L3 Access Control Concepts 存取控制概念

Introduction 介紹

- Types of access control, physical and logical controls and how they are combined to strengthen the overall security of an organization.
    - 不同的存取控制類型、實體和邏輯控制，以及它們如何結合以增強組織整體安全性。

Module 1 Understand Access Control Concepts 了解存取控制概念

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

What is Security Control? 安全控制是什麼?

- Access control involves **limiting what objects can be available to what subjects according to what rules**.
    - 存取控制涉及根據特定規則，限制哪些對象可以對哪些主體進行使用。

Controls Overview 控制概述

- 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?”**
    - 在這門課程的早期，我們通過風險管理、治理、事件響應、業務連續性和災難恢復的基礎探討了安全原則。但最終，安全問題歸結為「誰可以獲得對組織資產（建築物、數據、系統等）的訪問權限，以及他們在獲得訪問權限後可以做什麼？」
- 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.
    - 存取控制並不僅僅是關於限制對資訊系統和數據的訪問，而且也涉及允許訪問。它是關於向授權人員和流程授予適當的訪問級別，並拒絕未經授權的功能或個人的訪問。
- Access is based on three elements: 存取基於三個要素
    - 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: 主體：任何要求訪問我們資產的實體。請求訪問的實體可以是使用者、客戶、流程或程式，例如。主體是服務請求的發起者；因此，主體被稱為「主動方」。一個主體：
        - 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.
            - 是一個使用者、一個流程、一個程序、一個客戶（或服務器）、一個程式、一個設備，例如端點、工作站、智能手機或携帶式存儲設備，具有內部固件。
        - Is active: It initiates a request for access to resources or services.

        - 是主動的：它發起對資源或服務的訪問請求。
    - Requests a service from an object.
        - 向物件請求服務。
    - Should have a level of clearance (permissions) that relates to its ability to successfully access services or resources.
        - 應該具有與其成功訪問服務或資源相關的授權級別（權限）。

Controls Assessments 控制評估

- Risk reduction depends on the effectiveness of the control. It must apply to the current situation and adapt to a changing environment.
    - 風險降低取決於控制措施的有效性。它必須適用於當前的情況並適應不斷變化的環境。

Defense in Depth 縱深防禦

- 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.
    - 我們正在考慮所有的存取權限，包括進入建築物、伺服器機房、網路和應用程式以及工具的存取。這些都是存取控制的實施方式，也是組織所制定的分層防禦策略，也被稱為深度防禦。
- **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.
    - 深度防禦（Defense in depth）是一種信息安全策略，它整合人員、技術和運營能力，在組織的多個層面和任務中建立可變的防禦屏障。它以分層的方式應用多種對策，以實現安全目標。深度防禦應該被實施以預防或阻止網絡攻擊，但它不能保證不會發生攻擊。
- 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.
    - 深度防禦的技術示例是在多個技術控制層面上實施，例如，需要使用用戶名和密碼登錄帳戶，接著通過手機接收的驗證碼來驗證身份。這是一種使用兩個層面的多因素身份驗證方法，即「擁有某物」和「知道某事」。兩個層面的結合對於對手來說比單獨獲得任一身份驗證代碼要困難得多。
- 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.

    - 多層技術的另一個例子是使用額外的防火牆來分隔不受信任的網絡和具有不同安全需求的受信任網絡，例如將互聯網與組織中存放有敏感數據的服務器分開。當一家公司擁有多個敏感級別的信息時，可能需要通過多個防火牆上的規則對網絡流量進行驗證，最敏感的信息被存放在多個防火牆後面。

- 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.
    - 以非技術性的例子來看，考慮到要獲取數據中心中實際數據所需的多個層級。首先，門上的鎖提供了對數據存儲設備的物理隔離。其次，技術性的訪問規則阻止通過網絡訪問數據。最後，策略或管理控制定義了將訪問權限分配給授權人員的規則。

Principle of Least Privilege 最小權限原則

- 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.
    - 最小權限原則（NIST SP 800-179）是一種標準，僅允許使用者或程式所需的最低限度的存取權限，以履行其功能。使用者只被授予他們需要執行特定工作或任務的系統和程式的存取權限。

- 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**.
    - 為了保護資訊的機密性並確保只有授權人員可以查看，我們使用特權存取管理，該管理方法基於最小權限原則。這意味著每個使用者只被授予所需的存取權限，不多不少。

- 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.
    - 例如，只有負責帳單工作的人員才能查看消費者的財務資料，而且只有更少數的人員有權更改或刪除該資料。這樣做可以在確保機密性和完整性的同時，通過提供具有適當密碼或登錄的管理存取，以證明使用者具有訪問該資料的適當權限，從而實現可用性。

- 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.
    - 有時候有必要允許使用者透過臨時或有限的存取方式來存取資訊，例如，在特定時間段內或僅限於正常工作時間內。或者，存取規則可以限制個人可以存取的欄位。一個例子是在醫療環境中。

某些工作人員可能可以存取患者資料，但不能存取其醫療資料。個別醫生可能僅能存取與他們自己患者相關的資料。在某些情況下，這是受法律規範的，例如美國的HIPAA法案以及其他國家的特定隱私法律。

- 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.
    - 系統通常會監控對私人資訊的存取，如果日誌顯示某人未經適當權限嘗試存取資料庫，這將自動觸發警報。安全管理員將記錄該事件並通知相應的人員採取行動。
- 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.
    - 一個人可以存取的重要資訊越多，對該存取的安全性要求就越高。例如，他們絕對應該使用多因素驗證。

Privileged Access Management 特權訪問管理

- 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.
    - 特權存取管理提供了第一個且可能是最熟悉的使用案例。考慮一個人類使用者身份，在資料庫上被授予各種創建、讀取、更新和刪除的權限。如果沒有特權存取管理，系統的存取控制會將這些權限以靜態方式分配給管理使用者，有效地在每天 24 小時、每天都開放。安全性將依賴於登錄過程以防止該身份的誤用。相較之下，及時特權存取管理包括基於角色的特定權限子集，只有在身份要求使用資源或服務時才會即時啟用。

Privileged Accounts 特權帳戶

- 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: 特權帳戶是指擁有超出一般使用者權限的帳戶，例如經理和管理員。一般來說，這些帳戶擁有提升的特權，並由許多不同類別的使用者使用，包括：
    - Systems administrators, who have the principal responsibilities for operating systems, applications deployment and performance management.
        - 系統管理員負責操作系統、應用程式部署和性能管理等主要職責。
    - Help desk or IT support staff, who often need to view or manipulate endpoints, servers and applications platforms by using privileged or restricted operations.
        - 協助台或IT支援人員通常需要透過使用特權或受限操作來查看或操作終端、伺服器和應用程式平台。
    - Security analysts, who may require rapid access to the entire IT infrastructure, systems, endpoints and data environment of the organization.

        - 安全分析師可能需要快速存取組織的整個IT基礎架構、系統、終端和資料環境。

- 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.

    - 其他特權使用者帳戶可能會根據每個客戶或專案的基礎來建立，以允許該專案或客戶服務團隊的成員對資料和應用程式擁有更大的控制權。這些僅是一些例子，顯示組織常需要將管理和保護資訊資產的能力委派給不同級別的管理、監督、支援或領導人員，並擁有不同的權限和責任。當然，這種委派應該建立在信任的基礎上，因為濫用這些特權可能會對組織及其利益相關者造成損害。

- Typical measures used for moderating the potential for elevated risks from misuse or abuse of privileged accounts include the following: 用於減輕特權帳戶被濫用或濫用時潛在風險的典型措施包括以下內容：

    - More extensive and detailed logging than regular user accounts. The record of privileged actions is vitally important, as both a deterrent (for privileged account holders that might be tempted to engage in untoward activity) and an administrative control (the logs can be audited and reviewed to detect and respond to malicious activity).
        - 比普通使用者帳戶更廣泛且詳細的日誌記錄。特權操作的記錄非常重要，既可以作為遏制（對於可能被誘使從事不當活動的特權帳戶持有人）的手段，也可以作為管理控制（可以審核和檢查日誌以檢測和應對惡意活動）。
    - More stringent access control than regular user accounts. As we will see emphasized in this course, even nonprivileged users should be required to use MFA methods to gain access to organizational systems and networks. Privileged users—or more accurately, highly trusted users with access to privileged accounts—should be required to go through additional or more rigorous authentication prior to those privileges. Just-in-time identity should also be considered as a way to restrict the use of these privileges to specific tasks and the times in which the user is executing them.
        - 比普通使用者帳戶更嚴格的存取控制。正如我們在本課程中所強調的，即使是非特權使用者，在訪問組織系統和網絡時也應要求使用多重身份驗證方法。特權使用者，或更準確地說，具有特權帳戶訪問權限的高度信任的使用者，應在獲得特權之前通過額外或更嚴格的身份驗證。同時，也應考慮使用即時身份作為一種限制這些特權使用於特定任務和使用者執行任務的時間的方式。
    - Deeper trust verification than regular user accounts. Privileged account holders should be subject to more detailed background checks, stricter nondisclosure agreements and acceptable use policies, and be willing to be subject to financial investigation. Periodic or event-triggered updates to these background checks may also be in order, depending on the nature of the organization's activities and the risks it faces.
        - 比普通使用者帳戶更深入的信任驗證。特權帳戶持有人應接受更詳細的背景調查、更嚴格的保密協議和可接受使用政策，並願意接受財務調查。根據組織的活動性質和面臨的風險，可能需要定期或事件觸發的背景調查更新。

    - More auditing than regular user accounts. Privileged account activity should be monitored and audited at a greater rate and extent than regular usage.
        - 比普通使用者帳戶更多的審計。特權帳戶的活動應該以比常規使用更高的速率和範圍進行監控和審計。

Segregation of Duties 職責分離

- 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.
    - 授權的核心元素之一是「職責分離原則」（也稱為職務分離）。職責分離基於一項安全慣例，即不應該讓一個人完全控制一個高風險交易的始終。職責分離將交易分為不同的部分，並要求不同的人執行交易的每個部分。例如，員工可以提交付款給供應商的發票（或用於自己的報銷），但必須在付款之前經理人批准；在另一種情況下，幾乎任何人都可以提交對系統配置的更改提案，但該請求必須經過技術和管理審查並獲得批准，然後才能實施。
- 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.
    - 這些步驟可以在實施之前防止欺詐或檢測過程中的錯誤。例如，同一名員工可能被授權提交與某一組活動相關的發票，但不能批准它們，同時也有批准權限，但不能提交另一組活動的發票。當然，有可能兩個人故意合作以繞過職責分離，從而共同進行欺詐行為，這稱為共謀（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.
    - 另一種職責分離的實施方式是雙重控制。這在銀行中可以應用，例如保險庫的門上有兩個獨立的密碼鎖。一些人知道其中一個密碼，另一些人知道另一個密碼，但沒有任何一個人知道兩個密碼。兩個人必須共同合作才能打開保險庫，因此保險庫處於雙重控制之下。
- **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.

    - 雙人原則是一種安全策略，要求至少兩個人在同一區域內，使個人無法獨自進入該區域。許多存取控制系統會阻止個別持卡人進入特定的高安全區域，除非至少有一名其他人陪同。使用雙人原則可以通過要求至少有兩個人在任何時候都必須在場來減少對關鍵區域的內部威脅。它還用於安全區域的生命安全；如果一個人出現緊急情況，就會有人提供幫助。

How Users Are Provisioned 如何配置用戶

- Other situations that call for provisioning new user accounts or changing privileges include: 需要配置新用戶帳戶或更改權限的其他情況包括：
    - **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.
        - 新員工：當一位新員工被聘用時，招聘經理會向安全管理員發送一份建立新使用者帳號的請求。此請求授權建立新帳號並提供有關適當存取層級的指示。根據公司政策，可能需要額外的授權以獲得升級權限。
    - **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.
        - 職位變更：當員工晉升時，其權限和存取權可能會根據新職位的定義而變化，這將決定任何附加特權和存取更新。同時，新工作不再需要的任何存取將被移除。
    - **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.
        - 離職處理：當員工離開公司時，根據公司的政策和程序，他們的帳號必須在離職日期和時間之後被停用。建議在刪除之前將帳號停用一段時間，以保留可能由該使用者擁有的任何審計軌跡或檔案的完整性。由於帳號將不再使用，應將其從任何安全角色或其他存取設定檔中移除。這既保護了公司，使離職的員工無法在離職後存取公司數據，也保護了他們自己，因為其他人無法使用他們的帳號存取數據。

Module 2: Understand Physical Access Controls 了解實體存取控制

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

What Are Physical Security Controls? 實體安全控制是什麼?

- 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.
    - 物理存取控制是指您可以實際觸碰的物品，包括用於防止、監視或檢測對設施內系統或區域的直接接觸的物理機制。物理存取控制的例子包括保安人員、柵欄、動態偵測器、上鎖的門/閘門、封閉的窗戶、照明設施、電纜保護、筆記型電腦鎖、識別證、刷卡、警衛狗、攝像頭、閘門/旋轉閘和警報器。
- 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.
    - 物理存取控制是保護公司資產的必要措施，其中包括最重要的資產 — 人員的安全。在考慮物理存取控制時，人員的安全永遠是首要考量，其次才是保護其他物理資產。

Why Have Physical Security Controls? 為什麼要有物理安全控制

- 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.
    - 物理存取控制包括圍欄、障礙物、旋轉閘門、鎖等功能，以防止未經授權的人進入實體場所，例如工作場所。這是為了保護不僅僅是防止電腦等物理資產被盜竊，也保護內部人員的健康和安全。

Types of Physical Access Controls 物理訪問控制的類型

- 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.
    - 在一個環境中，可以部署多種物理存取控制機制來控制、監控和管理對設施的存取。這些機制從威懾手段到檢測機制各不相同。每個區域都需要獨特且專注的物理存取控制、監控和預防機制。

Badge Systems and Gate Entry 證件系統和閘門入口

- 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)
    - 人流量的物理安全控制通常使用諸如旋轉閘門、人籠和遠程或系統控制的門鎖等技術來實現。為了讓系統識別出授權的員工，需要使用訪問控制系統的註冊站點來分配和啟用訪問控制設備。通常，會製作並發放一個帶有員工識別信息的證件，註冊站點會給予員工特定可進入的區域。在高安全環境中，註冊可能還包括生物特徵。一般而言，訪問控制系統會將個人的證件與驗證的數據

庫進行比對。如果驗證成功，訪問控制系統會發送輸出信號，允許授權人員通過門或閘門進入受控區域。這些系統通常與組織的日誌系統集成，以記錄訪問活動（授權和未授權的）。

- 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
    - 一系列的卡片類型使得系統可以應用於各種環境中。這些卡片包括：條碼卡、磁條卡、近場感應卡、智能卡和混合卡。

Environmental Design 環境設計

- 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.
    - 通過環境設計防止犯罪（CPTED）是通過被動設計元素來創建更安全的工作空間的方法。這對於信息安全社區非常適用，因為安全專業人員設計、運營和評估組織的安全環境。其他做法，例如建築建設和數據中心的標準，也會影響我們對物理環境的控制實施。安全專業人員應該熟悉這些概念，以便能夠成功倡導創建、處理和存儲信息的功能性和有效的物理空間。
- 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.
    - CPTED提供了解決犯罪挑戰的指引，使用組織（人員）、機械（技術和硬體）和自然設計（建築和流通流程）方法。通過引導人流，使用被動技術來指示誰應該進入空間，誰不應該進入空間，並提供對原本隱藏空間的可見性，減少了某個區域內犯罪的可能性。

Biometrics 生物識別

- To authenticate a user’s identity, biometrics uses characteristics unique to the individual seeking access. A biometric authentication solution entails two processes.
    - 要驗證使用者的身份，生物特徵辨識使用的是與尋求進入的個體獨特的特徵。生物特徵認證解決方案包含兩個過程。
- 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.
    - 註冊（Enrollment）- 在註冊過程中，使用者的註冊生物特徵碼要麼存儲在系統中，要麼存儲在使用者保管的智能卡上。驗證（Verification）- 在驗證過程中，使用者呈現其生物特徵數據給系統，以便將生物特徵數據與存儲的生物特徵碼進行比對。
- 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.

    - 儘管生物特徵數據可能不是機密信息，但它是可識別個人身份的信息，協議在未經用戶同意的情況下不應揭示這些信息。生物特徵主要分為生理特徵和行為特徵兩種形式。
- 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.
    - 生理特徵系統測量人的特徵，例如指紋、虹膜掃描（眼球瞳孔周圍的有色部分）、視網膜掃描（眼球背部的血管模式）、手掌掃描和血管掃描（通過手掌血管的血液流動）。一些生物特徵設備將多種過程結合在一起，例如在指紋掃描器上檢測脈搏和溫度，以檢測偽造。
- 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).
    - 行為特徵系統通過測量聲紋、簽名動態和鍵入動態來評估一個人的行為。在鍵入過程中，鍵入動態系統測量行為特徵，如延遲速率（按鍵保持的時間長短）和轉換速率（在按鍵之間移動的速度）。
- 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.
    - 生物特徵識別系統被認為具有高度準確性，但由於購買設備和註冊所有使用者的成本高昂，實施和維護這些系統可能很昂貴。使用者可能對使用生物特徵識別感到不舒服，認為這是對隱私的侵犯，或者存在著泄露醫療信息的風險（因為視網膜掃描可以洩露醫療狀況）。另外，這些設備的消毒也是一個挑戰。

Monitoring 監控

- 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.
    - 在維護整體組織安全方面，使用物理存取控制、監控人員和設備的進出，以及對所有物理事件進行審計/記錄是主要要素。

Cameras 相機

- 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.

- 攝影機通常會整合到整體安全計劃中並進行中央監控。攝影機提供了一種靈活的監視和監控方法。它們可以作為犯罪活動的威懾手段，如果與其他感應器結合使用，可以檢測活動，並且如果有錄像記錄，可以提供證據。它們通常用於難以進入的地點或需要進行法醫記錄的地方。儘管攝影機為監視設施外部範圍提供了一種工具，但其他技術可以增強其檢測能力。各種運動感應器技術在室外位置上都能起到有效作用，包括紅外線、微波和瞄準調諧接收器的激光。其他感應器可以集成到門、閘門和旋轉閘中，而應變敏感電纜和其他震動感應器則可以檢測是否有人試圖攀爬圍欄。正確集成外部或周邊感應器將提醒組織是否有入侵者試圖跨越空地進入或試圖突破圍欄。

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.

    - 在本節中，我們專注於使用物理日誌，例如由安全警衛維護的簽到表，或者由管理物理進入的電子系統創建的日誌。捕獲軟體中系統和安全日誌的電子系統將在另一節中介紹。

- 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.

    - 日誌是事件發生的記錄。物理安全日誌對於支持業務需求至關重要。它們應該根據法律或業務需求的時間長短捕獲和保留信息。由於日誌可能需要證明遵守法規並協助法庭調查，所以必須保護日誌免受操縱。日誌還可能包含有關客戶或使用者的敏感數據，因此應該防止未經授權的披露。

- 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.

    - 組織應該制定政策，定期審查日誌，作為其安全計劃的一部分。作為組織日誌處理的一部分，必須建立並遵循有關日誌保留的指南。如果組織政策規定只保留標準日誌文件六個月，那麼組織應該確實執行這個規定。

- 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.

    - 日誌異常是指任何不尋常的情況。在審計和例行監控期間，識別日誌異常通常是識別與安全相關問題的第一步。有些異常明顯得很明顯，例如日期/時間戳記的間隔或帳戶鎖定。其他一些異常

則更難檢測，例如有人嘗試將數據寫入受保護的目錄。儘管可能認為記錄所有事情，以便不錯過任何重要數據是最好的方法，但大多數組織很快就會被收集到的大量數據淹沒。

- 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.
    - 對於日誌保留，商業和法律要求在不同的經濟體、國家和行業之間會有所不同。有些企業對於數據保留沒有特定要求，而其他企業則根據其業務性質或與商業合作夥伴的要求，必須遵守特定的數據保留要求。例如，支付卡行業數據安全標準（PCI DSS）要求企業保留一年的日誌數據以支持PCI。一些聯邦法規也包含了對數據保留的要求。
- 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.
    - 如果企業沒有任何業務或法律上保留日誌數據的要求，該組織應該保留多久呢？首先應該諮詢法律部門的意見。大多數法律部門對於數據保留都有非常具體的指導方針，而這些指導方針可能會制定日誌保留政策。

Security Guards 保安人員

- 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.
    - 保安人員是有效的實體安全控制手段。無論使用何種形式的實體進出控制，保安人員或其他監控系統都能夠阻止人們冒充他人或緊隨其後以獲得進入權限。這有助於防止設備或信息的盜竊和濫用。

Alarm Systems 報警系統

- 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.
    - 警報系統通常安裝在家庭和辦公樓的門窗上。它們的基本形式旨在在門窗意外開啟時警示相應人員。
- 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.
    - 例如，一位員工可能輸入代碼和/或刷卡以打開一扇門，這個動作不會觸發警報。相反地，如果同樣的門被以強制方式打開，而沒有人輸入正確的代碼或使用授權的證件，警報就會被觸發。
- 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.
    - 另一種警報系統是火災警報，它可能會因為感應器檢測到熱或煙霧而被啟動，並發出聽得見的警示聲，以保護附近的人的生命安全。它還可能聯絡當地應急人員以及最近的消防部門。
- 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.
    - 最後，另一種常見的警報系統是恐慌按鈕。一旦被啟動，恐慌按鈕將會向適當的警察或安全人員發出警報。

Module 3: Understand Logical Access Controls 了解邏輯存取控制

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

What are Logical Access Controls? 邏輯存取控制是什麼?

- 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: 與實體存取控制不同，邏輯存取控制是指電子方法或機制，用於限制某人對系統、甚至實體資產或區域的存取。邏輯存取控制的類型包括：

    - Passwords
        - 密碼
    - Biometrics (implemented on a system, such as a smartphone or laptop)
        - 生物辨識（在系統上實現，如智慧型手機或筆記型電腦）
    - Badge/token readers connected to a system
        - 連接到系統的識別證/令牌讀卡器

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

    - 些電子工具限制了誰可以在邏輯上獲得資產的訪問權限，即使該人已經具有物理訪問權限。

Discretionary Access Control (DAC) 自主訪問控制 (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**: 自主存取控制（Discretionary Access Control，DAC）是一種特定的存取控制政策，其適用於信息系統中的所有主體和對象。在DAC中，政策規定被授予對信息訪問權限的主體可以執行以下一個或多個操作：

    - Pass the information to other subjects or objects
        - 將信息傳遞給其他主體或對象。
    - Grant its privileges to other subjects
        - 將其特權授予其他主體。
    - Change security attributes on subjects, objects, information systems or system components
        - 更改主體、物件、資訊系統或系統元件上的安全屬性。
    - Choose the security attributes to be associated with newly created or revised objects; and/or
        - 選擇與新建或修改的物件關聯的安全屬性；和/或。
    - Change the rules governing access control; mandatory access controls restrict this capability

        - 更改控制存取的規則；強制性存取控制會限制此能力。

- **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**.
    - 世界上大部分的資訊系統都是 DAC 系統。在 DAC 系統中，使用者如果能夠存取某個檔案，通常也可以將該檔案分享或轉交給其他人。這使得使用者幾乎擁有與檔案原始擁有者相同的存取權限。基於規則的存取控制系統通常也屬於 DAC 的一種形式。
- 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.
    - 這種方法依賴於存取控制物件的擁有者來決定存取控制主體的具體權限。因此，物件的安全性實際上取決於物件擁有者的判斷。DAC 不太具有可擴展性，它依賴於每個個別物件擁有者所做的存取控制決策，當問題發生時，很難找到存取控制問題的來源。

Mandatory Access Control (MAC) 強制訪問控制 (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: 強制存取控制（MAC）政策是一種在資訊系統範圍內對所有主體和物件統一執行的存取控制策略。簡單來說，這意味著只有經過適當指定的安全管理員，作為受信任的主體，才能修改系統中為主體和物件設定的任何安全規則。這也意味著對於組織定義的所有主體（即其整合的身份管理和存取控制系統所知的主體），組織分配了一個子集的特權，用於一個子集的物件，以侷限主體不能執行以下操作：
    - Passing the information to unauthorized subjects or objects
        - 將資訊傳遞給未經授權的主體或物件
    - Granting its privileges to other subjects
        - 授予其特權給其他主體
    - Changing one or more security attributes on subjects, objects, the information system or system components
        - 更改一個或多個主體、物件、資訊系統或系統元件的安全屬性
    - Choosing the security attributes to be associated with newly created or modified objects
        - 選擇與新建或修改的物件關聯的安全屬性
    - Changing the rules governing access control
        - 更改控制存取權的規則
- 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**.

    - 雖然強制存取控制（MAC）聽起來與自主存取控制（DAC）非常相似，但主要的區別在於誰可以控制存取權。在強制存取控制中，安全管理員必須強制指派存取權限；而在自主存取控制中，則取決於物件擁有者的自主權。

Role-Based Access Control (RBAC) 基於角色的訪問控制 (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.

    - 角色基礎存取控制（RBAC），如其名所示，根據角色設定使用者權限。每個角色代表具有相似或相同權限的使用者。

- 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.

    - 基於角色的存取控制根據組織中的角色分配每個工作人員的權限。例如，只有人力資源人員可以存取人事檔案；只有財務部門可以存取銀行帳戶；每個經理可以存取其直屬報告人和所屬部門的資源。非常高層級的系統管理員可能可以存取所有內容；新員工的存取權限非常有限，僅限於完成工作所需的最低權限。

- 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.

    - 監控這些基於角色的權限非常重要，因為如果你因為某種特定原因擴展了某個人的權限，例如，一位初級員工的權限可能會擴展，以便他們暫時擔任部門經理的職務，但是當新的經理被聘用時，如果你忘記將他們的權限改回來，那麼下一個進入該初級職位的人可能會繼承這些權限，而對於他們來說並不適當。這種情況被稱為權限擴展或權限累積。我們之前在談論新用戶配置時已經討論過這個問題。

- 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.

    - 擁有不同組合權限的多個角色可能需要密切監控，以確保每個人都擁有執行工作所需的訪問權限，並且不會超出所需範圍。在這個工作環境不斷變化的世界中，這有時可能是一個難題，尤其是在擁有極度精細的角色和權限時。在招聘或更改角色時，最佳做法是不將用戶配置文件複製給

新用戶。建議建立標準角色，並根據這些標準創建新用戶，而不是使用實際用戶的配置。這樣，新員工就可以從適當的角色和權限開始。