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 5 月 30 日　　第 1 頁，共 9 頁

單選題 50 題（佔 100%）

B	1. 某攻擊者在大樓外面尋找可能含有密碼或機密訊息的廢棄紙張，此為下列何種攻擊法？ (A) 社交工程（Social Engineering） (B) 垃圾搜尋（Dumpster Diving） (C) 中間人攻擊（Man-in-the-middle Attack） (D) 後門攻擊（Backdoor Attack）
D	2. 下列敘述何者「不」正確？ (A) 機密性（Confidentiality）：使資訊不揭露給未經受權之人 (B) 可用性（Availability）：經授權之人，因應需求可存取或使用資訊、資產 (C) 完整性（Integrity）：使用之資產的精確度和完全性受到保護 (D) 可靠性（Reliability）：可追溯至事件的源頭
B	3. 某系統的重要資料被駭客入侵，置換成含有惡意程式的檔案，此為下列何種資訊安全特性被破壞了？ (A) 機密性（Confidentiality） (B) 完整性（Integrity） (C) 可用性（Availability） (D) 不可否認性（Non-repudiation）
A	4. 請問 ISO/IEC 27001 指導組織用下列何種方法來持續改善資訊安全管理系統（Information Security Management System, ISMS）活動，以落實控制措施之實施？ (A) P（規劃）→D（執行）→C（檢查）→A（行動） (B) D（執行）→P（規劃）→C（檢查）→A（行動） (C) C（檢查）→D（執行）→P（規劃）→A（行動） (D) A（行動）→D（執行）→C（檢查）→P（規劃）
B	5. 下列何者是國際標準組織（International Organization for Standardization, ISO）將資訊安全管理系統（Information Security Management System, ISMS）制定的資訊安全第三方驗證標準？ (A) ISO 27000 (B) ISO 27001 (C) ISO 27002 (D) ISO 27005
C	6. 建立資訊安全管理系統（Information Security Management System, ISMS）時，下列何者「最」常由管理階層執行？ (A) 撰寫資訊安全政策

	(B) 執行風險分析與評鑑 (C) 決定可接受風險等級 (D) 擔任教育訓練講師
C	7. 資訊安全管理系統之法規遵循與適法性要求，旨在降低公司單位違反法律的風險，請問若公司要避免違反智慧財產權的相關法律，下列何者「不」包含在智慧財產權中？ (A) 著作權（Literary Property） (B) 商標權（Trademark） (C) 電子簽章法（Electronic Signature） (D) 營業秘密（Trade Secret）
B	8. 關於資訊資產盤點作業，下列敘述何者正確？ (A) 資訊資產對組織而言基本上是固定的，所以盤點作業只需進行一次就好，不需定期執行 (B) 資訊資產之盤點，主要目的之一為釐清資產是否還存在，保管人是否有變動 (C) 資訊資產盤點的結果讓各單位自行了解即可，不需留下相關紀錄 (D) 資訊資產盤點作業發動者必須是資訊單位同仁，相關盤點作業之執行也一定只能由資訊單位同仁執行
C	9. 關於資訊資產分級作業，下列敘述何者正確？ (A) 資訊資產分級標準都會考量資產在會計帳面上之價值（如：採購金額大小） (B) 資訊資產分級標準都會考量資產的新舊（如：採購時間的遠近） (C) 資訊資產分級主要目的是想要確認資訊資產對組織的重要性 (D) 資訊資產分級主要目的是想要識別資訊資產會計帳面上的殘值
B	10. 在公司資產的生命過程中，欲達成資產的適當管理，如：確保資產已盤點造冊、確保資產已適切分級並受保護、定期審查重要資產之存取限制與分級等，建議採取下列何項控制措施「最」佳？ (A) 進行風險分析 (B) 指派資產擁有者 (C) 落實風險控制 (D) 實現嚴罰文化
C	11. 進行資產管理時，下列敘述何者「最」正確？ (A) 資產的分級不需要保持一致做法，所有人可依其需要自行將資訊資產分級 (B) 凡是機密資訊，都應以明顯的方式進行標示，以方便識別且不易竊取

	(C) 資產的例行工作可委派他人執行，但仍由資產擁有者負起責任 (D) 組織所有的財產，都應明列在資訊資產清冊上
B	12. 下列何者「不」適合用來決定組織的資產價值？ (A) 資產在市場上的行情 (B) 資產的存放位置 (C) 資產於初始和最終的採購、授權和維護成本 (D) 資產對組織生產經營的價值
C	13. 關於資產擁有者，下列敘述何者「不」正確？ (A) 資產擁有者須確保資產已盤點造冊 (B) 資產擁有者須確保資產已適切分級 (C) 重要資產的保護措施不為資產擁有者之責任 (D) 當刪除或銷毀資產時，資產擁有者應確保適當處置
D	14. 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，下列何者應納入評估面向？ (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
C	15. 若公司為資訊資產購買保險，當資訊安全事件發生時，所造成的損失由保險公司理賠，此種風險處置策略屬於下列何者？ (A) 風險接受 (B) 風險降低 (C) 風險移轉 (D) 風險避免
A	16. 關於風險改善計畫，下列敘述何者較「不」正確？ (A) 風險改善計畫不可變更 (B) 風險改善計畫應有期限 (C) 風險改善計畫完成後，應評估成效 (D) 風險改善計畫應針對超過可接受風險項目進行處置
B	17. 某公司之風險評鑑發現，公司全球網站設置於內部網路，將增加外部入侵內部網路的風險，下列何者是「迴避」（Avoid）上述風險的作法？ (A) 將網站改設置於公司內防火牆的非交戰區（Demilitarized zone, DMZ） (B) 將網站改設置於外部租用空間 (C) 增設網路監控設施，加強入侵監控機制 (D) 將網站設置於內部獨立網段

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 5 月 30 日　　第 4 頁，共 9 頁

A	18. 下列何者為資訊安全風險管理的要求？ (A) 資訊安全風險評鑑過程，以識別與機密性、完整性及可用性相關聯之風險 (B) 需有一位風險管理主管 (C) 相關之風險計算需納入年度預期損失的程序 (D) 需取得資產擁有者對資訊安全風險處理計畫之核准
C	19. 某公司的派工系統，原先未在高風險資產項目中，但近一年來接連遇到幾次服務中斷事件，造成極大的損失，若要重新檢視該公司資產風險評鑑要素，下列何者「不」是適當的考量項目？ (A) 資訊資產重要性 (B) 資訊資產威脅 (C) 資訊資產殘值 (D) 資訊資產脆弱點
B	20. 關於使用者帳號存取管理，下列敘述何者正確？ (A) 外部人員無需管理存取權限 (B) 隨時更新使用者資訊 (C) 職務無異動的人員無需定期檢視使用者帳號權限 (D) 高階主管可自訂密碼長度
C	21. 關於特權管理，下列敘述何者最「不」適切？ (A) 遠程遙控主機應該保留操作紀錄 (B) 若無法保留操作紀錄，應該透過跳板主機遙控主機，以利側錄操作紀錄 (C) FTP、SSH 連線之系統帳號，因牽涉系統連接，皆容許不須變更密碼 (D) 管理員帳號的使用，應確實使用執行為 Runas/sudo 命令與使用者帳戶控制（User Account Control, UAC）機制
C	22. 關於權限定期審核的作法，下列何者較「佳」？ (A) 所有系統無論重要與否皆每年執行一次權限審核 (B) 只挑選幾個使用人數較多的系統執行權限定期審核 (C) 綜合風險評估及衝擊分析的結果，決定各個系統權限定期審核的頻率 (D) 權限定期審核時，將特殊權限帳號排除，不檢核其權限
D	23. 關於控制的類型，下列何者「不」正確？ (A) 嚇阻性：為了讓有犯意的人，因恐懼而產生放棄，如：違反條款 (B) 偵測性：為了事件發生時，能夠產生警訊而察覺，如：入侵偵測 (C) 預防性：為了避免不希望的事情發生，如：設立門禁卡

	(D) 指導性：為了回復至正常運作的措施，如：回復正確設定
D	24. 關於特權帳號管理與控制中需要特別注意的項目，下列何者「不」正確？ (A) 特權帳號登入時間、頻繁次數 (B) 留下詳細的必要軌跡，每日進行盤點與稽核 (C) 使用雙授權的管理機制，增加控制點 (D) 避免特權帳號分散，帳號密碼應該統一，便於管理
B	25. 下列何者「不」適用於帳號特權管理的方式？ (A) 密碼分持 (B) 帳號密碼共用 (C) 以密碼函方式控管 (D) 定期審查具特殊存取權限之使用者
B	26. 關於身分認證（Authentication）技術中所謂的多因子（Multi-Factor）認證，下列何者「不」正確？ (A) 你/妳所知道的事物 (B) 你/妳所努力的事物 (C) 你/妳所擁有的事物 (D) 你/妳所具有的特徵
C	27. 下列何者「不」屬於存取控制之議題？ (A) 密碼定期變更 (B) 對於遠端連線應有申請程序並設定有效期限 (C) 對於程式開發與上線，應由不同人員進行 (D) 應對錯誤登入次數設定上限，超過時應有示警或其他因應措施
D	28. 關於日誌（Log）的定期檢視，下列敘述何者「最」正確？ (A) 僅能公司的稽核處人員進行 (B) 僅能由系統管理人員自己定期檢視，其他人員對系統不夠了解，無法分析 (C) 僅能由主管指派非管理該系統之人員進行檢視，以強化獨立性 (D) 主管應指派非該管理該系統人員定期進行檢視，系統管理人員也應定期執行
D	29. 關於身分認證（Authentication），下列敘述何者正確？ (A) 是個唯一且可電子讀取的名稱，電腦系統可以識別的使用者身分 (B) 會授予使用者讀、寫、執行、刪除等等權限的程序 (C) 是個會自動記錄軌跡，自己檢核的存取過程 (D) 是指通過一定的手段，完成對用戶身分的確認程序
A	30. 在存取控制中，下列何者為權限管理的最基本要求？

	(A) 最小權限 (B) 最大權限 (C) 適中權限 (D) 沒有權限
A	31. 關於系統管理者統一指定使用者對資源之權限存取策略，屬於下列何種安全模式？ (A) MAC（Mandatory Access Control）強存取控制 (B) DAC（Discretionary Access Control）自由存取控制 (C) RBAC（Role-Based Access Control）基於角色存取控制 (D) ABAC（Attribute-Based Access Control）基於屬性存取控制
C	32. 關於個人資料檔案（含實體紙本與電子檔案）之保存與銷毀，下列敘述何者「不」正確？ (A) 蒐集之個人資料，應善盡保護及管理責任，並訂定各類資料保存年限；若有法令規定者，保存期限不得低於法令要求；且非有特殊理由，原則上不得將個人資料檔案之保存期限定為永久保存 (B) 應將個人資料檔案之保存期限填寫於「個人資料檔案清冊」 (C) 紙本之個人資料封箱保存時，無需使用標示機制，以避免洩露過多資訊 (D) 資料銷毀之執行人員、方式、區域等應建立標準作業程序，執行時須確實記錄相關資訊
A	33. 為防止身分認證使用的帳號及密碼遭到攻擊破解，下列敘述何者最「不」正確？ (A) 密碼應與使用者帳號有關連，以免自身忘記 (B) 至少 8 個字元以上長度，包含數字、英文字母大小寫及特殊符號 (C) 密碼應定期更換，並不可重複使用 (D) 不可與人分享密碼或是使用懶人密碼
C	34. 關於數位簽章（Digital Signature）及數位信封（Digital Envelop），下列敘述何者正確？ (A) 數位簽章與數位信箱皆運用雜湊函式（Hash Function）達成效果 (B) 數位簽章主要是將訊息摘要加密後運用對稱金鑰加密 (C) 數位信封將資料以對稱金鑰加密，再將金鑰透過公開金鑰加密技術傳輸供收訊方解密 (D) 數位簽章及數位信封技術在訊息傳遞時皆已加密訊息
B	35. 關於數位簽章（Digital Signature），下列敘述何者「不」正確？ (A) 使用了公開金鑰基礎建設（Public Key Infrastructure, PKI） (B) 簽章時用公鑰（Public Key）加密

	(C) 公鑰（Public key）必須向接受者信任的數位憑證認證機構（Certificate Authority, CA）註冊 (D) 可以用 EIGamal 演算法來實做數位簽章
C	36. 關於資安事件發生時的應變，下列敘述何者較「不」正確？ (A) 疑似病毒入侵時，應優先拔除網路線，避免病毒擴散 (B) 遭受天然災害時（如：地震、火災），應在有限範圍內攜帶重要資料離開現場 (C) 事件發生的第一時間，不需浪費時間進行判斷，應立刻採取行動 (D) 應保留事件發生的所有證據，以利後續分析
C	37. 若公司電腦檔案被勒索軟體加密，下列何者「不」是正常應變處置程序？ (A) 斷網降低網路擴散之風險，並且進行鑑識追蹤感染來源 (B) 清查是否有相關版本的備份，或是從受保護安全區取回檔案 (C) 交付比特幣贖金以加速檔案解密 (D) 必須依據資安通報流程進行通報
B	38. 依據「行政院國家資通安全會報通報及應變作業流程」，各級政府機關於通報並著手處理資安事件後，若判定為 3 級或 4 級事件，應於幾小時內完成復原或損害管制？ (A) 24 小時 (B) 36 小時 (C) 48 小時 (D) 60 小時
B	39. 某公司遭駭客針對網站伺服器傳送大量特定封包而導致網站癱瘓，造成資訊系統部分功能降低或喪失，此稱為下列何者？ (A) 資訊安全事件（Event） (B) 資訊安全事故（Incident） (C) 資訊安全風險（Risk） (D) 資訊安全分析（Analysis）
A	40. 某公司規定重要系統與資料，在發生重大災難時，也不能發生過長營運中斷或是資料的遺失，當該公司建置異地備援中心時，下列何者「最」能符合上述要求？ (A) 熱備援（Hot Backup Site） (B) 暖備援（Warm Backup Site） (C) 冷備援（Cold Backup Site） (D) 無需建置備援中心
D	41. 若公司高階管理層希望對公司採取 ISO/IEC 27001 資訊處理措施，實

	施多重備援（Redundancies），應屬於下列何種控制措施？ (A) 紀錄之保護 (B) 系統安全測試 (C) 保護應用服務交易 (D) 資訊處理設施之可用性
C	42. 關於系統備援的方案：1.熱備援（Hot Backup Site）、2.暖備援（Warm Backup Site）、3.冷備援（Cold Backup Site）所需的資源成本，下列排序何者正確？ (A) 3＞1＞2 (B) 3＞2＞1 (C) 1＞2＞3 (D) 2＞1＞3
A	43. 若系統固定每星期日執行一次完整備份（Full Backup），則星期一到星期六每天備份後與星期日完整備份後不同的部分，稱為下列何者？ (A) 差異備份（Differential Backup） (B) 增量備份（Incremental Backup） (C) 循環備份（Circulatory Backup） (D) 緊急備份（Emergency Backup）
A	44. 關於復原時間目標（Recovery Time Objective, RTO）與復原點目標（Recovery Point Objectives, RPO），下列敘述何者「不」正確？ (A) RTO 為發生中斷後皆需達到原運作水準所需花費的時間目標 (B) RPO 為發生中斷後資料恢復的時間點目標 (C) RTO 與中斷時間有關，RPO 與資料遺失區間有關 (D) 因應 RPO 選用的技術有時也與 RTO 能恢復的時間有關
D	45. 關於異地備援（Remote Backup）的地點選擇，一般建議需離原來的機房有足夠距離，主要是考量下列何種要素？ (A) 建置的難度 (B) 建置的費用 (C) 災難發生的時間 (D) 災難的影響範圍
D	46. 個人資料保護法主要管轄個人資料的蒐集、處理和利用行為，下列何種行為「不」屬於個人資料保護法管轄範圍？ (A) 以任何方式取得個人資料 (B) 建立或利用個人資料檔案所為資料之記錄、編輯、更正、輸出或內部傳送 (C) 蒐集之個人資料為處理以外之使用

	(D) 陌生推銷壽險傳單
C	47. 關於隱私保護，下列敘述何者「不」正確？ (A) 領土隱私：限制入侵居家環境與工作場所等等 (B) 通訊隱私：規範任何形式的通訊安全與隱私，如：電子郵件、信件等 (C) 身體隱私：婚姻狀態、就業狀態等等 (D) 資訊隱私：規範個人資料收集、處理與利用，如：信用卡、醫療紀錄等
A	48. 下列何者「不」屬於受到智慧財產權保護的資產？ (A) 空白光碟片 (B) 原版軟體光碟片 (C) 軟體版權 (D) Windows 作業系統
D	49. 在資訊倫理領域中，常提到的四大議題（PAPA，學者 Mason 所提出），下列何者「不」在其中？ (A) 隱私權（Privacy） (B) 精確性（Accuracy） (C) 所有權/財產權（Property） (D) 可用性（Availability）
C	50. 由獨立的驗證單位所執行之稽核，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