# ITE 資訊專業人員鑑定

## 資訊安全管理類-資訊安全管理系統與風險控管試題

**試卷編號：SK102**

【注意事項】
一、本測驗為單面印刷試題，共計十頁。第二至十頁為四十道學科試題，每題 2.5 分，測驗時間 90 分鐘。
二、執行「ITE 測驗系統-Client 端程式」，請依指示輸入：
1.身份證號碼，如 A123456789 後按下『登錄』。
2.開始測驗畫面，聽候監考老師口令開始測驗。
三、有問題請舉手發問，切勿私下交談。

學科 100% （為單複選題，每題 2.5 分，共 100 分）

1. 有關實體存取控管的描述何者錯誤？

(A) 宜訂定明確之安全周界，並依其內之資產重要性及要求決定其強度
(B) 實體安全周界必須有人駐守
(C) 應考量防火門的設置
(D) 組織管理的資訊設備宜與第三方所管理之設備區隔

Ans：B

2. 資訊資產包含了以下哪些類型？

(A) 人員（內部人員、外部人員）
(B) 資料（資料、資訊）
(C) 硬體（伺服器系統、周邊及安全措施）
(D) 程序（標準及特殊）

Ans：ABCD

3. 資訊安全風險的衝擊會因為下列何者提高而降低？

(A) 現有控管強度
(B) 資訊資產價值
(C) 風險事件發生的機率
(D) 威脅及弱點的項目數

Ans：A

4. 下列何者非稽核計畫主要應考量事項？

(A) 稽核準則與範圍
(B) 稽核頻率與方法
(C) 先前稽核之結果
(D) 稽核報告的撰寫方式

Ans：D

5. 以下是跟營運持續管理相關的幾個時間，請問一般來說哪個時間最長？

(A) 目標回復時間（RTO）
(B) 最大可容忍中斷時間（MTPD）
(C) 系統回復原來狀況所需的時間
(D) 決定啓動營運持續計畫（BCP）的時間

Ans：C

6. 以下何者事項不包含於資訊安全政策之中？

(A) 管理階層意向的聲明
(B) 資訊安全整體目標及範圍
(C) 資訊安全查核程序
(D) 違反資訊安全政策的後果

Ans：C

7. 最近興起的公眾雲端網路的機制，增加最多的風險面向為下列何者？

(A) 資料的隱密性
(B) 資料的完整性
(C) 資料的可用性
(D) 資料的可歸責性

Ans：A

8. 有許多公司在辦理行銷活動（如：抽獎）時，會要求參與的顧客留下詳細的個人資料（姓名、身份證字號、生日、電話、電子郵件及地址），而這些個人資料可能會於保存在電腦中時有遭駭客竊取的風險，是以組織決定僅蒐集電子郵件做為聯絡之用，以控制資料外洩的風險，這是哪種風險控制策略？

(A) 降低風險（Mitigation）
(B) 轉移風險（Transference）
(C) 避免風險（Avoidance）
(D) 接受風險（Acceptance）

Ans：C

9. 下列何者最適合描述安全經理（Security managers）的權責為何？

(A) 負責監督日常資訊安全相關工作的管理
(B) 負責評估建立資訊安全導入計畫
(C) 負責資安技術的導入
(D) 負責資安政策的宣導

Ans：A

10. 人員到任前應進行適當的篩選，最主要包含以下哪些項目？

(A) 是否有合格的品格推薦信或可諮詢者
(B) 應徵者的學經歷檢核（完全性與準確性）
(C) 獨立的身分檢核
(D) 保密協議的簽署

Ans：ABC

11. 以下有關營運持續計畫（BCP）與災害復原計畫（DRP）的描述，何者有誤？

(A) 營運持續計畫（BCP）包含了災害復原計畫（DRP）
(B) 災害復原計畫主要係當特定系統特定事件發生災害時的處理程序
(C) 營運持續計畫（BCP）最主要的目標係指當重大災害發生時可確保關鍵業務/服務可及時回復
(D) 災害復原計畫（DRP）僅包含資訊系統的回復

Ans：D

12. 資訊安全的風險評鑑係屬於 P-D-C-A 的哪個階段？

(A) P（規劃；Plan）
(B) D（執行；Do）
(C) C（檢核；Check）
(D) A（行動方案；Act）

Ans：A

13. 有數種身份驗證的機制，其中使用一次性密碼（OTP）是屬於以下哪種方式？

(A) 你知道的事（Something You Know）
(B) 你擁有的事（Something You Have）
(C) 你是（Something You Are）
(D) 你產生的事（Something You Produce）

Ans：B

14. 以下哪幾個因素決定組織現行面臨風險的大小？
(1)資產價值 (2)事件發生機率 (3)威脅利用弱點時對資產造成的衝擊 (4)現有控制措施

(A) (1)、(2)、(3)、(4)
(B) (1)、(2)、(4)
(C) (1)、(2)、(3)
(D) (2)、(3)、(4)

Ans：A

15. 關於控制措施的可行性評估，下列何者不為主要應考量事項？

(A) 成本效益
(B) 作業可行性
(C) 技術可行性
(D) 執行人員

Ans：D

16. 風險評鑑包含了以下步驟：(1)辨識資產、(2)決定控制措施、(3)評估衝擊與風險等級、(4)辨識威脅及弱點、(5)決定可接受風險值，請選出正確的順序？

(A) (1)→(4)→(3)→(5)→(2)
(B) (1)→(2)→(4)→(3)→(5)
(C) (4)→(1)→(3)→(5)→(2)
(D) (1)→(2)→(4)→(5)→(3)

Ans：A

17. 資訊系統技術性稽核可採用以下哪些方法？

(A) 弱點掃瞄
(B) 滲透測試
(C) 帳號清查
(D) 修補程式更新

Ans：AB

18. 經風險評鑑及內部稽核後，發現組織未針對單位內人事調整訂定權限調整之流程檢核機制，致使調任人員擁有過當之權限，導致人員因操作錯誤將原本不應取得資料取走，故組織增加了組內人員異動時權限檢核機制，是以哪個量測方式以量測此控制措施的有效性為最佳？

(A) 帳號清查正確率
(B) 異動時權限檢核的執行率
(C) 資料外洩異常事故發生率
(D) 資料存取覆核的執行率

Ans：A

19. 以下哪個項目不是對環境威脅做的保護措施？

(A) 危險或易燃物品應與安全區域保持距離存放
(B) 後撤設備和備份媒體存放宜與主要場地保持安全距離
(C) 宜有適當的消防設備
(D) 設立門禁登記本

Ans：D

20. 以下有關資訊安全政策的描述何者有誤？

(A) 政策不能違反法令法規
(B) 政策應定期重新檢視以確認其有效性
(C) 政策應說明所有控制措施的執行方式
(D) 資安政策應符合組織目標的要求

Ans：C

21. 目標回復點（RPO）最主要會影響到以下何種項目？

(A) 備份週期的訂定
(B) 備援媒體的選擇
(C) 異地備援點的選擇
(D) 備援媒體存放的位置

Ans：A

22. 組織對資產資訊進行分類及價值判定是為了？

(A) 瞭解哪個資訊資產對組織的成功最關鍵
(B) 瞭解哪個資訊資產的替換成本最高
(C) 瞭解哪個資訊資產的財務價值最高
(D) 瞭解哪個資訊資產損失或破壞時會對組織帶來最大的損失或賠償

Ans：ABD

23. 人員離職應注意以下哪些事項？(1) 歸還資產 (2) 取消權限 (3) 清理電腦 (4) 終止責任

(A) (1)、(2)、(3)、(4)
(B) (2)、(3)、(4)
(C) (2)、(4)
(D) (1)、(2)、(4)

Ans：D

24. 資訊安全內部稽核人員的選擇，其最重要的考量是？

(A) 獨立性
(B) 資安知識
(C) 業務經驗
(D) 態度

Ans：A

25. 以下何者是預防性的控制措施？

(A) 線上事件通報
(B) 教育訓練及宣導
(C) 新增入侵偵測系統
(D) 縮短備份週期

Ans：B

26. 以下哪些議題應於組織之高階管理審查中定期討論？

(A) 審查發現的缺失
(B) 來自外部意見的回饋
(C) 組織及環境的變動
(D) 帳號清查的結果

Ans：ABC

27. 下列哪些為導入風險改善措施後還剩下的風險？

(A) 殘餘風險
(B) 固有風險
(C) 內部控制風險
(D) 查核風險

Ans：AB

28. 環境偵測器與 CCTVs 是屬於哪一類的控制措施？

(A) 偵測（Detective）、操作（Operational）
(B) 預防（Preventative）、操作（Operational）
(C) 偵測（Detective）、管理（Management）
(D) 預防（Preventative）、技術（Technical）

Ans：A

29. 以下哪幾項是屬於威脅的項目？

(A) 系統未設定密碼複雜度檢核機制
(B) 未經授權的存取資訊
(C) 員工隨意連上不明來源的網站
(D) 電腦病毒

Ans：BD

30. 以下哪個面向不是資訊安全考量的目標？

(A) 機密性（Confidentiality）、可究責性（Accountability）
(B) 完整性（Integrity）
(C) 可用性（Availability）、可識別性（Identification）
(D) 可管理性（Manageability）

Ans：D

31. 網路報稅所使用的電子簽章可確保資料的哪些性質？

(A) 機密性
(B) 不可否認性
(C) 完整性
(D) 可用性

Ans：BC

32. 資訊安全政策的訂定應考量以下哪些事項？

(A) 營運策略與目標一致性
(B) 相關法令法規要求
(C) 資訊安全內部查核的結果
(D) 過去曾發生之資安事故

Ans：AB

33. 資訊安全管理委員會（information security management committee）應由哪些人員參與最適當？

(A) 由管理部門及法務部門人員組成
(B) 由跨單位（包含資訊及非資訊部門）人員組成
(C) 由資訊部門人員組成
(D) 由資訊安全人員組成

Ans：B

34. 風險改善措施的量測最主要的目標是？

(A) 量測改善措施的有效性
(B) 量測控制措施的落實度
(C) 量測投入的成本
(D) 量測事件的數量

Ans：A

35. 以下有關威脅與弱點的描述何者錯誤？

(A) 弱點為資產本身存在可能被威脅利用的狀況
(B) 威脅必須利用弱點方能對資產造成損害
(C) 衝擊的大小只跟威脅的類型有關
(D) 控制措施通常是針對弱點設計

Ans：C

36. 以下哪項活動不屬於 P-D-C-A 內 C（Check）相關的活動？

(A) 內部稽核
(B) 管理審查
(C) 指標量測
(D) 程序制定

Ans：D

37. 組織指派的資訊資產擁有者最主要的責任為下列何者？

(A) 遵守組織的規定使用資訊資產
(B) 妥善的保管資訊資產
(C) 確保與資訊處理設施相關的資訊與資產被適切的分類
(D) 決定資訊資產的保管者與使用者

Ans：C

38. 使人員瞭解資訊安全的觀念，並提升人員安全認知是屬於以下何者活動，請選出最佳選項？

(A) 宣導（Awareness）
(B) 訓練（Training）
(C) 教育（Education）
(D) 測驗（Testing）

Ans：A

39. 有關內部稽核與外部稽核的差異，以下哪些為真？

(A) 一般來說，內部稽核比外部稽核查核深度深
(B) 外部稽核比內部稽核客觀
(C) 內部稽核為定期執行，外部稽核為不定期
(D) 外部稽核較內部稽核專業

Ans：AB

40. 下列哪些為組織執行風險評鑑的目的？

(A) 瞭解組織所面臨的風險全貌
(B) 決定風險控管的先後
(C) 將所有風險降到最低
(D) 避免組織從事有風險的行為

Ans：AB