資安要素和控制方法

**資安三要素**

* 機密性 (Confidentiality)
* 確保資料只有經授權的人才能存取。
* 例如：加密技術、存取控制。
* 案例：勒索軟體說不給錢就公開公司資料就是機密性的破壞。
* 完整性 (Integrity)
* 確保資料不被未經授權的更改。
* 例如：雜湊函數 、訊息鑑別碼 (MAC) 、數位簽章、校驗和 (Checksums)。
* 案例：公司官網首頁被置換就是完整性的破壞。
* 可用性 (Availability)
* 確保使用者在需要時，能及時存取與使用資源。
* 例如：備份還原、負載平衡、叢集架構、容錯機制。
* 案例：公司的服務被DDos攻擊無法使用就是可用性的破壞。
* 三要素的重要性排序：
  + 必須要情況看產業特性，例如金融業較重視機密性和完整性，但是醫院和工廠較重視可用性。

**資訊安全延伸要素**

* 真實性 (Authenticity)
* 確認訊息或行為的來源是否真實。
* 例如：郵件伺服器的 DKIM、SSH 公鑰信任。
* 案例：因為郵件的內容都可以偽造，所以你可以寫你是金城武寄信給別人，別人也無法驗證，這樣就缺乏真實性。
* 不可否認性 (Non-repudiation)
* 保證行為人在事後無法否認自己曾經做過某事(簽署文件、發送訊息等)，並具有法律層面的效力。
* 例如：數位簽章搭配由公開金鑰基礎建設 (PKI) 架構核發的「數位憑證」，如使用自然人憑證報稅等。
* 案例：網路購物下單後不可主張非本人下單，這樣就會天下大亂了。
* 大部分資安書要素主要講以上五種，iPAS考試多「身分識別性」和「可歸責性」，請參考表格如下。

| **要素** | **說明** | **反向詞** | **實作技術** | **常見攻擊** |
| --- | --- | --- | --- | --- |
| 機密性 (Confidentiality) | 確保資料只能被授權人員存取，包括在儲存和傳輸過程中的保護 | 資訊洩露 (Information Disclosure) | 加密技術、 存取控制 | 資料竊取、網路竊聽 |
| 完整性  (Integrity) | 確保資料的準確性和一致性，防止未經授權的修改 | 資料竄改 (Data Tampering) | 數位簽章、 訊息鑑別碼(MAC)、雜湊函數、校驗和 (Checksums) | 資料竄改 、中間人攻擊、SQL 注入 |
| 可用性  (Availability) | 確保資源和服務在需要時能被正常存取和使用 | 服務中斷 (Service Disruption) | 冗餘、備份、負載平衡、DDoS防護 | DDoS攻擊、系統故障、勒索軟體 |
| 不可否認性 (Non-repudiation) | 防止使用者否認已執行的操作，適用於操作和通訊，並具有法律層面的效力 | 可否認性 (Repudiation) | 數位簽章、數位憑證、公鑰基礎設施(PKI)。 | 交易否認、身份盜用 |
| 身分識別性 (Authentication) | 驗證使用者、系統或設備的身份，確保存取的合法性 | 身分冒充 (Identity Impersonation) | 密碼、多因素驗證、生物辨識、數位憑證 | 密碼攻擊、身份冒充、中間人攻擊 |
| 真實性 (Authenticity) | 確保資料、通訊或身份的真實性，防止偽造 | 偽造(Forgery) | 郵件伺服器的 DKIM、SSH 公鑰信任 | 網路釣魚、憑證偽造、假訊息/深偽技術 (Deepfakes) |
| 可歸責性 (Accountability | 追蹤和記錄系統活動，明確行為責任歸屬 | 匿名性 (Anonymity) | 審計日誌、日誌管理系統、存取控制列表(ACL) | 共用帳號，日誌刪除、身份隱藏、日誌竄改/偽造 |

**控制方法分類依方法**

* 管理控制 (Administrative Control)
  + 策略與規範。
  + 例如：政策文件。
  + 案例：ISO27001文件。
* 技術控制 (Technical Control)
  + 技術實作。
  + 例如：加密技術、防火牆、DLP。
  + 案例：密碼長度要12碼。
* 實體控制 (Physical Control)
  + 硬體與物理限制。
  + 例如：門禁卡、監視器。
  + 案例：機房的樓層只有電梯可以出入。

**控制方法分類依時間和類型**

* 事前控制：旨在防止錯誤、違規或安全事件發生。
* 預防性：避免事件發生。
  + 例如：員工教育訓練、存取權限控管、防火牆規則、資料輸入驗證、弱點掃描。
* 威攝性：嚇阻潛在攻擊者或內部人員進行未經授權的行為。
  + 例如：內有惡犬招牌、員工登入工作站時的合法使用公告。
  + 某些東西可能同時具有兩種屬性，例如監控攝影機又是威攝性，也屬於檢測性。
* 事中控制：偵測與回應安全事件。
* 檢測性：監控與發現問題。
  + 例如：監控攝影機、入侵偵測系統 (IDS)、日誌記錄與分析。
* 糾正性：修復當前問題。
  + 例如：入侵防禦系統 (IPS)、防毒軟體刪除可疑檔案、垃圾郵件偵測(SPAM)。
* 事後控制： 旨在將系統或流程從錯誤、違規或安全事件中恢復到正常運作狀態。
  + 還原性：回復正常運作。
    - 例如：備份還原、災難復原計畫。
    - 有時候考試會將還原性和糾正性合併。
* 當前述都無法完成控制
* 補償性：當主要的控制措施無法實施或效果不足時，用來補強或替代的控制措施。
  + - 例如：將無法更新的系統隔離至獨立網段，以防止該系統的漏洞被外部攻擊者利用或針對無法加密的資料採用嚴格的實體存取控制。

**考古題：**

4. 控制措施實施階段可分成事前、中及後等三項。請問下列哪些屬於事中控制類型（如偵測[Detective]）的應用方式？ （複選）

(A) 監控入侵檢測系統（IDS） (屬於偵測型控制，可以即時發現入侵行為)

(B) 檢核稽核日誌報表（Audit Log Report Reviews） (透過分析日誌，偵測系統異常或未經授權的活動)

(C) 定期弱點掃描（Vulnerability Scan） (預防或識別潛在風險的措施，故不屬於事中偵測控制)

(D) 監控錄影監視系統（CCTV） (藉由持續監控記錄現場情形，屬於偵測型措施)

規劃 114-1 答案ABD

26. Arc公司於數日前遭受電子郵件社交工程攻擊，員工點選外部寄來的電子郵件並開啟電子郵件夾帶的勒索軟體，造成公司內容多台電腦內的檔案被加密。經過事件風險評鑑後，發覺針對此類事件未來改善的方式為：事前缺乏教育訓練，以及事發時未有備份資料足以提供使用者復原使用。請問，上述所指二種控制措施，分別屬於何種控制措施類型？

(A) Detective & Corrective

(B) Corrective & Detective

(C) Preventive & Corrective

(D) Detective & Preventive

規劃 114-1 答案C

(**教育訓練**：屬於預防性（Preventive）控制措施，透過事前教育與訓練，可以降低員工受社交工程攻擊的風險。

**備份資料**：屬於糾正性（Corrective）控制措施，當事件發生後可利用備份資料還原受損檔案。

註：有時候還原性會合併到糾正性)

3. 導入下列何者措施，其主要目的「不」是提升機密性？

(A) 在內部重要網段增設防火牆

(B) 導入主機負載平衡系統 (負載平衡系統的主要目的是將工作負載分配到多個伺服器，以提高效能、可靠性和**可用性**，**並非直接提升機密性**)

(C) 導入資料加密系統

(D) 限制機密資料僅少數人員可以存取

規劃 113-2 答案B

4. 資訊安全三個主要基本要素「不」包含下列何項？

(A) 機密性

(B) 安全性

(C) 完整性

(D) 可用性

管理 113-2 答案B

(資訊安全三要素為機密性、完整性、可用性)

11. 在通訊安全中，「完整性」指的是下列何項？

(A) 確保數據資料在傳輸過程中未被未經授權的修改

(B) 確保網站的可用性，可隨時存取網站

(C) 確保所有使用者都有依最小原則設定權限

(D) 確保網絡傳輸速度與申請速率相符

技術 113-2 答案A

40. 2024年9月親俄駭客組織NoName057聲稱，將對臺灣政府機關、關鍵基礎設施的網站發動一系列的DDoS攻擊。請問此項攻擊主要目的是對被攻擊目標下列何項資訊安全要素造成影響？

(A) 機密性（Confidentiality）

(B) 完整性（Integrity）

(C) 可用性（Availability）

(D) 可歸責性（Accountability）

管理 113-2 答案C

(DDos攻擊主要讓服務不可用，為可用性受影響)

4. 關於保護資料之機密性、完整性與可用性描述，下列何項正確？

(A) 應用系統的可用性對組織而言，皆為同等級重要 (不同系統的可用性要求不同（如核心系統vs.一般系統) )

(B) 公司內部員工的個人資訊，不在機密性的保護範圍 (員工個資仍需保護隱私)

(C) 對所有資訊資料而言，機密性最為重要 (機密性、完整性、可用性的重要性依資料性質而異)

(D) 組織之公開資訊對外公布時，資料的完整性需審查後再開放 (公開資訊對外發布前，必須確保完整性（即資料正確且未遭篡改），因此需審查後開放)

管理 113-1 答案D

18. 規劃網路安全架構時，下列何項措施能「較有效」的保護資料的機密性？

(A) 資料傳輸加密 (這是保護資料機密性的最直接和有效的方法。透過加密，即使資料在傳輸過程中被攔截，攻擊者也無法讀取資料的內容，因為資料已經被轉換成無法理解的密文。這對於保護靜態資料(data at rest)和動態資料(data in transit)的機密性都至關重要。)

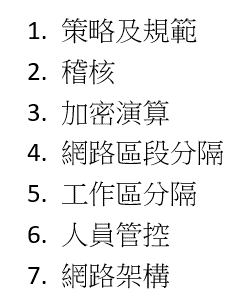
(B) 強化防火牆設置 （有幫助但次要）

(C) 定期資料備份 （主要保護可用性）

(D) 內部網路隔離 （可降低風險，但影響有限）

規劃 113-1 答案A

31. 關於下列資安作為，包含行政管管理類型、實體類型、技術類型等三項，各有其所相對應的安全控制方式。請問附圖中的項目哪些是屬於「技術」類型？（請選擇最適組合）



(A) 1、 2、 3

(B) 4、 5、 6

(C) 3、 4、 7

(D) 1、 4、 6

管理 113-1 答案C

(加密演算(3)、網路區段分隔(4)、網路架構(7)都需要透過IT技術來實作，屬於技術層面的安全控制。行政管理類：策略及規範(1)、稽核(2)、人員管控(6)，實體類：工作區分隔(5))

40. 關於密碼學（Cryptography）所能達成之主要目的敘述，下列何項最「不」適切？

(A) 機密性（confidentiality）

(B) 完整性（Integrity）

(C) 可用性（Availability）

(D) 不可否認性（Non-Repudiation）

管理 113-1 答案C

(因為密碼學主要用於確保資料的機密性、完整性和不可否認性，而可用性是透過系統架構和備援機制來實現的，與密碼學無直接關係。)

1. 下列何項系統建置規劃並「不」是以可用性作為主要之考量基準？

(A) 建置伺服器負載平衡系統

(B) 重要資料導入高可用性（High Availability）系統

(C) 建置資料加密管理系統 (機密性)

(D) 使用針對重要系統建置即時備援機制

規劃 112-2 答案C

2. 使用微軟提供的功能將檔案加密，主要目的是增加下列資訊安全的何種特性？

(A) 可歸責性（Accountability）

(B) 可用性（Availability）

(C) 機密性（Confidentiality）

(D) 完整性（Integrity）

管理 112-2 答案C

(檔案加密的主要目的是確保資料的機密性(Confidentiality)，因為加密後只有擁有解密金鑰的授權人才能讀取內容，防止未經授權的人存取資料。)

3. 關於確保資訊安全機密性的方法，下列敘述何者較「不」正確？

(A) 建立防火牆

(B) 限制資料存取權限

(C) 使用多因素身份驗證

(D) 定期更新修補程式以及病毒碼

管理 112-2 答案D

(定期更新修補程式和病毒碼主要是確保系統的完整性(Integrity)和可用性(Availability)，而不是直接保護資料的機密性(Confidentiality)，所以是較不正確的選項。其他選項都直接控制資料的存取，確保只有授權人員能接觸機密資料。)

4. 關於維護資料完整性之控制措施，下列敘述何者正確？

(A) 密碼學技術

(B) 防火牆

(C) 資料庫備份

(D) 電子郵件加密

管理 112-2 答案A

(密碼學技術(如數位簽章、雜湊函數)可以確保資料的完整性(Integrity)，因為它能驗證資料是否被竄改或修改過。當資料內容有任何改變時，密碼學的驗證值也會跟著改變，因此能立即發現資料是否遭到竄改。)

1. 下列何者為資訊安全的「機密性」之定義？

(A) 確保資訊不會被揭露或被未經授權的個人、實體和流程所取得

(B) 確保資訊的正確和完全性 (完整性)

(C) 確保資訊在需要時可被存取和使用 (可用性)

(D) 確保資訊在傳輸過程中已確認兩方的身分和合法性 (不可否認性)

管理 112-1 答案A

(機密性(Confidentiality)的核心定義就是「確保資訊不會被未經授權的對象取得或揭露」，也就是要確保資料只能被經過授權的人存取。)

4. 駭客侵入銀行資料庫竄改存款金額，主要在破壞資訊系統的何種特性？

(A) 機密性（Confidentiality）

(B) 完整性（Integrity）

(C) 可用性（Availability）

(D) 可靠性（Accountability）

管理 112-1 答案B

(駭客竄改銀行存款金額主要破壞了資料的完整性(Integrity)，因為完整性代表資料的正確性和未被未經授權的修改。當駭客更改存款金額時，資料已經不再保持其原始正確的狀態，因此是破壞了資料的完整性。)

6. 請問下列什麼方式，最適合來確認資料的完整性（Integrity）？

(A) 最低權限

(B) 設定記憶體的特定資料段「執行禁用位元（NX bit）」

(C) 數位簽章

(D) 使用 Base64 編碼

技術 112-1 答案C

(數位簽章透過雜湊摘要確認資料的完整性)

8. 券商集體遭 DDoS（分散式阻斷服務）攻擊勒索信件，其中有多家券商的網站下單系統更實際遭受網路 DDoS攻擊，造成交易量降低。該案例網站下單系統被攻擊，最直接影響是下列何種資訊安全特性？

(A) 機密性

(B) 完整性

(C) 可用性

(D) 不可否認性

技術 112-1 答案C

(DDoS影響的是可用性，造成服務無法被正常存取)

35. 憑證記載了個人資料、公開金鑰、憑證單位名稱、數位簽章、以及憑證有效期限及用途等資訊，下列何者「不」是憑證的特性？

(A) 機密性（Confidentiality）

(B) 不可否認性（Non-Repudiation）

(C) 身分識別（Authentication）

(D) 可用性（Availability）

管理 112-1 答案D

(數位憑證主要目的是提供身分識別(Authentication)、不可否認性(Non-repudiation)和保護通訊的機密性(Confidentiality)，可用性(Availability)並不是憑證本身的主要特性。憑證是否可用取決於憑證授權機構(CA)的系統運作狀況，而不是憑證本身的功能特性。)

1. 使用專用帳號及密碼登入CRM（Customer Relationship

Management）系統，主要是基於下列何種原則？

(A) 可靠性

(B) 可用性

(C) 機密性

(D) 完整性

管理 111-2 答案C

(機密性確保非有權人員無法登入系統)

3. 請問資訊安全的定義是下列何項最正確？

(A) 保護資訊資產的機密性與完整性

(B) 保護資訊資產的完整性與可用性

(C) 保護資訊資產的機密性與可用性

(D) 保護資訊資產的機密性、完整性與可用性

管理 111-2 答案D

(資訊安全的三要素為機密性、完整性和可用性)

27. 公司ERP（Enterprise Resource Planning）系統針對不同職務功能給予不同權限的目地，與下列何項關聯性較高？

(A) 機密性、完整性

(B) 可用性、完整性

(C) 機密性、可用性

(D) 機密性、可用性、完整性

管理 111-2 答案A

(針對不同職務功能給予不同權限的目地跟可用性無關)

28. 門禁卡與機房進出需要特定密碼控制實體出入，是下列哪一個目的？

(A) 偵測性

(B) 指導性

(C) 預防性

(D) 嚇阻性

管理 111-2 答案C

(帳號控管是事前所以跟預防性有關)

36. 關於密碼學（Cryptography）所能達成之主要目的，下列

何項錯誤？

(A) 機密性（confidentiality）

(B) 完整性（Integrity）

(C) 可用性（Availability）

(D) 不可否認性（Non-Repudiation）

管理 111-2 答案C

(密碼學裡使用對稱式加解密 (例如：AES) 達成機密性、使用雜湊函數 (例如：SHA-256) 達成完整性、使用數位簽章搭配數位憑證 (例如：RSA 數位簽章與 X.509 數位憑證) 達成不可否認性，但沒有可用性)

38. 資料備份的最主要目的，是保護資料的哪一個特性？

(A) 機密性

(B) 可用性

(C) 鑑別度

(D) 完整性

技術 111-2 答案B

(備份的核心目標是確保在資料因硬體故障、人為誤刪、攻擊（如勒索軟體）或災害等情境下，仍能恢復資料並維持系統或業務的持續運作。這直接對應到資訊安全的「可用性」（Availability），即確保授權使用者能在需要時存取資料。)

41. 請問存錄系統管理者或操作者操作系統的紀錄，並予以適當的保護，其主要的目的是要確保下列對於系統管理者或操作者的何項特性？

(A) 機密性（Confidentiality）

(B) 完整性（Integrity）

(C) 可用性（Availability）

(D) 可歸責性（Accountability）

技術 111-2 答案D

(主要是要追朔到誰使用這個行為，產生問題時可歸責)

6. 使用Wireshark工具，主要可能影響資訊安全中的何種特性？

(A) 機密性（Confidentiality）

(B) 可用性（Availability）

(C) 完整性（Integrity）

(D) 真確性（Authenticity）

技術 111-1 答案A

(Wireshark 工具主要是擷取網路封包，查看內容會破壞機密性)

10. 下列何者「不」是提升服務可用性（Availability）的有效策略？

(A) 導入內容遞送網路（Content Delivery Network, CDN）服務

(B) 建置應用程式防火牆

(C) 設計自動擴展機制

(D) 規劃伺服器負載平衡架構

規劃 111-1 答案B

(應用程式防火牆主要用於保護應用程式免受各種網絡攻擊，如SQL注入、跨站腳本（XSS）等。雖然它能增強系統的安全性，但其主要目的是防禦攻擊，而非直接提升服務的可用性。)

29. 公司將資訊系統的資料進行備份，最主要是為了保護資訊安全中的何種特性？

(A) 機密性（Confidentiality）

(B) 可用性（Availability）

(C) 完整性（Integrity）

(D) 真確性（Authenticity）

技術 111-1 答案B

(備份的核心目標是確保在資料因硬體故障、人為誤刪、攻擊（如勒索軟體）或災害等情境下，仍能恢復資料並維持系統或業務的持續運作。這直接對應到資訊安全的「可用性」（Availability），即確保授權使用者能在需要時存取資料。)

40. 下列何種作法與保護資料機密性較「無」直接相關？

(A) 將資料複製成數個副本，放在不同的儲存媒體 (可用性)

(B) 將資料進行加密

(C) 將資料拆分成不同片段交由不同人分持

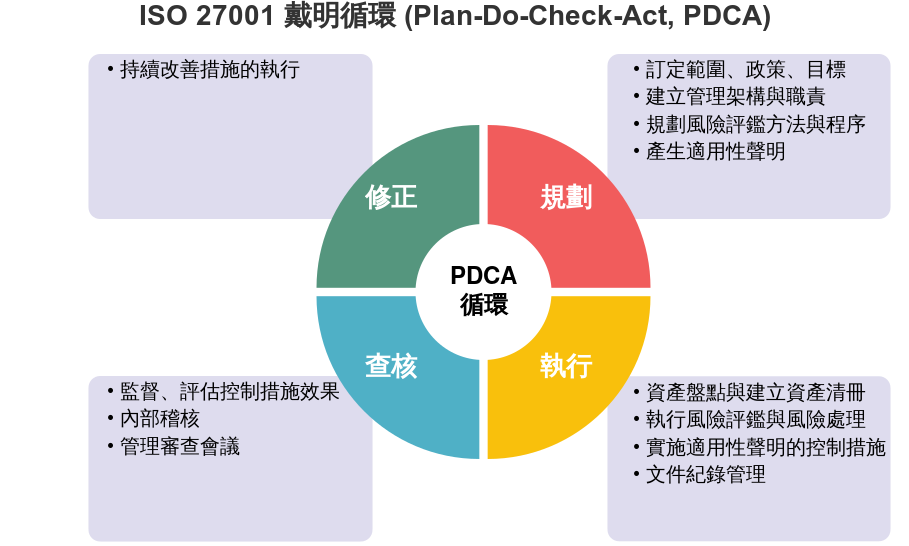
(D) 將資料設定特定權限，只有被授權的人才可開啟

技術 111-1 答案A

資訊安全管理系統

**資訊安全管理系統**

* 資訊安全管理系統 (Information Security Management System, ISMS)：是一套系統化的政策、流程、程序和控制措施，用於建立、實施、維護並持續改進組織的資訊安全管理能力，確保能有效地識別、管理及降低資訊安全風險，並符合相關法規及利害關係人的要求。
* 需特別留意的是，「資訊安全管理系統」並非等同於「ISO 27001」，ISO 27001 只是眾多資訊安全管理框架中的一種標準化規範，並非唯一選項。組織應根據自身業務性質與需求，適當選擇 NIST CSF、COBIT、CIS Controls等資安框架，建立符合組織特性、兼顧風險管理及持續改進的資訊安全管理系統體系，真正達成資訊安全有效管理的目的，而非僅追求標準的認證。
* 戴明循環 (Plan-Do-Check-Act, PDCA) ：是 ISO 27001 資訊安全管理系統的核心理念與運作基石，提供了一個持續改進的框架，確保資訊安全的有效管理與持續強化。
  + 規劃(Plan)：
    - 訂定範圍、政策、目標
    - 建立管理架構與職責
    - 規劃風險評鑑方法與程序
    - 產生適用性聲明
  + 執行(Do)：
    - 資產盤點與建立資產清冊
    - 執行風險評鑑與風險處理
    - 實施適用性聲明的控制措施
    - 文件紀錄管理
  + 查核(Check)：
    - 監督、評估控制措施效果
    - 內部稽核
    - 管理審查會議
  + 修正(Act)：
    - 持續改善措施的執行



* PDCA 並非單一、一次性的過程，而是持續循環、反覆改善的模式。透過持續的規劃、執行、查核與行動，組織能有效提升自身的資訊安全防禦能力，降低潛在風險，並確保資訊安全管理系統符合 ISO 27001 等資安標準要求。這種持續改進的精神，也正是 ISO 27001 得以協助組織建構完善資訊安全管理體系的核心價值所在。

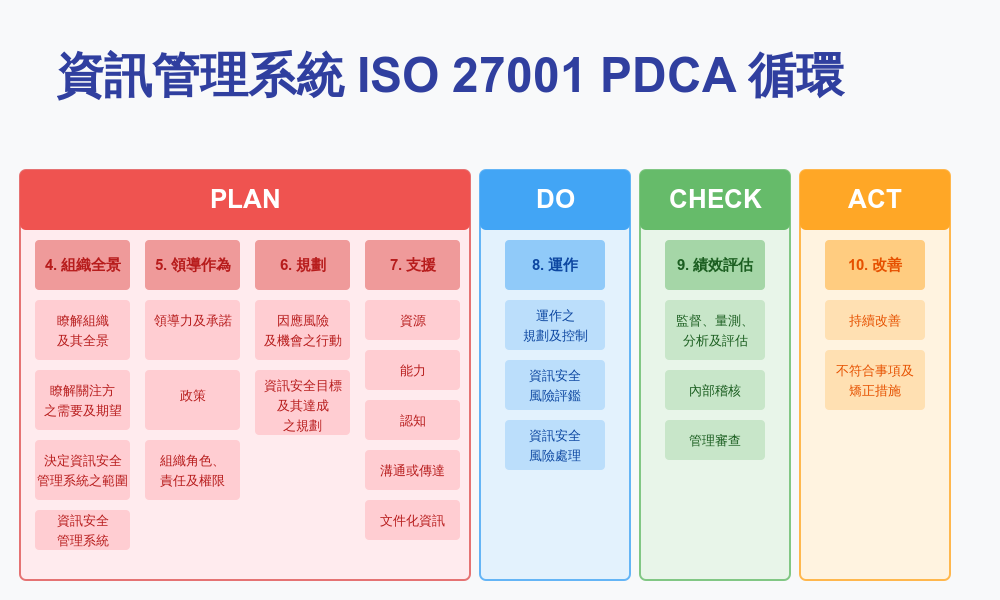
**文件化**

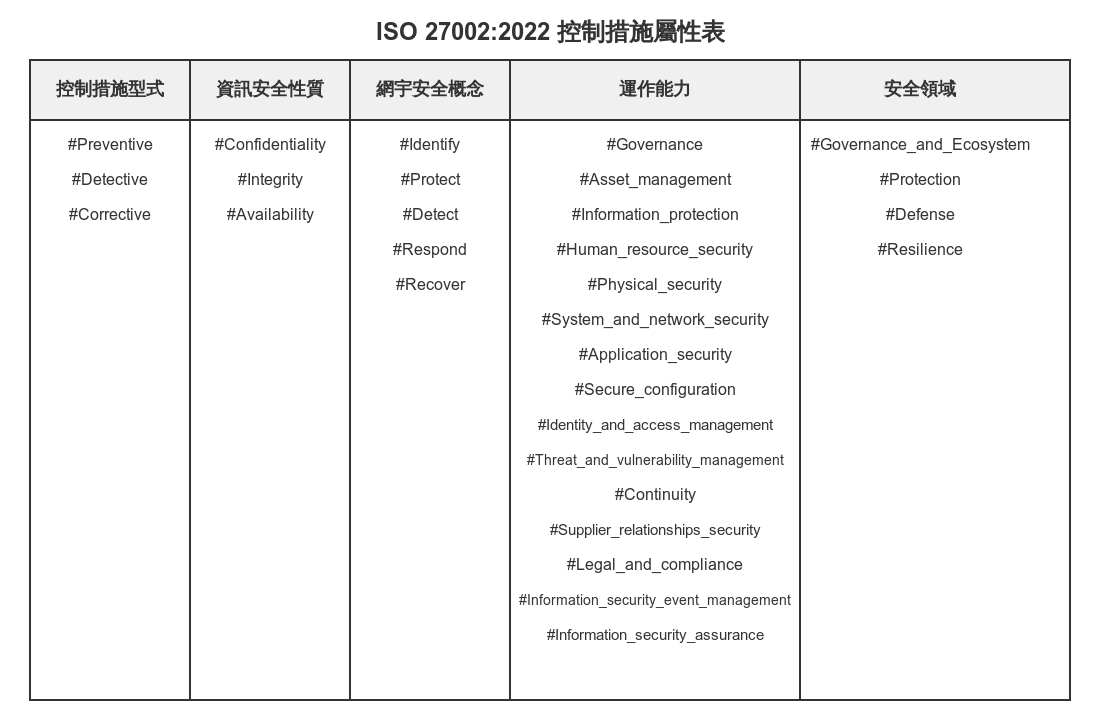
* 在資訊安全管理或其他管理系統的文件管制作業中，通常強調的是：
  + 文件在發布前要經過正式審核與核可程序。
  + 文件發布後需要確保所有應用人員可以取得並使用正確版本，並且定期檢討與更新。
  + 文件的格式（紙本或電子檔）並沒有嚴格限制，重要的是要有一致且可追溯的控管機制。
  + 文件採取措施保護，防止機密性洩露、不當使用或完整性受損。
* ISO 27001 並未規定文件化一定必須採用固定的階層數量或架構，其核心原則是：「組織必須能證明其資訊安全管理系統符合相關標準與要求。」組織可依據自身的規模、業務性質、風險程度以及管理需求，彈性選擇最適合的文件層次與架構設計。
* 常見的文件層次架構包含三階或四階：
  + 三階文件架構：通常包括「政策文件」、「程序書」以及「表單與紀錄」。
  + 四階文件架構：則進一步細分為「政策文件」、「程序書」、「作業規範」及「紀錄與表單」。
* 不論採用何種文件層次，重點是文件必須清晰易懂、易於溝通，並且便於日常維護與更新。以下為一個常見的四階文件架構及其說明：
  + 第一階文件：政策文件（Policy）
    - 資訊安全政策（Information Security Policy）：作為組織資訊安全的最高指導文件，清楚定義組織對資訊安全的整體承諾、政策目標和指導原則。此文件須由最高管理階層批准並公告全體員工。
  + 第二階文件：程序書（Procedures）
    - 描述如何執行特定的流程或作業，以達成資訊安全政策設定的目標，並滿足 ISO 27001 標準要求。
    - 程序書內容通常包含：程序目的與適用範圍、職責與權限分配、具體的活動與步驟、相關參考文件或附錄。
  + 第三階文件：作業規範（Work Instructions）
    - 提供程序書內步驟更詳細且具體的操作步驟說明，使執行人員能夠明確且一致地執行資訊安全相關作業。
    - 作業規範可使用文字步驟、流程圖或檢核表（Checklist）等形式，為組織內必須遵守的操作指引。
  + 第四階文件：紀錄與表單（Records & Forms）
    - 紀錄（Records）：提供證據證明資訊安全管理系統各項作業已依規劃執行，並可用於審核、監控與持續改善之用。紀錄形式可包括紙本文件、電子檔案、照片、錄音等。
    - 表單（Forms）：用於收集、填寫與儲存資訊，支援追蹤、記錄與分析資訊安全管理系統執行成效與狀況。常見形式包含電子表格、調查表、檢查清單等。

| **階層** | **名稱** | **說明** | **範例** |
| --- | --- | --- | --- |
| **第一階** | 政策 (Policy) | 組織資訊安全總體承諾與原則 | 資訊安全政策（含實體安全、網路安全、人員安全、存取控制、風險管理等等） |
| **第二階** | 程序書 (Procedure) | 說明如何達成政策的流程與步驟 | 實體安全管理程序書（門禁管理程序） |
| **第三階** | 作業規範 (Work Instructions) | 說明程序中具體的作業步驟（步驟明確） | 門禁系統操作作業規範 |
| **第四階** | 紀錄與表單 (Records & Forms) | 作業執行證據（紀錄與表單） | 門禁進出登記表 |

* ISO 27001各章節概要：

| **章節** | **說明** |
| --- | --- |
| 第 1 章： 適用範圍 | 說明 ISO 27001 的目的與適用範圍，強調建立、實施、維護與持續改進資訊安全管理系統的要求與框架。 |
| 第 2 章： 引用標準 | 列出 ISO 27001 標準內引用的其他相關標準，這些標準為資訊安全管理系統建置及實施提供必要支援與依據。 |
| 第 3 章： 用語和定義 | 清楚定義 ISO 27001 中的重要術語與定義，以確保對標準內容的理解一致且無歧義。 |
| 第 4 章： 組織全景 | 要求組織分析並理解自身所處的內、外部環境，以及相關方的需求與期望，做為建置資訊安全管理系統的基礎。 |
| 第 5 章： 領導作為 | 強調組織最高管理階層應展現領導力與承諾，制定明確的資訊安全政策，並確保資訊安全管理系統與整體業務戰略一致。 |
| 第 6 章： 規劃 | 要求組織進行資訊安全風險評估，識別、分析與評估風險，並規劃有效的風險處理措施，以達成資訊安全目標。 |
| 第 7 章： 支持 | 要求組織提供充足的資源、培訓人員並提高其資訊安全意識，以及建立有效的溝通機制，確保資訊安全管理系統順利運作。 |
| 第 8 章： 運作 | 要求組織根據風險處理計畫實際實施各項控制措施，並建立及維持相關流程，以有效管理並降低資訊安全風險。 |
| 第 9 章： 績效評估 | 要求組織監控與測量資訊安全管理系統的成效，包括進行內部稽核與管理審查，確保其持續符合標準與組織需求。 |
| 第 10 章： 改善 | 要求組織針對不符合事項採取糾正措施，並持續改善資訊安全管理系統，以提升整體的資訊安全績效。 |
| 附錄 A： 參考資訊安全控制措施 | 提供資訊安全控制措施的建議清單，供組織根據自身需求與風險評估結果進行選擇與實施（具體內容主要參考 ISO 27002:2022 標準）。 |





7.3 保全辦公室、房間及設施



**5. 組織控制措施**

| 5.1 資訊安全政策 | 5.2 資訊安全之角色及責任 | 5.3 職務區隔 |
| --- | --- | --- |
| 5.4 管理階層責任 | 5.5 與權責機關之聯繫 | 5.6 與特殊關注群組之聯繫 |
| 5.7 威脅情資 | 5.8 專案管理之資訊安全 | 5.9 資訊及其他相關聯資產之清冊 |
| 5.10 可接受使用資訊及其他相關聯資產 | 5.11 資產之歸還 | 5.12 資訊之分類分級 |
| 5.13 資訊之標示 | 5.14 資訊傳送 | 5.15 存取控制 |
| 5.16 身分管理 | 5.17 鑑別資訊 | 5.18 存取權限 |
| 5.19 供應者關係中之資訊安全 | 5.20 於供應者協議中闡明資訊安全 | 5.21 管理ICT供應鏈中之資訊安全 |
| 5.22 供應者服務之監視、審查及變更管理 | 5.23 使用雲端服務之資訊安全 | 5.24 資訊安全事故管理規劃及準備 |
| 5.25 資訊之評鑑及決策 | 5.26 對資訊安全事故之回應 | 5.27 由資訊安全事故中學習 |
| 5.28 證據之蒐集 | 5.29 中斷期間之資訊安全 | 5.30 營運持續之ICT備妥性 |
| 5.31 法律、法令、法規及契約要求事項 | 5.32 智慧財產權 | 5.33 紀錄之保護 |
| 5.34 隱私及PII保護 | 5.35 資訊安全之獨立審查 | 5.36 資訊安全政策、規則及標準之遵循性 |
| 5.37 書面記錄之運作程序 |  |  |

**6. 人員控制措施**

| 6.1 篩選 | 6.2 聘用條款及條件 | 6.3 資訊安全認知及教育訓練 |
| --- | --- | --- |
| 6.4 獎懲過程 | 6.5 聘用終止或變更後之責任 | 6.6 機密性或保密協議 |
| 6.7 遠端工作 | 6.8 資訊安全事件通報 |  |

**7. 實體控制措施**

| 7.1 實體安全周界 | 7.2 實體進入 | 7.3 保全辦公室、房間及設施 |
| --- | --- | --- |
| 7.4 實體安全監視 | 7.5 防範實體及環境威脅 | 7.6 於安全區域內工作 |
| 7.7 桌面淨空及螢幕淨空 | 7.8 設備安置及保護 | 7.9 場所外資產之安全 |
| 7.10 儲存媒體 | 7.11 支援之公用服務事業 | 7.12 佈纜安全 |
| 7.13 設備維護 | 7.14 設備汰除或重新使用之保全 |  |

**8. 技術控制措施**

| 8.1 使用者端點裝置 | 8.2 特殊存取權限 | 8.3 資訊存取限制 |
| --- | --- | --- |
| 8.4 對原始碼之存取 | 8.5 安全鑑別 | 8.6 容量管理 |
| 8.7 防範惡意軟體 | 8.8 技術脆弱性管理 | 8.9 組態管理 |
| 8.10 資訊刪除 | 8.11 資料遮蔽 | 8.12 資料洩露預防 |
| 8.13 資訊備份 | 8.14 資訊處理設施之多備 | 8.15 存錄 |
| 8.16 監視活動 | 8.17 鐘訊同步 | 8.18 具特殊權限公用程式之使用 |
| 8.19 運作中系統之軟體安裝 | 8.20 網路安全 | 8.21 網路服務之安全 |
| 8.22 網路區隔 | 8.23 網頁過濾 | 8.24 密碼技術之使用 |
| 8.25 安全開發生命週期 | 8.26 應用系統安全要求事項 | 8.27 安全系統架構及工程原則 |
| 8.28 安全程式設計 | 8.29 開發及驗收中之安全測試 | 8.30 委外開發 |
| 8.31 開發、測試與運作環境之區隔 | 8.32 變更管理 | 8.33 測試資訊 |
| 8.34 稽核測試期間資訊系統之保護 |  |  |

2. 下列何項「不」是ISO/ IEC 27001:2022資訊安全目標應滿足之事項？

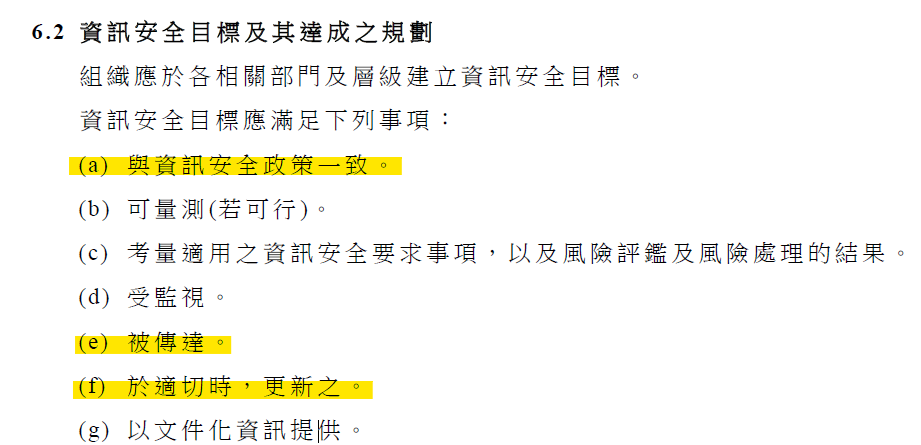
(A) 與資訊安全政策一致 (a)

(B) 於適切時，更新之 (f)

(C) 被傳達 (e)

(D) 以紙本文件提供 (並未要求資訊安全目標必須以紙本文件形式提供，文件形式可以是電子或其他方式)

114-1 規劃 答案D



12. 依照CNS 27002:2023的建議，於使用電子通訊設施進行資訊傳送時，規則、程序及協議宜考量下列那些項目？（複選）

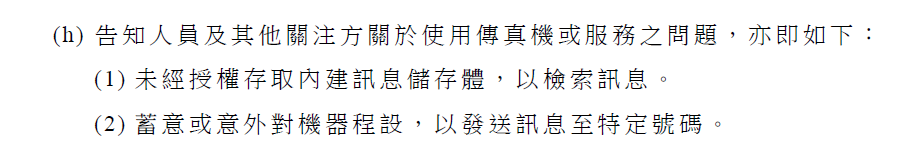
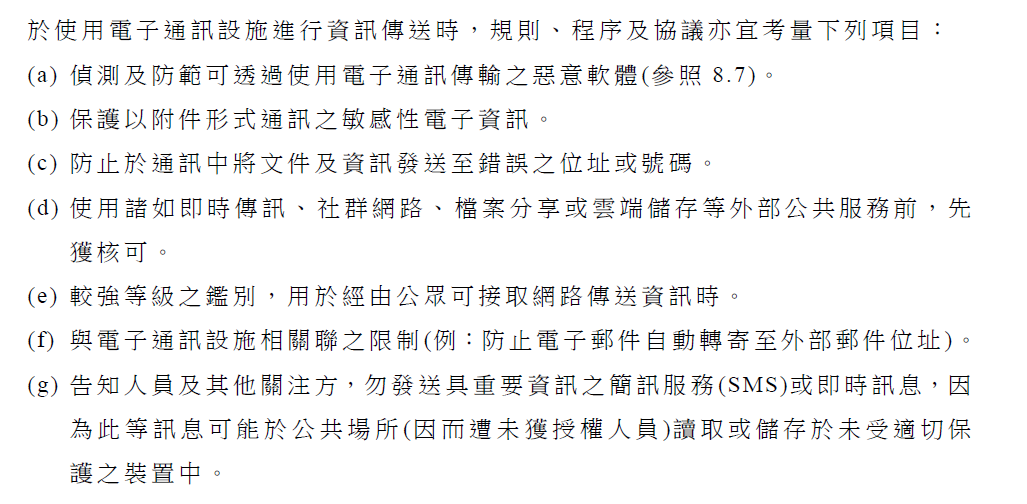
(A) 偵測及防範可透過使用電子通訊傳輸之惡意軟體 (a)

(B) 方便使用者存取，電子郵件自動轉寄至外部郵件位址 (此舉可能導致資訊外洩，不符合安全通訊規範。)

(C) 保護以附件形式通訊之敏感性電子資訊 (b)

(D) 依使用者習慣自主使用即時傳訊等外部公共服務 (使用外部公共服務存在較大的風險，應在管理上加以限制而非放任使用。)

114-1 規劃 答案AC



1. X公司為在中華民國註冊登記之公司，該公司將於在2024年導入資安管理制度。並預計於2025年第一季通過國際資安驗證，請問下列何項制度最適合X公司做為導入資訊安全管理制度依循之參考？

(A) ISO/IEC 27001 : 2013 (2013 為較舊版本，而ISO/IEC 27001 : 2022 為最新版本，能更符合最新的資訊安全趨勢與要求。)

(B) ISO/IEC 27004 : 2016 (主要聚焦於資訊安全測量，而非完整的管理系統架構)

(C) ISO/IEC 20000 : 2018 (則是針對 IT 服務管理的標準，不適用於資訊安全管理系統的架構。)

(D) ISO/IEC 27001 : 2022

113-2 防護 答案D



1. 關於資訊安全管理系統的描述，下列何項正確？

(A) 資訊安全管理系統最主要在提供組織用以建立、實作、維持及持續改善與資訊安全有關的事項 (正確描述了資訊安全管理系統的主要功能，即為組織提供一個系統化的框架，以建立、實施、維持與持續改進資訊安全相關的策略和措施。)

(B) 影響資訊安全管理系統的風險因素，皆不會隨時間而改變 (影響ISMS的風險因素會隨著威脅環境、技術進步以及組織內外部環境的變化而改變。)

(C) 組織所採用的資訊安全管理系統實作的措施，皆不會隨時間而改變 (組織所採用的資訊安全措施必須隨著風險評估、技術進步和業務需求而進行調整與更新，不能一成不變。)

(D) 組織資訊安全管理系統的建立及實作，不會因為規模大小及性質所影響 (組織的規模、性質和業務範圍會影響資訊安全管理系統的範圍、資源配置和實施方式，因此建立及實作資訊安全管理系統必須考慮這些因素。)

113-2 管理 答案A

2. 組織向第三方驗證公司申請ISO 27001資訊安全管理系統證書，下列步驟何項正確？

(A) 初次驗證通過後，需要不定期重新驗證以取得證書 (ISO 27001 證書取得後並非「不定期」重新驗證，而是需要定期進行監督審核（通常每年）以及每三年進行一次再認證審核。)

(B) 初次申請驗證流程，分為文件審查與實地審查兩個階段

(C) 重新審查只需要進行文件審查即可 (重新審查（監督審核或再認證）通常也包括現場審查，不僅僅是文件審查。)

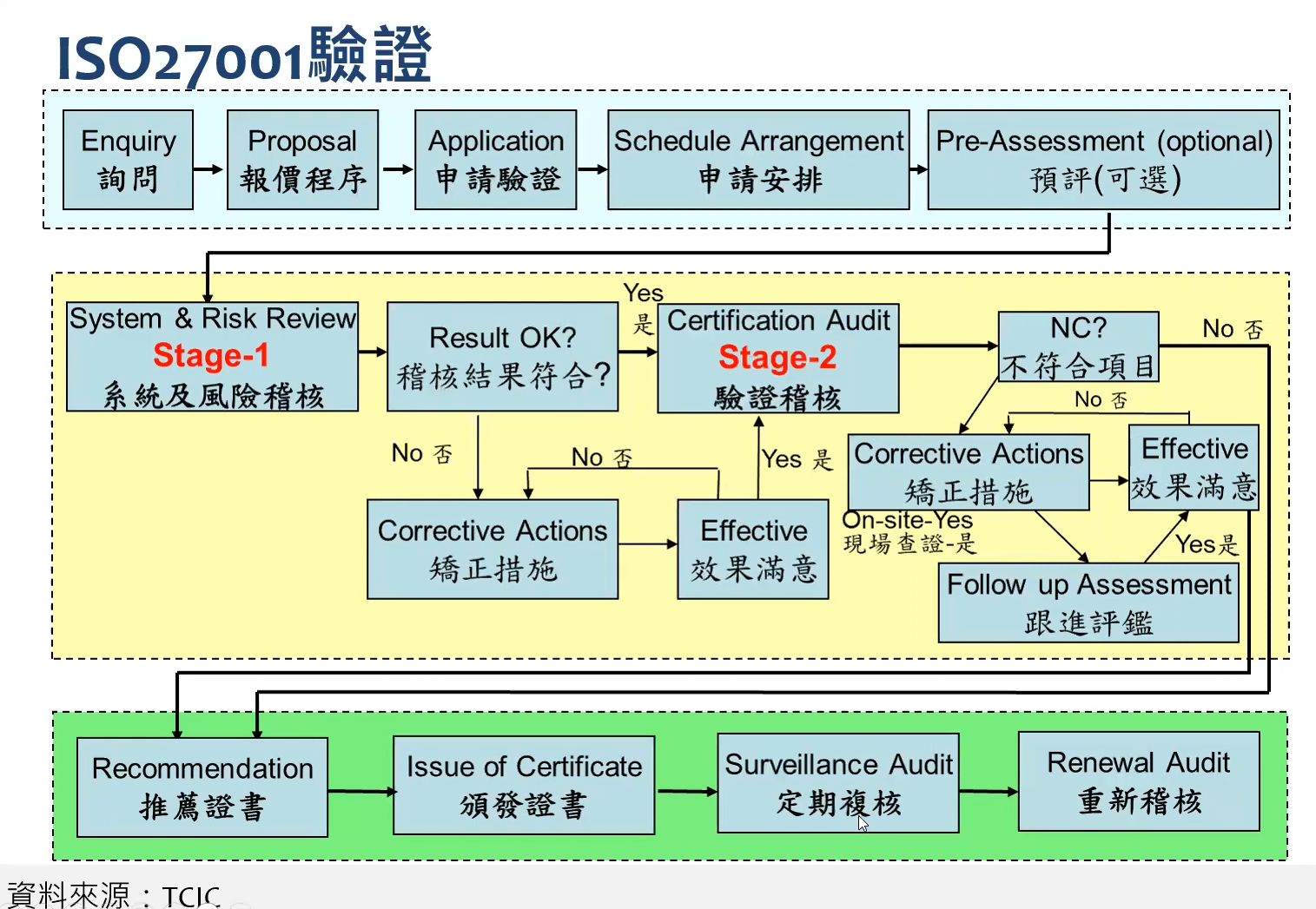
(D) 組織取得通過驗證證書後，三年進行一次重新審查即可延續證書有效期限 (雖然認證有效期一般為三年，但在此期間必須進行定期監督審核，僅三年一次再認證並不足以延續證書有效期限。)

113-2 管理 答案B

(ISO 27001 認證的初次申請流程一般分為兩個主要階段：

文件審查（Stage 1 Audit）：這階段主要檢查組織的文件、程序、範圍定義等是否符合標準要求，以及準備情況如何。

實地審查（Stage 2 Audit）：實地審查則是到現場進行驗證，評估實際執行情況是否符合已制定的管理制度和標準要求。)



資料來源：TCIC

3. 下列何者「不」是ISO/IEC 27001:2022轉版變化的重點？

(A) 管理系統與ISO結構的一致性 (新版本進一步與 ISO 的高階結構（Annex SL）保持一致，以便與其他管理系統標準整合。)

(B) 簡化標題 (透過簡化與重新命名部分條款與標題，使文件結構更加明晰與易於理解。)

(C) 新增控制項目 (在附錄 A 中對控制項目進行了調整，有的控制項被合併，有的則是新增，以反映現代資訊安全需求。)

(D) 驗證範圍調整 (並非此次轉版的重點。ISO/IEC 27001 的修訂並未特別強調對驗證（認證）範圍的調整，驗證範圍仍由組織依其自身環境和需求來定義。)

113-2 管理 答案D



5. 組織應於各相關部門及層級建立資訊安全目標，請問下列何項「不」是規劃資訊安全目標主要考慮事項？

(A) 與資訊安全政策一致

(B) 以文件化資訊提供

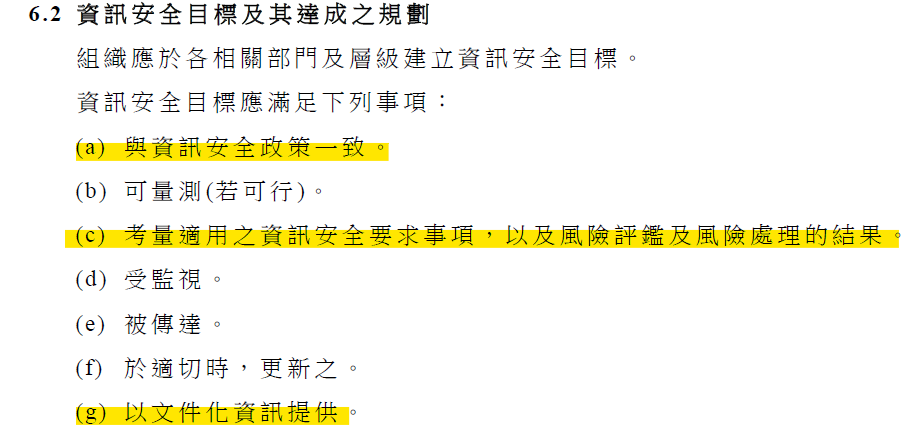
(C) 應符合適切性

(D) 容易達成

113-2 管理 答案D

(在規劃資訊安全目標時，應考慮以下主要事項：

* 目標必須與資訊安全政策一致，確保整體方向協同一致。
* 目標應針對組織的風險、需求與資源狀況，達到適當性（即適用且合理）。
* 目標通常需要記錄成文件，便於傳達與追蹤（但這屬於文件化管理的要求，而非目標內容本身的考量）。)



1. ISO 27001 ISMS最新版本已於2022年修正發布了，相較於

前一個2013年版本，該文件增加了哪些安全管理用詞？

(A) Cybersecurity；Information Security

(B) Privacy Protection；Information Security

(C) Cybersecurity；Privacy Protection；Information Security

(D) Cybersecurity；Information Security；Data Protection

113-1 管理 答案C

(ISO/IEC 27001:2022 在更新版本中，除了繼續強調「Information Security」外，還引入了額外的安全管理用詞，包括「Cybersecurity」以及「Privacy Protection」兩個概念。這些用詞的加入旨在更全面地涵蓋現代資訊環境中網路安全與隱私保護的重要性，相較於 2013 版本，ISO 27001:2022 在安全管理的維度上更加廣泛和細緻。)



3. 資訊安全管理系統（Information Security Management System ISMS）的導入步驟中，稽核活動的主要目的為下列何項？

(A) 確保該管理系統的完整性

(B) 評估員工的績效表現

(C) 檢查環境硬體設備的完整程度

(D) 確保該管理系統內部控制的有效性

113-1 管理 答案D

(內部稽核在資訊安全管理系統中主要的目的在於評估和確認組織內部控制措施的執行效果，確保這些控制措施能夠達到預期的安全目標，從而保障整個管理系統的運作符合規範。這與檢查硬體設備的完整程度或評估員工績效無關。)

1. 關於資訊安全管理系統的敘述，下列何者錯誤？

(A) ISO 27001 2022是目前最新版本 (ISO/IEC 27001 在 2022 年發布了新版，是目前最新版。)

(B) 建立資訊安全管理系統必須以ISO 27001為架構 (雖然 ISO/IEC 27001 是全球普遍採用的資訊安全管理系統標準，但建立資訊安全管理系統並非「只」能依循 ISO 27001，也可以依據其他框架（如 NIST、COBIT、企業自訂框架等）。因此「必須」的說法過度絕對，並不正確。)

(C) 機密性、可用性、完整性是 ISO 27001最主要的資安3要素 (這是資訊安全的核心三要素，亦為 ISO 27001 中的重要概念。)

(D) ISO 27001資訊安全管理系統是一個持續改善的架構 (ISO 27001 採用 PDCA 循環，強調不斷檢討與改進。)

112-2 管理 答案B

8. 關於 ISO 27001 2022的敘述，下列何者錯誤？

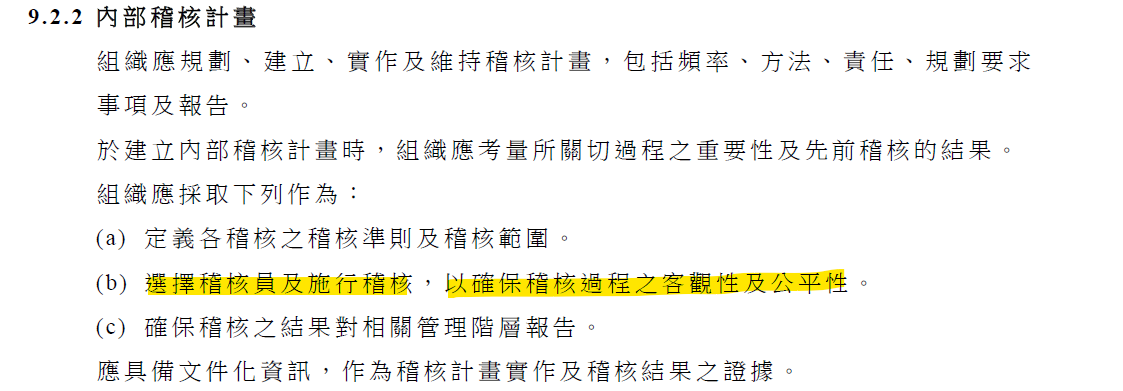
(A) ISO 27001 2022關於內部稽核活動之安排，內部稽核員可以查核自己的工作 (依 ISO 27001 的要求，內部稽核需維持客觀性與公正性，避免利益衝突。通常明確規範稽核人員「不得稽核自己本身負責之工作」(不可自我稽核)，以確保獨立性。)

(B) ISO 27001 2022強調持續改善之要求 (ISO 27001（不論是 2013 或 2022 版）都遵循 PDCA 循環，強調持續改善。)

(C) ISO 27001 2022附錄A區分為4個領域 (2022 版的附錄 A 依據 「組織控制」、「人員控制」、「實體控制」以及「技術控制」 這四個大類來重新整理控制項。)

(D) ISO 27001 2022附錄A共有 93個控制項 (從 2013 版的 114 項精簡整合為 93 項，同時新增了屬性標籤等概念。)

112-2 管理 答案A



1. X公司為在中華民國註冊登記之公司，該公司將於2023年導入資安管理制度並預計於2024年第一季通過國際資安驗證，請問下列何項制度最適合X公司做為導入資訊安全管理制度依循之參考？

(A) ISO/IEC 27001 : 2013 (是較舊的版本（2013 年版），目前已有 2022 年版可用。)

(B) ISO/IEC 27004 : 2016 (主要針對資訊安全測量（Measuring ISMS）的原則，並非用來建立整體 ISMS 的完整框架。)

(C) ISO/IEC 20000-1 : 2018 (為 IT 服務管理（IT Service Management）的國際標準，並非資訊安全管理系統的標準。)

(D) ISO/IEC 27001 : 2022

112-1 規劃 答案D



2. 關於文件管制措施，下列敘述何者正確？

(A) 所有制定的SOP皆須以書面發行 (現代管理常使用電子檔案、雲端文件或網頁等方式發佈 SOP，未必需要紙本發行。)

(B) 制定的各項管理制度、程序，不宜以電子檔案公佈 (電子方式便於更新與取得，目前組織普遍以電子形式公佈、維護與查詢。)

(C) 所制訂相關作業程序必須以四階文件來發行 (文件層級的劃分方式沒有「一定要四階文件」的硬性規定，不同組織可以自行設計文件層級與結構。)

(D) 文件管制宜制定標準作業核可及發行流程，以利組織成員遵循 (文件管制的核心在於有系統的審核、核可、發行以及後續的版本管控，確保組織成員使用到正確、有效的文件。)

112-1 管理 答案D

3. 資訊安全政策是資訊安全管理系統中的最高指導原則，有不可缺少的重要性，下列敘述何者正確？

(A) 滿足相關的要求事項的承諾後，無需定期審查目前要求 (資訊安全政策需因應環境、法規、組織需求的變化而定期檢討與修正。ISO 27001 也要求政策應定期評估並更新。)

(B) 資訊安全政策不一定須由最高管理階層審核 (資訊安全政策屬於組織資訊安全管理之最高層級文件，必須經過最高管理階層的批准與支持，才能確保在組織內部落實執行。)

(C) 建立的資訊安全政策必須與組織的目的及資安目標相容一致 (資訊安全政策需反映組織的使命、目標、策略，並和資訊安全管理的其他方針與目標相互呼應。)

(D) 屬於內部或機密文件，不可對外公告 (雖然資訊安全政策的細節（如內部程序）可能不完全公開，但組織通常會對外釋出一份高階或概括的資訊安全政策聲明（或摘要），以展示組織對資訊安全的承諾。)

112-1 管理 答案C

5. 請問在資訊安全管理系統中的風險評鑑（Risk Assessment）作業，是在Plan（規劃）、Do（執行）、Check（檢查）、Act（改善）循環中的那一部分？

(A) Plan（規劃）

(B) Do（執行）

(C) Check（檢查）

(D) Act（改善）

112-1 管理 答案B

(ISO 27001在「條款 6 Planning」中，確實包含了「6.1.2 資訊安全風險評鑑」。但在實務或某些考題中，會將「實際去做盤點、做評鑑」視為執行面 (Do)，而「訂定要如何盤點、用什麼方法做風險評鑑」視為策劃面 (Plan)。  
如果題目的脈絡是「組織已開始動手做盤點、實際建立清冊並進行風險評鑑」，很可能該題目就將此動作歸類為「Do」，因為他們認為「Plan」是先前已經完成了「確立目標、制定計畫」的過程。)

8. 立案於我國的A公司主要營業活動市場位於中華人民共和國及新加坡並將以ISO 27001架構公司之資訊安全管理系統，下列何項要求在其架構資訊安全管理系統時，並非優先考量項目？

(A) ISO 27001：2022 (A 公司要導入資訊安全管理系統，本身就要遵循此標準。)

(B) 個人資料保護法（中華民國） (雖然營業市場在中國大陸與新加坡，但 A 公司「立案於台灣」且在台灣經營，也必須遵守台灣的個資法，尤其若公司有處理台灣境內個人資料。)

(C) 歐盟一般資料保護法規（General Data Protection Regulation, GDPR） (GDPR 主要適用於歐盟境內的個人資料處理。題目並沒有說 A 公司在歐盟有業務或客戶，亦未提及歐盟用戶的資料。)

(D) 網路安全法（中華人民共和國） (A 公司主要營業活動在中國大陸，必然要遵循當地關於資訊安全與個資保護的法令，包括《網路安全法》及相關配套措施。)

112-1 管理 答案C

12. 從 ISO 27001:2022附錄 A「參考控制目標及控制措施」中，

下列哪些是「實體控制措施」相關的規範或控制措施？

(A) 實體進入控制措施

(B) 遠端工作應提出申請 (這與組織對「遠端工作」的策略、流程與授權有關，屬於較偏組織性或人員控制，而非專注在「實體場域」的安全。)

(C) 維護設備，以確保其持續之可用性及完整性

(D) 未經事前授權，不得將設備、資訊帶出場域外

112-1 規劃 答案ACD

21. ISO/IEC 27001是資訊安全管理的國際標準，ISO 27001認證

是在確保公司擁有一套安全穩固的資訊管理系統來保護公司內部重要的資訊財產。下列敘述何者錯誤？

(A) ISO/IEC 27001設計是針對IT部門進行管理 (ISO/IEC 27001並非只局限於 IT 部門，而是針對組織整體資訊資產的管理。它適用於整個組織的資訊安全管理體系，包括流程、人員、技術及組織治理等面向。並不是「只給 IT 部門使用」或「只管 IT 技術」而已。)

(B) 建構資訊安全管理系統（Information Security Management System, ISMS）是以具系統性的方法來保護資訊安全。取得 ISMS的認證也能增加企業或組織的可信度，並且為公司帶來正面的影響及信任

(C) 組織應架構一項風險處理計畫以鑑別適當管理措施、資源、職責及優先順序，以便管理資訊安全風險

(D) 組織應依規劃之期間施行內部稽核，以提供資訊安全管理系統相關資訊，最後階段必須保存文件化資訊作為稽核計畫及稽核結果之證據

112-1 防護 答案A

35. ISO/IEC 27002於2022年2月發布最新版本，該版本與 2013年版本的差異之一，是增加控制措施的屬性標籤，其中一項是「類別」，共有預防、偵測與矯正等3項，請問系統資料備份比較偏向下列哪一類型？

(A) 預防（Preventive）

(B) 偵測（Detective）及矯正

(C) 矯正（Corrective） (「系統資料備份」本身的核心用途是：在發生資料損毀或意外時，可透過備份進行還原，恢復到先前的正常狀態。因此，它主要是用來「矯正」受損的系統與資料，而非直接阻止事件發生或偵測事件。)

(D) 預防及偵測

112-1 規劃 答案C

(在 ISO/IEC 27002 的控制措施分類中，通常可區分為下列三種類型：

1. 預防（Preventive）：在安全事件發生前就先阻止或避免事件發生。例如存取控制（限制未授權使用者進入）、防毒軟體阻擋惡意程式執行等。
2. 偵測（Detective）：用於偵測或發現已經發生的事件或異常狀況。例如日誌記錄、入侵偵測系統（IDS）等。
3. 矯正（Corrective）：發生事件或異常後，用於恢復或修正系統與資料，將狀態矯正至正常。如備份還原機制、災難復原計畫（DRP）等。)

2. 高階管理階層（資安長）在資訊安全管理系統中所展現領導與承諾，「不」包含下列何項？

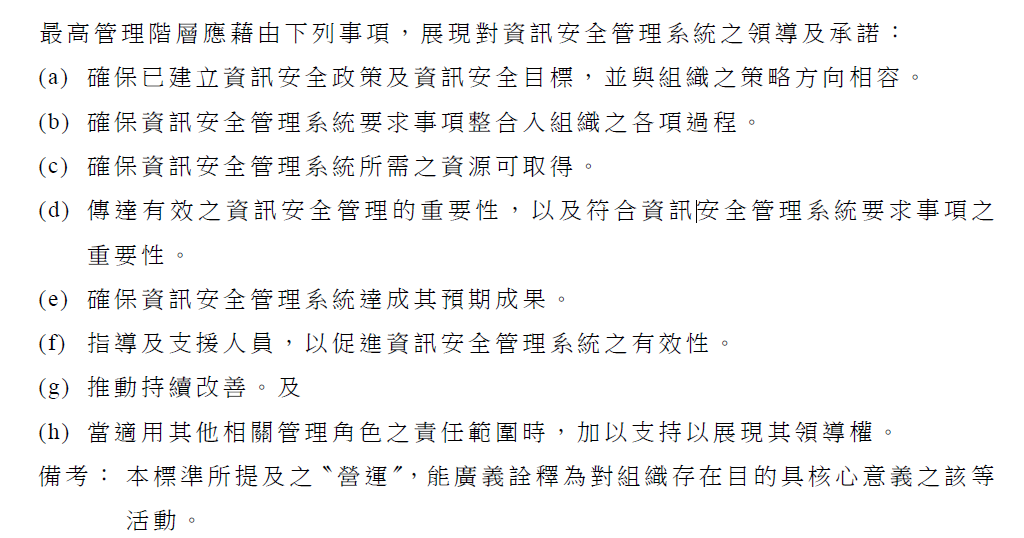
(A) 確保建立的資訊安全政策及資訊安全目標，必須與組織發展方向相容 (a)

(B) 整合人員、組織及提供所需的支援，確保資訊安全管理系統的要求 (b)

(C) 向組織內部所有人員說明資訊安全產品的設定 (此為較「技術與執行層級」的工作內容，通常由資訊部門或具備相關專業技術的人員執行。高階管理階層主要負責政策與資源、方向與支持，並不會(也不應)親自教導每個人如何設定安全產品。)

(D) 確保資訊安全管理系統達成預期的成效 (e)

111-2 管理 答案C



5. 資訊安全管理系統遵照計畫（Plan）、執行（Do）、檢查（Check）及行動（Act）等四個程序，不斷的改進。請問「建立及執行管理程序」是屬於下列哪一個程序？

(A) 計畫（Plan） (訂定目標與策略、規劃要如何達成目標、建立政策與需求，制訂大方向及計畫書。)

(B) 執行（Do） (依照先前規劃的內容去落實、建立並執行各項管理程序或控制措施。)

(C) 查核（Check） (監控與衡量執行結果，並進行內部稽核或審查。)

(D) 行動（Act） (根據檢查結果進行改善與修正，調整計畫或程序以持續優化。)

111-2 管理 答案B

1. 在 ISO27000系列標準中，下列何者為建置資訊安全管理系統的實作指引 (Information security management systems — Guidance)？

(A) ISO/IEC 27001 (規範資訊安全管理系統之「要求」，屬於可用來認證的標準。)

(B) ISO/IEC 27002 (提供資訊安全管控措施的「實務準則」，著重在管控措施的選擇與指引。)

(C) ISO/IEC 27003 (提供資訊安全管理系統之「建置與實作指引」，協助組織導入、推行資訊安全管理系統的操作說明。)

(D) ISO/IEC 27004 (著重在「資訊安全管理測量」的架構與方法。)

111-1 規劃 答案C

2. 組織已開始著手進行資訊資產之盤點、建立清冊，並實施風險評鑑作業，請問此作業屬於PDCA循環之何者階段？

(A) P（Plan）

(B) D（Do）

(C) C（Check）

(D) A（Act）

111-1 管理 答案B

(ISO 27001在「條款 6 Planning」中，確實包含了「6.1.2 資訊安全風險評鑑」。但在實務或某些考題中，會將「實際去做盤點、做評鑑」視為執行面 (Do)，而「訂定要如何盤點、用什麼方法做風險評鑑」視為策劃面 (Plan)。  
如果題目的脈絡是「組織已開始動手做盤點、實際建立清冊並進行風險評鑑」，很可能該題目就將此動作歸類為「Do」，因為他們認為「Plan」是先前已經完成了「確立目標、制定計畫」的過程。)

3. 下列何者為國際上受到業界認可，並可驗證的資訊安全管理系統

（Information Security Management System, ISMS）標準？

(A) ISO 9001 (品質管理系統標準，與資訊安全無直接關係。)

(B) ISO 27000 (資訊安全管理系統家族標準的術語及基本原則說明，無法進行驗證。)

(C) ISO 27001 (國際公認之資訊安全管理系統標準，是業界廣泛認可且可接受第三方驗證（認證）的標準。)

(D) ISO 27002 (資訊安全控制措施之實務指引，提供詳細的實施指引與建議，但無法用於驗證與認證。)

111-1 管理 答案C

19. 關於資訊安全管理系統在決定驗證範圍時，須包含下列哪些考量議題？（複選）

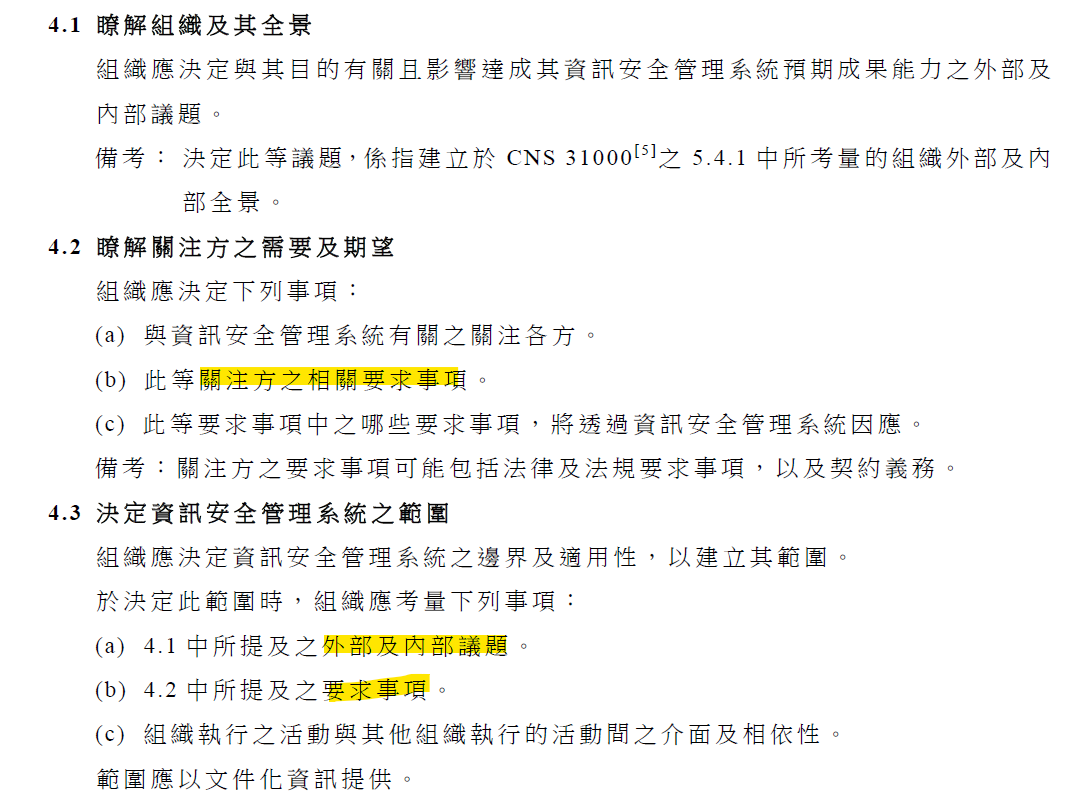
(A) 組織內部與外部的議題 (資訊安全管理系統必須考量組織內外環境、利害關係人的需求及期待，以確保範圍的適切性。)

(B) 主管機關的要求 (主管機關或監管單位提出的特定規範或要求，需納入資訊安全管理系統範圍。)

(C) 適用法令與法規的要求 (法規要求通常是資訊安全管理系統必須遵守的重要因素，必須納入考量。)

(D) 組織與其他組織履行活動間的介面及相依性 (因為其他組織可能影響或受影響於該組織的資訊安全，故需納入考量。)

111-1 規劃 答案ABCD



38. 資訊安全管理系統（Information Security Management System, ISMS）採用PDCA 循環的概念，下列何者「不」包含在此流程中？

(A) 高階管理審查會議 ( 屬於「Check」階段)

(B) 業務達成率審查 (屬於業務經營績效審查，非直接與資訊安全管理系統相關，不在PDCA流程中)

(C) 內部稽核執行 (屬於「Check」階段)

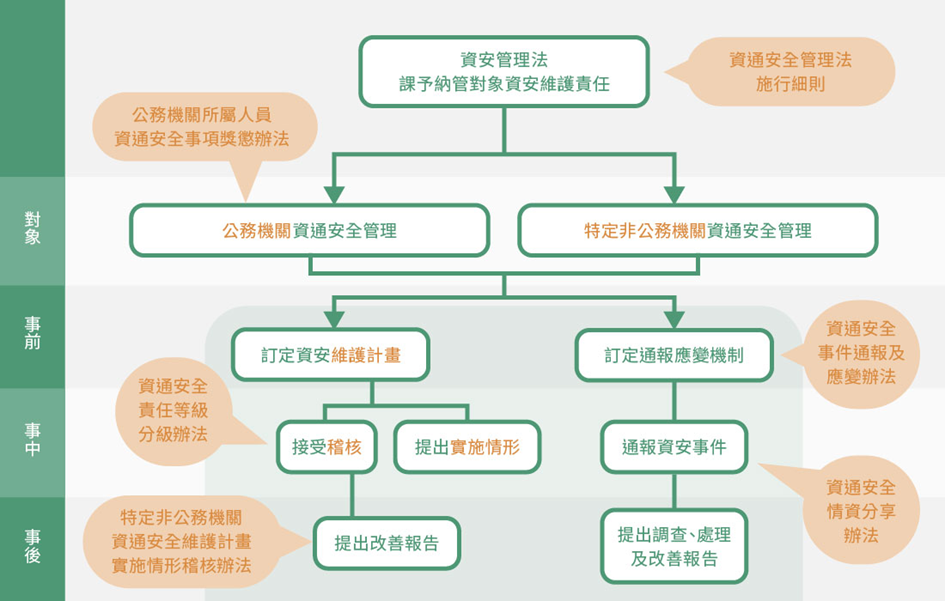
(D) 災難復原計畫演練 (屬於「Do」階段)

111-1 管理 答案B

資通安全管理法

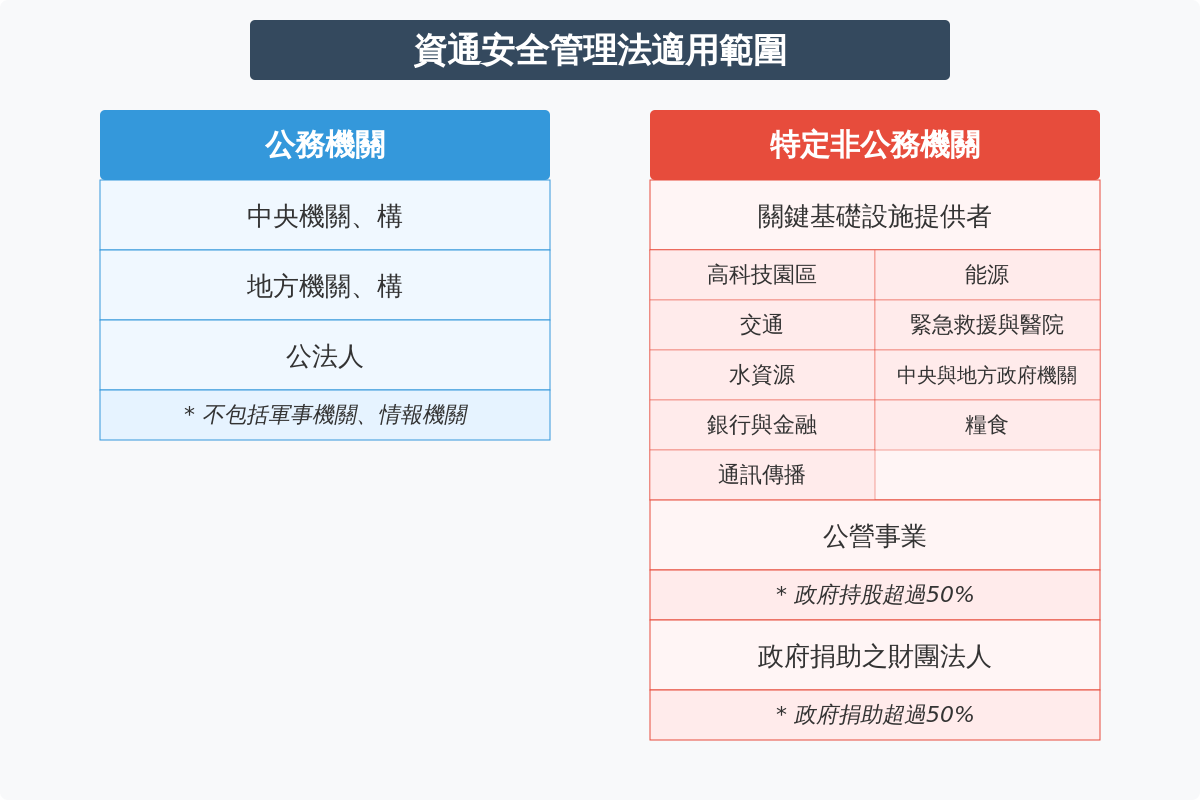
**資通安全管理法**

* 制定目的：為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。
* 法條框架：
  + 主法：
    - 資通安全管理法。
  + 次法：
    - 資通安全管理法施行細則。
    - 資通安全責任等級分級辦法。
    - 資通安全事件通報及應變辦法。
    - 特定非公務機關資通安全維護計畫實施情形稽核辦法。
    - 資通安全情資分享辦法。
    - 公務機關所屬人員資通安全事項獎懲辦法。



(資料來源：數位發展部資通安全署)

* 納管對象：
  + 公務機關：中央、地方機關，不含軍事和情報機關。
  + 非特定公務機關：關鍵基礎設施提供者、公營事業、政府捐助財團法人。



(資料來源：筆者自行整理，114年2月關鍵基礎設施新增糧食)

**資通安全維護計畫**

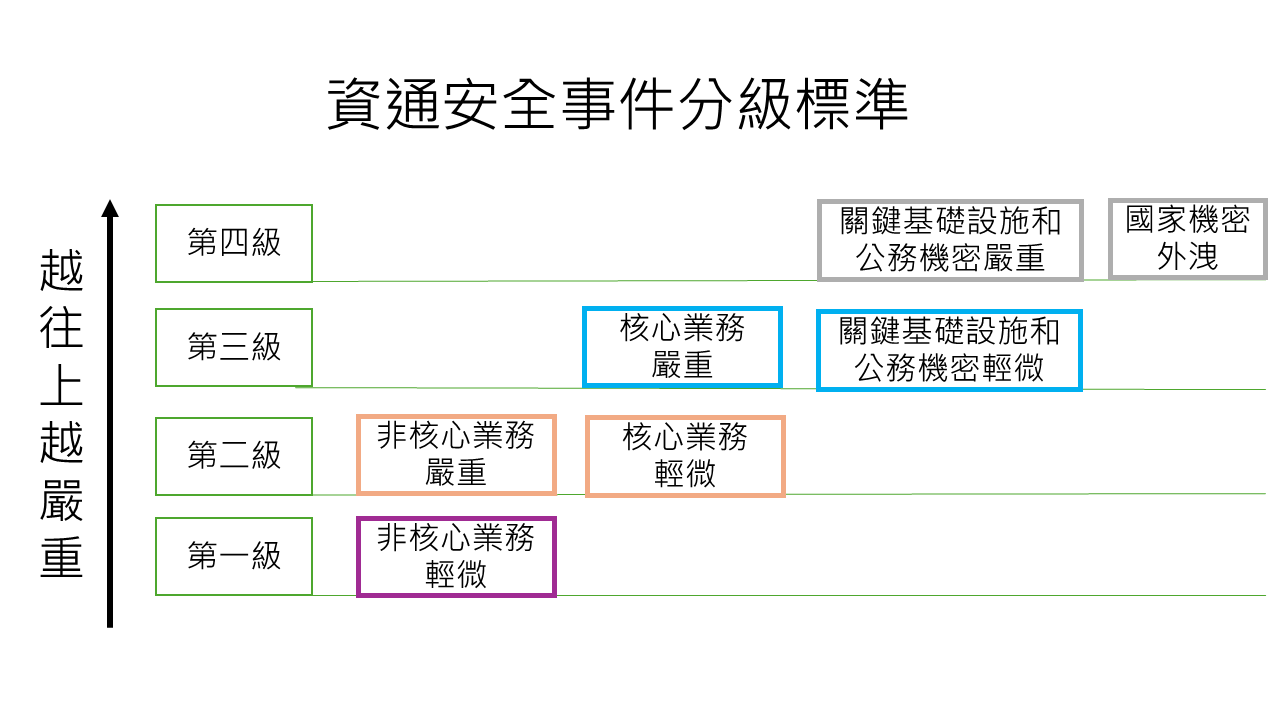
* 一、核心業務及其重要性。
* 二、資通安全政策及目標。
* 三、資通安全推動組織。
* 四、專責人力及經費之配置。
* 五、公務機關資通安全長之配置。
* 六、資通系統及資訊之盤點，並標示核心資通系統及相關資產。
* 七、資通安全風險評估。
* 八、資通安全防護及控制措施。
* 九、資通安全事件通報、應變及演練相關機制。
* 十、資通安全情資之評估及因應機制。
* 十一、資通系統或服務委外辦理之管理措施。
* 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。
* 十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

**資通安全責任等級分級辦法**

* 分級規則：
  + A級：全國性重要 (如油水電關鍵基礎設施提供者)。
  + B級：區域或地區性重要。(如公立區域醫院或地區醫院)
  + C級：自行或委外設置、開發之資通系統。
  + D級：自行辦理資通業務，未維運自行或委外設置、開發之資通系統者。
  + E級：無資通系統且未提供資通服務。
* 要求：
  + C級以上機關要求較多，機關等級以下按風險降低逐步減少要求。
* 資通系統防護需求分級原則：
  + 分級依據：根據機密性、完整性、可用性、法律遵循性四構面中最高需求等級決定。
  + 分級類別：分為高、中、普三等級。
  + 執行依據：按資通系統防護基準實施控制措施。

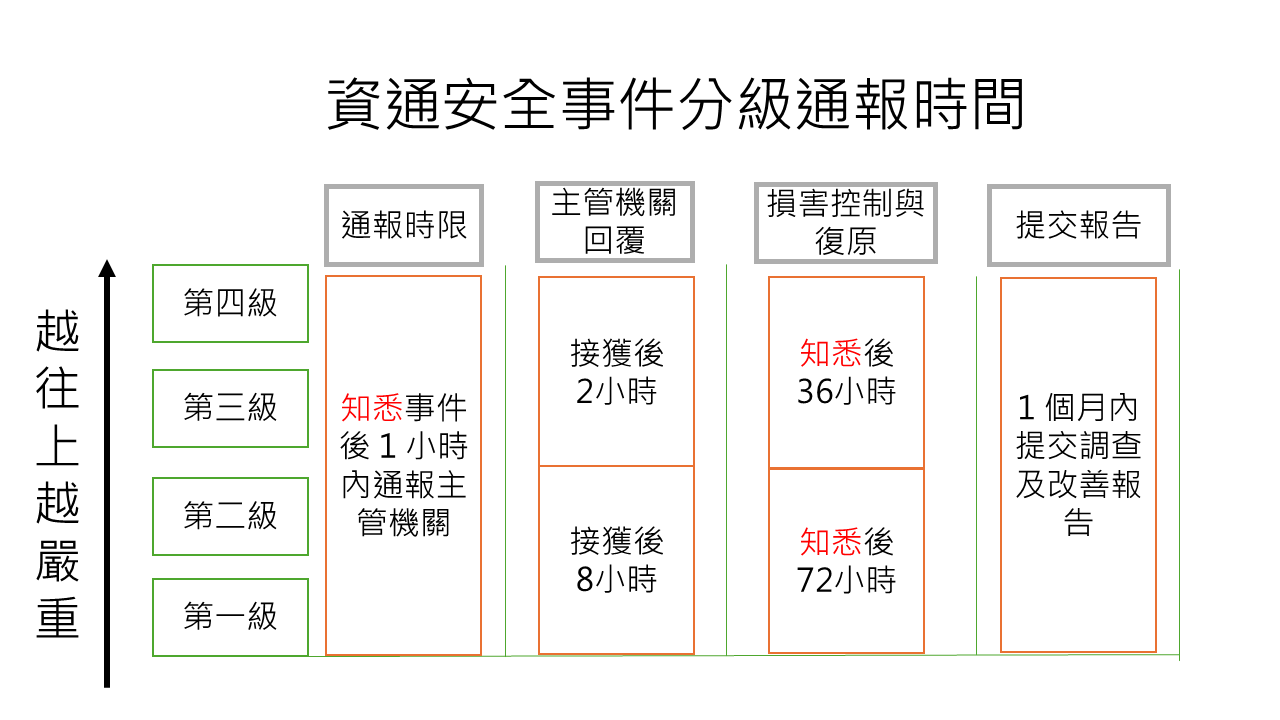
**資通安全事件通報及應變辦法**

* 分級標準（四級事件）
  + 第一級：非核心業務輕微影響。
  + 第二級：非核心業務嚴重影響，或核心業務輕微影響。
  + 第三級：核心業務嚴重影響，或關鍵基礎設施和公務機密輕微影響。
  + 第四級：關鍵基礎設施或公務機密嚴重影響，國家機密外洩。



(資料來源：筆者自行整理)

* 通報內容：
  + 一、發生機關。
  + 二、發生或知悉時間。
  + 三、狀況之描述。
  + 四、等級之評估。
  + 五、因應事件所採取之措施。
  + 六、外部支援需求評估。
  + 七、其他相關事項。
* 通報規範：
  + 通報時限：知悉事件後 1 小時內通報主管機關。
  + 主管機關回覆時間：
    - 第一級與第二級：8小時內。
    - 第三級與第四級：2小時內。
  + 損害控制與復原：知悉事件後
    - 第一級與第二級：72小時內。
    - 第三級與第四級：36小時內。
  + 報告提交：1 個月內依主管機關指定之方式，送交調查、處理及改善報告提交調查及改善報告。
* 資通安全演練作業：
  + 公務機關和特定非公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包含：
    - 網路攻防演練
    - 情境演練
    - 其他必要之演練



(資料來源：筆者自行整理)

**資通安全管理法罰則**

* 公務機關
  + 按其情節輕重，依相關規定予以懲戒或懲處。(記法：公務機關罰鍰沒用)
* 非公務機關
  + 未依規定通報通報資通安全事件：由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。
  + 其他：由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰。

**考古題：**

4. 2024/05/13韓國警察廳國家搜查本部發出聲明，韓國法院近1TB資料遭竊，是該國司法單位首度遭到敵對駭客攻擊。攻擊者至少從 2021年 1月 7日就入侵該國法院，但因記錄過期遭到清除，無法確認是否早已滲透，亦無從得知事故原因。借鑒此案例，若依據我國「資通安全責任等級分級辦法」與「各機關資通安全事件通報及應變處理作業程序」 等所規定，資安事件跡證保存之規劃下列那些最正確？ （複選）

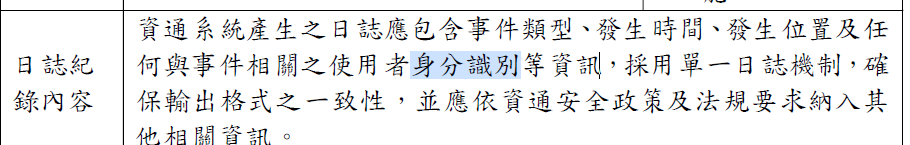
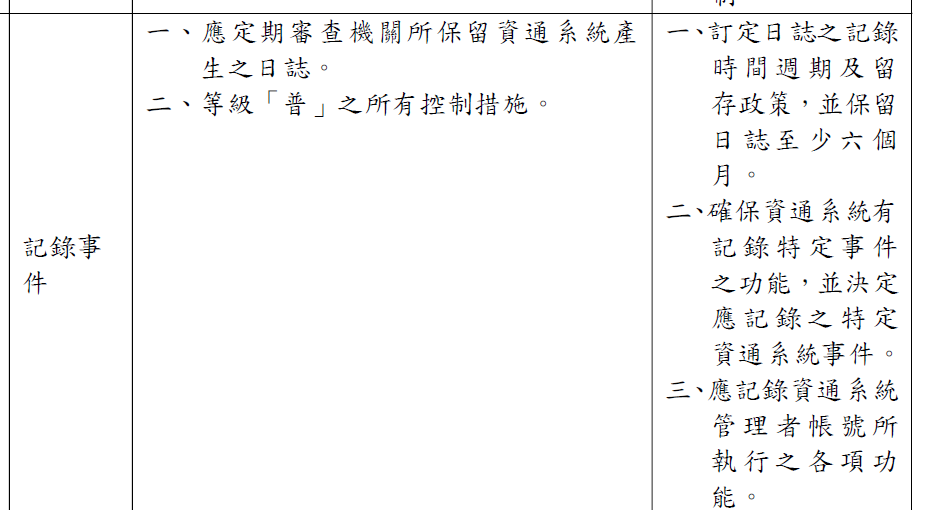
(A) 日誌留存依機關等級而異，等級「普」至少六個月而等級「高」為兩年 (普中高都是六個月)

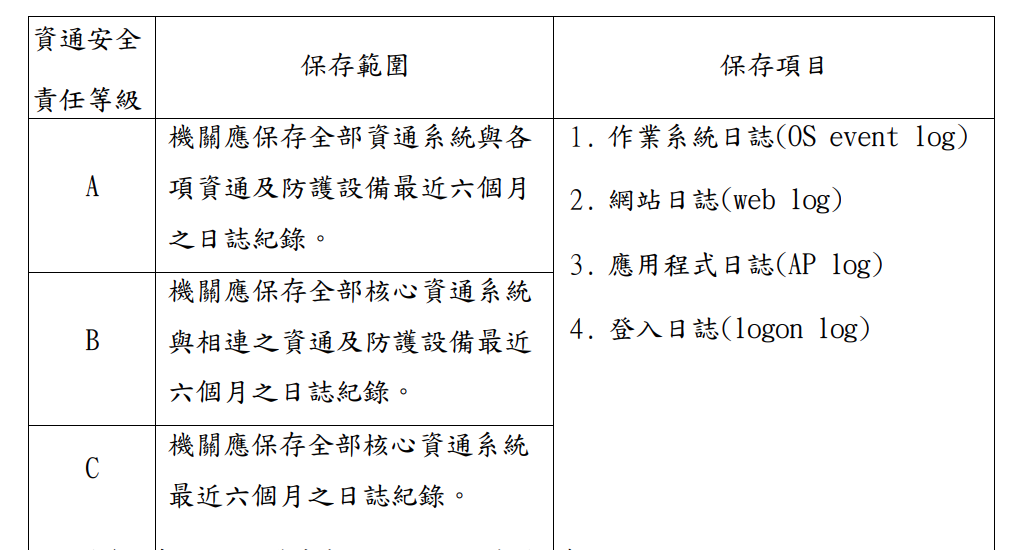
(B) 日誌保存範圍涵蓋各項資通系統，與資通及防護設備日誌紀錄

(C) 日誌宜保存項目為作業系統日誌、網站日誌、應用程式日誌與登入日誌

(D) 日誌內容宜應含事件類型、發生時間與位置，及事件相關之使用者身分識別等資訊

規劃 112-2 答案BCD





9. 根據資通安全管理法之規定，主管機關應於其自身完成資通安全事件之通報後，依規定時間完成該資通安全事件等級之審核，下列敘述何項正確？

(A) 通報為第三級或第四級資通安全事件者，於接獲後四小時內

(B) 通報為第三級或第四級資通安全事件者，於接獲後六小時內

(C) 通報為第一級或第二級資通安全事件者，於接獲後八小時內

(D) 通報為第一級或第二級資通安全事件者，於接獲後二小時內

管理 113-2 答案C

(三、四級是2小時，一、二級是8小時)

11. 關於中華民國「資通安全管理法」之條文內容，下列何項正確？

(A) 為保障著作人著作權益，調和社會公共利益，促進國家文化發展 《**著作權法**》

(B) 為保障營業秘密，維護產業倫理與競爭秩序，調和社會公共利益 《**營業秘密法**》

(C) 為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用 《**個人資料保護法**》

(D) 為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益

管理 113-2 答案D

(資通安全管理法第 1 條：為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法)

7. 下列「資通安全管理法」的哪一項子法，有定義資通安全演練作業 項目之子法為何？

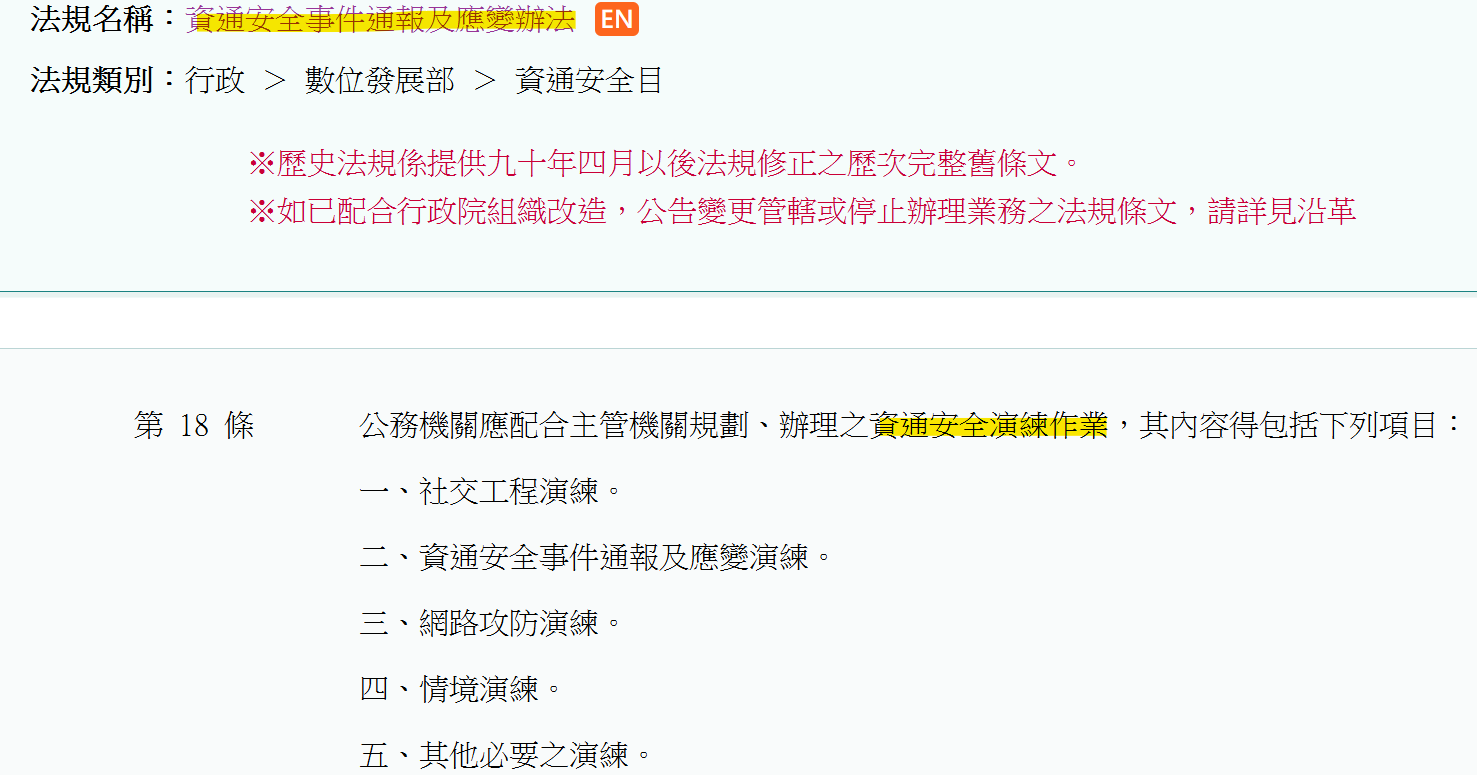
(A) 資通安全責任等級分級辦法

(B) 資通安全管理法施行細則

(C) 資通安全情資分享辦法

(D) 資通安全事件通報及應變辦法 (如下圖)

管理 113-1 答案D



10. 資通安全管理法將資通安全事件分為四級，請問下列何項是屬於三級資通安全事件？

(A) 非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏 (關鍵字：非核心嚴重，屬於二級)

(B) 非核心業務資訊遭輕微洩漏 (關鍵字：非核心輕微洩漏，屬於一級)

(C) 一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏 (關鍵字：公務、關鍵基礎設施嚴重或國家機密，屬於四級)

(D) 未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏(關鍵字：公務機密輕微、關鍵基礎設施維運之核心業務輕微，屬於三級)

非核心業務：輕微→一級；嚴重→二級。

核心業務 ：輕微→二級；嚴重→三級。

關鍵基礎設施或公務機密：輕微→三級；嚴重→四級。

國家機密→四級 (沒分等級)。

管理 113-1 答案D

43. 關於資安事故通報處理過程之敘述，下列何者有誤？

(A) 事故通報僅能依正式之書面表單向權責主管進行通報

(B) 事故處理單位應迅速處理以減輕公司損失

(C) 事故處理完成後，應將處理過程及結果進行報告

(D) 事故處理完成後，應分析事故發生原因，進行矯正措施

管理 113-1 答案A

(應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告，非僅能依正式書面而應以約定之方式)

44. 下列何項「不」是執行資安事件通報時必須提供的資訊？

(A) 受影響的系統及範圍

(B) 事件發生的時間

(C) 嫌疑人的身份

(D) 預估可能的處理時間

管理 113-1 答案C

(通報內容：

一、發生機關。

二、發生或知悉時間。 (B)

三、狀況之描述。 (A)

四、等級之評估。

五、因應事件所採取之措施。 (D)

六、外部支援需求評估。

七、其他相關事項。)

6. 依據資通安全責任等級分級辦法之規定，下列有關資通安全責任等級的敘述，下列何者正確？

(A) 業務涉及全國性民眾服務或跨~~特定非~~公務機關共用性資通系統之維運，其資通安全責任等級為A級 (全國性)

(B) 業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理，其資通安全責任等級為B級

(C) 各機關維運自行或委外設置、開發且具權限區分及管理功能之資通系統者，其資通安全責任等級為~~A~~(C)級 (有資通系統)

(D) 無資通系統但提供資通服務，其資通安全責任等級為~~E~~(D)級 (僅使用資通系統但無自行維護之資通系統)

管理 112-2 答案B

7. T通訊公司為我國政府依照資通安全法相關規定，列為資通安全責任等級A級之特定非公務機關。假設其發生第三級資通安全事件時，應於下列何者時間內完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜？

(A) 於知悉該事件後 24小時內

(B) 於知悉該事件後 36小時內 (第三級與第四級事件)

(C) 於知悉該事件後 48小時內

(D) 於知悉該事件後 72小時內 (第一級與第二級事件)

管理 112-2 答案B

20. 依照我國「資通安全事件通報及應變辦法」的規定，當發現一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改之情事時，公務機關知悉資通安全事件後，應依規定在多少時間之內完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜？

(A) 12 小時

(B) 24 小時

(C) 36 小時

(D) 72 小時

規劃 112-2 答案C

(第三級為關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改，因此是36小時)

45. 某一特定非公務機關知道所經管的一個核心資通系統發生異常，並判別為遭受嚴重竄改，故依據「資通安全事件通報及應變辦法」相關規定，須於36小時內完成損害控制或復原作業（含通報中央目的事業主管機關）。 收到通報的中央目的事業主管機關，應於接獲通報後幾小時內完成該事件之等級審核？

(A) 2 (36小時內完成損害控制或復原作業為第三級與第四級事件，因此上級機關需於2小時內完成審核)

(B) 4

(C) 6

(D) 8

管理 112-2 答案A

7. 關於資通安全管理法所定義「公務機關」的敘述，下列何者正確？

(A) 依法行使公權力之軍事機關 (條文上排除)

(B) 依法行使公權力之中央機關、地方機構

(C) 依法行使公權力之情報機關 (條文上排除)

(D) 政府捐助並依法行使公權力之財團法人 (非特定公務機關)

管理 112-1 答案B

22. 依照我國「資通安全事件通報及應變辦法」的規定，公務機關知悉資通安全事件後，應於多少時間之內，依主管機關指定之方式及對象，進行資通安全事件之通報？

(A) 1小時內

(B) 8小時內

(C) 24小時內

(D) 72小時內

防護 112-1 答案A

(知悉後1小時內)

8. 關於公務機關未遵守資通安全管理法規定的敘述，下列何者正確？

(A) 應按其情節輕重，依相關規定按次處新臺幣十萬元以上一百萬元以下罰鍰

(B) 應按其情節輕重，依相關規定按次處新臺幣三十萬元以上五百萬元以下罰鍰

(C) 應按其情節輕重，依相關規定予以懲戒或懲處 (公務機關罰鍰沒用，通常只會對企業罰鍰)

(D) 應按其情節輕重，依相關規定按次處新臺幣三萬元以上五十萬元以下罰鍰

管理 111-2 答案C

(資通安全管理法第四章罰則第 19 條

公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。)

9. 關於資通安全管理法對於委託機關於委外辦理資通系統之建置、維運或資通服務之提供，選任及監督受託者時，應注意「適任性查核」的敘述，下列何者錯誤？

(A) 應查核有無曾犯洩密罪，或於動員戡亂時期終止~~前~~(後)，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案

(B) 應查核有無曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案

(C) 應查核有無曾受到外國政府之利誘、脅迫，從事不利國家安全或重大利益情事

(D) 應查核有無曾受到大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事

管理 111-2 答案A

10. 當某關鍵基礎設施提供者之核心業務資訊遭受嚴重之洩漏時，該關鍵基礎設施提供者就該資通安全事件通報的敘述，下列何者錯誤？

(A) 知悉資通安全事件後應於一小時內進行資通安全事件之通報

(B) 通報內容應包含為因應該事件所採取之措施

(C) 應於知悉該事件後三十六小時內完成損害控制或復原作業

(D) 完成損害控制或復原作業候應持續進行事件之調查及處理並於~~二個月~~(一個月)內送交調查處理及改善報告

管理 111-2 答案D

(關鍵基礎設施提供核心系統洩漏為第四級，知悉一小時內通報，通報內容包含因應事件所採取之措施，通報後主管機關二小時完成核定等級，知悉後三十六小時完成災損控制或復原作業，並於一個月內提交改善報告)

42. 依據「 資通安全事件通報及應變辦法」，主管機關於接獲通報後，若判定為1級或2級事件，應於幾小時內完成審核？

(A) 2 小時

(B) 4 小時

(C) 8 小時

(D) 12 小時

管理 111-2 答案C

(上級回覆時間：第一級與第二級：8小時內。)

11. 依據我國《資通安全管理法施行細則》條文中規定，下列何者「不」是資通安全維護計畫應（或強制要求）包括的事項？

(A) 核心業務及其重要性

(B) 資通安全稽核組織

(C) 資通安全政策及目標

(D) 專責人力及經費之配置

規劃 111-1 答案B

(資通安全管理法施行細則第六條  
本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：

一、核心業務及其重要性。

二、資通安全政策及目標。

四、專責人力及經費之配置。)

12. 依據「資通安全事件通報及應變辦法」，主管機關於接獲通報後，若判定為3級或4級事件，應於幾小時內完成審核？

(A) 2 小時

(B) 4 小時

(C) 8 小時

(D) 12 小時

管理 111-1 答案A

(上級回覆時間：第三級與第四級：2小時內。)

20. 關於資安事件應變通報與情資分享，下列敘述哪些「不」正確？ ？（複選）

(A) 資通安全管理法子法規定，公務機關辦理資通安全事件之通報，

應於事件發生後一小時內進行通報 (知悉)

(B) 資安事件分享屬 ISAC服務範圍之一

(C) 資通安全管理法子法規定之事件嚴重等級共分四級，第一級為最

嚴重，第四級為最輕微 (顛倒)

(D) 我國 ISAC機制設計，針對跨領域之資安情資分享，建議採用

STIX與 TAXII之格式與機制

防護 111-1 答案 AC

36. 依據資通安全事件通報及應變辦法所訂定的資安事件影響等級，共分為幾種等級？

(A) 3 級

(B) 4 級

(C) 5 級

(D) 6 級

管理 111-1 答案B

37. 請問資通安全管理法的何項子法，有定義資通系統防護基準要求？

(A) 資通安全事件通報及應變辦法

(B) 資通安全情資分享辦法

(C) 公務機關所屬人員資通安全事項獎懲辦法

(D) 資通安全責任等級分級辦法

管理 111-1 答案D

個人資料保護法

**個人資料保護法**

* 保護範圍
* 目的：為規範個人資料 (自然人) 之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用
* 基本原則：
  + 需有特定目的，不得任意他用
  + 符合必要範圍，不得過度蒐集
* 個資定義：能識別個人的資料
  + 直接識別：姓名、身分證號、指紋
  + 間接識別：出生年月日 (需與其他資料組合)
  + 不是個資：公司地址 (非自然人) 、員工電子郵件 (已合法公開)
* 蒐集方式：指以任何方式取得個人資料
* 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送
* 利用：指將蒐集之個人資料為處理以外之使用
* 國際傳輸：指將個人資料作跨國 (境) 之處理或利用
* 去識別化 (De-identification) 有兩種：
  + 匿名化 (Anonymization) ：資料無法再識別特定個人，例如：林OO。
  + 假名化 (Pseudonymization) ：資料則因可能透過額外資訊重新識別，例如：姓名：代號 P12345，身分證字號：AXXXXXXXXX，出生日期：1990年XX月XX日，如果得知資料庫代號對照表可從重新識別。
* 當事人權利保障
* 五大基本權利(不得預先拋棄或以特約限制之)
  + 一、查詢或請求閱覽。
  + 二、請求製給複製本。
  + 三、請求補充或更正。
  + 四、請求停止蒐集、處理或利用。
  + 五、請求刪除。
* 特定目的消失時：個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。
* 當事人請求閱覽其個人資料，公務機關或非公務機關於三十日內告知不予同意 (十五日+十五日)
* 查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用
* 特種個資特別保護
* 範圍：病歷、醫療、基因、性生活、健康檢查、犯罪前科
* 原則：除法定例外，不得任意蒐集處理
* 告知與安全維護
* 個人資料之蒐集、處理或利用，不得逾越特定目的之必要範圍
* 蒐集時應告知
  + 一、公務機關或非公務機關名稱。
  + 二、蒐集之目的。
  + 三、個人資料之類別。
  + 四、個人資料利用之期間、地區、對象及方式。
  + 五、當事人依第三條規定得行使之權利及方式。
  + 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
* 得以言詞、書面 (考試有考僅能使用書面) 、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。
* 安全維護計畫
  + 一、配置管理之人員及相當資源。
  + 二、界定個人資料之範圍。
  + 三、個人資料之風險評估及管理機制。
  + 四、事故之預防、通報及應變機制。
  + 五、個人資料蒐集、處理及利用之內部管理程序。
  + 六、資料安全管理及人員管理。
  + 七、認知宣導及教育訓練。
  + 八、設備安全管理。
  + 九、資料安全稽核機制。
  + 十、使用紀錄、軌跡資料及證據保存。
  + 十一、個人資料安全維護之整體持續改善。
* 違法責任
* 公務員加重：公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

**考古題：**

8. 關於個人資料保護法（以下簡稱：個資法）之規定，下列何者敘述有誤？

(A) 個資法第三條所規範之當事人權利，不得預先要求拋棄 (個人資料保護法第三條)

(B) 個資法第八條規定蒐集個人資料應明確告知當事人之事項，~~應以書面為之~~(得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之) (施行細則第十六條)

(C) 當事人查詢或請求閱覽個人資料或製給複製本者，可以收取必要之成本費用 (個人資料保護法第十四條)

(D) 對個人資料之蒐集或處理應有特定目的 (個人資料保護法第十五條第一項和第十九條第一項)

管理 113-1 答案B

9. 下列何者行為違反個人資料保護法之規定？

(A) 特定目的消失時，公司即刪除該個資 (個人資料保護法第十一條第三項)

(B) 首次利用非由當事人提供之個人資料，立即告知當事人取得來源及應行告知之事項 (個人資料保護法第九條)

(C) 保險公司要求出險之被保險人提供相關之醫療記錄 (個人資料保護法第六條第一項第二款)

(D) 當事人請求閱覽其個人資料，公司於~~45~~(30)天~~後~~(內)告知不予同意 (個人資料保護法第十三條第一項)

管理 113-1 答案D

11. 關於中華民國「個人資料保護法」中明定「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之」的敘述，下列何項錯誤？

(A) 查詢或請求閱覽 (個人資料保護法第三條第一項第一款)

(B) 請求補充或更正 (個人資料保護法第三條第一項第三款)

(C) 請求公開或製給複製本

(D) 請求停止蒐集、處理或利用 (個人資料保護法第三條第一項第四款)

管理 113-1 答案C

9. 我國個人資料保護法施行細則第12條所稱適當安全維護措施，「不」包括下列何項？

(A) 個人資料之風險評估及管理機制 (第十二條第二項第三款)

(B) 認知宣導及教育訓練 (第十二條第二項第七款)

(C) 導入ISO管理架構

(D) 資料安全稽核機制 (第十二條第二項第九款)

管理 112-2 答案C

11. 關於中華民國「個人資料保護法」之定義，下列何項錯誤？

(A) 蒐集：指以~~特定~~(任何)方式取得個人資料

(B) 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送

(C) 利用：指將蒐集之個人資料為處理以外之使用

(D) 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合

管理 112-2 答案A

13. 當某公益團體舉辦抽獎活動，而需蒐集參與者個人資料時，請問下列何種方式最「 不 」合適？

(A) 直接保留參與者個人資訊，以供其他用途使用 (個人資料保護法第五條「個人資料之蒐集，不得逾越特定目的之必要範圍」)

(B) 明確告知參與者，所蒐集個人資訊的用途(個人資料保護法第八條告知義務：蒐集時應告知目的)

(C) 提供參與者請求停止蒐集個人資訊的管道 (個人資料保護法第八條第一項第五款當事人依第三條規定得行使之權利及方式、第三條第一項第四款「請求停止蒐集、處理或利用」)

(D) 應視活動需求，只蒐集必須的個人資訊 (個人資料保護法第5條：「依誠實及信用方法為之，不得逾越特定目的之必要範圍」)

管理 112-2 答案A

6.關於個人資料蒐集之特定目的消失或期限屆滿時之作為，下列何者錯誤？

(A) 應主動停止蒐集該個人資料

(B) 應主動停止處理該個人資料 (個資法第11條第3項)

(C) 應主動停止利用該個人資料 (個資法第11條第3項)

(D) 應主動刪除該個人資料 (個資法第11條第3項)

管理 112-1 答案A

10. 下列何者「不」是個人資料保護法中，當事人對於個人資料的權利？

(A) 查詢或請求閱覽 (個人資料保護法第三條第一項第一款)

(B) 請求補充或更正 (個人資料保護法第三條第一項第三款)

(C) 請求刪除 (個人資料保護法第三條第一項第五款)

(D) 請求永久保留

管理 112-1 答案D

12. 下列何者屬於中華民國「個人資料保護法」第6條規範中的「特種個人資料」？

(A) 身分證統一編號

(B) 基因 (個人資料保護法第六條第一項)

(C) 生物特徵

(D) 血統

管理 112-1 答案B

6. 下列何者「不」屬於特種個資？

(A) 性生活

(B) 病歷

(C) 健康檢查

(D) 指紋

管理 111-2 答案D

(特種個資為病歷、醫療、基因、性生活、健康檢查、犯罪前科)

7. 關於公務員假借職務上之權力、機會或方法，犯個人資料保護法所訂之罪者，加重刑罰的比例為下列何項？

(A) 加重其刑至五分之一

(B) 加重其刑至四分之一

(C) 加重其刑至三分之一

(D) 加重其刑至二分之一

管理 111-2 答案D

(個資法第44條公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一)

11. 公務或非公務機關在進行個人資料蒐集時，應明確告知當事人事項，請問其告知內容「不」包含下列何項？

(A) 個人資料蒐集的目的 (第八條第一款第二項)

(B) 個人資料的類別 (第八條第一款第三項)

(C) 個人資料儲存方式

(D) 個人資料利用的期間與地區 (第八條第一款第四項)

管理 111-2 答案C

12. 下列何者「不」屬於個人資料？

(A) 以直接方式識別該個人之資料

(B) 以間接方式識別該個人之資料

(C) 公司營業據點的地址

(D) 個人的出生年月日

管理 111-2 答案C

(公司是法人非自然人，因此不是個人資料)

39. 因應個人資料保護法之要求，許多公司在處理和個人資料有關的日誌時，會將敏感資訊進行處理，例如將姓名改成陳OO，請問這樣的處理，通常稱下列何項？

(A) 正規化

(B) 去識別化

(C) 最佳化

(D) 初始化

技術 111-2 答案B

(是去識別化中的匿名化)

15. 關於個人資料保護，下列何者為「不」可直接識別個人資料？

(A) 身分證統一編號

(B) 出生年月日

(C) 護照號碼

(D) 指紋

管理 111-1 答案B

(出生年月日需要搭配其他資料才可以識別到個人)

18. 下列何種為個人資料保護法中所定義的特種個人資料？

(A) 離婚身份

(B) 犯罪前科

(C) 住家電話

(D) 銀行負債情形

管理 111-1 答案B

(特種個資為病歷、醫療、基因、性生活、健康檢查、犯罪前科)

智慧財產權

**智慧財產權(著作權、專利權、商標權和商業秘密)**

| **特徵** | **著作權** | **專利權** | **商標權** | **營業秘密** |
| --- | --- | --- | --- | --- |
| 定義 | 保護文學、藝術、科學等創作 | 保護具有產業利用性的技術發明 | 保護區別商品或服務來源的標識 | 符合以下必要條件的資訊：  1.非公眾所知悉  2.具經濟價值  3.已採取合理保密措施 |
| 保護對象 | 文學、音樂、視覺藝術、電腦程式等 | 1.發明專利：新穎、進步的技術發明  2.新型專利：物品形狀、構造創作  3.設計專利：物品的形狀、花紋、色彩創作 | 文字、圖形、記號、顏色、聲音、立體形狀等 | 方法、技術、製程、配方、程式、設計等 |
| 權利內容 | 重製、公開播送、公開傳輸、改作、編輯、出租等 | 專屬製造、販賣、使用該發明 | 專屬使用於指定商品或服務 | 禁止他人不正當取得、使用或洩漏 |
| 保護期限 | 作者終身加死後50年 | 發明專利20年  新型專利10年  設計專利15年 | 10年，  可無限次續展 | 保密措施有效且資訊未公開 |
| 取得方式 | 自動取得，創作完成即享有 | 需向智慧財產局申請並獲准 | 需向智慧財產局申請並獲准 | 符合法定要件即受保護 |
| 資安重點 | 防止未授權複製、散布、下載 | 保護專利文件、圖紙機密性 | 防止商標數位仿冒、網路濫用 | 實施嚴格資訊存取控制、加密、保密協議 |

12. 依據營業秘密法的規定 ，下列何者正確？

(A) 工程師於職務上研究或開發之營業秘密，歸工程師所有 (依據法律，員工在職務上完成的研發成果，包括營業秘密，通常歸屬於雇主公司。這是因為員工利用了公司的資源、時間和設備進行開發，故產權歸公司所有。)

(B) 營業秘密不得讓與他人或與他人共有 (營業秘密可以透過契約的方式轉讓或授權給他人使用，亦可與他人共有。企業之間常常簽訂保密協議，以共享或轉移營業秘密，以促進合作與發展。)

(C) 營業秘密不得為質權及強制執行之標的 (營業秘密法第八條)

(D) 營業秘密指方法、技術、製程、配方，程式則不屬營業秘密，應屬著作權 (程式（軟體）可以同時受到著作權法和營業秘密法的保護。如果程式的源碼未公開，並經過企業合理的保密措施保護，它即屬於營業秘密的範疇。此外，著作權保護的是表達形式，而營業秘密保護的是未公開的技術與資訊)

112-2 管理 答案C

13. 如附圖所示，依照創用CC（Creative Commons）授權的規定，下列何種使用方式違反附圖中授權標示的規定？



(A) 使用者必須按照著作人或授權人所指定的方式，表彰其姓名 (符合 BY (姓名標示) 的要求，這是允許的使用方式。)

(B) 使用者將該素材用於公益的用途上 (符合 NC (非商業性使用) 的要求，這是允許的使用方式。)

(C) 使用者將該素材用於商業廣告上 (違反 NC (非商業性使用) 的要求。商業廣告明顯屬於商業用途，不符合授權規定。)

(D) 使用者重製、散布、傳輸著作時，亦不得修改該著作 (符合 ND (禁止改作) 的要求，這是允許的使用方式。)

112-1 管理 答案 C

(圖中顯示的CC授權標示包含三個元素：

1. BY (姓名標示)
2. NC (非商業性使用)
3. ND (禁止改作) )

16. 下列何者「不」是保護智慧財產權的適當做法？

(A) 向知名且信譽良好的店家購買電腦軟體

(B) 從網路下載破解版的軟體 (下載 **破解版的軟體** 不僅無法保護智慧財產權，還直接侵犯了它。使用盜版或破解的軟體違反了法律，也是不尊重創作者勞動成果的行為。同時，這些軟體可能包含惡意程式或病毒，對電腦安全造成威脅。)

(C) 制訂保護智慧財產權的政策

(D) 定期審查是否僅安裝經授權的軟體

111-1 管理 答案B

17. 下列何者「不」在著作權的保護範圍內？

(A) 自創音樂

(B) 小說創作

(C) 公文內容

(D) 攝影作品

111-1 管理 答案C

( 著作權法第 9 條

下列各款不得為著作權之標的︰

一、憲法、法律、命令或公文。

二、中央或地方機關就前款著作作成之翻譯物或編輯物。

三、標語及通用之符號、名詞、公式、數表、表格、簿冊或時曆。

四、單純為傳達事實之新聞報導所作成之語文著作。

五、依法令舉行之各類考試試題及其備用試題。

前項第一款所稱公文，包括公務員於職務上草擬之文告、講稿、新聞稿及其他文書。)

32. 智慧財產權（Intellectual Property Rights）是指由人類思想、智慧、創作而產生具有財產價值的產物。下列何者「不」屬於智慧財產權？

(A) 肖像權

(B) 專利權

(C) 著作權

(D) 軟體版權

111-1 管理 答案A

(肖像權屬於人格權的範疇，是保護個人形象不受侵害的權利)