanisms that limit someone from getting access to an area or asset, logical access controls are electronic methods that limit someone from getting access to systems, and sometimes even to tangible assets or areas. Types of logical access controls include:

- Passwords
- Biometrics (implemented on a system, such as a smartphone or laptop)
- Badge/token readers connected to a system

These types of electronic tools limit who can get logical access to an asset, even if the person already has physical access.

Discretionary Access Control (DAC)

Discretionary access control (DAC) is a specific type of access control policy that is **enforced over all subjects and objects in an information system**. In DAC, the policy specifies that **a subject who has been granted access to information can do one or more of the following**:

- Pass the information to other subjects or objects
- Grant its privileges to other subjects
- Change security attributes on subjects, objects, information systems or system components
- Choose the security attributes to be associated with newly created or revised objects; and/or
- Change the rules governing access control; mandatory access controls restrict this capability

Most information systems in the world are DAC systems. In a DAC system, a user who has access to a file is usually able to share that file with or pass it to someone else. This grants the user almost the same level of access as the original owner of the file. **Rule-based access control systems are usually a form of DAC**.

This methodology relies on the discretion of the owner of the access control object to determine the access control subject's specific rights. Hence, security of the object is literally up to the discretion of the object owner. DACs are not very scalable; they rely on the access control decisions made by each

individual object owner, and it can be difficult to find the source of access control issues when problems occur.

Mandatory Access Control (MAC)

A mandatory access control (MAC) policy is one that is **uniformly enforced across all subjects and objects within the boundary of an information system**. In simplest terms, **this means that only properly designated security administrators, as trusted subjects, can modify any of the security rules that are established for subjects and objects within the system**. This also means that for all subjects defined by the organization (that is, known to its integrated identity management and access control system), the organization assigns a subset of total privileges for a subset of objects, such that the subject is constrained from doing any of the following:

- Passing the information to unauthorized subjects or objects
- Granting its privileges to other subjects
- Changing one or more security attributes on subjects, objects, the information system or system components
- Choosing the security attributes to be associated with newly created or modified objects
- Changing the rules governing access control

Although MAC sounds very similar to DAC, **the primary difference is who can control access**. With Mandatory Access Control, **it is mandatory for security administrators to assign access rights or permissions**; **with Discretionary Access Control, it is up to the object owner's discretion**.

Role-Based Access Control (RBAC)

Role-based access control (RBAC), as the name suggests, sets up user permissions based on roles. Each role represents users with similar or identical permissions.

Role-based access control provides each worker privileges based on what role they have in the organization. Only Human Resources staff have access to personnel files, for example; only Finance has access to bank accounts; each manager has access to their own direct reports and their own department. Very high-level system administrators may have access to everything; new employees would have very limited access, the minimum required to do their jobs.

Monitoring these role-based permissions is important, because if you expand one person's permissions for a specific reason—say, a junior worker's permissions might be expanded so they can temporarily act as the department manager—but you forget to change their permissions back when the new manager is hired, then the next person to come in at that junior level might inherit those permissions when it is not appropriate for them to have them. This is called privilege creep or permissions creep. We discussed this before, when we were talking about provisioning new users.

Having multiple roles with different combinations of permissions can require close monitoring to make sure everyone has the access they need to do their jobs and nothing more. In this world where jobs are ever-changing, this can sometimes be a challenge to keep track of, especially with extremely

granular roles and permissions. Upon hiring or changing roles, a best practice is to not copy user profiles to new users. It is recommended that standard roles are established, and new users are created based on those standards rather than an actual user. That way, new employees start with the appropriate roles and permissions.