112 年度第 2 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期： 112 年 11 月 25 日

單選題 50 題（佔 **100%**）

B	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 (B) 建立資訊安全管理系統必須以 ISO 27001 為架構 (C) 機密性、可用性、完整性是 ISO 27001 最主要的資安 3 要素 (D) ISO 27001 資訊安全管理系統是一個持續改善的架構
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）
D	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
A	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
B	5. 若要驗證資訊安全管理系統，且能有效達成稽核作業，如稽核方案之管理、內部稽核之執行等，可參考下列哪一項標準？ (A) ISO 27002 (B) ISO 27007 (C) ISO 27017 (D) ISO 27037

B	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 (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 級 (D) 無資通系統但提供資通服務，其資通安全責任等級為 E 級
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 (C) 於知悉該事件後 48 小時內 (D) 於知悉該事件後 72 小時內
A	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 (B) ISO 27001：2022 強調持續改善之要求 (C) ISO 27001：2022 附錄 A 區分為 4 個領域 (D) ISO 27001：2022 附錄 A 共有 93 個控制項
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 (B) 認知宣導及教育訓練

	(C) 導入 ISO 管理架構 (D) 資料安全稽核機制
C	10. 根據歐盟一般資料保護規則（General Data Protection Regulation, GDPR），網站記錄使用者資訊（Cookie）時，提供下列何種資訊給使用者確認「較」為合適？ (A) 網站的所有內容 (B) 使用者的個人身份證明 (C) 關於 Cookie 的明確和具體的資訊 (D) 購物車的內容
A	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
C	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 (B) 營業秘密不得讓與他人或與他人共有 (C) 營業秘密不得為質權及強制執行之標的 (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
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 (B) 明確告知參與者，所蒐集個人資訊的用途 (C) 提供參與者請求停止蒐集個人資訊的管道 (D) 應視活動需求，只蒐集必須的個人資訊

B	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 (C) 清除資訊資產 (D) 增加資訊資產價值
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 (C) 只在資產設備更新時進行 (D) 不必定期進行
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 (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 (D) 使用的服務無需列入資訊資產
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 (C) 確認資訊資產的風險 (D) 確認資訊資產的擁有者
A	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
B	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 (C) 服務類資產 (D) 文件類資產
D	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
B	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 (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
C	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 (D) 風險處理
A	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） (B) 風險修改（Risk Modification） (C) 風險保留（Risk Retention） (D) 風險分擔（Risk Sharing）
B	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 (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
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 (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
B	26. 關於零信任（Zero Trust）的敘述，下列何者正確？ (A) 零信任是不用始終驗證 (B) 僅提供必要的權限 (C) 不需保持網路可見性 (D) 非所有流量都是不安全的前提下進行零信任設計
B	27. 近來 FIDO（Fast Identity Online）標準被廣泛應用在身分識別，下列描述何者錯誤？ (A) FIDO 匯集生物識別（指紋、虹膜、聲紋和臉部識別）、Token、晶片卡等各種認證技術方法 (B) FIDO 因具備無密碼身分識別，並無整合多因子驗證 (C) 可透過 FIDO 身分鑑別和身分認證以確認使用者身分，減少帳號盜用 (D) FIDO 將認證資料存於使用者端
C	28. 下列何者「非」重要系統權限管理常見之安全管理措施？ (A) 系統權限申請必須經過權責主管核准 (B) 臨時權限到期即自動停用 (C) 每月備份重要系統

	(D) 每半年定期檢視管理者及使用者權限是否異常
C	29. 下列何者「非」保護密碼安全的管控措施？ (A) 限制錯誤次數 (B) 要求定期更改密碼 (C) 自動註銷一定期間未活動之帳戶 (D) 密碼傳輸過程加密
D	30. 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
C	31. 指紋等生物特徵認證，屬於密碼學身分認證中的何種認證因素？ (A) 所知之事（something you know） (B) 所持之物（something you have） (C) 所具之形（something you are） (D) 所分享之物（Something you share）
B	32. 如附圖所示，為有效強化身分認證機制，常會使用多因子（Multi-factor authentication, MFA）認證機制，下列哪些應用組合屬於多因子認證類型？ 1. 聲紋辨識+帳號密碼（Password） 2. 指紋辨識+圖形驗證碼（Captcha） 3. 臉型辨識+指靜脈辨識+虹膜 4. 帳號密碼＋自然人憑證 IC 卡 5. 帳號密碼+虹膜+自然人憑證 IC 卡 6. 帳號密碼+指紋辨識+圖形驗證碼（Captcha）

	(A) 1、2、3、5 (B) 1、4、5、6 (C) 1、2、3 (D) 2、3、5
D	33. 下列何者「不」屬於存取控制認證技術型式一：你所知道的事物（Something you know）？ (A) 密碼 (B) 你喜歡的數字 (C) 通行語 (D) 指紋
D	34. 要防止透過無人管控的終端直接連接到主機上進行非法的查詢，下列何項安全控制效果最佳？ (A) 使用設有密碼的螢幕保護程式 (B) 使用工作站腳本程序檢查硬碟 (C) 對主機數據資料文件加密 (D) 自動註銷不活動的用戶
C	35. 資訊系統存取權限管理，下列何項較「不」正確？ (A) 提供臨時人員暫時存取權限 (B) 更新職務已異動者之存取權限 (C) 拒絕職務代理需求之暫時存取權限 (D) 撤銷已離職員工之存取權限
C	36. 關於對稱式密碼學（Symmetric cryptography）的敘述，下列何項錯誤？ (A) 加密（Encryption）與解密（Decryption）使用相同金鑰 (B) 通常加密速度相較於非對稱密碼學更快 (C) 通常運算成本相較於非對稱密碼學更高 (D) 缺點為金鑰交換須另外建立保護機制
D	37. 關於 HTTPS 協議中所使用數位憑證（Digital Certification）的敘述，下列何項錯誤？

	(A) 其為 X.509 電腦網路標準，並使用 X.500 資料模組定義屬性 (B) 用於驗證所代表之實體（Entity），例如：主機、組織或個人 (C) 可透過憑證確認其發行者的數位簽章（Digital Signature） (D) 每張憑證僅能用於驗證一個網站（Website）
D	38. 下列何種密碼演算法，其加密與解密使用的金鑰不同？ (A) DES (B) 3 DES (C) AES (D) RSA
D	39. 金鑰管理之各項安全過程中，「不」包含下列哪一項過程？ (A) 儲存 (B) 封存 (C) 配發 (D) 破解
C	40. 下列何者「不」屬金鑰配發問題（Key Distribution Problem）的解決方法？ (A) 事前共有 (B) 金鑰分配中心（KDC） (C) 利用漢明碼（Hamming Code）進行密鑰交換 (D) 公開金鑰加密
A	41. 關於組織內資訊安全事故的處理流程，下列敘述何者較正確？ (A) 須建立內部資訊安全事故發生時的管理責任及實施程序 (B) 資訊安全事故的回應程序，僅針對組織內部同仁 (C) 為了其真實性，由外部來的資訊安全事故資訊等外部關注方告知，不須主動聯繫確認

	(D) 資訊安全事故處理的優先順序需先獲得高階管理階層同意後方可執行
B	42. 關於資訊安全事故處理的相關敘述，下列何者較正確？ (A) 發生資訊安全事故時先予以處理，後續再蒐集相關資料 (B) 事故發生後，應針對事故留存相關紀錄並檢討與改進 (C) 發生資訊安全事故時先予以處理，處理完後再通報相關主管機關 (D) 日常發生與資訊安全相關的議題，盡量以事件處理不要提升至事故等級
B	43. 關於資訊安全稽核日誌留存的敘述，下列何者正確？ (A) 資訊安全稽核日誌紀錄不宜太過詳細，以免揭露風險 (B) 若系統稽核日誌留存與個人資料存取相關，須予以保留一定的期限符合法規的要求 (C) 為了管理系統的日常作業，系統管理者得給予對系統稽核日誌的異動權限 (D) 系統稽核日誌的留存，端看硬體空間容量可保留多久的期限
A	44. 試問有關資訊安全事件（Information Security Event）與資訊安全事故（Information Security Incident）之敘述，下列何者錯誤？ (A) 資訊安全事件是系統或網路中任何可觀察到的現象或徵兆，可以無須理會 (B) 防毒軟體攔截到一個病毒係屬於資訊安全事件 (C) 資訊安全事故已經對組織造成影響 (D) 駭客入侵組織內部網路竊取資料係屬資訊安全事故
A	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 (B) 4 (C) 6 (D) 8
B	46. 關於備份的敘述，下列何者較正確？ (A) 因為資源的分配，所有需要備份的資料都是每天備份一次 (B) 備份的頻率應該依照所需備份資料的重要性來分配 (C) 備份於磁帶的資料可儲存於同層樓的辦公室 (D) 備份可儲存於同一台硬體設備上
C	47. 關於營運持續規劃階段的敘述，下列何者較正確？ (A) 組織在規劃營運持續時，須將所有的資訊系統納入 (B) 組織應以目前資訊系統資源，來規劃資訊系統營運持續的實施 (C) 組織於營運持續規劃的階段就須將資訊安全納入考量 (D) 營運持續的規劃因為資源的限制，以同地做為考量即可
C	48. 關於資訊處理設施備援規劃的敘述，下列何者錯誤？ (A) 組織可視資訊系統允許中斷時間要求，備妥資訊處理設施所需數量，以符合可用性之目標 (B) 考量資訊處理設施備援規劃時，不只主機相關設備的備援，亦需要考慮到其他支援設施，如：發電機等 (C) 規劃資訊處理設施的備援時，以可用性要求為主，不需要特別考慮機密性或完整性的議題 (D) 規劃維持營運持續使用到的備援設備，也需要安排時間確認其可用性
A	49. A 公司災害緊急應變措施對於重要系統資料的恢復點目標（Recovery Point Objective, RPO）設定為 4 小時。關於此公

	司重要系統資料的備份週期，下列何項最適合？ (A) 每 2 小時備份 (B) 每日備份 (C) 每 8 小時備份 (D) 每週備份
D	50. 在組織遇到資安事件時，可能需要尋找適宜的替代場地，請問關於替代場地的敘述，下列何者較正確？ (A) 冷備援站點（Cold site）：場地和設備皆有，於事件發生時依需求執行回復工作 (B) 暖備援站點（Warm site）：異地備援端備有同樣之系統，事件發生時在可接受的時間內恢復啟用，待資料載入後即可投入營運 (C) 熱備援站點（Hot site）：有提供基本設備，但仍須自行安裝系統 (D) 行動備援站點（Mobile hot site）：在移動車輛中安裝設備與系統，當事件發生時，可迅速移動至適當地點啟用