113 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目：I11 資訊安全管理概論

考試日期： 113 年 6 月 1 日

單選題 50 題（佔 **100%**）

C	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
C	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 (B) 供應商提供查閱的產品目錄 (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
D	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
D	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 (B) 公司內部員工的個人資訊，不在機密性的保護範圍 (C) 對所有資訊資料而言，機密性最為重要 (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
A	5. 資訊安全長（CISO）是組織中負責資訊安全的最高級別的管理職位，下列資訊安全長主要職責何者較「不」適切？ (A) 資訊系統例行性維護

	(B) 評估和管理資訊安全風險 (C) 負責確保已施行適當的安全控制措施 (D) 資訊安全策略制定
C	6. 歐盟執委會（European Commission，EC）修正後的 2022/2555（EU）指令（即 Security of Network and Information Systems，NIS 2 Directive），已於 112 年 1 月 16 日生效，以改善歐盟現有的資訊安全態勢，本次修正內容包括擴大該指令所適用的類別與規模，附圖中哪些產業是本次新納管的產業（Sectors）？ 1. Drinking water（飲用水） 2. ICT service management（ICT 服務管理） 3. Space（太空） 4. Health（健康） 5. Banking（銀行） 6. Waste water（廢水處理） (A) 1、2、3、5、6 (B) 1、4、5、6 (C) 2、3、6 (D) 1、4、6
D	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
B	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 (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 (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 (D) 對個人資料之蒐集或處理應有特定目的
D	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 (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 (C) 保險公司要求出險之被保險人提供相關之醫療記錄 (D) 當事人請求閱覽其個人資料，公司於 45 天後告知不予同意
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 (B) 非核心業務資訊遭輕微洩漏 (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 (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
C	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 (B) 請求補充或更正 (C) 請求公開或製給複製本 (D) 請求停止蒐集、處理或利用
C	12. 下列何者「非」屬 GDPR（General Data Protection Regulation）明確列入之特種個資？

	(A) 哲學信仰 (B) 生物特徵 (C) 犯罪前科 (D) 政治意見
C	13. 關於機密性與隱私權保護的敘述，下列何者有誤？ (A) 機密性通常結合密碼學的方式來保護資料 (B) 隱私權保護其中一個作法是去識別化儲存 (C) 機密性與隱私權保護的控制機制無法共存 (D) 良好權限控管機制有助於強化機密性或隱私權保護
A	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 (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
D	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
B	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

	(C) 提高資產可用性 (D) 降低資產建置成本
C	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 (D) 確保公開的資訊受到適切等級的保護
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 (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
D	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
C	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 (D) 一般

C	21. 如附圖所示，下列何項內容為風險回應的主要方式？ 1. 風險避免（Risk Avoidance） 2. 風險接受（Risk Acceptance） 3. 風險曝險（Risk Exposure） 4. 風險轉移（Risk Transfer） 5. 風險減緩（Risk Mitigation） (A) 123 (B) 12345 (C) 1245 (D) 145
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 (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
D	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
A	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 (B) 蓄意破壞 (C) 設施功能失效

	(D) 資訊事件
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 (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 (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 (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
A	26. 若採行多因素身分驗證，除了原本的帳號密碼之外，下列何項的內容可以當成第二階段認證的方式？（請選擇最佳的組合） (A) 個別員工之 IC 識別證、傳輸至個人手機的隨機驗證碼 (B) 身份證字號、傳輸至個人手機的隨機驗證碼 (C) 身份證字號、出生年月日 (D) 出生年月日、個別員工之 IC 識別證
D	27. 關於存取控制的基本管理敘述，下列何者錯誤？ (A) 「責任分擔」是避免高機密資訊由某人完整的持有 (B) 「最低權限」要求每個人都只能擁有完成任務的最低權限 (C) 「知的必要性」是指對於負責的業務需求性有「知的權利」 (D) 「資訊分類」使用者必須完整掌握其權限以外的對應系統與資料
A	28. 關於身份認證技術的敘述，下列何者正確？ (A) 採用生物資訊認證技術需考量錯誤接受率（FAR）與錯誤拒絕率（FRR） (B) 指紋屬於所持之物（Something you have）

	(C) 一次性密碼（OTP）屬於所知之事（Something you know） (D) 申辦時提供雙證件確認屬多因子認證（MFA）
B	29. 系統管理人員應該對系統使用者的密碼實施一些管制措施，下列何項措施「不」是管理人員會採行的管制措施？ (A) 強制要求使用者定期變更密碼 (B) 允許與先前密碼重複 (C) 限制指定時間內連續嘗試登入的次數 (D) 要求密碼的複雜度
D	30. 如附圖所示，採用生物識別作為身分認證機制時，生物特徵識別系統的辨識精確度會有其誤差值的存在，請問附圖中哪些是「最」常用以評估誤差值的種類？ 1. FAR（False Acceptance Rate） 2. EER（Equal Error Rate） 3. CER（Crossover Error Rate） 4. FRR（False Rejected Rate） (A) 1、2、3 (B) 1、2 (C) 2、4 (D) 1、4
C	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） 1. 策略及規範 2. 稽核 3. 加密演算 4. 網路區段分隔 5. 工作區分隔 6. 人員管控 7. 網路架構

	(A) 1、2、3 (B) 4、5、6 (C) 3、4、7 (D) 1、4、6
A	32. FIDO 是確保登入流程中伺服器透過與終端裝置協定的安全機制。請問下列何項敘述有誤？ (A) 由 IETF（網際網路工程任務組織）所訂定的一套網路識別標準 (B) 這套識別標準透過公開金鑰加密（Public Key Cryptography）的架構進行多重因素驗證（MFA）以及生物辨識登入來強力且嚴密地保護雲端帳號的個資 (C) FIDO 是 Fast Identity Online 的縮寫 (D) FIDO 是採用公開金鑰基礎架構的驗證模式，在 FIDO 認證伺服器端（FIDO Authentication Server）只保存相對應的公鑰，而私鑰則僅保存在使用者的裝置端，因此使用者在登入時只需提供個資給終端裝置解鎖私鑰，再透過這個步驟解鎖公鑰進行登入
A	33. 零信任架構（ZTA）的假設前提是：在確認可信之前，沒有任何連線、使用者或資產可以信任。主要目的是解決現今網路環境複雜造成信任邊界不明之資安窘境，期望透過對任何資料存取皆永不信任且必須驗證的原則，達成不論在何時何地存取資料皆保證一致安全性之相關技術。請問下列關於 ZTA 的描述何者較「不」正確？ (A) 聚焦保護網路存取，非保護資料/應用存取 (B) 參考美國國家標準技術研究院（NIST）零信任架構，採取資源門戶之部署方式（Resource Portal-Based Deployment），包含 3 大核心機制：身分鑑別、設備鑑別、信任推斷 (C) 根據美國國家標準技術研究院（NIST）頒布標準文件 NIST SP800-207 將 ZTA 分成核心組件與支援組

	件，「資料存取政策」歸類在支援組件中 (D) ZTA 架構中的決策引擎組件是負責接收存取請求、決定允許與否與授予存取憑證
A	34. 下列何項「不」是資料庫的資料加密方式？ (A) 資料遮罩（Data Masking） (B) 透明資料加密（Transparent Data Encryption，TDE） (C) 資料欄位加密 (D) 資料庫檔案加密
D	35. 關於僅知原則（Need to Know）、最小權限原則（Principle of Least Privilege）、僅用原則（Need to Use）的描述，下列何者最「不」適切？ (A) 僅知原則強調只有當成員需要特定資訊來完成其職務時，才應該給予存取該資訊的權限 (B) 最小權限原則要求給予成員執行其工作所需的最少權限 (C) 僅用原則指出應該限制成員對系統資源的存取，以防止資訊洩漏和不當使用 (D) 僅知原則、僅用原則及最小權限原則也可應用在資料加密之理論基礎
A	36. 為確保資料安全，有效降低駭客入侵，最「不」應該進行下列何項措施？ (A) 建立強大的密碼和帳戶管理，實施單一身份驗證 (B) 建立備份和恢復計劃，或是高可用性機制 (C) 使用加密技術 (D) 定期進行安全測試和漏洞掃描
A	37. 關於對稱式加密（Symmetric Encryption）與非對稱式加密（Asymmetric Encryption）的敘述，下列何者錯誤？ (A) 非對稱式加密算法包括 DES、3DES、AES 等，這些算法使用相同的密鑰對資料進行加密和解密 (B) 對稱式加密使用相同的密鑰（也稱為加密鑰）來加

	密和解密資料。在對稱式加密中，發送方和接收方必須共享相同的密鑰，並且使用該密鑰對資料進行加密和解密 (C) 非對稱式加密是一種加密技術，使用一對密鑰（公鑰和私鑰）來加密和解密資料 (D) 對稱式加密需要發送方和接收方共享相同的密鑰，因此密鑰的管理和分發比較困難
B	38. 數位簽章驗證程序，是執行附圖中的哪些作業行為？ 1. 簽章產生 2. 內容加密 3. 內容解密 4. 簽章驗證 5. 保密傳輸 (A) 2、4 (B) 1、4 (C) 2、3 (D) 1、5
A	39. 關於密碼技術使用的基本要求，兼顧成本與效率之考量，下列敘述何項最為適切？ (A) 選用密碼技術時，須納入適用法律及法規要求事項 (B) 選用密碼技術時，無須考量資訊機密性 (C) 不論所要求保護資訊分類之等級，密碼演算法的強度皆須為一致 (D) 使用密碼技術主要用以保護使用者端點裝置上資訊，網路傳輸不在考量範圍內
C	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）
A	41. 當資訊安全事故發生時，下列敘述何者正確？ (A) 資訊安全事故的發生，最好將細節全部記錄下來，以做日後分析使用 (B) 因為是資訊安全事故，僅對內部告知，細節要求不需告知與資訊處理相關的供應商 (C) 資訊安全事故發生如果無法找到根本原因，可以先予以結案 (D) 因為成本資源的限制，增加此資訊安全事故不再重複發生的控制措施，可於日後再實施
C	42. 關於系統稽核日誌的保護機制敘述，下列何者正確？ (A) 稽核日誌紀錄留存的時間，應以設備硬體空間能儲存多久的時間而制定 (B) 系統管理與使用者，需要參考稽核日誌的結果，所以存取權限設定可予以開放 (C) 因應系統稽核日誌也是資訊安全事故的有效證據，所以控管存取權限是最重要的議題 (D) 當保留稽核日誌紀錄受到防毒軟體的限制時，可考量不予以留存
A	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

C	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
D	45. 資安事故的通報程序「不」包括下列何項？ (A) 向連絡窗口通報 (B) 記錄相關細節 (C) 向警察機關報案 (D) 產生事故結案報告
D	46. 關於資訊備份的敘述，下列何者錯誤？ (A) 資訊允許可遺失的時間，就是備份必須實施的頻率依據 (B) 備份媒體因為有機密性的考量，所以適時的加密是要增加的機制 (C) 確認備份媒體的可用性，是定期需要實施的機制 (D) 備份媒體置放於異地後，無須定期盤點
D	47. 關於實作營運持續的敘述，下列何者錯誤？ (A) 營運持續實作的所有過程，皆須以文件化程序留存使用 (B) 啟動營運持續實作過程時，操作同仁須具備一定的經驗及能力 (C) 營運持續實作時可允許中斷時間的依據，需與規劃階段的時間相符合 (D) 營運持續的實作時間與資訊部門可提供資源有所相關，實作時間無須符合管理階層同意的持續性目標
A	48. 試問有關復原時間目標（Recovery Time Objective，RTO）與復原點目標（Recovery Point Objective，RPO）之敘述，下列何者錯誤？ (A) 復原點目標是指在組織發生中斷事件後，該組織就

	業務面衡量其所保存資料與發生中斷前 24 小時之資料，差距有多少 (B) 復原點目標主要觀察與評判該機關執行資料備份與備份資料異地存放之頻率，以做為決定是否實施資料備份與備份頻率 (C) 復原時間目標是指機關於發生中斷事件後，該機關對於回復其所提供產品或服務之時間性目標 (D) 主要是做為機關衡量針對該關鍵活動所具備之營運持續能力
A	49. 下列何種系統備援方案提供了最快的恢復時間？ (A) 熱備援 (B) 冷備援 (C) 暖備援 (D) 離線備份
B	50. 異地備援為將企業內所需之資料/系統，分開兩地同步存放。請問關於異地備援的說明下列何項最「不」適切？ (A) 當一地發生事故時，另一地能持續接手運轉提供服務 (B) 有了異地備援便無資料丟失之風險 (C) 可適用於需要業務不中斷的企業組職 (D) 異地備援的建置可能導致投入成本增加