L1: Security Principles 安全原則

Module 1 Understand the Security Concepts of Information Assurance 了解信息保障的安全概念

Domain D1.1.1, D1.1.2, D1.1.3, D1.1.4, D1.1.5, D1.1.6

Confidentiality 機密

- It relates to permitting authorized access to information, while at the same time protecting information from improper disclosure. Difficulties to achieve confidentiality are related to: **many users are guests or customers**, and it is not clear if the access comes from a compromised machine or vulnerable mobile application. To avoid those difficulties, security professionals must regulate access, permitting access to authorized individuals, for that protecting the data that needs protection.
    - 它涉及允許授權訪問信息，同時保護信息免受不當披露。實現機密性的困難與以下問題相關：**很多用戶都是訪客或客戶**，並且不清楚訪問是否來自被入侵的機器或有漏洞的移動應用程序。為了避免這些困難，安全專業人員必須規範訪問，允許授權人員訪問並保護需要保護的數據。
- Data that needs protections is also known **as PII or PHI**. 需要保護的數據也被稱為 **PII 或 PHI**
    - **PII** stands for Personally Identifiable Information and it is related to the area of confidentiality and it means any data that could be used to identify an individual.
        - **PII** 代表個人可識別信息，它與機密性領域有關，指的是可以用於識別個人的任何數據。
    - **PHI** stands for Protected Health Information and it comprehends information about one's health status, and classified or sensitive information, which includes trade secrets, research, business plans and intellectual property.
        - **PHI** 代表受保護的健康信息，包括關於個人健康狀況的信息，以及分類或敏感信息，其中包括商業機密、研究、業務計劃和知識產權。
- Related to confidentiality is **the concept sensitivity a measure of the importance assigned to information by its owner**, or the purpose of denoting its need for protection. **Sensitive information** is information that if improperly disclosed (confidentiality) or modified (integrity) would harm an organization or individual. In many cases, sensitivity is related to the harm to external stakeholders; that is, people or organizations that may not be a part of the organization that processes or uses the information.
    - 與機密性相關的是**敏感度概念，它是根據信息擁有者對信息所賦予的重要性進行衡量**，或者用於表示其需要受到保護的目的。**敏感信息**是指如果被不當披露（機密性）或修改（完整性），將對組織或個人造成損害的信息。在許多情況下，敏感性與對外部利益相關方的損害有關；也就是說，這些人或組織可能不是處理或使用信息的組織的一部分。
- Threat related to confidentiality are: 與保密相關的威脅是：
    1. Snooping involves gathering information that is left out in the open. Clean desk policies protect against snooping.
        - 窺探行為涉及收集那些公開可見的信息。整潔辦公桌政策可防止窺探行為的發生。

    - 2. Dumpster diving also looking for sensitive materials, but in the dumpster, a paper shredding protects against it.
        - 垃圾探測是指在垃圾箱中搜尋敏感資料，但通過使用紙張碎紙機可以保護免受垃圾探測的侵害。
    - 3. Eavesdropping occurs when someone secretly listen to a conversation, and it can be prevent with rules about sensitive conversations
        - 竊聽是指某人秘密聆聽對話，可以通過關於敏感對話的規定來預防。
    - 4. Wiretapping is the electronic version of eavesdropping, the best way against that is using encryption to protect the communication.
        - 窃听是竊聽的電子版本，對抗窃听的最佳方式是使用加密來保護通信。
    - 5. Social Engineering, the best defense is educate users to protect them against social engineering.
        - 社交工程攻擊，最佳的防禦方法是教育使用者以保護他們免受社交工程攻擊。

Integrity 完整性

- It is the property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose, which can be applied **to information or data**, **system and process for business operations**, **organizations**, **people and their actions**. Furthermore, restrict to data integrity, it is an assurance that data has not been altered in an unauthorized manner, covering data **in storage**, during **processing**, and while **in transit**.
    - 完整性是信息的一項屬性，通過記錄、使用和維護的方式確保其完整性、準確性、內部一致性和對於指定目的的有用性，這可以應用於**信息或數據**、**用於業務運營的系統和流程**、**組織**、**人員及其行動**。此外，限於數據完整性，它是一種保證數據未經未經授權的方式進行更改的保證，涵蓋了**存儲**的數據、處理過程中的數據以及**傳輸過程中**的數據。
- **Consistency** is another concept related to integrity and requires that all instances of the data be identical in form, content and meaning. When related to system integrity, it refers to the maintenance of a known good configuration and expected operational function as the system processes the information. Ensuring integrity begins with an awareness of state, which is the current condition of the system. Specifically, this awareness concerns the ability to document and understand the state of data or a system at a certain point, **creating a baseline**. A baseline, which means a documented, lowest level of security configuration allowed by a standard or organization, can refer to the current state of the information—whether it is protected.
    - **一致性**是與完整性相關的另一個概念，要求數據的所有實例在形式、內容和含義上都是相同的。當涉及到系統的完整性時，它指的是在系統處理信息時維護已知的良好配置和預期的操作功能。確保完整性始於對系統狀態的認識，即系統的當前狀態。具體而言，這種認識涉及在某一點上記錄和了解數據或系統的狀態，即**創建基準**。基準指的是根據標準或組織允許的安全配置的文件化最低級別，可以指的是信息的當前狀態，即是否受到保護。
- To preserve that state, the information must always continue to be protected through a transaction. Going forward from that baseline, the integrity of the data or the system can always be ascertained by comparing the baseline with the current state. If the two match, then the integrity of the data or the system is intact; if the two do not match, then the integrity of the data or the system has been compromised. Integrity is a primary factor in the reliability of information and systems. The need to

safeguard information and system integrity may be dictated by laws and regulations. Often, it is dictated by the needs of the organization to access and use reliable, accurate information.

    - 為了保持這種狀態，信息必須始終通過交易來保護。從基準出發，可以通過將基準與當前狀態進行比較來確定數據或系統的完整性。如果兩者相匹配，則數據或系統的完整性保持完好；如果兩者不匹配，則數據或系統的完整性已被破壞。完整性是信息和系統可靠性的主要因素。保護信息和系統完整性的需要可能受到法律和法規的規定。通常情況下，這是根據組織對可靠、準確信息的訪問和使用需求來確定的。
- 1. Unauthorized modification attacks make changes without permission. The best way to protect against that is the least privilege principle.
    - 未經授權的修改攻擊是指在未經許可的情況下進行更改。保護自身免受此類攻擊的最佳方式是最小權限原則。
- 2. Impersonation attacks pretend to be someone else. User education protects against impersonation attack.
    - 冒名攻擊是指假冒他人身份。使用者教育可預防冒名攻擊。
- 3. Man-In-The-Middle (MITM) attacks place the attacker in the middle of a communication session, monitoring everything that's occurring.
    - 中間人攻擊（Man-In-The-Middle，MITM攻擊）將攻擊者置於通信會話的中間，監視一切正在發生的事情。
- 4. Replay attacks eavesdrop on logins and reuse the captured credentials.
    - 重放攻擊是指竊聽登錄信息並重複使用被截獲的憑證。

- To both MITM and Replay attacks the best approach is encryption.
    - 對於 MITM 和 Replay 攻擊，最好的方法是加密。

Availability 可用性

- It means that systems and data are accessible at the time users need them. It can be defined as timely and reliable access to information and the ability to use it, and for authorized users, timely and reliable access to data and information services. The core concept of availability is that data is accessible **to authorized users when and where it is needed and in the form and format required**. This does not mean that data or systems are available 100% of the time. Instead, the systems and data meet the requirements of the business for timely and reliable access.
    - 這表示系統和數據在用戶需要時可被訪問。它可以被定義為及時可靠地訪問信息並能夠使用它，對於授權用戶而言，及時可靠地訪問數據和信息服務。可用性的核心概念是數據在需要的時間和地點以所需的形式和格式對授權用戶可訪問。這並不意味著數據或系統始終可用100%的時間。相反，系統和數據符合業務對及時可靠訪問的需求。
- **Some systems and data are far more critical than others**, so the security professional **must ensure that the appropriate levels of availability are provided**. This requires consultation with the involved business to ensure that critical systems are identified and available. Availability is often associated with the term **criticality**, which means a measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function (NIST SP 800-60), because it represents the importance an organization gives to data or an information system in performing its operations or achieving its mission

    - **某些系統和數據比其他系統更加重要**，因此安全專業人員**必須確保提供適當水平的可用性**。這需要與相關業務進行協商，以確定關鍵系統的識別和可用性。可用性通常與**重要性**這一術語相關聯，重要性衡量的是組織在任務或業務功能的成功中依賴該信息或信息系統的程度（NIST SP 800-60），因為它代表了組織對數據或信息系統在執行其業務或實現其使命中的重要性。
- 1. Denial of Service can be mitigated using firewalls to block unauthorized connections
    - 使用防火牆阻止未經授權的連接可以減輕阻斷服務攻擊。
- 2. Power outages can be mitigated using redundant power and generators
    - 使用冗餘電源和發電機可以減輕停電情況。
- 3. Hardware failures can be mitigated using redundant components
    - 使用冗餘組件可以減輕硬件故障的影響。
- 4. Destruction can be mitigated using backups
    - 使用備份可以減輕破壞的影響。
- 5. Service outages
    - 服務中斷

Three steps to gain access, known as triple A, which means Authentication, Authorization, Accounting

- 獲取訪問權限的三個步驟，稱為「三個A」，即認證（Authentication）、授權（Authorization）和記帳（Accounting）。

Identification 鑑別

- Consist of making a claim of identity
    - 包括提出身份聲明

Authentication 認證

- When users have stated their identity, it is necessary **to validate that they are the rightful owners of that identity**. This process of verifying or proving the user's identification is known as authentication, which means in another terms access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single-factor or SFA) or more (multi-factor authentication or MFA) factors of authentication. Simply put, authentication is a process to prove the identity of the requestor.
    - 當用戶聲明了他們的身份後，有必要驗證他們是否是該身份的合法擁有者。這個驗證或證明用戶身份的過程稱為認證，也就是在其他術語中，通過比較一個（單因素認證或SFA）或多個（多因素認證或MFA）認證要素，來驗證系統已知用戶或實體聲稱的身份。簡單來說，認證是一個證明請求者身份的過程。
- There are three common methods of authentication: 常見的認證方式有以下三種：
    - Something you know: Passwords or paraphrases
        - 你知道的東西：密碼或釋義
    - Something you have: Tokens (NISTIR 7711), memory cards, smart cards
        - 您擁有的東西：令牌 (NISTIR 7711)、存儲卡、智能卡
    - Something you are: Biometrics , measurable characteristics
        - 你是什麼：生物識別，可測量的特徵

Methods of Authentication 認證方法

- There are two types of authentication. Using only one of the methods of authentication stated previously is **known as single-factor authentication (SFA)**. Granting users access only after successfully demonstrating or displaying two or more of these methods is **known as multi-factor authentication (MFA)**.
    - 有兩種類型的認證。僅使用前述認證方法之一被稱為單因素認證（SFA）。只有在成功展示或應用兩種或更多方法後，才允許用戶獲取訪問，這被稱為多因素認證（MFA）。
- **Common best practice is to implement at least two of the three common techniques for authentication**: 常見的最佳實踐是實施至少三種常見的認證技術中的兩種：
    - Knowledge-based 知識為基礎
    - Token-based 令牌為基礎
    - Characteristic-based 特徵為基礎
- Knowledge-based authentication uses a passphrase or secret code to differentiate between an authorized and unauthorized user. If you have selected a personal identification number (PIN), created a password or some other secret value that only you know, then you have experienced knowledge-based authentication. The problem with using this type of authentication alone is that it is often vulnerable to a variety of attacks. For example, the help desk might receive a call to reset a user's password. The challenge is ensuring that the password is reset only for the correct user and not someone else pretending to be that user. For better security, a second or third form of authentication that is based on a token or characteristic would be required prior to resetting the password. The combined use of a user ID and a password consists of two things that are known, and because it does not meet the requirement of using two or more of the authentication methods stated, it is not considered MFA.
    - 基於知識的認證使用密語或秘密代碼來區分授權和未授權的用戶。如果您選擇了個人識別號碼（PIN）、創建了密碼或其他只有您知道的秘密值，那麼您就體驗過基於知識的認證。僅使用此類認證存在的問題是，它常常容易受到各種攻擊。例如，幫助台可能會接到一個要求重置用戶密碼的電話。挑戰在於確保密碼只為正確的用戶重置，而不是別人冒充該用戶。為了提高安全性，在重置密碼之前，需要使用基於令牌或特徵的第二或第三種認證形式。僅使用用戶ID和密碼的組合屬於已知的兩個因素，因為它不滿足使用兩種或更多的認證方法的要求，因此不被視為多因素認證（MFA）。

Password 密碼

- Password length requirements set a minimum number of chars
    - 密碼長度要求設置最小字符數
- Password complexity requirements describe the types of characters that must be included
    - 密碼複雜性要求描述了必須包含的字符類型
- Password expiration requirements force password changes. Nowadays, that requirement isn't used, companies change to an approach where force password change is required when there is any evidence that the password has been compromised.
    - 密碼過期要求強制更改密碼。 如今，該要求已不再使用，公司改為在有任何證據表明密碼已被洩露時需要強制更改密碼的方法。
- Password history requirements prevent password reuse.

    - 密碼歷史要求可防止密碼重複使用。
- Provide a way to change the password quickly and easily.
    - 提供一種快速輕鬆地更改密碼的方法。
- Encourage users to not reuse the same password across multiple sites
    - 鼓勵用戶不要在多個站點重複使用相同的密碼
- Password managers facilitate the use of strong, unique passwords
    - 密碼管理器有助於使用強而獨特的密碼

Authorization 授權

- Ensuring that an action is allowed.
    - 確保允許操作。

Accounting

- Its maintains logs of activity
    - 它維護活動日誌

Non-repudiation 不可否認性

- Non-repudiation is a legal term and is defined as the protection against an individual falsely denying having performed a particular action. It provides the capability to determine whether a given individual took a particular action, such as created information, approved information or sent or received a message.

    - 不可否認性是一個法律術語，被定義為防止個人虛假否認執行特定操作的保護。它提供了確定特定個人是否執行了特定操作的能力，例如創建信息、批准信息或發送或接收消息。

- In today's world of e-commerce and electronic transactions, **there are opportunities for the impersonation of others or denial of an action, such as making a purchase online and later denying it**. It is important that all participants trust online transactions. **Non-repudiation methodologies ensure that people are held responsible for transactions they conducted**.

    - 在當今的電子商務和電子交易世界中，存在著冒充他人或否認行為的機會，例如在網上購物後否認購買行為。重要的是，所有參與者都要信任線上交易。不可否認的方法確保人們對他們進行的交易負責。

Base Concepts 基本概念

- 1. Authorization: the right or a permission that is granted to a system entity to access a system resource
    - 授權：授予系統實體訪問系統資源的權利或許可權。
- 2. Integrity: the property that data has not been altered in an unauthorized manner
    - 完整性：指數據未經未授權的方式被更改的屬性。
- 3. Confidentiality: the characteristic of data or information when it is not made available or disclosed to unauthorized persons or process
    - 保密性：當數據或信息未被提供或披露給未經授權的個人或過程時的特性。
- 4. Privacy: the right of an individual to control the distribution of information about themselves
    - 隱私：個人對於控制有關自己的信息分發的權利。

- 5. Availability: Ensuring timely and reliable access to and use of information by authorized users
  - 可用性：確保授權使用者能夠及時可靠地訪問和使用信息。
- 6. Non-repudiation: The inability to deny taking an action, such as sending an email message
  - 不可否認性：無法否認執行某一行動的能力，例如發送電子郵件。
- 7. Authentication: Access control process that compares one or more factors of identification to validate that the identity claimed by a user or entity is known to the system
  - 身份驗證：一種存取控制過程，通過比較一個或多個身份識別因素，驗證使用者或實體聲稱的身份在系統中已知。

Privacy 隱私

- Privacy is **the right of an individual to control the distribution of information about themselves**. While security and privacy both focus on the protection of personal and sensitive data, there is a difference between them. With the increasing rate at which data is collected and digitally stored across all industries, the push for privacy legislation and compliance with existing policies steadily grows. In today's global economy, privacy legislation and regulations on privacy and data protection can impact corporations and industries regardless of physical location. **Global privacy is an especially crucial issue when considering requirements regarding the collection and security of personal information**. There are several laws that define privacy and data protection, which periodically change. Ensuring that protective security measures are in place is not enough to meet privacy regulations or to protect a company from incurring penalties or fines from mishandling, misuse, or improper protection of personal or private information. An example of a law with multinational implications is the European Union's General Data Protection Regulation (GDPR) which applies to all organizations, foreign or domestic, doing business in the EU or any persons in the EU. Companies operating or doing business within the United States may also fall under several state legislations that regulate the collection and use of consumer data and privacy. Likewise, member nations of the EU enact laws to put GDPR into practice and sometimes add more stringent requirements. These laws, including national- and state-level laws, dictate that any entity anywhere in the world handling the private data of people in a particular legal jurisdiction must abide by its privacy requirements. As a member of an organization's data protection team, you will not be required to interpret these laws, but you will need an understanding of how they apply to your organization.
  - 隱私是個體控制有關自己的信息分發的權利。雖然安全性和隱私性都專注於保護個人和敏感數據，但它們之間存在差異。隨著各行各業數據的不斷收集和數字化存儲速度加快，對隱私法規和遵守現有政策的推動也在穩步增長。在當今全球經濟中，隱私立法和數據保護的規定可以影響無論實體位置如何的企業和行業。當考慮有關個人信息收集和安全性要求時，全球隱私問題尤為重要。有幾項法律定義了隱私和數據保護，這些法律定期變化。確保採取了保護性安全措施並不足以滿足隱私法規或保護公司免受對個人或私人信息的處理、濫用或不當保護而產生的罰款或處罰。一個具有跨國影響的法律例子是歐盟的《一般數據保護規則》（GDPR），它適用於在歐盟經營業務的所有組織，無論是國內還是外國的，以及在歐盟境內的任何人。在美國運營或從事業務的公司也可能受到幾個州法律的約束，這些法律對消費者數據和隱私的收集和使用進行了規範。同樣，歐盟成員國通過法律實施GDPR，有時還增加了更嚴格的要求。這些法律，包括國家和州級法律，規定在特定法律管轄區內處理人們的私人數據的任何實體必須遵守其隱私要求。作為組織數據保護團隊的成員，您不需要解釋這些法律，但您需要了解它們如何適用於您的組織。

Module 2 Understand the risk management process 了解風險管理流程

Domain D1.2.1, D1.2.2

- Risks and security-related issues represent **an ongoing concern** of businesses as well as the field of cybersecurity. Assessing and analyzing risk should be **a continuous and comprehensive** exercise in any organization. As a member of an organization's security team, you will work through **risk assessment, analysis, mitigation, remediation and communication**.
    - 風險和與安全相關的問題代表著企業和信息安全領域持續關注的問題。評估和分析風險應該是任何組織中持續而全面的工作。作為組織安全團隊的成員，您將通過風險評估、分析、緩解、修復和溝通來進行工作。
- **Risk** is a measure of the extent to which an entity is threatened by a **potential** circumstance or event. It is often expressed as a combination of: 風險 是衡量一個實體受到潛在情況或事件威脅程度的度量。通常以以下幾個方面的組合來表示：
    - the **adverse impacts that would arise if the circumstance or event occurs**, and
        - 如果發生該情況或事件，所產生的不良影響。
    - the **likelihood** of occurrence.
        - 發生的**可能性**
- Information security risk reflects the potential adverse impacts that result from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems. This definition represents that **risk is associated with threats, impact and likelihood**, and it also indicates that IT risk is a subset of business risk.
    - 信息安全風險反映了未經授權的訪問、使用、披露、干擾、修改或破壞信息和/或信息系統可能導致的潛在不良影響。這個定義表明，風險與威脅、影響和可能性相關，並且指出IT風險是業務風險的一個子集。
- Matrix: Probability X Impact generates four possible combinations: 矩陣：概率 X 影響生成四種可能的組合：
    - 1. low probability, low impact
        - 低概率，低影響
    - 2. low probability, high impact
        - 低概率，高影響
    - 3. high probability, low impact
        - 高概率，低影響
    - 4. high probability, high impact
        - 高概率，高影響

Risk Management Terminology 風險管理術語

- **An asset** is something in need of protection because it has value to the organization. It could be a tangible asset or intangible, such as information.
    - 資產是指需要保護的東西，因為它對組織具有價值。它可以是有形的資產或無形的，例如信息。
- **A vulnerability** is a gap or weakness in an organization's protection of its valuable assets, including information. (NIST SP 800-30). A vulnerability is an inherent weakness or flaw in a system or

component, which, if triggered or acted upon, could cause a risk event to occur. An organization's security team strives to decrease its vulnerability. To do so, **they view their organization with the eyes of the threat actor**, asking themselves, **"Why would we be an attractive target?"** The answers might provide steps to take that will discourage threat actors, cause them to look elsewhere or simply make it more difficult to launch an attack successfully. **Managing vulnerabilities starts with one simple step: Learn what they are**.

    - 漏洞是指組織在保護其有價值的資產（包括信息）方面存在的缺口或弱點。（NIST SP 800-30）。漏洞是系統或組件中的固有弱點或缺陷，如果被觸發或利用，可能導致風險事件發生。組織的安全團隊致力於降低其漏洞性。為此，他們以威脅角色的視角來看待自己的組織，自問："為什麼我們會成為一個有吸引力的目標？"答案可能提供相應的措施，以阻止威脅角色，讓他們轉向其他目標，或者僅僅使成功發起攻擊變得更加困難。管理漏洞始於一個簡單的步驟：了解它們是什麼。

- **A threat** is something or someone that aims to exploit a vulnerability to gain unauthorized access. A threat is a person or thing that takes action to exploit (or make use of) a target organization's system vulnerabilities, as part of achieving or furthering its goal or objectives.

    - 威脅是指旨在利用漏洞獲取未經授權訪問的事物或人。威脅是指針對目標組織的系統漏洞進行行動以實現或推進其目標或目的的人或物。

- Likelihood, when determining an organization's vulnerabilities, the security team will consider **the probability**, or likelihood , of **a potential vulnerability being exploited within the construct of the organization's threat environment**. **Likelihood of occurrence is a weighted factor based on a subjective analysis of the probability that a given threat or set of threats is capable of exploiting a given vulnerability or set of vulnerabilities.**

    - 在確定組織的漏洞時，安全團隊將考慮組織的威脅環境中，潛在漏洞被利用的概率或可能性。發生的可能性是基於主觀分析的權衡因素，評估給定的威脅或一組威脅能否利用給定的漏洞或一組漏洞。

- Finally, the security team will consider the likely results if a threat is realized and an event occurs. Impact is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

    - 最後，安全團隊將考慮如果威脅實現並發生事件，可能的後果。影響是指由於未經授權的信息披露、未經授權的信息修改、未經授權的信息破壞或信息或信息系統可用性損失所預期產生的損害程度。

- Think about the impact and the chain of reaction that can result when an event occurs by revisiting the pickpocket scenario: **Risk comes from the intersection of those three concepts**.

    - 想像一下事件發生時可能產生的影響和連鎖反應，重新思考扒手的情境：風險源於這三個概念的交集。

Risk Identification 風險識別

- In the world of cyber, **identifying risks is not a one-and-done activity**. It's a recurring process of identifying different possible risks, characterizing them and then estimating their potential for

disrupting the organization.

    - 在網絡世界中，識別風險不是一次性的活動。這是一個循環過程，涉及識別不同的可能風險，對其進行特徵描述，然後估計其對組織的潛在擾亂程度。

- Takeaways to remember about risk identification: 關於風險識別要記住的要點：

    - Identify risk to communicate it clearly.
        - 識別風險以清楚地傳達它。
    - Employees at all levels of the organization are responsible for identifying risk.
        - 組織各級員工都有責任識別風險。
    - Identify risk to protect against it.
        - 識別風險以防範它。

- As a security professional, you are likely to assist in risk assessment at a system level, focusing **on process, control, monitoring or incident response and recovery activities**. If you're working with a smaller organization, or one that lacks any kind of risk management and mitigation plan and program, you might have the opportunity to help fill that planning void.

    - 作為一名安全專業人員，你可能會在系統層面上協助進行風險評估，重點是處理流程、控制、監控或事件響應和恢復等活動。如果你在一家較小的組織工作，或者該組織缺乏任何形式的風險管理和減輕計劃，你可能有機會幫助填補這一規劃上的空白。

Risk Assessment 風險評估

- Risk assessment is defined as **the process of identifying**, **estimating and prioritizing risks to an organization's operations** (including its mission, functions, image and reputation), **assets**, **individuals**, **other organizations and even the nation**. Risk assessment should result in aligning (or associating) **each identified risk resulting from the operation of an information system with the goals, objectives, assets or processes that the organization uses, which in turn aligns with or directly supports achieving the organization's goals and objectives**. A risk assessment can prioritize items for management to determine the method of mitigation that best suits the assets being protected. The result of the risk assessment process is **often documented as a report or presentation given to management for their use in prioritizing the identified risk(s)**. This report is provided to management for review and approval. In some cases, management may indicate a need for a more in-depth or detailed risk assessment performed by internal or external resources.
    - 風險評估被定義為「識別、估計和優先考量對組織運作（包括其使命、功能、形象和聲譽）、資產、個人、其他組織甚至國家的風險的過程」。風險評估應該將由信息系統運營產生的每個已識別風險與組織使用的目標、目標、資產或流程相關聯，從而與或直接支持實現組織的目標和目標相一致。風險評估可以優先考慮項目，以便管理層確定最適合保護資產的減輕方法。風險評估過程的結果通常被記錄為報告或提交給管理層使用來優先考量已識別的風險。此報告將提交給管理層審查和批准。在某些情況下，管理層可能會表示需要由內部或外部資源進行更深入或詳細的風險評估。

Risk Treatment 風險處理

- Risk treatment relates **to making decisions about the best actions to take regarding the identified and prioritized risk**. The decisions made are dependent on the attitude of management

toward risk and the availability—and cost—of risk mitigation. The options commonly used to respond to risk are:

    - 風險處理涉及「對已識別並進行優先考量的風險做出最佳行動決策」。所做的決策取決於管理層對風險的態度以及風險減輕的可用性和成本。常用的應對風險的選項有：

- Avoidance: **It is the decision to attempt to eliminate the risk entirely**. This could include ceasing operation for some or all of the activities of the organization that are exposed to a particular risk. **Organization leadership may choose risk avoidance when the potential impact of a given risk is too high or if the likelihood of the risk being realized is simply too great**.

    - 避免：這是試圖完全消除風險的決策。這可能包括停止組織中某些或全部與特定風險相關的活動。當特定風險的潛在影響過大或風險實現的可能性極高時，組織的領導層可能會選擇避免風險。

- Acceptance: Risk acceptance is taking **no action to reduce the likelihood of a risk occurring**. Management may opt for conducting the business function that is associated with the risk **without any further action on the part of the organization**, either because the impact or likelihood of occurrence is negligible, or because the benefit is more than enough to offset that risk.

    - 接受：風險接受是不採取任何行動減少風險發生的可能性。管理層可能選擇在風險相關的業務功能上不進一步採取組織方面的行動，無論是因為影響或發生的可能性微不足道，或者因為效益足以彌補風險。

- Mitigation: Risk mitigation **is the most common type of risk management and includes taking actions to prevent or reduce the possibility of a risk event or its impact**. Mitigation can involve **remediation measures**, **or controls**, **such as security controls, establishing policies, procedures, and standards to minimize adverse risk**. Risk cannot always be mitigated, but mitigations such as safety measures should always be in place.

    - 緩解：風險緩解是最常見的風險管理類型，包括採取行動以防止或減少風險事件或其影響的可能性。緩解可以涉及糾正措施或控制措施，例如安全控制、建立政策、程序和標準，以最小化不利風險。風險不總是可以緩解，但應始終建立緩解措施，例如安全措施。

- Transfer: **Risk transference is the practice of passing the risk to another party**, who will accept the financial impact of the harm resulting from a risk being realized in exchange for payment. Typically, this is an insurance policy.

    - 轉移：風險轉移是將風險轉移給另一方的做法，該方將接受風險實現所產生的損害的財務影響，以換取支付。通常，這是指保險政策。

Base Concepts 基本概念

- Mitigation: Taking action to prevent or reduce the impact of an event
    - 減輕：採取行動以防止或減少事件的影響。
- Acceptance: Ignoring the risks and continuing risky activities
    - 接受：忽略風險並繼續進行冒險的活動。
- Avoidance: Ceasing the risky activity to remove the likelihood that an event will occur
    - 避免：停止冒險活動以消除事件發生的可能性。
- Vulnerability: An inherent weakness or flaw

    - 弱點：一個內在的弱點或缺陷。
- Asset: Something of value that is owned by an organization, including physical hardware and intellectual property
    - 資產：組織擁有的具有價值的事物，包括實體硬體和智慧財產。
- Threat: A person or an entity that deliberately takes actions to exploit a target
    - 威脅：有意針對目標進行行動以獲取利益的個人或實體。
- Transference: Passing risk to a third party
    - 轉移：將風險轉移給第三方。

Risk Priorities 風險優先級

- When risks have been identified, it is time to prioritize and analyze core risks through qualitative risk analysis and/or quantitative risk analysis. This is necessary to determine **root cause and narrow down apparent risks and core risks**. Security professionals work with their teams to conduct both qualitative and quantitative analysis.

    - 當風險被確定後，就是時候進行定性風險分析和/或定量風險分析，以優先考慮和分析核心風險。這是為了確定根本原因並縮小明顯風險和核心風險。安全專業人員與他們的團隊合作進行定性和定量分析。

- Understanding the organization's overall mission and the functions that support the mission helps **to place risks in context**, **determine the root causes and prioritize the assessment and analysis of these items**. In most cases, management will provide direction for using the findings of the risk assessment to determine a prioritized set of risk-response actions.

    - 了解組織的整體使命和支持使命的功能有助於將風險放入其背景中，確定根本原因並優先考慮評估和分析這些事項。在大多數情況下，管理層將提供指導，以利用風險評估的結果來確定一組有優先順序的風險應對措施。

- One effective method to prioritize risk is to use **a risk matrix**, which helps identify priority **as the intersection of likelihood of occurrence and impact**. It also gives the team a common language to use with management when determining the final priorities. For example, a low likelihood and a low impact might result in a low priority, while an incident with a high likelihood and high impact will result in a high priority. Assignment of priority may relate to business priorities, the cost of mitigating a risk or the potential for loss if an incident occurs.

    - 一種有效的優先考慮風險的方法是使用風險矩陣，它有助於將優先順序確定為發生可能性和影響的交集。它還為團隊在確定最終優先順序時與管理層使用共同的語言。例如，低發生可能性和低影響可能導致低優先順序，而高發生可能性和高影響的事件將導致高優先順序。優先順序的分配可能與業務優先事項、降低風險的成本或發生事件時的潛在損失相關。

Decision Making Based on Risk Priorities 基於風險優先級的決策

- When making decisions based on risk priorities, organizations must evaluate the likelihood and impact of the risk as well as their tolerance for different sorts of risk. **A company in Hawaii is more concerned about the risk of volcanic eruptions than a company in Chicago, but the Chicago company will have to plan for blizzards**. In those cases, determining risk tolerance is up to the executive management and board of directors. If a company chooses to ignore or accept risk, exposing workers to asbestos, for example, it puts the company in a position of tremendous liability.

- 在基於風險優先順序做出決策時，組織必須評估風險的發生可能性和影響，以及對不同風險類型的容忍度。例如，夏威夷的一家公司更關注火山爆發的風險，而芝加哥的一家公司則需要計劃暴風雪的風險。在這些情況下，確定風險容忍度由執行管理層和董事會負責。如果一家公司選擇忽視或接受風險，例如讓工人接觸石棉，這將使該公司面臨巨大的法律責任。

Risk Tolerance 風險承受能力

- The perception management takes toward risk is often likened to the **entity's appetite for risk**. **How much risk are they willing to take?** Does management welcome risk or want to avoid it? The level of risk tolerance varies across organizations, and even internally: Different departments may have different attitudes toward what is acceptable or unacceptable risk.
    - 管理層對風險的看法通常被比作實體的風險接受程度。他們願意承擔多少風險？管理層是否歡迎風險或希望避免風險？風險容忍度的水平因組織而異，甚至在內部也有差異：不同部門對可接受或不可接受的風險可能有不同的態度。
- Understanding the organization and senior management's attitude toward risk is usually the starting point for getting management to take action regarding risks. Executive management and/or the Board of Directors determines what is an acceptable level of risk for the organization. Security professionals aim to maintain the levels of risk within management's limit of risk tolerance.
    - 了解組織和高級管理層對風險的態度通常是促使管理層針對風險採取行動的起點。執行管理層和/或董事會確定組織所能接受的風險水平。安全專業人員的目標是在管理層風險容忍度的限制範圍內維持風險水平。
- Often, risk tolerance is dictated by geographic location. For example, companies in Iceland plan for the risks that nearby volcanoes impose on their business. Companies that are outside the projected path of a lava flow will be at a lower risk than those directly in the path's flow. Similarly, the likelihood of a power outage affecting the data center is a real threat in all areas of the world. In areas where thunderstorms are common, power outages may occur more than once a month, while other areas may only experience one or two power outages annually. Calculating the downtime that is likely to occur with varying lengths of downtime will help to define a company's risk tolerance. If a company has a low tolerance of the risk of downtime, they are more likely to invest in a generator to power critical systems. A company with an even lower tolerance for downtime will invest in multiple generators with multiple fuel sources to provide a higher level of assurance that the power will not fail.
    - 通常，風險容忍度是由地理位置所決定的。例如，冰島的公司會規劃附近火山對他們業務所帶來的風險。位於熔岩流預計路徑之外的公司風險較低，而直接位於路徑流動區域內的公司風險較高。同樣，停電對資料中心的影響在全球各地都是一個真實的威脅。在雷雨頻繁的地區，停電可能每月發生一次以上，而其他地區則可能每年只發生一到兩次停電。根據不同的停電時間長度來計算可能發生的停機時間，有助於界定公司的風險容忍度。如果公司對停機風險容忍度較低，他們更有可能投資於發電機來為關鍵系統提供電力。對於對停機容忍度要求更低的公司，他們將投資於多個發電機和多種燃料來源，以提供更高的保證電力不會中斷。

Module 3 Understand Security Control 了解安全控制

Domain D1.3.1, D1.3.2, D1.3.3

What are security controls? (FIBS PUB 199) 什麼是安全控制？

- Security controls pertain to the **physical**, **technical** and **administrative mechanisms** that act as **safeguards or countermeasures prescribed for an information system to protect the confidentiality**, **integrity and availability of the system and its information**. The implementation of controls should **reduce risk**, hopefully to an acceptable level.
    - 安全控制涉及對信息系統採取的物理、技術和行政機制，作為系統和其信息的保密性、完整性和可用性的防護措施或對策。控制的實施應該能夠減少風險，希望能達到一個可接受的水平。
- Physical control: it addresses process-based security needs using **physical hardware devices**, such as **badge readers**, **architectural features of buildings and facilities**, **and specific security actions to be taken by people**. They typically provide ways of controlling, directing or preventing the movement of people and equipment throughout a specific physical location, such as an office suite, factory or other facility. **Physical controls also provide protection and control over entry onto the land surrounding the buildings**, **parking lots or other areas that are within the organization's control**. In most situations, physical controls are supported by technical controls as a means of incorporating them into an overall security system.
    - 物理控制：它使用物理硬體設備，例如識別卡閱讀器、建築物和設施的結構特徵以及人員需執行的特定安全措施，來應對基於流程的安全需求。這些控制通常提供了在特定物理位置（例如辦公套間、工廠或其他設施）中控制、指導或防止人員和設備移動的方式。物理控制還提供了對建築周圍土地、停車場或其他在組織控制範圍內的區域進行進入的保護和控制。在大多數情況下，物理控制作為一種手段，通常與技術控制相互支援，以將它們納入整體安全系統。
- Technical control: it (also called logical controls) is security controls that **computer systems and networks directly implement**. These controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations and support security requirements for applications and data. Technical controls can be configuration settings or parameters stored as data, managed through a software graphical user interface (GUI), or they can be hardware settings done with switches, jumper plugs or other means. However, the implementation of technical controls always requires significant operational considerations and should be consistent with the management of security within the organization. Many of these will be examined in more depth as we look at them in later sections in this chapter and in subsequent chapters.
    - 技術控制（也稱為邏輯控制）：這些是由計算機系統和網路直接實施的安全控制。這些控制可以提供自動化的保護，以防止未經授權的訪問或濫用，促進檢測安全違規行為，並支援應用程序和數據的安全要求。技術控制可以是存儲為數據的配置設置或參數，通過軟件圖形用戶界面（GUI）進行管理，或者可以通過開關、跳線塞或其他方式進行硬件設置。然而，實施技術控制始終需要進行重要的操作考慮，並應與組織內的安全管理保持一致。在本章的後續部分和後續章節中，我們將更深入地研究這些技術控制。
- Administrative control: it (also known as managerial controls) is **directives**, **guidelines** or **advisories aimed at the people within the organization**. They provide frameworks, constraints and standards for human behavior, and should cover the entire scope of the organization's activities and its interactions with external parties and stakeholders. It is vitally important to realize that administrative controls **can and should be powerful, effective tools for achieving information security**. Even the simplest security awareness policies can be an effective control, if you can help the organization fully implement them through systematic training and practice. Many organizations are improving their

overall security posture by integrating their administrative controls into the task-level activities and operational decision processes that their workforce uses throughout the day. This can be done by providing them as in-context ready reference and advisory resources, or by linking them directly into training activities. These and other techniques bring the policies to a more neutral level and away from the decision-making of only the senior executives. It also makes them immediate, useful and operational on a daily and per-task basis.

    - 管理控制（也稱為管理控制）：這些是針對組織內部人員的指示、指南或建議。它們為人類行為提供框架、約束和標準，應覆蓋組織活動的整個範圍以及與外部方和利益相關者的互動。重要的是要意識到，管理控制可以且應該成為實現信息安全的強大、有效的工具。即使是最簡單的安全意識政策，如果您能通過系統性的培訓和實踐幫助組織全面實施它們，也可以成為有效的控制措施。許多組織通過將管理控制納入到員工日常使用的任務級活動和運營決策過程中，提升了整體安全狀態。這可以通過提供上下文相關的參考和建議資源，或直接將其與培訓活動相鏈接來實現。這些和其他技術使政策達到了更中立的水平，遠離僅由高級執行人員作出的決策。它還使它們在每天和每個任務的基礎上成為即時、有用和可操作的。

- Some examples:

    - Administrative: acceptable use policy, emergency operations procedures, employee awareness training
        - 管理控制：可接受使用政策、緊急操作程序、員工意識培訓。
    - Physical: Badge reader, stop sign in parking lot, door lock
        - 實體控制：識別證閱讀器、停車場停止標誌、門鎖。
    - Technical: access control list
        - 技術：訪問控制列表

Module 4 Understand Governance and Elements and Process 了解治理、要素和流程

Domain D1.5.1, D1.5.2, D1.5.3, D1.5.4

Governance Elements 治理要素

- When leaders and management implement the systems and structures that the organization will use to achieve its goals, they are **guided by laws and regulations created by governments to enact public policy**. **Laws and regulations guide the development of standards, which cultivate policies, which result in procedures**.

    - 當領導者和管理層實施組織將用來實現其目標的系統和結構時，他們**受政府制定的法律和法規的指導，以製定公共政策。 法律法規引導制定標準，制定政策，制定程序。**

- **Procedures** are the detailed steps to complete a task that support departmental or organizational policies.

    - **程序**是完成支持部門或組織政策的任務的詳細步驟。

- **Policies** are put in place by organizational governance, such as executive management, to provide guidance in all activities to ensure that the organization supports industry standards and regulations.

    - **政策**由組織治理（例如執行管理）制定，以在所有活動中提供指導，以確保組織支持行業標準和法規。

- **Standards** are often used by governance teams to provide a framework to introduce policies and procedures in support of regulations.
    - **標準**經常被治理團隊用來提供一個框架來引入支持法規的政策和程序。
- **Regulations** are commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for noncompliance.
    - **法規**通常以法律的形式發布，通常來自政府（不要與治理混淆），並且通常會對違規行為進行經濟處罰。
- Regulations -> Standards -> Policies -> Procedures
    - 法規 -> 標準 -> 政策 -> 程序

Module 5 Understand (ISC)² Code of Ethics 了解 (ISC)² 道德規範