113 年度第 2 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 11 月 23 日

單選題 50 題（佔 **100%**）

A	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 (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 (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 (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
B	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 (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 (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
D	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 (B) 簡化標題 (C) 新增控制項目 (D) 驗證範圍調整
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

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
D	6. 下列何者目前並非數位發展部資通安全署認可之資通安全專業證照？ (A) ISO 27001 LA (B) CISSP (C) iPAS 中級資訊安全工程師 (D) ISO 29100 Lead Privacy Implementer
C	7. 下列何項是支付卡產業資料安全標準？ (A) HIPAA (B) SOC II (C) PCI DSS (D) IEC 62443
D	8. 依據《上市上櫃公司資通安全管控指引》第 12 條規定，「定期辦理資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊」。請問，該規定所稱定期辦理風險評估，所代表用意為下列何項最為適切？ (A) 可以解決先前評估作業者所遺漏之項目 (B) 可以使用不同的評估技術及方法 (C) 有助於提高員工的風險意識 (D) 組織的業務發展帶來的威脅不斷改變

C	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
B	10. 上市櫃公司發生資安事件時，依照證交所規範，下列何者需要發布為重大訊息的可能性最小？ (A) 公司官網遭分散式阻斷服務攻擊（DDoS），無法正常提供服務，但公司核心業務不受影響 (B) 內部員工訂便當系統當機，導致員工無法訂便當 (C) 內部文件外洩，但不涉及機密或顧客資料，僅有員工個人資料 (D) 共用檔案系統遭勒索軟體攻擊並加密，但有完整備份，所有資料可迅速恢復
D	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 (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 (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 (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

A	12. 下列何種標準是針對雲端服務個人隱私資料的保護？ (A) ISO/IEC 27018 (B) ISO/IEC 27701 (C) ISO/IEC 27001 (D) ISO/IEC 27017
D	13. 請問我國個人資料保護法列為特種個資，但歐盟 GDPR 卻未明確列入特種個資的個人資料是下列何項？ (A) 基因 (B) 健康檢查 (C) 生物特徵 (D) 犯罪前科
D	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
D	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
D	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

C	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
C	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
A	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
D	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

B	21. 依據 ISO 27001:2022 標準條款要求有關組織應定義及應用資訊安全風險處理過程之敘述，下列何者錯誤？ (A) 考量風險評鑑結果，選擇適切之資訊安全風險處理選項 (B) 對所選定資訊安全風險處理選項，其控制措施皆選擇不實作 (C) 產生適用性聲明 (D) 制定資訊安全風險處理計畫
A	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）
C	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

C	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風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
C	25. 如附圖所示。為辦理資通系統安全風險評鑑事宜，組織應訂定該評鑑作業有關作業程序，依照國家資通安全研究院發行之《資通系統風險評鑑參考指引》所介紹之風險評鑑技術及方法，可使用下列何項工具與技術組合？ 1.根本原因分析法（Root Cause Analysis, RCA） 2.後果/機率矩陣法（Probability and Impact Matrix） 3.強弱危機分析法（SWOT） 4.德爾菲法（Delphi） 5.蝴蝶效應分析法（Butterfly effect） 6.查檢表（Checklist） 7.墨菲定律（Murphy's Law） 8.企業營運衝擊分析法（Business Impact Analysis, BIA） (A) 2、3、4、5、6 (B) 1、3、4、5、7 (C) 1、2、4、6、8 (D) 1、2、6、7、8

D	26. 關於存取控制技術的描述，下列何者錯誤？ (A) 任意型存取控制（Discretionary Access Control, DAC）是主體存取客體之權限由擁有者設定 (B) 強制型存取控制（Mandatory Access Control, MAC）是依照主體與客體之分類標籤（Classification Label）給予權限，即使是管理者也無法給予特別權限 (C) 角色為基礎的存取控制（Role-Based Access Control, RBAC）使用角色（Role）來管理權限，對於使用者位於同一個單位或執行相關的工作十分方便有效 (D) 基於屬性的存取控制（Attribute Based Access Control, ABAC）僅能透過單一屬性設定存取控制來達到安全的管控
A	27. 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，如果組織需要加強進出人員安全管控時，下列何項是生物特徵識別系統要分別增加及減少誤差值的種類？ (A) 增加 FRR（False Rejected Rate）、減少 FAR（False Acceptance Rate） (B) 增加 FRR（False Rejected Rate）、減少 CER（Crossover Error Rate） (C) 增加 FAR（False Acceptance Rate）、減少 FRR（False Rejected Rate） (D) 增加 CER（Crossover Error Rate）、減少 FAR（False Acceptance Rate）

D	28. 如附圖所示。在雲端服務的存取權限控管中，下列哪些做法組合最能有效避免過度授予權限？ 1. 根據角色和職責設置最小權限（Least Privilege），確保員工只能存取必要資源 2. 定期檢查所有使用者的權限，並移除不再需要的存取權限 3. 針對高階人員限制權限，只讓他們擁有讀取權限，避免操作錯誤 4. 啟用自動權限審查，並根據使用者的日常行為動態調整權限 5. 為每個管理員帳戶設置多重要素驗證（Multi-factor authentication, MFA），以防止身分被冒用 6. 記錄並審查管理員操作，確保權限使用的合法性 7. 合併所有管理員帳戶以集中管理權限，並定期審查系統操作記錄以避免權限濫用 (A) 1、2、5、7 (B) 1、3、5、6 (C) 1、2、4、6 (D) 1、2、5、6
B	29. 生物特徵辨識應用在存取權限控制時，所扮演的角色是下列哪一項？ (A) 授權（Authorization） (B) 身分驗證（Authentication） (C) 可問責（Accountability） (D) 正確率（Accuracy）

B	30. 存取控制是用以控制使用者與系統、系統與系統之間進行資訊交換和溝通，其概念是作業系統為控制一個主體（Subject），能依照其所得到的權限進行客體（Object）之存取。請問附圖中的選項哪些可以作為客體？ 1. 電子檔案 2. 使用者 3. 運作之程式 4. 印表機 5. 資料集 6. 個人電腦（PC） (A) 2、3、4 (B) 1、4、5、6 (C) 2、3、6 (D) 1、2、5、6
B	31. 在一個醫療場域中，有不同的資料進出需求，下列針對存取控制情境的描述何者較「不」適當？ (A) 應該採用白名單機制，限制未授權的連線 (B) 醫療儀器可以直接透過網際網路遠端維護 (C) 以防火牆區隔辦公區與診間 (D) 讓外部網站可以顯示看診進度
A	32. 採用 FIDO2 作為身分認證是目前的趨勢，關於 FIDO2 的敘述下列何者有誤？ (A) 須加入 FIDO 聯盟認證 (B) 可以應用在企業內部作為身分認證 (C) 可以應用在網際網路之金融應用 (D) 是屬於零信任架構的一環

B	33. 政府零信任網路架構係參考 NIST 零信任架構，同時結合向上集中之防護需求，採取資源門戶部署（Resource Portal-Based Deployment）方式，下列何項「不」屬於該核心機制？ (A) 身分鑑別 (B) 系統識別 (C) 設備鑑別 (D) 信任推斷
D	34. 關於 RuBAC（Rule-based Access Control）、MAC（Mandatory Access Control）、DAC（Discretionary Access Control）、RoBAC（Role-Based Access Control）的描述，下列何者最「不」適切？ (A) RuBAC 根據安全規則來決定使用者是否有存取資源的權限 (B) MAC 是一種存取控制機制，其中存取權限由系統中的政策決定，不允許使用者或擁有者更改 (C) DAC 允許資源的擁有者或使用者決定誰可以存取該資源，提供較大的靈活性 (D) RoBAC 將存取控制權限分配給特定使用者，由存取控制規則決定
C	35. 當公司允許員工使用外部生成式 AI 服務（如 ChatGPT）時，下列存取控制措施，何者最能有效保護公司機密資料不被洩露？ (A) 限制只能在公司內部網路中使用生成式 AI 服務，並通過 VPN 進行監控 (B) 要求員工在使用生成式 AI 服務前，簽署保密協議，承諾不輸入機密資料 (C) 採用資訊分類，並使用適當之過濾技術阻止機密資料被輸入生成式 AI 服務的系統中 (D) 設置使用權限，僅允許經批准的員工使用生成式 AI 服務，並定期審核使用情況

B	36. 下列何者並非 RSA 金鑰機制的相關特性？ (A) 使用非對稱加密演算法 (B) 使用單一金鑰加解密 (C) 私密金鑰（private key）不可交給他人 (D) 公開金鑰（public key）可公開讓有需要之人取得
A	37. 憑證管理中心（CA）所管理的憑證中，有部分憑證已有安全顧慮時，應運用下列何種處置方式最為合適？ (A) 註銷憑證 (B) 憑證審核 (C) 發佈憑證 (D) 交互認證
D	38. 如附圖所示，在檢查一個利用第三方服務的電子資料交換系統（EDI）應用情況時，資訊安全人員應該確認和證實哪些項目？ 1. 確認加密金鑰符合使用者要求 2. 證實服務供應商只使用了 PSDN（Public Switched Data Network） 3. 確認是否已經對服務供應商的營運情況進行了獨立檢查 4. 證實服務供應商的合約包了必要的條款，例如稽核查核的權力 (A) 1、3 (B) 1、4 (C) 2、3 (D) 3、4
A	39. 「生日攻擊法」（Birthday Attack）主要針對下列何種加密演算法進行攻擊？ (A) MD5 (B) Rijndael (C) 3DES (D) RSA

C	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）
B	41. 關於資訊安全事件相關稽核日誌的敘述，下列何者正確？ (A) 系統管理者使用而觸發的系統稽核日誌，皆先留存日後再予以審查 (B) 組織可先討論針對系統稽核日誌關心的項目審查，一旦觸發時可優先通知權責主管進行後續處理 (C) 系統管理者因為管理上的需要，可使用到共用的管理帳號 (D) 網路設備留存的稽核日誌，雖然有異常登入的紀錄，但已被阻擋未有資訊安全事故發生，就不須再予以審查
D	42. 依據 SP 800-61 Rev. 2 - Computer Security Incident Handling Guide 文件對於事故回應生命週期（Incident Response Life Cycle）之敘述，下列何者錯誤？ (A) 準備（Preparation） (B) 偵測與分析（Detection and Analysis） (C) 封鎖、根除與復原（Containment, Eradication and Recovery） (D) 備份（Backup）

B	43. 關於一般資安事件與重大資安事故的描述，下列何者較「不」適當？ (A) 事件處理時間超過規定時，會升級為事故 (B) 影響資安指標達成之因素或事項者，依其嚴重性評估不會被判定為事件 (C) 一般資安事件與重大資安事故可依照對公司組織的影響程度作為區分 (D) 重要資訊設備失效，通常會歸類為重大資安事故
C	44. 關於資安事件通報，下列何項較「不」是主要目的？ (A) 維護公司形象 (B) 遵守法律法規 (C) 獲得保險理賠 (D) 快速解決問題
B	45. 如附圖所示。當公私部門妥善收集與共享網路威脅情資，將能更快地識別威脅並找出因應之道，進而讓尚未受到威脅衝之組織能因此主動防禦減少事件發生之可能性。我國「國家資通安全研究院」已於《領域 ISAC 實務建置指引》定義「ISAC 情資類型」包含：資安訊息情資（ANA）、資安預警情資（EWA）、網頁攻擊情資（DEF）、入侵攻擊情資（INT）、回饋情資（FBI）等五類。本題提供之情資內容如附圖，請問依情資最適合判別為下列何者？ 司法院資安單位系統監控結果發現，有駭客疑偽冒監察院名義，以公職人員財產申報為由，寄送夾帶惡意附檔之社交工程釣魚郵件予下轄的 A 單位，且已知相關攻擊郵件特徵行為，但尚未確切證據已說明 A 單位已遭受入侵。 (A) 入侵攻擊情資（INT） (B) 資安預警情資（EWA） (C) 網頁攻擊情資（DEF） (D) 回饋情資（FBI）

B	46. 關於營運持續性計畫的敘述，下列何者正確？ (A) 營運持續性計畫考量完成時間即可，各關鍵步驟時間有可能會有些微差距 (B) 如果實施營運持續計畫需要供應商的協助，其到場時間亦須納入計畫中 (C) 因為營運持續計畫演練時，操作同仁皆已於異地準備，所以交通時間可以不需納入考量 (D) 啟動營運持續計畫，如果設備有前置準備時間，已於演練前準備完成，該步驟可以不需納入考量
C	47. 關於組織進行營運衝擊分析所需包含之內容敘述，下列何者錯誤？ (A) 辨識關鍵業務相關之活動 (B) 辨識各活動中斷時，會對機關所造成的衝擊 (C) 確認各活動之最小可容忍中斷時間（Maximum Tolerable Period of Disruption, MTPD） (D) 根據各活動復原之優先順序加以分類，藉以鑑別機關之關鍵活動
B	48. 關於災害復原（Disaster Recovery）和營運持續（Business Continuity）差別的敘述，下列何者較「不」適當？ (A) 災害復原確保業務流程所需要的資源能夠得以回復的程序 (B) 災害復原強調業務的韌性以及客戶關係的管理 (C) 營運持續規劃因應事故或營運中斷的策略 (D) 營運持續使業務能在預先規劃的服務等級上持續運行

B	49. 災難發生時，下列何項是最重要的？ (A) 物理資產的保護 (B) 人員生命安全的保護 (C) 維持公司的股票價值 (D) 市場行銷活動的持續進行
A	50. 請問下列何項備援方式，異地備援機制所需時間最長？ (A) 冷備援（Cold site） (B) 熱備援（Hot site） (C) 溫備援（Warm site） (D) 公司機房內建備援