# 初級資訊安全工程師 能力鑑定樣題



**單選題 50 題（佔 100%）**

| | |
|---|---|
| B | 1. 學生侵入學校的伺服器，偷偷竄改自己的期末考成績。這是破壞了資訊的哪一項特性？<br>(A) 保密性（Confidentiality）<br>(B) 完整性（Integrity）<br>(C) 可用性（Availability）<br>(D) 責任性（Accountability） |
| C | 2. 組織對外服務之官方網站遭受駭客透過 DDoS 攻擊，請問此為下列哪項遭受破壞？<br>(A) 機密性<br>(B) 完整性<br>(C) 可用性<br>(D) 可讀性 |
| B | 3. 請問下列何項說明內容是關於「可用性」的敘述？<br>(A) 使用者以專用帳號及密碼登入 ERP 系統<br>(B) 電信商機房故障，暫時無法使用網路<br>(C) 親自遞送機密文件給總經理核閱<br>(D) 出勤系統異常，導致薪資計算錯誤 |
| C | 4. 請問下列敘述何者正確？<br>(A) 衝擊是威脅利用弱點對資產造成風險的可能性<br>(B) 衝擊是資產利用弱點對威脅造成風險的可能性<br>(C) 風險是威脅利用弱點對資產造成衝擊的可能性<br>(D) 風險是資產利用弱點對威脅造成衝擊的可能性 |
| A | 5. 下列何項非為成功建立資訊安全管理系統之必要項目？<br>(A) 導入 ISO 國際標準<br>(B) 最高管理階層的參與及支持<br>(C) 組織提供建立資訊安全管理系統（Information Security Management System, ISMS）所需之資源<br>(D) 確立資訊安全管理的政策及目標 |
| C | 6. 在資訊安全管理系統中，進行資安內部查核時，下列敘述何者不正確？<br>(A) 在查核前擬定稽核計畫<br>(B) 招開行前會議，說明稽核計畫<br>(C) 稽核人員可稽核所屬單位，無須具備獨立性<br>(D) 建立稽核程序書或文件 |

| | |
|---|---|
| B | 7. 下列何種作為，展現了最高管理階層對資訊安全管理系統（Information Security Management System, ISMS）之領導和承諾？<br>(A) 確保資訊安全政策和目標需至少維持三年不變<br>(B) 確保資訊安全的要求已整合至組織的各項作業流程<br>(C) 確保在未來一年內降低組織的營運成本<br>(D) 確保適當規劃和制訂完成組織的年度營運計畫 |
| B | 8. 資訊安全管理系統的導入，實際執行 PDCA（計畫-執行-檢查-行動）的過程中，不包含下列何者？<br>(A) 最高管理階層審查會議<br>(B) 業務部門績效審核<br>(C) 內部稽核計畫執行<br>(D) 災害復原計畫演練 |
| D | 9. 關於資訊資產之擁有、使用、保管，下列敘述何者正確？<br>(A) 保管者（Custodian）負責獲得適當的授權，得以檢視、使用、存取或異動資訊資產<br>(B) 擁有者（Owner）對於資訊資產負有管理的權責，通常由各使用者擔任或其指派之人員擔任<br>(C) 使用者（User）負責資訊資產的相關處理與保管工作<br>(D) 為釐清資訊資產之擁有、保管與使用的權責，確保資產由適當的人員保管及使用，應由各部門權責主管指定適當之擁有者、保管者與使用者 |
| C | 10. 資產是對組織有價值的任何事物，而資訊也是資產的一種。請問下列何種不是資訊資產？<br>(A) 員工人事資料<br>(B) 電腦<br>(C) 辦公桌<br>(D) 套裝軟體 |
| C | 11. 關於資訊資產分級的目的，下列敘述何者正確？<br>(A) 確保員工及承包商之相關安全責任<br>(B) 限制對資訊及資訊處理設施的存取<br>(C) 確保資產依其對組織之重要性，受到適切等級的保護<br>(D) 確保運作中系統的完整性 |
| D | 12. 在進行資產管理時，下列哪一項應優先建立？<br>(A) 稽核計畫<br>(B) 溝通管理<br>(C) 風險登記表<br>(D) 資產清冊 |

| | |
|---|---|
| D | 13. 關於資產分級盤點施作方式，下列敘述何者不正確？<br>(A) 保管人離職轉移，需要進行相關資產歸戶變更<br>(B) 異地備援端相關系統，需另標示位置資訊，以為識別<br>(C) 電腦規格需依據製造商規格項列於資訊紀錄中<br>(D) 資訊設備送修，無法列入盤點，可以不用處置追蹤 |
| C | 14. 下列何者非資產擁有者所負責執行之工作？<br>(A) 確保資產已盤點並造冊<br>(B) 確保資產已經適切分級，並實施適當之保護<br>(C) 確保資產以最低之成本進行採購<br>(D) 確保資產的銷毀已採取適當之處置程序 |
| C | 15. 下列何者為建立組織資訊安全管理系統（Information Security Management System, ISMS）活動中優先於另三項需要進行的任務？<br>(A) 識別弱點<br>(B) 識別現有及已規劃之控制措施<br>(C) 識別資訊資產<br>(D) 識別威脅 |
| A | 16. 如果資訊安全事件的攻擊者的獲益小於成本時，或是預估的損失在組織可以容忍的範圍內，此時可以採取哪一種風險處置策略？<br>(A) 風險接受<br>(B) 風險降低<br>(C) 風險移轉<br>(D) 風險避免 |
| D | 17. 以下何者非風險評鑑後，對於超出風險事項首要處理方式？<br>(A) 風險規避<br>(B) 風險轉嫁<br>(C) 風險控制<br>(D) 風險再評鑑 |
| C | 18. 關於風險分析（Risk Analysis），下列敘述何者不正確？<br>(A) 在現有的控制方法下，系統性運用有效資訊，以判斷特定事件發生的可能性及其影響的嚴重程度<br>(B) 將可接受風險與主要風險分開，並提供風險評量所需的資料<br>(C) 風險分析的步驟之一為畫出風險圖像，依分析資料結果畫出風險圖像，橫軸代表機率，縱軸代表時間<br>(D) 風險分析的步驟之一為蒐集資訊，包括紀錄經驗、國外的應用、出版文獻、調查與研究、專家判斷、模型應用、實驗及原型 |

| | |
|---|---|
| C | 19. 關於資訊安全管理系統中的風險處理，下列敘述何者不正確？<br>(A) 依照風險等級，實施控制措施，降低風險<br>(B) 可選擇風險轉移；比方購買地震或防火保險<br>(C) 所有風險都可以選擇直接接受<br>(D) 移除風險來源 |
| D | 20. 下列何者不是定量風險分析中所使用的計算因子？<br>(A) 年度發生率（Annualized Rate of Occurrence, ARO）<br>(B) 資產價值（Assets Value）<br>(C) 暴露因子（Exposure Factor, EF）<br>(D) 均線（Moving Average, MA） |
| D | 21. 關於存取控制措施，下列敘述何者不正確？<br>(A) 應建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序<br>(B) 組織應在符合資訊存取限制條件下，讓授權的使用者可指派分享的存取權限<br>(C) 對於每一種允許的遠端存取類型，都應先取得授權，建立使用限制、組態/連線需求及實作指引，並予以文件化<br>(D) 資訊系統無需對行動裝置之連線要求授權 |
| C | 22. 存取控制大概可分為三類，系統、實體與網路存取控制。以下哪種行為是屬於實體存取控制？<br>(A) 讀取公司郵件<br>(B) 列印生產報表<br>(C) 進入機房巡檢<br>(D) 上網瀏覽新聞 |
| B | 23. 新進員工好奇嘗試操作公司資訊系統，發現很多功能都無法使用，但其主管使用時卻無此問題。關於上述情境，最可能發生的原因何？<br>(A) 系統有缺陷造成<br>(B) 最小權限原則<br>(C) 硬碟發生壞軌<br>(D) 系統感染電腦病毒 |

| | |
|---|---|
| C | 24. 下列何種權限管理行為較不適當？<br>(A) 公司負責人擁有 ERP 所有系統的唯讀權限，並另外擁有最高管理者的帳號密碼<br>(B) 採購主管擁有 ERP 採購系統除單據（紀錄）刪除外的所有權限，並擁有物料庫存數量的查詢權限<br>(C) 資訊人員擁有 ERP 系統設定權限，並同時擁有 ERP 系統採購單據的新增、編輯、刪除權限<br>(D) 會計主管擁有 ERP 系統每月結轉權限 |
| B | 25. 關於身分認證（Authentication），下列敘述何者正確？<br>(A) 擁有系統的帳戶與密碼，可以登入電子系統<br>(B) 確認使用電子身分的是使用者本人的程序<br>(C) 給予使用者聽、說、讀、寫、執行、刪除等等權限<br>(D) 留下使用者的使用軌跡，並且自動稽核 |
| A | 26. Faker 是公司的資訊人員，主要職責為避免非法存取控制的資安事件發生。請問以下「不是」他應有的作為？<br>(A) 將多台電腦共用同一組存取密碼<br>(B) 記錄所有登入的事件<br>(C) 呼籲同仁在離開電腦時需上鎖<br>(D) 呼籲同仁切勿將自己的帳戶提供他人使用 |
| B | 27. 下列何者不屬於實體控制（Physical Controls）層面？<br>(A) 門禁系統<br>(B) 安全政策<br>(C) 纜線保護<br>(D) 大樓保全或警衛 |
| D | 28. 關於 OTP（One-Time Password）的特性，下列敘述何者不正確？<br>(A) 不可預測<br>(B) 使用一次<br>(C) 不可重複<br>(D) 能防止釣魚網站 |
| D | 29. 身份認證主要是來證明使用者的身份，相關的機制設計主要包含三要素，請問下列何者不包含在其中？<br>(A) Something you know<br>(B) Something you have<br>(C) Something you are<br>(D) Something you need |

| | |
|---|---|
| A | 30. 使用通關密碼或是 PIN 碼來登入資訊系統，這是屬於下列何種身份認證方式？<br>(A) 所知之事<br>(B) 所持之物<br>(C) 所具之形－靜態特徵<br>(D) 所具之形－動態特徵 |
| D | 31. 下列何者不是 Biometric Systems 識別身分驗證技術？<br>(A) Fingerprint<br>(B) Retina<br>(C) Iris<br>(D) OTP |
| C | 32. 下列哪一個工具無法進行身分認證？<br>(A) 記名悠遊卡<br>(B) 信用卡<br>(C) 超商集點卡<br>(D) 健保卡 |
| B | 33. 某家國防工業公司，員工被要求需使用智慧卡（Smart Card）和個人識別碼（Personal Identification Number, PIN）登入公司資訊系統，請問這家公司使用的是哪一種驗證方法？<br>(A) 時間基礎的一次密碼（Time-based One-Time Password, TOTP）<br>(B) 多因子認證法（Multifactor）<br>(C) 相互認證法（Mutual Authentication）<br>(D) 聯邦認證法（Federal Authentication） |
| C | 34. 使用帳號及密碼進行身分認證，是時下網路上最常用的方法，破解密碼就可以有效攻擊身分認證，下列何項不是針對破解密碼的攻擊？<br>(A) 窮舉攻擊（Brute-Force Attack）<br>(B) 字典攻擊（Dictionary Attack）<br>(C) 跨網站指令碼攻擊（Cross-Site Scripting）<br>(D) 網路釣魚網站（Phishing） |
| C | 35. 關於資安事件發生前的預先準備計畫，下列敘述何者不正確？<br>(A) 應訂定災害預防計畫<br>(B) 應規劃建置資通安全整體防護環境<br>(C) 利用防火牆等設備隔離受害主機<br>(D) 應定期實施安全稽核 |

| | |
|---|---|
| D | 36. 下列名詞解釋何者不正確？<br>(A) 年度損失預測值（ALE），一年內預期資產因風險造成之金錢損失<br>(B) 間接價值（Indirect Value），資訊資產受損或遺失，因置換或回復所估之價值<br>(C) 社會價值（Societal Value），公眾對於資訊安全事件之對錯判別<br>(D) 機會價值（Opportunity Value），從特定資安活動取得已知估計正價值 |
| C | 37. 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 1 級或 2 級事件，應於幾小時內完成復原或損害管制？<br>(A) 24 小時<br>(B) 48 小時<br>(C) 72 小時<br>(D) 96 小時 |
| B | 38. 請問發生資安事故的第一步驟為何？<br>(A) 蒐集證據<br>(B) 記錄<br>(C) 將系統回復<br>(D) 檢討原因 |
| C | 39. 當組織遇到資訊安全事件時，必須採取正確、有效的處理程序。處理事件的第一步驟是？<br>(A) 問題隔離<br>(B) 問題分析<br>(C) 問題分類<br>(D) 問題調查 |
| A | 40. 您是資安經理，正在分析異地備援的模式，公司將以最低成本考量，您將建議下列何者方案？<br>(A) 冷備援站（Cold Site）<br>(B) 暖備援站（Warm Site）<br>(C) 熱備援站（Hot Site）<br>(D) 冗餘備援站（Redundancy Site） |
| D | 41. 下列何者與營運持續計畫之規劃的關聯度較低？<br>(A) 風險評鑑的結果<br>(B) 可接受 RTO（回復時間目標）、RPO（回復點目標）的標準<br>(C) 營運衝擊分析的結果<br>(D) 資訊資產的盤點結果 |

| | |
|---|---|
| A | 42. 請問同樣的系統資料，採用下列三種備份方式，當要將資料還原時，下列何者執行還原作業所需的時間最長？<br>甲：完整備份（Full Backup） 乙：增量備份 （Incremental Backup）<br>丙：差異備份（Differential Backup）<br>(A) 甲<br>(B) 乙<br>(C) 丙<br>(D) 三者相同 |
| D | 43. 下列何者是營運持續管理的國際標準？<br>(A) ISO 9000<br>(B) ISO 14000<br>(C) ISO 20000<br>(D) ISO 22301 |
| C | 44. 在訂定企業營運持續計畫時，下列何者是首要進行的事？<br>(A) 訂定災難復原計畫（Disaster Recovery Plan, DRP）<br>(B) 執行營運衝擊分析（Business Impact Analysis, BIA）<br>(C) 獲得高階管理階層的支持<br>(D) 鑑別關鍵性業務 |
| D | 45. 先進的網路技術，開啟了個人電腦使用挖掘大量資料的可能性，因此能比過去難以想像的大規模及精準地侵犯個人隱私。下列何者不算個人隱私？<br>(A) 醫療、健康狀況<br>(B) 性生活<br>(C) 財務情況、社會活動<br>(D) 公開競選活動之 DM 上的照片 |
| D | 46. 下列何種不是智慧財產相關的法令規範？<br>(A) 專利法<br>(B) 著作權法<br>(C) 商標法<br>(D) 公司法 |
| B | 47. 下列何者不是個人資料的當事人可行使的權利？<br>(A) 查詢當事人的個人資料<br>(B) 查詢親友的個人資料<br>(C) 請求製給複製本<br>(D) 請求補充或更正 |

| | |
|---|---|
| C | 48. 請問下列敘述何者不屬於稽核員的主要工作？<br>(A) 依據稽核規劃與時程執行稽核活動<br>(B) 在稽核的過程中，紀錄相關發現與待確認事項<br>(C) 針對前一次稽核活動中的發現事項，規劃並執行相關的矯正預防作為<br>(D) 在稽核結束會議前，與受稽者再次釐清並確認相關稽核發現事項 |
| A | 49. 組織內部的人員擔任稽核人員，進行內部稽核，又稱為？<br>(A) 第一方稽核<br>(B) 第二方稽核<br>(C) 第三方稽核<br>(D) 驗證稽核 |
| D | 50. 請問下列何者不可作為稽核證據？<br>(A) 受稽人員口述<br>(B) 檢視紙本紀錄之結果<br>(C) 利用稽核工作檢測之結果<br>(D) 稽核人員之主觀判斷 |