資訊資產盤點

**資訊資產定義與分類**

* 資訊資產定義
  + 資訊資產：任何與「資訊」及其處理、儲存或傳輸流程有直接關聯，並且對組織具有價值或影響的事物，包括有形（例如：硬體、文件）和無形（例如：軟體、資料）。
    - 備註：此處的「無形」並非嚴格按照會計定義，而是指非實體的資訊本身，例如軟體的功能與授權、資料的內容與價值，而非其儲存媒介。
* 資訊資產盤點的目的
  + 掌握資產現況：
    - 了解組織擁有什麼資訊資產。
    - 知道這些資產在哪裡、由誰負責。
    - 資產目前的狀態（例如：是否正常運作、是否需要更新）。
  + 風險評估與管理：
    - 識別潛在的資訊安全風險。
    - 評估風險發生的可能性和影響。
    - 採取適當的控制措施來降低風險。
  + 資源最佳化：
    - 避免資源閒置或重複投資。
    - 確保資源被有效利用。
    - 為未來的採購和規劃提供依據。
  + 合規性：
    - 確保符合相關法規和標準（例如：個人資料法、ISO 27001）。
    - 證明組織已盡到保護資訊資產的責任。
  + 支援決策：
    - 為資訊安全策略、預算編列提供參考。
    - 協助評估資訊安全投資的效益。
* 資訊資產盤點時機：
  + 定期盤點：通常每年至少一次，以確保資訊的準確性。
  + 重大變更：
    - 新系統上線
    - 組織架構調整
    - 重大資安事件發生後
* 資訊資產分類
* 分類方式並無一定標準，可依公司需求調整。一般常見分類如下：
* 人員資產
* 全職員工
* 駐點人員
* 工讀生
* 委外廠商人員
* 通訊設備
* 網路設備（如路由器、交換器）
* 電話系統
* 伺服器通訊模組
* 軟體資產
* 作業系統
* 應用程式
* 套裝軟體
* 資料庫管理系統
* 硬體資產
* 電腦（桌機、筆電）
* 伺服器
* 儲存設備（如硬碟、磁帶機）
* 印表機、掃描器
* 文件資產
* 紙本文件
* 公文
* 合約
* 列印表單
* 資料資產
* 資料庫
* 資料集
* 資料分析報表
* 環境資產
* 電力供應系統
* 空調系統
* 消防設備
* 門禁系統
* 非資訊資產：辦公室桌椅等固定資產，雖然對組織運作有價值，但不直接涉及資訊處理，因此通常不列入資訊資產盤點。

**資訊盤點內容 - 基本識別資訊**

* 資產名稱：清楚描述資產的名稱。
* 資產類型：歸類到上述的七大類之一。
* 資產標籤：例如資產編號、條碼，便於追蹤。
* 位置資訊：資產存放地點或使用位置。
* 權責單位：
  + 資產擁有者 (Asset Owner)：通常是部門主管，負責資產的整體管理。
  + 資產保管者 (Asset Custodian)：負責資產的日常保管與維護。
  + 資產使用者 (Asset User)：實際使用資產的人員。
* 案例：資訊處採購讀卡機簽屬公文使用。
  + 資產擁有者：資訊處主管
    - 理由：由資訊處統一採購、管理、維護讀卡機，並對其可用性負責。
  + 資產保管者：資訊處設備管理人員
    - 理由：負責讀卡機的入庫、保管、發放、追蹤、報廢等作業。
  + 資產使用者：資訊處部門需要使用讀卡機的員工
    - 理由：向資訊處設備管理人員申請借用或領用讀卡機，並在工作上實際使用。
* 資訊資產價值評估
* 根據資產的「機密性、完整性、可用性 (CIA)」和「法規遵循」進行分級，並以四者中的最高分作為該資產的綜合價值。
* 機密性 (Confidentiality) 評級：
  + 分析未授權存取或洩漏的風險和影響。
  + 例如：客戶資料、財務報表屬於高度機密。
* 完整性 (Integrity) 評級：
  + 評估資料被未經授權修改或破壞的風險。
  + 例如：交易紀錄、醫療紀錄的完整性非常重要。
* 可用性 (Availability) 評級：
  + 評估系統或服務中斷對業務運作的影響。
  + 例如：線上交易系統、生產線控制系統需要高度可用性。
* 法規遵循 (Compliance) 評級：
  + 評估是否符合相關法律、法規或合約要求。
  + 例如：個資保護法、支付卡產業資料安全標準 (PCI DSS)。
* 範例：



**資料處理分級**

* 資料分級方式並無一定標準，可依公司需求調整。一般常見分級如下：
* 公開資料 (Public)：
  + 可對外公開，無需特別保護。
  + 例如：公司年報、產品公開規格。
* 內部資料 (Internal)：
  + 僅限公司內部使用，需避免非授權存取。
  + 例如：內部會議記錄、部門工作報告。
* 敏感資料 (Sensitive)：
  + 外洩可能對組織造成聲譽、財務或營運上的損害。
  + 例如：人事資料、客戶合約、薪資資料。
* 機密資料 (Confidential)：
  + 具有高度機密性，僅限特定授權人員存取。
  + 例如：財務報表、策略計劃、研發中的技術文件或可口可樂的配方。

**資料處理角色與責任**

* 資料所有者 (Data Owner)：
* 通常是部門主管或業務負責人。
* 責任：
  + 負責資料的盤點、分類和分級。
  + 制定資料的存取控制策略。
  + 確保資料受到適當的保護。
* 資料保管者 (Data Custodian)：
* 通常是IT部門或系統管理人員。
* 責任：
  + 負責資料的儲存、備份和安全維護。
  + 執行資料所有者制定的安全控制措施。
  + 確保資料的可用性和完整性。
* 資料使用者 (Data User)：
* 所有需要存取和使用資料的人員。
* 責任：
  + 遵守資料使用規定。
  + 在授權範圍內合理使用資料。
  + 不得擅自複製、洩漏或修改資料。
* 範例：人資系統
  + 資料所有者 (Data Owner)：人資部門主管
  + 責任：
    - 定義人資系統中的資料範圍（員工個資、薪資、考績等）。
    - 將資料分級（例如：薪資為機密資料）。
    - 設定存取權限（例如：員工僅能看自己的資料，主管可看部門員工資料）。
  + 資料保管者 (Data Custodian)：資訊處系統管理員
  + 責任：
    - 負責人資系統的穩定運行與資料備份。
    - 執行人資主管設定的權限，確保資料安全。
    - 定期進行系統安全更新與漏洞修補。
  + 資料使用者 (Data User)：全體員工（依職責有不同權限）
  + 責任：
    - 依權限使用人資系統（例如：員工只能申請自己的假單、主管審核假單）。
    - 妥善保管帳號密碼，不得洩漏或借給他人。
    - 不得未經授權存取、修改或下載資料。

**考古題**

14. 僅就資訊資產管理作業必須考慮的諸多因素中，下列敘述何者錯誤？

(A) 資訊資產分類

(B) 資產盤點

(C) 資訊資產分級

(D) 安全控制措施

管理 113-2 答案D

(安全控制措施要等風險評鑑才施行)

15. 下列何者「不」屬於資訊資產清冊可用來支援的項目？

(A) 風險管理

(B) 稽核活動

(C) 事故回應

(D) 財產報廢

管理 113-2 答案D

(資訊資產不一定跟財產資產相同，比方說辦公室桌椅)

16. 在建立資訊資產分級政策時，若某資產分類的依據是依其「對企業的營運影響」，下列何者較「不」屬於影響考量？

(A) 資產損失對公司聲譽的影響

(B) 該資產對企業盈利能力的潛在影響

(C) 資訊資產外洩對合作夥伴的潛在影響

(D) 資產所需的技術維護成本

管理 113-2 答案D

(依據是對公司營運的影響，而非資產本身或維護的價值)

17. 針對資訊資產的盤點，下列何項資訊資產「不」須列入盤點？

(A) 虛擬資產：如虛擬機器、雲端伺服器等

(B) 久未使用但仍在線上的資料庫

(C) 公司徵才公告

(D) 員工用於工作的平板電腦

管理 113-2 答案C

(徵才公告跟資訊資產無關)

18. 進行資訊資產分類時，｢加密系統作業管理程序」通常會歸在下列四項中的何項類別？

(A) 硬體

(B) 環境

(C) 文件

(D) 軟體

管理 113-2 答案C

(程序是屬於文件類)

19. 在定期進行資訊資產盤點的過程中，發現有些資產未被列入資產清單。這可能對資產管理有何直接影響？

(A) 資產的風險評估無法準確進行

(B) 資產的可用性可能會受到影響

(C) 資產的所有者無法進行適當的存取控制

(D) 資產將喪失機密性

管理 113-2 答案A

(資訊資產盤點的目的是要提供保護，未列入會導致風險評估無法準確進行)

20. 某公司在進行資訊資產分級時，發現部分資產被多個業務部門使用，不同部門對該資產的重要性評估存在差異。為了確保這類跨部門資產能夠被有效管理，應採用下列何項措施最為適當？

(A) 每個部門獨立分級，根據各部門的需求各自進行保護

(B) 跨部門共享的所有資產，一律採用最高安全等級進行保護

(C) 透過跨部門協調達成共識，將資產設定為中等安全級別

(D) 從有評估的部門中，選擇最高安全等級進行管理

管理 113-2 答案D

(當資訊資產跨多個業務部門共享，而各部門對資產重要性的評估存在差異時，為了確保資產得到充分保護，應該採用風險最保守的做法，也就是從所有評估中選擇最高的安全等級進行管理。這樣可以避免因低評估而導致資產保護不足，從而引發風險。因此，答案為 (D)。)

2. 下列何項是最有可能把資料被歸類為「機密」等級的情境？

(A) 公司員工皆可訪問的內部通訊錄 (內部)

(B) 供應商提供查閱的產品目錄 (公開)

(C) 客戶資料中儲存的信用卡號碼

(D) 公司對外公開發布的新聞稿 (公開)

管理 113-1 答案C

(客戶資料中儲存的信用卡號碼為個人資料須妥善保護)

15. 關於實施資訊資產盤點作業必須考慮的諸多因素中，下列敘

述何者錯誤？

(A) 資訊資產的價值

(B) 資訊資產的名稱

(C) 資訊資產的存放位置

(D) 資訊資產的風險 (盤點重點在資產的名稱、位置與價值，風險非盤點主要因素)

管理 113-1 答案D

16. 資訊資產分類分級的目的為下列何項？

(A) 增加資產價值

(B) 管理資產風險 (分級的目的是協助管理資產風險，因此下一步舊式風險評鑑)

(C) 提高資產可用性

(D) 降低資產建置成本

管理 113-1 答案B

17. 關於實施「資訊分類」作業主要目的之敘述，下列何者最為適切？

(A) 防止儲存在媒體的資訊被經授權的移除

(B) 防止儲存在媒體的資訊被經授權的揭露

(C) 確保組織重要的資訊受到適切等級的保護 (分類的目的是確保重要資訊受到適切保護)

(D) 確保公開的資訊受到適切等級的保護

管理 113-1 答案C

18. 關於紙本類之資訊資產保護原則，下列敘述何者最「不」適切？

(A) 內部使用級之紙本類資訊資產，於保管人員暫時離開座位時，不得置於開放空間處

(B) 內部使用級之紙本類資訊資產，於保管人員長時間離開座位時，應放置於上鎖空間或上鎖櫃並隨時上鎖

(C) 密級之紙本類資訊資產，於保管人員暫時離開座位時，得置於開放空間處 (密級紙本資料不得放置於開放空間，即使暫時離開座位也不可以)

(D) 密級之紙本類資訊資產，於保管人員進出上鎖空間或借用上鎖櫃之鑰匙時應作成紀錄

管理 113-1 答案C

19. 盤點資訊資產時，最可能是使用下列何項分級的基本原則？

(A) 資產的物理大小

(B) 採購成本和效益

(C) 資產外觀的可愛程度

(D) 重要性和敏感性 (分級應根據資產的重要性與敏感性)

管理 113-1 答案D

20. 若公司機密等級區分為四個等級：極機密、機密、內部使用、一般。有一份資料僅供公司同仁使用、查閱，亦不須加密。請問這份資料歸類於下列何項機密等級最為合適？

(A) 極機密

(B) 機密

(C) 內部使用 (僅供同仁使用且無需加密的資料應歸類為內部使用)

(D) 一般

管理 113-1 答案C

14. 資訊資產盤點的主要目的為下列何項？

(A) 銷售資訊資產

(B) 識別和管理資訊資產 (盤點的主要目的是識別並管理資訊資產)

(C) 清除資訊資產

(D) 增加資訊資產價值

管理 112-2 答案B

15. 對於資訊資產盤點的敘述， 下列何者較正確？

(A) 只在資產報廢時進行

(B) 定期進行 (資訊資產盤點應定期進行，或是重大變更例如新系統上線，以確保資訊資產管理的資訊是最新且準確的)

(C) 只在資產設備更新時進行

(D) 不必定期進行

管理 112-2 答案B

16. 關於資訊資產評價與分類的描述，下列何者較正確？

(A) 資產價值評估以機密性最為重要 (資產價值評估應同時考慮機密性、完整性和可用性三個面向，例如醫院的可用性可能更重要)

(B) 資產的分級主要為了便於釐清資產的重要性

(C) 資產的評價以人員資產為主 (資訊資產包含多種類型：硬體、軟體、資料、文件、人員、環境等)

(D) 使用的服務無需列入資訊資產 (包括網路服務、雲端服務、外包服務等都應該納入資產管理範圍)

管理 112-2 答案B

17. 關於資訊資產分類的目的，下列敘述何者較正確？

(A) 確認資訊資產的價值

(B) 確認資訊資產的類型 (資產分類的目的在於確認資訊資產的類型，以便後續管理。)

(C) 確認資訊資產的風險

(D) 確認資訊資產的擁有者

管理 112-2 答案B

18. 關於資訊資產的分類描述，下列何者錯誤？

(A) 人員可以是全體同仁、駐點人員與工讀生，委外廠商人員不屬於組織人員故不列入

(B) 軟體應包括作業系統 、 應用系統程式、套裝軟體等

(C) 文件應該包括所有紙本形式存在的文書資料，包含公文與列印的表單

(D) 環境資產可包含電力與消防設施等

管理 112-2 答案A

(委外廠商人員雖然不是正式員工，但他們可能接觸組織的重要資訊資產、參與重要系統的維護和操作、具有系統存取權限、對資訊安全有直接影響，因此委外廠商人員應該納入資訊資產的人員類別進行管理需要透過合約規範其資安責任與義務)

19. 在進行資訊資產分類時，企業資源管理（ERP）系統較適合分類至下列何種資訊資產？

(A) 硬體類資產

(B) 軟體類資產 (ERP 系統屬於軟體類資產，包括應用程式和管理功能)

(C) 服務類資產

(D) 文件類資產

管理 112-2 答案B

20. 進行資訊資產分類時，應分為幾類？

(A) 5類

(B) 6類

(C) 7類

(D) 由各個公司、組織視其環境及運作所需，自行設計資訊資產之分類 (資產分類應依公司運作需求自行設計。)

管理 112-2 答案D

14. 在公司資產管理中，為達成識別組織之資產並定義適切之保護責任，應優先建議採取下列何種控制措施？

(A) 金鑰管理

(B) 懲處過程

(C) 變更管理

(D) 資產盤點 (資產盤點是識別並定義保護責任的首要控制措施。)

管理 112-1 答案D

15. 關於可移除式媒體（如：USB隨身碟），下列敘述何者較「不」適當？

(A) 所有可移除式媒體依製造商的規格要求，儲存於安全的環境

(B) 針對儲存於可移除式媒體上的敏感資料進行加密

(C) 不再需要使用可移除式媒體時，將所儲存的資料徹底移除

(D) 不將可移除式媒體登載於資產清冊上，以減少資料遺失的機會 (可移除式媒體應登載於資產清冊，便於管理和追蹤。)

管理 112-1 答案D

16. 關於紙本類之資訊資產標示原則，下列敘述何者最「不」適當？

(A) 內部使用級之紙本類資訊資產標示原則可為無需標示 (內部使用級資訊資產應標示或有保護措施，無標示不適當。)

(B) 內部使用級之紙本類資訊資產標示原則可為使用不透明卷宗

(C) 密級之紙本類資訊資產標示原則可為文件首頁標明機密等級或使用紅色卷宗

(D) 密級之紙本類資訊資產標示原則可為文件封面標明機密等級或使用紅色卷宗

管理 112-1 答案A

17. 關於資產盤點之程序，下列敘述何者最適當？

(A) 可由組織個別之業務活動流程開始進行盤點 (資產盤點應從業務活動流程開始，確保全面性和關聯性)

(B) 應由資訊類資產開始進行盤點

(C) 應由軟體類資產開始進行盤點

(D) 應由硬體類資產開始進行盤點

管理 112-1 答案A

18. 關於資訊資產盤點作業的描述，下列何者「不」最適當？

(A) 資訊資產盤點即是資訊設備盤點 (資產盤點不僅限於設備，應涵蓋所有類型的資訊資產。)

(B) 資訊資產盤點在確認資產的使用狀況

(C) 資訊資產盤點應考量全面性

(D) 資訊資產盤點應確認資產的可用性

管理 112-1 答案A

19. 關於資產分類分級的敘述，下列何者錯誤？

(A) 建立資訊資產清冊，並定期清查資訊資產

(B) 資訊資產不須指派人員負責管理事宜 (資訊資產必須指派人員負責管理，確保責任明確)

(C) 人員異動或離職前，須確實移交所保管之相關資訊資產

(D) 資訊資產報廢時，應依資產類別循相關安全程序辦理銷毀

管理 112-1 答案B

20. 關於實施「資訊分類」作業主要目的之敘述，下列何者最正確？

(A) 防止儲存在媒體的資訊被經授權的移除

(B) 防止儲存在媒體的資訊被經授權的揭露

(C) 確保組織重要的資訊受到適切等級的保護 (資訊分類的目的是確保重要資訊得到適當等級的保護)

(D) 確保公開的資訊受到適切等級的保護

管理 112-1 答案C

15. 關於實施「資訊分類」作業主要目的之敘述，下列何者最正確？

(A) 防止儲存在媒體的資訊被經授權的移除

(B) 防止儲存在媒體的資訊被經授權的揭露

(C) 確保組織重要的資訊受到適切等級的保護

(D) 確保公開的資訊受到適切等級的保護

管理 111-2 答案C

16. 關於資訊資產控管原則，下列敘述何者正確？

(A) 關鍵系統設備不需建立備援機制 (需要)

(B) 網路設備不用建立備用系統 (要建立)

(C) 個人使用之套裝軟體，其存取權限的賦予，應與使用者的角色與職責相符

(D) 公開資料未經權責主管之授權核可，禁止複製 (公開資料就是給公開瀏覽的，不需要核可)

管理 111-2 答案C

17. 通常資訊類的資產分級，可區分為公開、內部使用以及密級等三種，關於資訊類資產分級為「密級」之敘述，下列何者錯誤？

(A) 若流傳至組織外部，不會對組織造成任何有形或無形的傷害者

(B) 資料外洩可能造成個人與組織之困擾，造成聲譽受損或財務損失者

(C) 含有病例、醫療、基因、性生活、健康檢查及犯罪前科等之個人資料之資訊，僅有經過授權之人員始得存取者

(D) 含有可直接或間接識別特定個人之未公開個人資料

管理 111-2 答案A

(密級就是機密資訊，類似個資，外流會對公司造成影響)

18. 關於紙本類之資訊資產保護原則，下列敘述何者最「不」正確？

(A) 內部使用級之紙本類資訊資產，於保管人員暫時離開座位時，不得置於開放空間處

(B) 內部使用級之紙本類資訊資產，於保管人員長時間離開座位時，應放置於上鎖空間或上鎖櫃並隨時上鎖

(C) 密級之紙本類資訊資產，於保管人員暫時離開座位時，得置於開放空間處 (應放置上鎖空間)

(D) 密級之紙本類資訊資產，於保管人員進出上鎖空間或借用上鎖櫃之鑰匙時應作成紀錄

管理 111-2 答案C

19. 關於資產盤點之執行方式，下列敘述何者最「不」正確？

(A) 所有軟體類資產之盤點可藉由軟體掃描工具來輔助執行

(B) 所有硬體類資產之盤點可藉由軟體掃描工具來輔助執行

(C) 所有資訊類資產之盤點可藉由檔案搜尋工具來輔助執行

(D) 所有人員類資產之盤點可藉由組織架構與業務職掌表來輔助執行

管理 111-2 答案B

(未連網設備、印表機和工控設備無法安裝軟體掃描工具，需搭配人工盤點)

20. 資訊安全管理系統（Information Security Management System, ISMS）中，電力供應是屬於下列何種資產類型？

(A) 服務資產

(B) 資訊資產

(C) 硬體資產

(D) 軟體資產

管理 111-2 答案A

(服務資產就是指電力、環控之類的設備清單)

20. 下列何者為資訊安全資產清冊製作及維持的主要目的？

(A) 方便帳務管理

(B) 適切的保護資產

(C) 對於財產價值的管理

(D) 便於資訊備份

管理 111-1 答案B

(製作資訊安全資產清冊的目的就是為了要適切的保護資產)

23. 在資訊安全管理系統（Information Security Management System, ISMS）中定義並進行資訊資產分級，下列何者最適合納入評估面向？

(A) 資訊資產的變現金額

(B) 資訊資產的折舊

(C) 資訊資產的流動性

(D) 資訊資產的機敏性

管理 111-1 答案D

(資產分級要考量到資訊資產的機密性、完整性、可用性和法遵)

24. 關於資訊資產的分級，下列敘述何者較「不」正確？

(A) 透過資訊資產分級，可讓資產受到適當程度的保護，也可以兼顧

資安執行成本

(B) 依照各類資產所具有之機密性、完整性、可用性對該資產之價值

進行評估

(C) 公司公開教育訓練手冊和主管的電腦檔案，兩者的價值不同，應

投入相同保護資源

(D) 為確保資產被系統性管理，可透過資產編號、條碼等方式來進行

分類標示

管理 111-1 答案C

(機敏性不同應該搭配不同的保護措施和資源)

30. 為了確保資訊依其對組織之重要性，受到適切等級的保護，下列何者「不」為其控制要求？

(A) 資訊之分級

(B) 資訊之標示

(C) 資訊之處置

(D) 資訊之統計

管理 111-1 答案D

40. 關於資產分類分級，下列敘述何者較「不」正確？

(A) 可以依照資訊安全三大指標CIA 進行分類

(B) 大致上可以分為一般、限閱、敏感、機密四種

(C) 分類可以根據各企業組織自行制定自己的分類方式

(D) 資產分類的目的僅是方便識別

管理 111-1 答案D

(目的就是為了要適切的保護資產)

50. 企業網路電路的使用較符合資訊安全管理系統（Information Security Management System, ISMS）的何種資產類型？

(A) 軟體資產

(B) 資訊資產

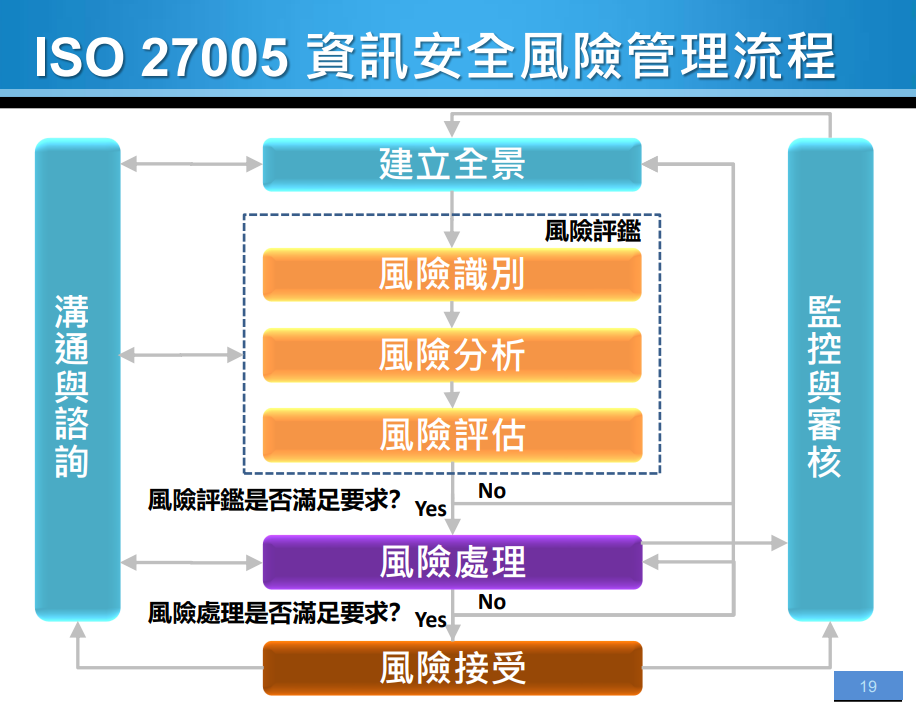
(C) 韌體資產

(D) 服務資產

管理 111-1 答案D

(服務資產為電力、空調、消防設備)

風險管理

****

(資料來源：博創資訊訓練教材，https://tinyurl.com/366byr9m)

**風險管理基礎概念**

* 風險定義
  + 風險 (Risk)：目標的不確定性效應，包含可能的威脅與弱點。
  + 風險要素：
    - 威脅 (Threat) ：主動的，可以發起或觸發威脅事件的「來源或實體」。
      * 自然威脅：地震、洪水、颱風等不可抗力災害。
      * 人為蓄意威脅：駭客攻擊、內部員工惡意破壞、恐怖攻擊。
      * 人為非蓄意威脅：操作失誤、配置疏失、無意洩漏。
    - 弱點 (Vulnerability) ：系統或組織中「被動存在的缺陷」，可能被威脅利用。
      * 技術弱點：程式漏洞 (如SQL注入) 、系統配置錯誤、未更新更新程式。
      * 組織弱點：缺乏安全政策、員工安全意識不足、實體環境保護不足。
    - 威脅事件：威脅來源成功利用弱點後發生的「具體行為或事件」。
      * 駭客 (威脅) 利用未修補的漏洞 (弱點) 植入惡意程式。
    - 影響 (Impact)：威脅事件造成的「直接負面後果」。
      * 技術面：系統停擺、服務中斷。
      * 財務面：修復成本、法律賠償。
      * 商譽面：客戶信任度下降、品牌形象受損。
* 風險管理目的
  + 確定可接受風險範圍。
  + 識別和分析潛在風險。
  + 制定應對策略，降低風險影響。

**風險評鑑過程**

* 風險評鑑包含三個組件：「風險識別」、「風險分析」和「風險評估」。
* 風險識別 (Risk Identification)
  + 確認與資訊資產相關的威脅、弱點和風險事件。
  + 識別項目：
    - 資訊資產 (Asset) ：如硬體、軟體、資料。
    - 威脅 (Threat) ：如駭客攻擊、自然災害。
    - 弱點 (Vulnerability) ：如弱密碼設定。
* 風險分析 (Risk Analysis)
  + 目標：分析風險發生的可能性與影響程度。
  + 分析參考：
    - 主管機關公文來函要求事項
    - 法律法規適用的要求事項
    - 客戶合約的要求
    - 組織本身內部與外部的議題
  + 方法：
    - 定性分析：主觀分類，如「高、中、低」風險。
    - 定量分析：根據歷史資料，計算損失金額或風險分值(可能性 × 影響)。
      * 年度損失預期值 (ALE) = 單一損失預期值 (SLE) \* 年度發生比率 (ARO)，又單一損失預期值 (SLE) = 資產價值 (Asset Value) \* 暴露因素 (Exposure Factor, E.F)
      * 舉例來說，20年才會出現一次的地震，其中「曝露因子」(E.F)=25%、資通系統價值＝ 50萬元。），ALE = 50萬 \* 0.25 \* 1/20 = 6,250 。
* 風險評估 (Risk Evaluation)
  + 目標：將風險值與既定準則 (可接受風險值) 比較。
  + 判斷風險是否可接受，篩選需進一步處理的風險。

**風險處理策略**

* 風險處理方式
  + 風險規避 (Risk Avoidance)：
    - 定義：停止可能引發風險的行動。
    - 例如：停止高風險業務或搬遷不安全之機房。
  + 風險降低 (Risk Reduction)：
    - 定義：採取控制措施，減少風險可能性或影響。
    - 例如：加強防火牆、提升備援能力、補償性措施。
  + 風險轉移 (Risk Transfer)：
    - 定義：將風險移交第三方承擔。
    - 例如：影響高但極少發生的自然災害，購買保險、外包服務。
  + 風險保留 (Risk Retention)：
    - 定義：將損失納入可承受範圍，無額外處置。
    - 例如：低風險、處理成本過高。
* 風險處理流程
  + 制定風險改善計畫。
  + 監控執行進度與成效。
  + 評估殘餘風險 (Residual Risk)，殘餘風險為原始風險經風險處理之後剩下的風險值，需低於公司可接受風險值 (Acceptable Risk) 才可以風險接受。

**綜合範例**

* 風險識別：
  + 風險事件：客戶資料外洩。
  + 簡述：由於公司網站系統存在安全漏洞，或內部人員操作疏失，導致客戶資料被未經授權的第三方存取或洩露。
* 風險分析：
  + 風險來源：
    - 外部威脅：駭客網路攻擊、惡意軟體入侵。
    - 內部威脅：員工疏失操作、內部惡意行為。
    - 系統漏洞：網站程式碼漏洞、伺服器設定不當。
  + 潛在後果：
    - 客戶隱私洩露：客戶個人資料、交易紀錄被洩露。
    - 聲譽損害：客戶對企業信任度降低，品牌形象受損。
    - 法律責任：違反個資法等相關法規，面臨罰款或訴訟。
    - 財務損失：客戶流失、賠償費用、系統修復成本。
  + 現有控制措施：
    - 已安裝防火牆
    - 基本網站安全設定
    - 員工帳號權限管理
* 風險評估
  + 評估方法：我們採用定性風險評分矩陣，依據 「可能性」 與 「嚴重性」兩個維度來評估風險等級。
  + 可能性 (Likelihood) 評分標準：
    - 1 分 - 極低 (幾乎不可能發生)
    - 2 分 - 低 (不太可能發生)
    - 3 分 - 中等 (可能發生)
    - 4 分 - 高 (很可能發生)
    - 5 分 - 極高 (幾乎肯定會發生)
  + 嚴重性 (Severity) 評分標準：
    - 1 分 - 極輕微 (幾乎無影響)
    - 2 分 - 輕微 (可忽略的影響)
    - 3 分 - 中等 (可察覺但可管理的影響)
    - 4 分 - 嚴重 (重大影響，需要積極應對)
    - 5 分 - 極度嚴重 (災難性影響，可能導致組織無法持續運作)
  + 風險評估結果
    - 可能性評估：我們評估「客戶資料外洩」的可能性為4 分 (高)。 理由是線上零售業是駭客常見攻擊目標，且我們目前的安全措施可能仍有不足之處。
    - 嚴重性評估：我們評估「客戶資料外洩」 的嚴重性為 5 分 (極度嚴重)。 因為一旦發生大規模客戶資料外洩，將對我們的聲譽、客戶信任、法律責任造成極度嚴重的負面影響。
  + 風險評分計算
    - 風險評分 = 資產價值 (機密性、完整性、可用性、法遵取最高) x 可能性評分 × 嚴重性評分 = 5分 x 4 分 × 5 分 = 100 分，資產價值是從資產盤點清冊來的。
  + 可接受風險 (Acceptable Risk) 設定
    - 假設我們組織設定的「可接受風險」閾值為：30 分。
    - 簡述：任何風險評分超過 30 分的風險，都視為超出可接受風險範圍，需要立即進行風險處理。
  + 風險評估結果與可接受風險比較：
    - 風險評分 (100 分) > 可接受風險 (30 分)
    - 結論：「客戶資料外洩風險」 超出了我們組織的可接受風險水平，屬於高優先級風險，必須立即進行風險處理。
* 風險處理
  + 簡述**：** 由於風險評估結果超出可接受風險，我們必須制定並執行風險處理計畫，我們採取「風險降低」方式，降低「客戶資料外洩風險」。
  + 風險處理措施
    - 強化網站安全防護：購買網站應用程式防火牆 (WAF)
    - 加強資料存取控制：導入多因素身份驗證
    - 加強資安防護：定期網站滲透測試演練
    - 提升員工資安意識：加強釣魚郵件、社交工程演練
    - 建立資料外洩應變計畫：定期演練應變計畫
* 風險接受
  + 風險處理目標：透過上述控制措施，將「客戶資料外洩風險」的可能性降低到2分和嚴重性降低到2分，使得最終的風險評分(20分)降低到可接受風險(30分)以下。

**風險管理循環**

* 動態管理
  + 風險管理為持續過程，需定期更新並針對重大事件重新評估。
* 循環步驟
  + 全景建立 → 識別風險 → 分析風險 → 評估風險 → 處理風險 → 全程都要監控與溝通。

**補充重要概念**

* 風險擁有者 (Risk Owner)
  + 定義：對特定風險負責的人，確保該風險被適當識別、評估和處理。
  + 主要責任：
    - 核准風險處理計畫與殘餘風險。
    - 監控風險狀況，確保控制措施有效。
  + 範例：
    - 資安風險：資安主管負責。
    - 財務風險：財務經理負責。
    - 供應鏈風險：採購主管負責。
* 風險再評鑑 (Risk Reassessment)
  + 定義：定期或因重大事件重新檢視風險狀態與處理計畫的過程。
  + 目的：確認控制措施持續有效，識別新風險。
  + 時機：
    - 定期檢查（如每三個月）。
    - 重大事件後（如法規變更、供應鏈中斷）。
  + 範例：疫情期間重新評估供應鏈穩定性。
* 風險胃納 (Risk Appetite) 和可接受風險值 (Acceptable Risk Level)
  + 定義**：**
    - 風險胃納 (Risk Appetite)： 組織在追求其目標的過程中，願意接受的風險類型和總體程度。
    - 可接受風險值 (Acceptable Risk Level)： 在具體的風險評鑑中，針對單一風險或特定業務流程設定的風險閾值。
    - 風險偏好(Risk-seeking)和風險趨避(Risk-averse)：不同行業、不同規模、不同發展階段、甚至不同文化背景的組織，都應該有與自身情況相匹配的風險胃納，例如新創公司一般來說都是風險偏好而銀行業通常都是風險趨避，這沒有對錯，風險胃納應該服務於組織的策略目標。
  + 關係：
    - 風險胃納是制定可接受風險值的依據。
    - 可接受風險值是風險胃納的具體體現。
  + 資安考試要點：
    - 兩者高度相關，許多情況下可視為同一個概念的延伸。
    - 可接受風險值是風險胃納在具體風險評估中的應用。

考古題：

27. 關於風險分析與評估之敘述，下列何者最「不」適切？

(A) 公司最好至少每年定期執行一次風險評鑑

(B) 公司營運重大改變時，應進行風險評鑑

(C) 重大風險項目完成風險處理後，不需進行風險再評估

(D) 進行風險分析與評估前，應先了解相關背景資訊（例如：法規要求、技術環境…）

規劃 114-1 答案C

(風險評估是一個持續性的過程，即使是重大風險項目在完成處理後，也需要進行風險再評估，以確保風險控制措施仍然有效，並追蹤是否有新的風險或變化出現。因此，選項 (C) 說明「不需進行風險再評估」是不適切的。)

28. 甲公司因A製程所用之所有機台當機，造成生產線停工、影響產品生產，經公司資安人員分析評估後，確認發生原因為廠商透過USB更新機台應用程式過程控制不當，導致機台程式異常所致。請問下列哪些選項為降低機台程式更新異常的風險緩解（Risk Mitigation）措施？（複選）

(A) 將A製程委外處理 (將A製程委外處理並非直接針對機台程式更新異常的風險緩解措施)

(B) 要求USB使用前，應掃毒確認無異常 (這是一項預防措施，可在更新前確保USB沒有攜帶病毒或惡意軟體，降低更新過程中因感染而導致程式異常的風險)

(C) 要求負責機台之廠商提供保證金，減少公司因此產生可能的營運損失 (要求廠商提供保證金屬於風險轉移或經濟補償措施，不屬於降低程式更新異常風險的技術或作業控制)

(D) 要求機台需分多批次更新程式，每批更新確認安全無誤後，方可進行下一批之更新作業 (透過分批次更新並確認安全，可以及早發現並修正問題，降低一次性大規模更新帶來的風險)

規劃 114-1 答案BD

33. 有關風險處理選項之敘述，下列何項「有誤」？

(A) 風險處理選項一定為相互排斥的

(B) 選擇最適當的風險處理選項應包含達成目標所獲得之潛在利益及實施的成本

(C) 風險處理選項包含承受或增加風險以尋求機會

(D) 風險處理選項包含移除風險來源

規劃 114-1 答案A

(風險處理選項並非必然相互排斥，實際上在面對風險時，常常需要綜合運用多種策略來降低風險。例如，一個組織可能同時採取風險轉移與風險降低的措施來管理單一風險，因此風險處理選項不一定是互斥的。)

34. 針對風險處理的描述，下列何者最「不」適切？

(A) 風險處理計畫的核准，須取得風險擁有者的核准

(B) 風險處理需考量組織所獲得之潛在利益與實施的成本等因素，選擇最適當的風險處理方式

(C) 執行完風險處理後，預計會降低到可接受風險以下，剩餘之資訊安全風險不需要風險擁有者再次的核可

(D) 風險處理可以選取多種方式同時進行

規劃 114-1 答案C

(在風險處理過程中，即使風險處理措施預計會將風險降低到可接受水準以下，剩餘的資訊安全風險仍然需要風險擁有者進行核可與確認。風險處理計畫需由風險擁有者參與並核准，以確保所有殘餘風險均在其可接受範圍內。)

35. 有關如何進行風險處理的描述，下列何者最「不」適切？

(A) 在風險處理的過程中，有可能會需要因為導入的工具，管理新的風險

(B) 超過可接受風險之資產，應先將此風險列入觀察，後續再予以處理

(C) 風險擁有者與利害相關者，都需要瞭解風險處理後之剩餘風險的結果

(D) 風險處理後之殘餘風險，必須文件化記錄並定期審查，確認風險處理是有效控制風險的

規劃 114-1 答案B

(當資產的風險超出可接受水準時，應立即採取措施降低或轉移風險，而非僅僅將該風險列入觀察，再延後處理。觀察僅適用於較低風險或暫時無法即時處理的情況，對於超出可接受範圍的風險，等待處理可能使損失風險持續存在或惡化。)

22. 在風險評鑑過程，辨識出的低風險項目，多數常以下列何種方式進行風險回應？

(A) 風險保留（Risk Retention）

(B) 風險避免（Risk Avoidance）

(C) 風險降低（Risk Reduction）

(D) 風險轉移（Risk Transfer）

管理 113-2 答案A

(低風險處理不符合成本效益，通常會進行風險保留)

23. 風險是指不確定性對目標的影響，或是損失的不確定性。下列何項「非」不確定性所指的三種情況之一？

(A) 不確定事件是否發生

(B) 不確定何時發生

(C) 不確定發生的地點

(D) 不確定造成的嚴重性

管理 113-2 答案C

(地點通常是已知的，例如公司機房)

24. 關於資通安全（Cyber Security）的風險擁有者（Risk Owner）的角色描述，下列何者較「不」合適？

(A) 風險擁有者負責評估責任範圍內的資訊安全風險，並核定資通安全風險處理計畫

(B) 風險擁有者應確保資安險處理計畫被妥善執行，以降低組織面臨的資通安全風險

(C) 風險擁有者一定要是資通安全領域的專業人士，才有能力評估和處理資訊安全風險

(D) 風險擁有者有責任與其他部門合作，共同識別、評估和管理資訊安全風險

管理 113-2 答案C

(風險擁有者通常是業務部門的主管)

25. 與資訊安全風險分析相關議題的敘述，下列何者錯誤？

(A) 主管機關公文來函要求事項，可納入風險分析的參考

(B) 法律法規適用的要求事項，可納入風險分析的參考

(C) 客戶合約的要求，可以不用納入風險分析的參考 (客戶合約中可能包含特定的資訊安全要求，例如資料保護、事件通知等。如果組織未能滿足這些要求，可能會導致違約、罰款和聲譽損失等風險。因此，**客戶合約的要求必須納入風險分析的參考**)

(D) 組織本身內部與外部的議題，可納入風險分析的參考

規劃 113-2 答案C

26. 風險分析其中一個功能是利用量化計算公式估算並詮釋風險程度，身為組織資通安全主管的您，正進行組織官網系統的安全風險評估，現在的情境為估算一個 20年才會出現一次的地震，將可能造成之風險值為下列何項？（其中「曝露因子」(E.F)=25%、資通系統價值＝ 50萬元。）

(A) 125000

(B) 6250

(C) 2500000

(D) 0（無風險）

規劃 113-2 答案B

(模擬風險量化分析的計算。我們需要用到以下公式

單一預期損失 (SLE) = 資產價值 (AV) \* 曝險因子 (EF)

年度化損失期望 (ALE) = 單一預期損失 (SLE) \* 年度化發生率 (ARO)

讓我們根據題目提供的資訊逐步計算：

計算單一預期損失 (SLE):

資產價值 (AV) = 50 萬元

曝險因子 (EF) = 25% = 0.25

SLE = 50 萬元 \* 0.25 = 12.5 萬元

計算年度化損失期望 (ALE):

單一預期損失 (SLE) = 12.5 萬元

年度化發生率 (ARO) = 20 年發生一次 = 1/20 = 0.05

ALE = 12.5 萬元 \* 0.05 = 6250 元

因此，20 年才會出現一次的地震，將可能造成之風險值為 6250 元。

答案是 (B) 6250。)

28. 一般常見風險評鑑流程報包括：識別背景、風險辨識、風險評估與分析、風險回應、風險監督；下列敘述哪些屬於「風險評估與分析」階段？（複選）

(A) 執行風險評鑑作業發現 68個風險項目 (這屬於**風險辨識**階段，而不是風險評估與分析)

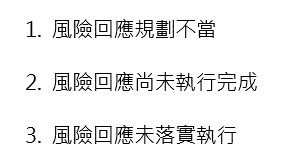
(B) 已確認 55個低風險項目，屬風險可接受範圍，決定維持現狀不做改變 (這屬於**風險回應**階段，基於風險分析的結果做出決策)

(C) 將風險項目區分為 3個高風險項目、 10個中風險項目、 55個低風險項目 (這是典型的**風險評估與分析**活動，將風險根據其可能性和影響進行分級)

(D) 使用定量的方法，將風險進行排序 (這也是**風險評估與分析**的一部分，通過量化分析（例如計算年度化損失期望）來確定風險的優先順序)

規劃 113-2 答案C、D

33. 公司規定於風險回應後 3個月，須對該項風險進行風險再評估。當風險再評估時發現該風險並未如預期降至風險胃納（Risk appetite）之內。如附圖所示的項目之中，哪些是可能的原因？



(A) 1、 2

(B) 2、 3

(C) 1、 3

(D) 1、 2、 3

規劃 113-2 答案D

(分析題目：風險再評估時發現風險未如預期降低，以上三個原因都可能導致這個結果。

* **1. 風險回應規劃不當**：如果一開始的計畫就有問題，那麼無論執行得多好，都難以達到預期效果。
* **2. 風險回應尚未執行完成**：如果措施還沒執行完，自然無法評估其完整效果。
* **3. 風險回應未落實執行**：即使計畫沒問題，也執行了，但如果執行不到位，也無法達到預期效果。)

14. 關於資產盤點與風險評估的重要性，下列敘述何者錯誤？

(A) 資產盤點與風險評估可以幫助組織確定其所有的資訊資產，只涵蓋硬體與軟體。就可以讓組織了解其擁有哪些資產以及這些資產的位置 (資產盤點與風險評估涵蓋所有資訊資產，不僅限於硬體與軟體。)

(B) 資產盤點與風險評估可以幫助組織確定其資訊資產的價值，包括其對業務運營的重要性和價值。這可以讓組織確定保護這些資產的重要性和程度

(C) 資產盤點與風險評估可以幫助組織確定其資訊資產的風險，包括潛在的威脅和弱點

(D) 資產盤點與風險評估可以幫助組織對其資訊資產進行管理，包括資產的維護、儲存和刪除等。這可以確保資產被正確管理和保護

管理 113-1 答案A

21. 如附圖所示，下列何項內容為風險回應的主要方式？



(A) 123

(B) 12345

(C) 1245 (風險回應的主要方式為規避（Avoidance）、接受（Acceptance）、轉移（Transfer）、降低（Mitigation），不包含風險曝險（Exposure）)

(D) 145

管理 113-1 答案C

22. 依據 CNS 27001:2023標準條款要求有關組織應定義及應用資訊安全風險評鑑過程之敘述，下列何者錯誤？

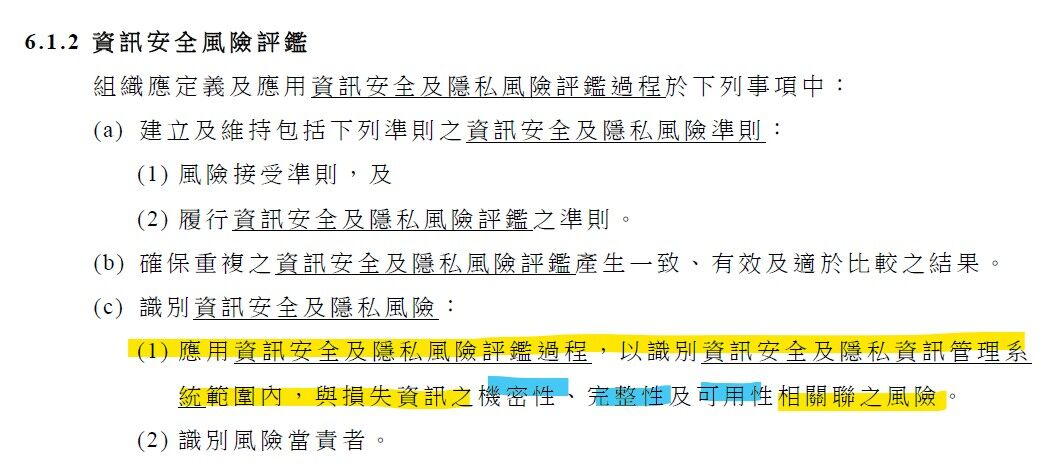
(A) 建立及維持資訊安全風險準則

(B) 資訊安全風險準則應包含風險接受準則以及執行資訊安全風險評鑑之準則

(C) 識別資訊安全風險包含識別資訊安全管理系統範圍內與喪失資訊之機密性、完整性、可用性以及不可否認性相關聯之風險 (C選項的描述超出CNS 27001:2023標準範疇，「不可否認性」並未列為資訊安全風險識別的核心範圍。)

(D) 分析資訊安全風險以識別風險實際發生時， 應包含可能導致的潛在後果以及風險發生的實際可能性

管理 113-1 答案C



(在標準的第 6.1.2 條款「資訊安全風險評鑑」中，明確指出組織應識別與資訊的機密性、完整性和可用性（CIA 三元組）相關的風險。

雖然不可否認性（Non-repudiation）在資訊安全中也是一個重要的屬性，但在 ISO/IEC 27001 的風險評鑑條款中，並未將其列為必須考量的核心要素。)

23. 在風險處理的成本考量下，下列何種風險處理策略可能是成本最高的？

(A) 接受所有風險

(B) 將風險進行轉移

(C) 盡力降低風險

(D) 追求零風險 (追求零風險幾乎無法實現，且成本極高，並非可行的風險處理策略)

管理 113-1 答案D

24. 颱風、水災及地震等是屬於下列何項風險事件？

(A) 環境災害 (颱風、水災和地震屬於自然環境災害事件，為典型環境風險來源)

(B) 蓄意破壞

(C) 設施功能失效

(D) 資訊事件

管理 113-1 答案A

25. 關於資通安全風險管理內容的描述，下列何者較為正確？

(A) 資通安全風險管理是循環的過程，應該定期重新評鑑風險，並根據風險的變動調整控制措施 (資通安全風險管理是動態且循環的過程，應隨環境與風險變化定期更新控制措施)

(B) 資通安全風險管理應該排除所有風險，確保組織完全沒有風險曝露 (零風險成本太高)

(C) 僅需進行一次性的資通安全風險評鑑，資通安全風險一旦識別和處理，便不會發生變化 (定期風險評價或發生重大影響時)

(D) 資通安全風險管理僅需著重法律和規範要求的符合，不需考慮組織的特定資安需求和環境現況 (除了法律外也要考慮組織業務需求)

管理 113-1 答案A

25. 關於風險管理流程之敘述，下列何者錯誤？

(A) 有些辨識出的風險經過分析與評估之後，可以考量接受該風險

(B) 風險處理的成本與風險的嚴重性可能沒有直接關係

(C) 通過 ISO 27001驗證之公司，進行風險評鑑時，必須通過ISO 31000風險管理系統驗證 (這是錯誤的。ISO 27001 是資訊安全管理系統 (ISMS) 的標準，而 ISO 31000 是風險管理的指導標準。ISO 27001 中確實要求進行風險評鑑，但並未強制要求必須通過 ISO 31000 驗證。ISO 31000 可以作為實施 ISO 27001 風險管理的一個參考框架，但它不是必須的。公司可以根據自身情況選擇合適的風險評鑑方法)

(D) 決定處理風險優先項目，是依據風險分析與評估後，所判斷

的風險嚴重性做為依據

規劃 113-1 答案C

27. 風險分析的其中一個用以詮釋量化計算公式，包含「單一損失預期

值」（ Single Loss Expectancy SLE）、「年度發生比率」（ Annual Rate of Occurrence ARO）、和「年度損失預期值」（ Annual Loss Expectancy ALE），請問三者的關係為下列何項？

(A) ALE= ARO\*SLE

(B) ARO= ALE\*SLE

(C) ALE= ARO/SLE

(D) ARO= SLE/ALE

規劃 113-1 答案A

(**年度損失預期值 (ALE) = 單一損失預期值 (SLE) \* 年度發生比率(ARO)**

舉例來說，如果一個資產遭受某種攻擊的單次損失預期為 10,000 美元 (SLE)，且預計該攻擊每年會發生 2 次 (ARO)，那麼該資產因該攻擊造成的年度損失預期值為 20,000 美元 (ALE = 10,000 \* 2)。)

33. 有關資訊安全之風險處理，下列何項敘述「有誤」？

(A) 應依據風險評估準則與導致該等風險之事故情境之關係，訂定優先序之風險清單

(B) 風險處理時若已選擇降低風險，則無需進行風險處理計畫 (即使選擇了降低風險，仍然需要制定風險處理計畫。該計畫應該詳細說明要採取哪些措施來降低風險、負責人是誰、時間表是什麼、以及如何監控風險降低措施的有效性等。風險處理計畫是確保風險得到有效管理的重要工具)

(C) 風險處理應由高風險項目優先處理

(D) 對於所識別出之風險，只要經過風險處理後所剩下來的殘餘風險即可 (雖然風險處理的目標是降低風險，但**僅僅關注殘餘風險是不夠的，更重要的是要評估殘餘風險是否在可接受的範圍內**。)

規劃 113-1 答案B或D

34. A銀行風險評估後，決定不使用雲端廠商提供之服務，此項屬下列

何項風險回應措施？

(A) 風險緩解（Risk mitigation）

(B) 風險避免（Risk avoidance） (不使用是風險避免)

(C) 風險保留（Risk retention）

(D) 風險分擔（Risk sharing）

規劃 113-1 答案B

35. 有關風險處理目的之敘述，下列何項正確？

(A) 風險處理之目的係選擇並實施識別風險的選項

(B) 風險處理之目的係選擇並實施評估風險的選項

(C) 風險處理之目的係選擇並實施分析風險的選項

(D) 風險處理之目的係選擇並實施處理風險的選項

規劃 113-1 答案D

36. 關於「風險」與「風險管理」的敘述，下列哪些正確？（複選）

(A) 風險是外部威脅利用弱點對內部資產造成衝擊的可能性 (風險是威脅利用弱點對資產造成衝擊的可能性，威脅可以是內部的或外部的。)

(B) 通常風險管理都會以 ISO/IEC 27005 風險管理指引作為參

考

(C) 風險分析可依可用性、完整性、機密性加以質化後，決定風

險等級 (風險分析可以透過質化或量化的方式，依據可用性、完整性、機密性以及發生的可能性來評估，並決定風險等級。)

(D) 進行風險識別須包含威脅識別與弱點識別

規劃 113-1 答案 B、D

21. 關於風險的敘述，下列何項錯誤？

(A) 風險是對目標不確定性之效應

(B) 進行風險分析及排序時，須以量化方式進行 (風險分析並不一定以量化方式進行，許多時候會採用質化方法)

(C) 風險與控制並非總是一對一的形式，有時一個風險是透過多控制作業在管理

(D) 風險回應成本的高低與風險嚴重度並非高度正相關

管理 112-2 答案B

22. 下列何者 「不」是一般常見資訊安全風險管理的作業流程？

(A) 全景建立

(B) 風險識別

(C) 風險承受能力 (風險承受能力是風險管理中的參考指標，但不屬於常見的作業流程（全景建立、風險識別、風險處理是主要流程）)

(D) 風險處理

管理 112-2 答案C

23. S公司為電器製造商並於歐洲經營網路電器零售業務，為了因應 GDPR（General Data Protection Regulation），該公司關閉歐洲的零售業務。依據此內容，公司此項管理行為屬下列何項風險回應對策？

(A) 風險避免（Risk Avoidance）(關閉歐洲業務是避免相關風險的行為，屬於風險規避（Risk Avoidance）)

(B) 風險修改（Risk Modification）

(C) 風險保留（Risk Retention）

(D) 風險分擔（Risk Sharing）

管理 112-2 答案A

24. 當公司使用雲端服務時，面對風險的態度及處理方式，下列何者較 「 不 」 適宜？

(A) 參考業界同業的使用經驗，從中選擇合適的雲端服務供應商

(B) 因為採用雲端服務，所以公司在這樣服務不會有風險存在 (採用雲端服務並不代表無風險，此為錯誤的態度。風險仍需評估與管理)

(C) 當某服務發生失效時，加以記錄相關情況，視情況重新評估其風險

(D) 因該服務前3年都沒有失效的記錄，故其發生風險的機率較低

管理 112-2 答案B

25. 面對風險的態度，下列何者較 「 不 」 合適？

(A) 視實際情況決定可接受風險等級

(B) 無論如何，皆應致力追求零風險 (追求零風險不切實際且成本極高，並非適合的風險態度。)

(C) 參考可接受風險等級擬訂風險處理計畫

(D) 定期評估風險處理計畫執行成效

管理 112-2 答案B

25. 與資訊安全風險評估相關議題的敘述，下列何者較為正確？

(A) 需先進行風險評估，再將風險評鑑適用的準則予以建立 (應該先建立評鑑準則，才能進行有效的風險評估)

(B) 風險評估會依照風險分析的結果，安排其風險處理的優先順序

(C) 風險評鑑的順序，是先執行風險識別、再進行風險評估、風險分析 (風險識別、再進行風險分析、風險評估 )

(D) 在風險評估的過程中 ，無需識別風險的擁有者

規劃 112-2 答案B

27. 關於資訊資產價值計算之因子，下列敘述何者錯誤？

(A) 包含該資產之機密性因子在內

(B) 包含該資產之完整性因子在內

(C) 包含該資產之可用性因子在內

(D) 包含該資產之購買金額因子在內 (資訊資產的價值更多是基於其對組織的業務影響、機密性、完整性和可用性，而非初始購買成本。)

規劃 112-2 答案D

33. 關於風險處理的敘述，下列何者正確？

(A) 風險可接受準則需先定義清楚，風險評鑑結果超過此準則就必須進行風險處理，以降低風險

(B) 風險處理須實施的控制措施，皆必須參考 ISO 27001 的附錄Ａ(ISO 27001 的附錄 A 是一個控制措施參考列表，它提供了一系列可以考慮實施的控制措施。但**並非強制性要求**必須實施所有這些控制措施。組織可以根據自身需求、行業標準或其他框架選擇適合的控制措施。)

(C) 風險處理計畫及殘餘風險的結果，須由資產擁有者確認 (風險處理計畫及剩餘風險的結果，應該由風險擁有者 (Risk Owner) 確認和接受)

(D) 風險處理後所剩餘的風險必須為零 (風險處理的目標是將風險降低到**可接受的程度**，而不是消除所有風險。)

規劃 112-2 答案A

34. 關於必須進行風險評估的狀況，下列敘述何者錯誤？

(A) 依據 ISMS（Information Security Management System）要求，必須定期施行風險評估

(B) 決定到美國設立新的工廠，將公司研發團隊遷往美國

(C) 一般員工國外旅遊 (一般員工的國外旅遊不屬於必須進行全面風險評估的情況，除非涉及特定的資訊安全風險。)

(D) 將本地端所有資訊系統密遷到 Azure雲端服務

規劃 112-2 答案C

35. 某作業流程經過風險評估（Assessment）後的固有風險值，遠低於所設定的可接受風險水準時， 下一步行動方案 ，下列何者較「不」適當？

(A) 檢視剩餘風險的水準

(B) 向管理階層報告合規結果

(C) 實施控制措施再降低風險 (如果固有風險已經遠低於可接受風險水準，再投入資源實施額外的控制措施可能**不符合成本效益**。此時應該考慮的是現有控制措施是否過度，是否有簡化或優化的空間。過度控制會增加不必要的成本和複雜性。)

(D) 持續監控作業流程的變化

規劃 112-2 答案C

36. X公司與 Y公司進行網路服務業務合作之風險超過公司所設定之風險胃納（Risk appetite）。 X公司最後決定與 Y公司進行合作，下列哪些項目是合適的風險回應選擇？（複選）

(A) 風險規避（Risk avoidance） (風險規避是指完全停止或避免從事可能導致風險的活動。由於 X 公司決定**繼續**與 Y 公司合作，因此風險規避不是一個合適的選擇。)

(B) 風險保留（Risk retention）(風險保留是指接受風險及其可能的後果。由於風險超過了公司的風險胃納，因此直接接受風險並不是一個合適的選擇。)

(C) 風險緩解（Risk mitigation）

(D) 風險分擔（Risk sharing）

112-2 規劃 答案 C、D

(風險胃納是指組織在追求其目標的過程中，願意接受的風險類型與程度。)

21. 當進行風險評估，發現機密資料外洩風險是組織內部最大之風險時，組織進行了相對應之風險處理方法，其中包含了購買資料外洩保險，此為下列何種風險處理方式？

(A) 風險保留（Risk Retention）

(B) 風險降低（Risk Reduction）

(C) 風險轉移（Risk Transfer） (購買資料外洩保險將風險的經濟後果轉移給保險公司，屬於風險轉移（Risk Transfer）)

(D) 風險避免（Risk Avoidance）

管理 112-1 答案C

22. 風險評鑑（Risk Assessment）後的風險處理方式有以下哪幾種方法？

(A) 接受、降低、轉移、避免 (風險處理的主要方式包括接受、降低、轉移、避免，涵蓋完整的管理方法)

(B) 規劃、評估、排序、避免

(C) 面對、處理、解決、接受

(D) 評估、分析、處理、降低

管理 112-1 答案A

23. 關於風險評鑑（Risk Assessment）的敘述，下列何者較正確？

(A) 應建立一套適用於全公司（組織）之準則

(B) 不同類別被評鑑項目，無須依不同類別區分風險 (不同類別的風險必須分開評估，因為評估標準和處理方式都不同)

(C) 可接受風險一定要在風險評鑑前先決定 (可接受風險標準可以根據評鑑結果動態調整，不是固定不變的)

(D) 風險改善計畫，執行單位應再選擇是否需執行 (風險改善計畫一旦確定就必須執行，不是由執行單位決定要不要做)

管理 112-1 答案A

24. 關於風險轉移（Risk Transfer）的敘述，下列何者「不」正確？

(A) 藉由其他的團體，來承擔或分擔部份的風險

(B) 當風險全部或部分被轉移時，可能會遭遇新的風險

(C) 將風險轉移給其他團體時，可以降低風險對自身的影響

(D) 可以有效減低風險發生的機率 (風險轉移可分擔風險影響，但無法降低風險發生的機率)

管理 112-1 答案D

25. 下列何者「不」是風險處理的選項？

(A) 風險降低（Risk Reduction）

(B) 風險轉移（Risk Transfer）

(C) 風險忽略（Risk Neglect）(風險處理的主要方式為規避、降低、轉移、保留，並無「風險忽略」這一項)

(D) 風險保留（Risk Retention）

管理 112-1 答案C

25. 與資訊安全風險分析相關議題的敘述，下列何者錯誤？

(A) 主管機關公文來函要求事項，可納入風險分析的參考

(B) 法律法規適用的要求事項，可納入風險分析的參考

(C) 客戶合約的要求，可以不用納入風險分析的參考

(D) 組織本身內部與外部的議題，可納入風險分析的參考

規劃 112-1 答案C

(風險建立全景包含利害關係人要求、法規、合約、組織的內外部議題)

26. 關於風險分析與評估之敘述，下列何者錯誤？

(A) 公司最好至少每年定期執行一次風險評鑑

(B) 公司營運重大改變時，應進行風險評鑑

(C) 重大風險項目完成風險回應後，不需進行風險再評估 (風險需要持續分析和監控)

(D) 進行風險分析與評估前，應先了解相關背景資訊（例如：法規要求、技術環境...）

規劃 112-1 答案C

28. 關於風險分析及風險評估議題的敘述 ，下列哪些正確？（複選）

(A) 風險評估的過程，須將目前已實施的措施結果納入考量

(B) 風險分析時產出的後果與可能性的評估方式應定義清楚

(C) 風險識別僅需將與機密性有關風險識別清楚 (完整性、可用性，或是其他例如法遵)

(D) 以風險評鑑工具直接執行的過程與結果皆須留存紀錄

規劃 112-1 答案A、B、D

33. 關於風險處理的敘述，下列何者錯誤？

(A) 風險處理計畫是定義行動並實施所需的控制，以降低無法接受風險的管理文件

(B) 風險處理計畫中要考量風險處理之優先順序

(C) 風險處理計畫如果完成時間較長，如需導入工具，可以先以接受該高風險處理 (如果風險被評估為不可接受，則**不應該直接接受**。即使風險處理計畫需要較長時間才能完成，也應該考慮)

(D) 風險處理計畫中，所需資源及交付事項，皆須完整計畫考量

規劃 112-1 答案C

34. 關於風險評估準則的敘述，下列何者錯誤？

(A) 組織應定義用於評估風險重要性的準則

(B) 不同組織可能採用不同的方法跟準則

(C) 這些準則應反映組織的價值觀、目標和資源

(D) 風險評估準則應與組織的管理政策可以不一致 (風險評估準則**必須與組織的管理政策保持一致**。管理政策為風險管理提供了指導原則和框架，風險評估準則應該在這些政策的框架內制定和執行。不一致會導致風險管理工作的混亂和低效)

規劃 112-1 答案D

36. 關於風險處理相關議題的敘述，下列哪些正確？（複選）

(A) 制定資訊安全目標，可依據風險處理的實施狀況來量化其達成結果

(B) 風險處理的計畫，需細部描述其內容，包含實施內容及相關負責人員等

(C) 風險處理的方式必須以修正風險的選項處理 (風險處理有修正、避免、分擔、接受四種方式)

(D) 風險分析結果可能性高、衝擊大的可考量選用避免風險

規劃 112-1 答案A、B、D

21. 下列敘述何者符合風險移轉？

(A) 投保機房火險

(B) 建立備援網路系統 (風險降低)

(C) 停止網路平台交易業務 (風險避免)

(D) 增加開啟系統權限的簽核流程 (風險降低)

管理 111-2 答案A

(保險是一種風險移轉)

22. 關於風險評鑑管理程序，下列敘述何者「不」正確？

(A) 建立全景係界定風險評鑑範圍

(B) 詳細風險評鑑包括風險識別、風險分析與風險評估

(C) 風險處理若合意，則進入風險接受階段

(D) 風險評鑑若不合意，則進入風險溝通階段

管理 111-2 答案D

( 風險評鑑若不合意，則回到建立全景階段)

23. 下列何者的處理方式無法降低風險？

(A) 風險避免(Risk avoidance)

(B) 風險保留(Risk retention)

(C) 風險修改(Risk modification)

(D) 風險分擔(Risk sharing)

管理 111-2 答案B

(風險保留即是風險接受無法降低風險)

24. 為了降低風險，下列何者最「不」是實施風險控制措施的考量因素？

(A) 法規要求與限制

(B) 組織的目標與規範

(C) 實施的可能成本

(D) 資訊資產類別

管理 111-2 答案D

(需要根據風險來決定，而不是資產類別，資產類別是風險評估的輸入資訊，而非決定是否實施控制的考量因素)

25. 下列何者是「殘餘風險」（Residual Risk）的敘述？

(A) 單位可以承受的風險

(B) 沒有被識別的風險

(C) 已經被識別，但是沒有指定處置方法的風險

(D) 執行風險處理措施後，還殘留下來的風險

管理 111-2 答案D

4. 下列何者「不」是風險評鑑過程中主要的活動？

(A) 風險鑑別

(B) 風險分析

(C) 風險處理

(D) 風險評估

管理 111-1 答案C

(風險管理流程有高點金乃傑老師的口訣

被評理 (風險背景 風險評鑑 風險處理)

是悽涼 (風險識別 風險分析 風險評量)

避降轉保 (風險規避 風險降低 風險移轉 風險保留))

5. 下列何者「不」屬於威脅來源之一？

(A) 天然災害 (自然威脅)

(B) 憤怒的員工 (人為蓄意威脅)

(C) 未經授權存取機密資料 (比較像是威脅事件)

(D) 程式的瑕疵 (弱點)

管理 111-1 答案D，個人覺得C也是錯的

7. 「 商業公司使用防毒和反垃圾郵件機制，以保護公司的電子郵件系

統。」請問上述屬於下列何種風險處理對策？

(A) 風險避免（Risk avoidance）

(B) 風險保留（Risk retention）

(C) 風險修改（Risk modification）

(D) 風險分擔（Risk sharing）

規劃 111-1 答案C

(通過採取措施來減少風險的發生概率或降低其影響，風險修改等同於風險降低)

14. 關於風險管理步驟由先至後， 下列排序何者正確？（1） 全景建立、（2）風險處理、 （3） 風險識別、 （4）監控風險處理、 （5） 風險評估

(A)（1）（2）（3）（4）（5）

(B)（1）（3）（5）（2）（4）

(C)（1）（5）（3）（2）（4）

(D)（3）（5）（2）（1）（4）

規劃 111-1 答案B

16. ISO/IEC 27001中所採用的風險評鑑（Risk Assessment 主要包含下列哪些步驟？（複選）

(A) 風險評估（Risk Evaluation）

(B) 風險分析（Risk Analysis）

(C) 風險分類（Risk Classification）

(D) 風險識別（Risk Identification）

規劃 111-1 答案A、B、D

34. 下列何種人員負責風險評鑑後風險處理與殘餘風險結果的核可？

(A) 資產擁有者（Asset Owner）

(B) 風險擁有者（Risk Owner）

(C) 設備擁有者（Device Owner）

(D) 資料擁有者（Data Owner）

管理 111-1 答案B

(對特定風險負責的人，確保該風險被適當識別、評估和處理)

41. 下列何者「不」屬於風險評鑑之範圍及執行步驟？

(A) 風險分析

(B) 防護措施的選擇

(C) 風險接受

(D) 營運持續計畫

管理 111-1 答案D

42. 下列何者「不」是風險評鑑後，對於風險事項的處理方式？

(A) 風險規避

(B) 風險移轉

(C) 風險控制

(D) 風險再評鑑

管理 111-1 答案D

(風險再評鑑為定期或因重大事件重新檢視風險狀態與處理計畫的過程)