109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全管理概論
考試日期：109 年 11 月 28 日　　第 1 頁，共 9 頁

單選題 50 題（佔 100%）

B	1. 下列何者為「公司網路系統必須 24 小時運作」的主要原因？ (A) 機密性 (B) 可用性 (C) 完整性 (D) 不可否認性
C	2. 在建置與運作資安系統時，常用戴明循環（Deming Cycle）協助管理，下列何項是戴明循環（Deming Cycle）正確的順序？ (A) Plan – Act – Do – Check (B) Do – Check – Plan – Act (C) Plan – Do – Check – Act (D) Act – Check – Do – Plan
B	3. 關於資訊安全管理系統（Information Security Management System, ISMS），下列敘述何者較「不」正確？ (A) 瞭解組織資訊安全要求，建立資訊安全之政策與目標的需求 (B) 基於主觀的量測，並且持續改善 (C) 監視與審查資訊安全管理系統（ISMS）的績效與有效性 (D) 在組織的運作中實作與運作各項控制措施，並管理組織的資訊安全風險
C	4. 在進行資安內部稽核時，下列何者「不」是組織應該採取的做法？ (A) 由稽核小組規劃和建立內部稽核的計畫 (B) 在稽核計畫中定義稽核的範圍和準則 (C) 為確保稽核專業度，由資訊人員稽核其所負責的資訊系統 (D) 在完成稽核之後，將稽核結果報告給相關管理階層
B	5. 下列何種網路攻擊手法，主要目的是在破壞資料的「可用性或完整性」？(1)社交工程（Social Engineering）、(2)Google 駭客（Google-Hacking）、(3)拒絕服務（Denial-of-Services）、(4)駭客侵入銀行資料庫竄改存款金額 (A) (1), (2) (B) (3), (4) (C) (2), (3), (4) (D) (1), (3), (4)
A	6. 下列何者與保護「個人資訊隱私」有關？ (A) 個人資料保護法 (B) 專利法 (C) 商標法 (D) 著作權法

A	7. 請問資訊倫理常探討的四大議題（PAPA，學者 Mason 所提出）中，個人可保護自有資訊，具有決定是否公開或保密的權利，所指的是下列何者？ (A) 隱私權 (B) 正確性 (C) 存取權 (D) 廣泛性
B	8. 請問主管機關對所屬機構（如：金管會對銀行）執行之稽核，稱為下列何者？ (A) 第一方（First Party）稽核 (B) 第二方（Second Party）稽核 (C) 第三方（Third Party）稽核 (D) 聯合/合併（Joint）稽核
B	9. 下列何者「不」是經濟合作及發展組織（Organization for Economic Cooperation and Development, OECD）之個人資料保護原則？ (A) 限制蒐集原則（Collection Limitation Principle） (B) 分享原則（Share Principle） (C) 公開原則（Openness Principle） (D) 個人參與原則（Individual Participation Principle）
C	10. 下列何種稽核可做出建議 ISO 27001 通過驗證發出證書？ (A) 第一方（First Party）稽核 (B) 第二方（Second Party）稽核 (C) 第三方（Third Party）稽核 (D) 第四方（Fourth party）稽核
C	11. 關於智慧財產權（Intellectual Property Right, IPR），下列敘述何者「不」正確？ (A) 商標權是使用文字、標語和標誌的權利，註冊商標後，註冊人即享有商標專用權 (B) 專利權是對發明授予的權利，對專利權人之發明予以保護 (C) 著作權是為保護著讀者的權益，不被非授權複製與使用 (D) 營業秘密是指不為公眾所知悉，能為權利人帶來經濟利益，具有實用性並對權利人採取保密措施的技術資訊和經營資訊
C	12. 在個資法中，關於個資隱私損害賠償的規範，當被害人無法證明實際損害金額的時候，可以請求法院依傷害情節，以多少金額計算？ (A) 每人一事件新台幣 100 以上，30,000 元以下 (B) 每人一事件新台幣 200 以上，20,000 元以下 (C) 每人一事件新台幣 500 以上，20,000 元以下

	(D) 每人一事件新台幣 1,000 以上，30,000 元以下
C	13. 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」包含下列何者？ (A) 個人資料蒐集的目的 (B) 個人資料的類別 (C) 個人資料儲存方式 (D) 個人資料利用的期間與地區
C	14. 關於資訊安全管理系統（Information Security Management System, ISMS）之資訊資產盤點，下列敘述何者較「不」正確？ (A) 資訊資產應分級，且進行盤點與造冊管理 (B) 資訊資產盤點後，需進行風險評鑑 (C) 資訊資產盤點後，進行下一年度的採購預算與成本編列 (D) 資訊資產盤點應包括硬體、軟體、文件、人員
C	15. 關於資訊安全管理系統（Information Security Management System, ISMS）之資產清單，較「不」可能包含下列何者？ (A) 資產名稱 (B) 資產保管人 (C) 資產外觀 (D) 資產價值
B	16. 關於資訊安全管理系統（Information Security Management System, ISMS）之資產分類與盤點，下列敘述何者較「不」正確？ (A) 對企業與組織具其價值的都屬於資產 (B) 資產賦值以資產購入價格來衡量 (C) 資產可以被分類與分級，利於尋找與風險評估 (D) 資產的價值取決於重要程度與敏感程度
D	17. 下列何者「不」是在進行資訊分級時，應採取的適當依據？ (A) 依法律要求 (B) 依資訊的價值 (C) 依資訊的重要性 (D) 依資訊檔案的大小
D	18. 關於資訊安全管理系統（Information Security Management System, ISMS）中資產擁有者的工作，下列敘述何者較「不」正確？ (A) 確保資產已盤點造冊 (B) 確保資產已適切分級並受保護 (C) 當刪除或銷毀資產時，確保適當處置 (D) 例行維運工作須由資產擁有者親自完成

D	19. 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
D	20. 關於電力供應，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) 硬體資產 (D) 服務資產
A	21. 資訊安全管理系統（Information Security Management System, ISMS）中，下列何者為資訊分類的主要目標？ (A) 確保資訊依其對組織的重要性，受到適切等級的保護 (B) 確保與資訊有關的資產，已被正確的識別和記錄 (C) 確保與資訊有關的資產，已被正確的盤點 (D) 確保資訊資產於員工離職時，已經完整的歸還
D	22. 在資訊安全管理系統（Information Security Management System, ISMS）中，風險識別「不」含下列何者？ (A) 識別各項資產的脆弱性 (B) 分析資安事故或事件對組織帶來的衝擊程度 (C) 評估環境或新技術帶來的威脅 (D) 建議購買軟硬體設備清單
C	23. 關於風險規避（Risk Avoidance），下列敘述何者「不」正確？ (A) 決定不涉入風險處境 (B) 決定退出風險處境 (C) 通常不考量主管機關的影響，而會有躲避風險的傾向 (D) 會造成不願面對風險或淡化處理風險所需要的成本
A	24. 關於風險評鑑與風險處理，下列敘述何者正確？ (A) 經過風險評鑑，低風險或處理成本過高的風險項目，可能會被組織選擇接受 (B) 風險評鑑可以百分百找出可能的風險項目，並且進行風險處置 (C) 風險處理可以百分百消除風險項目，確保資訊安全 (D) 風險處理後，組織就不再需要進行風險評鑑作業
A	25. 風險分析所使用的方法，除了「定量法（Quantitative Method）」之外，

	還可以採用下列何種方法？ (A) 定性法 (B) 類比法 (C) 平均法 (D) 參數法
C	26. 關於風險管理，下列敘述何者較「不」正確？ (A) 應依照風險改善計畫的期限，執行改善作業 (B) 執行完風險改善計畫後，應進行風險再評鑑作業 (C) 當時間已遠超過風險改善計畫期限時，仍應持續執行原訂風險改善計畫 (D) 針對超過風險胃納（Risk Appetite）的項目，應提出風險改善計畫
A	27. 關於程式原始碼存取及權限管理，下列敘述何者「不」正確？ (A) 管理人員應開放程式設計人員程式上線權限 (B) 管理人員應將系統公用程式與應用程式隔離存放 (C) 管理人員應將開發中及正式作業之程式及資料庫分開存放 (D) 管理人員應將程式目錄清單、資料及相關電子檔進行備份
D	28. 關於特權帳號的管理方式，下列何者較「不」適當？ (A) 定期檢視特權帳號的執行紀錄 (B) 定期檢視特權帳號的人員及其權限 (C) 定期更改系統管理者密碼，並避免使用系統預設帳號進行管理 (D) 不使用預設帳號，所有系統皆使用單一管理者帳號進行管理
B	29. 下列何者「不」是存取控制中，身分驗證的三個要素？ (A) 所知之事：帳號/密碼 (B) 所謂何事：共用信箱 (C) 所持之物：智慧卡 (D) 所具之形：生物特徵
B	30. 在挑選以生物辨識（Biometrics）為主的驗證設備時，下列何種評估要素「不」是常用來比較設備間的優劣性？ (A) 錯誤接受率（False Acceptance Rate, FAR） (B) 正確拒絕率（True Rejection Rate, TRR） (C) 錯誤拒絕率（False Rejection Rate, FRR） (D) 交叉錯誤率（Crossover Error Rate, CER）
A	31. 下列何者「不」是存取控制具體實施時的類型？ (A) 還原控制（Recovery Control） (B) 管理控制（Administrative Control） (C) 技術控制（Technical Control）

	(D) 實體控制（Physical Control）
C	32. 銀行櫃檯出納員的存取控制最適合實施下列何種存取控制？ (A) 強制性存取控制（Mandatory Access Control） (B) 規則基礎存取控制（Rule-based Access Control） (C) 角色基礎存取控制（Role-based Access Control） (D) 自由決定存取控制（Discretionary Access Control）
C	33. 關於可歸責性（Accountability）的定義，下列何者正確？ (A) 對使用者所提出的可識別資訊加以驗證 (B) 使用者必須提供可識別的資訊給系統 (C) 成功登入系統後，對於使用者的操作行為必須完整的記錄 (D) 管理階層的管理機制，將管理工作分成多人分層負責
D	34. 關於職務區隔（Segregation of Duties, SoD），下列敘述何者較為正確？ (A) 只提供執行業務上所需知道的資訊 (B) 定期審查權限 (C) 權限開放時採用最低權限原則 (D) 重要工作切分給多個人來執行
C	35. 關於委外使用者存取管理，下列敘述何者較「不」正確？ (A) 應透過管理階層，核准委外廠商申請系統權限 (B) 應要求委外作業人員簽署保密合約 (C) 應由委外廠商自行更新線上程式 (D) 委外作業人員調職或離職後，應立即移除或封鎖其存取權限
D	36. 關於特權管理，下列敘述何者較正確？ (A) 管理者登入主機應該使用 Administrator or Root 帳號，以利管理權限之使用 (B) 資料庫管理員可利用管理者帳號備份資料外，還可以讀取資料及調校資料庫效能 (C) 基於代理人機制，系統管理員除了網路管理帳號外，也需主機管理者權限 (D) 應該定期審查特權帳號，若有人員離職也須立即審查相關系統帳號之使用
D	37. 關於金鑰與憑證管理，下列敘述何者「不」正確？ (A) 金鑰都應受保護不被修改和破壞，並應使用實體安全來保護用於產生、儲存和歸檔金鑰的設備，以避免金鑰遭受不當修改、不慎遺失或銷毀等情況 (B) 基於業務需要，須自行建置、委託建置或選用憑證機構（Certificate Authority）時，應綜合考量憑證機構之技術、管理、人員及財務

	的安全風險等 (C) 憑證機構資訊系統（含應用系統、密碼模組等）之安全驗證，應遵照權責主管機關訂定之規範作業，以確保其安全性 (D) 憑證機構使用之電子簽章或加密金鑰長度，視系統的安全需求，由組織自行決定
B	38. 密碼學常被認為是提供數位身分認證的基礎，請問一套加密系統「不」包含下列何者？ (A) 明文 (B) 暴力破解機制 (C) 加密演算法 (D) 密文
D	39. 某銀行近日疑似遭遇駭客以彩虹表（Rainbow Table）攻擊法破解內部伺服器的密碼系統，為了能夠抵擋類似的攻擊手法再度發生，請問銀行的內部密碼系統該如何因應？ (A) 更換加密雜湊演算法 (B) 制定更嚴謹的密碼政策 (C) 啟用密碼鎖定原則 (D) 使用加鹽的金鑰延伸函式（Key Derivation Function with a Salt）
D	40. 下列何種加密技術，屬於「非對稱式金鑰加密技術」？ (A) 國際資料加密演算法（International Data Encryption Algorithm, IDEA） (B) 進階加密標準（Advanced Encryption Standard, AES） (C) 資料加密標準（Data Encryption Standard, DES） (D) 橢圓曲線密碼學（Elliptic Curve Cryptography, ECC）
D	41. 關於「對稱式金鑰加密」與「非對稱金鑰加密」，下列敘述何者「不」正確？ (A)「非對稱金鑰加密」在加解密使用不同金鑰 (B)「對稱金鑰加密」在金鑰洩露後，其加密效果即時失效 (C)「非對稱金鑰加密」的特性，可以實作數位簽章（Digital Signature） (D)「非對稱金鑰加密」的計算，效能比「對稱金鑰加密」佳
D 全部皆給分	42. 依據「行政院國家資通安全會報通報及應變作業流程」，判定事故影響等級時，應評估資安事故造成之機密性、完整性以及可用性衝擊，下列何者「不」是 1 級事件？ (A) 非核心業務一般資料遭洩漏 (B) 非核心業務系統或資料遭竄改 (C) 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作

	(D) 非核心業務系統且無系統或設備運作受影響
D	43. 關於資安事故（Security Incident），下列敘述何者「不」正確？ (A) 指已經造成服務或營運中斷之資安事件（Security Event） (B) 指極可能造成服務或營運中斷之資安事件（Security Event） (C) 當造成中斷過久時，需啟動營運持續計畫 (D) 通常會先觀察，暫不處理
A	44. 下列何者可從多種資料來源中即時收集或從歷史資安事件分析而產生的威脅偵測及資安事故應變，同時也提供合適的報表以及歷史資安事故的分析？ (A) 安全資訊與事件管理（Security Information & Event Management, SIEM） (B) 入侵偵測系統（Intrusion Detection Systems, IDS） (C) 入侵預防系統（Intrusion Prevention Systems, IPS） (D) 網頁應用防火牆（Web Application Firewall, WAF）
B	45. 關於資通安全管理法中之事件通報之要求，下列敘述何者正確？ (A) 資通安全管理法對資安事件嚴重等級共分三級 (B) 對於公務機關，應於知悉資安事件後一小時內進行通報 (C) 對於公務機關，應於資安事件發生後二小時內進行通報 (D) 對於資通安全法所納管之特定非公務機關，應於資安事件發生後八小時內進行通報
B	46. 關於營運持續計畫（Business Continuity Plan, BCP）與災難復原計畫（Disaster Recovery Plan, DRP）下列敘述何者較正確？ (A) BCP 與 DRP 的處理程序完全沒有關聯 (B) BCP 較著重於營運能力的恢復 (C) BCP 的資源要求通常較 DRP 為多 (D) DRP 所要求的回復時間較短
B	47. 組織要如何確認營運持續計畫的有效性？ (A) 以文件化方式呈現 (B) 進行營運持續演練 (C) 指派一位同仁負責計畫的撰寫 (D) 指派一組同仁負責計畫的撰寫
C	48. 在營運持續管理過程中，對下列(a)(b)(c)三種時間（Time）的關係之敘述，何者最正確？(a)最大容許中斷時間（Maximum Tolerable Period of Disruption, MTPD）、(b)復原時間目標（Recovery Time Objective, RTO）、(c)復原點目標（Recovery Point Objective, RPO） (A) (a)＜(c)＜(b)

	(B) (a)＞(b)＞(c) (C) (a)＞(b)，(c)與另二者無直接關聯 (D) (a)＞(c)，(b)與另二者無直接關聯
C	49. 關於復原點目標（Recovery Point Objective, RPO），下列敘述何者正確？ (A) 系統硬碟所儲存的資料量 (B) 系統進行備份所需要的時間 (C) 在災害發生之後，預計要將資料復原到特定的某一時間 (D) 在災害發生之後，預計資料無法回復的時間
D	50. 下列三種備份方式，依其執行備份所需的時間，下列何者較為正確？ 甲：完全備份（Full Backup）、乙：增量備份（Incremental Backup）、丙：差異備份（Differential Backup） (A) 甲＞乙＝丙 (B) 甲＜丙＜乙 (C) 甲＝乙＞丙 (D) 甲＞丙＞乙