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：SK100

【注意事項】
一、本測驗為單面印刷試題，共計十一頁。第二至十一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. 在建置資訊安全管理系統(ISMS)過程中，管理階層的職責應包括哪些？

(A) 核定資安政策
(B) 風險分析
(C) 資訊運用的硬體設備
(D) 決定接受風險與可接受風險等級的準則

Ans：AD

2. 在 ISMS 的建立及管理過程中，非常重要的第一步是？

(A) 辨認及分析資訊資產的相關風險
(B) 界定 ISMS 之範圍
(C) 減低風險之等級及其可能之影響
(D) 決定適當的保護措施及控制方法

Ans：B

3. 定義 ISMS 範圍後，所產生的介面如何約定？

(A) 口頭承諾
(B) 協議書
(C) 合約
(D) 備忘錄

Ans：BCD

4. 有關資訊安全政策，下列敘述哪些正確？

(A) 依照全員共識決議，提供給客户作為資訊安全之要求
(B) 由管理階層核准，並公布傳達給所有員工與相關各外部團體
(C) 依規劃之期間或發生重大變更時審查，以確保其持續的適用性、充分性及有效性
(D) 若資訊安全政策散布到組織外，宜注意勿揭露敏感性資訊

Ans：BCD

5. 資安政策文件應包括下列哪些事項的具體陳述？

(A) 資安政策範圍
(B) 法令法規遵循性
(C) 組織的資產弱點
(D) 風險管理的策略

Ans：ABD

6. 為確保資安政策的適用性、充分性及有效性，組織應於哪些時刻進行審查？

(A) 定期進行
(B) 資安政策發生重大變更時
(C) 管理階層被告知時
(D) 資安政策規劃期間

Ans：BD

7. 組織設定存取控制政策時，應考慮下列哪些要點？

(A) 個別應用系統之安全需求
(B) 不同資訊系統或網路間之安全政策應具備差異性
(C) 應定期審查使用者權限
(D) 原則開放，例外禁止

Ans：AC

8. 為每項資產或安控措施指定一個特定人，負責該資產日常的保護及管理責任。此特定人稱為：

(A) 使用者
(B) 管理者
(C) 控制者
(D) 擁有者

Ans：D

9. 「員工於工作中使用私人的資訊處理設施」是屬於資訊處理設施的授權及管理過程中的下列何種程序？

(A) 管理程序
(B) 使用程序
(C) 核准程序
(D) 檢驗程序

Ans：C

10. 資訊安全組織的目標為：

(A) 達成及維持組織資產的適切保護
(B) 確保員工、承包者及第三方使用者瞭解其責任，並勝任其所被認定的角色，以降低竊盜、詐欺或設施誤用的風險
(C) 於組織內管理資訊安全維持及由外部團體所存取、處理、管理或與其通信之組織資訊與資訊處理設施的安全
(D) 防止組織場所與資訊遭未經授權的實體存取、損害及干擾

Ans：C

11. 聘僱與安全相關工作的人員前，有哪些安全控制措施？

(A) 定義角色與職責
(B) 安全篩選與背景查核
(C) 同意並簽署其聘僱契約之條款與條件
(D) 申請並開通使用者存取權限

Ans：ABC

12. 人員之資訊安全角色與責任包括：

(A) 保護資產不受未經授權的存取
(B) 確保組織百分之百安全
(C) 執行特定的各項安全過程或活動
(D) 向組織通報安全事件或潛在的事件或其他安全風險

Ans：ACD

13. 人員聘僱終止或變更時之安全控制措施不包括下列哪一項？

(A) 終止職責
(B) 確定人事命令正確性
(C) 歸還資產
(D) 移除存取權限

Ans：B

14. 「門禁進出卡片再加上個人識別碼（Personal Identification Number, PIN）或通行碼」是屬於何種實體進入控制措施？

(A) 進出記錄 (Record)
(B) 進出識別 (Identification)
(C) 進出鑑別 (Authentication)
(D) 進出授權 (Authorization)

Ans：C

15. 設備安全管理之控制目標為？

(A) 防止資產的遺失、損害、竊盜或破解，並防止組織活動的中斷
(B) 確保正確與安全地操作資訊處理設施
(C) 使系統失效的風險最小化
(D) 保護軟體與資訊的完整性

Ans：A

16. 實體與環境安全管理之控制措施可分為下列哪兩類？

(A) 建立程序
(B) 安全區域
(C) 盤點資產
(D) 設備安全

Ans：BD

17. 下列有關資安內部稽核之敘述，何者不正確？

(A) 應於稽核前擬定稽核計畫
(B) 稽核人員應具備獨立性
(C) 稽核結果及不符合事項應及時改善，並經主管確認後結案
(D) 應建立稽核程序書

Ans：C

18. 組織執行資安內部稽核，以瞭解是否達到下列哪些要求？

(A) 符合國際標準或法規要求
(B) 符合風險規避的要求
(C) 落實年度預算執行要求
(D) 符合內部程序要求

Ans：AD

19. 管理階層審查（Management Review）是 PDCA 管理模式中哪一項活動？

(A) Plan
(B) Do
(C) Check
(D) Act

Ans：C

20. 下列何者不屬於資訊安全管理「技術遵循性查核」之實作重點？

(A) 由有經驗的系統工程師以手動方式履行
(B) 使用自動化的工具協助，產生後續由技術專家進行解讀的技術報告
(C) 不可使用滲透測試(penetration testing)
(D) 僅限由合格、經過授權的人員執行，或在其監督下執行

Ans：C

21. 下列何者不是「資產管理」的控制措施？

(A) 應明確識別所有資產，並製作與維持所有重要資產的清冊
(B) 與資訊處理設施相關的所有資訊及資產應由組織指定的部門"擁有"
(C) 在賦予客户存取組織資訊或資產的權限之前，應闡明所有已識別的安全要求
(D) 資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類

Ans：C

22. 資訊資產有許多型式，包括：

(A) 資訊：資料庫與資料檔案等
(B) 軟體資產：應用軟體、系統軟體、開發工具及公用程式
(C) 貨幣資產：股票、基金
(D) 人員：其資格、技能及經驗

Ans：ABD

23. 下列何者不屬於硬體資產之弱點？

(A) 缺乏定期檢查
(B) 專業訓練不足
(C) 不斷電系統缺乏維護
(D) 儲存媒體的劣化

Ans：B

24. 下列何者為「威脅(threat) 」的定義？

(A) 非所欲事件的潛在原因，其可能導致對系統或組織傷害
(B) 能被威脅利用之一項或一群資產的一個弱點
(C) 某事件發生的機率與其結果之組合
(D) 系統、服務或網路發生一個已識別的狀態，其指示可能的資訊安全政策違例或保護措施失效，或是可能與安全相關而先前未知的狀況等

Ans：A

25. 下列何者不屬於識別風險的活動？

(A) 識別 ISMS 範圍內之各項資產以及此等資產之擁有者
(B) 識別對該等資產的各項威脅
(C) 識別此等威脅可能利用之各項脆弱性
(D) 決定風險是否可接受

Ans：D

26. 組織進行風險評鑑（Risk Assessment）的主要功能與目的，下列何者為錯？

(A) 評估資產的脆弱性
(B) 評估事件可能對組織造成的衝擊影響
(C) 預估所需的軟硬體需求
(D) 識別資產所面臨的威脅

Ans：C

27. 評鑑安全失效時可能造成對組織之營運衝擊時，應對資產損失的後果納入考量。下列何者不在考量範圍？

(A) 機密性之損失
(B) 完整性之損失
(C) 可用性之損失
(D) 流動性之損失

Ans：D

28. 下列何者之定義為：風險分析與風險評估的整體過程？

(A) 風險分析 (Risk Analysis)
(B) 風險評鑑 (Risk Assessment)
(C) 風險處理 (Risk Treatment)
(D) 風險管理 (Risk Management)

Ans：B

29. 風險處理的可能選項包括：

(A) 採用適切的控制措施以降低各項風險
(B) 若風險明確的滿足組織之政策與風險接受準則，則知悉與客觀地接受此等風險
(C) 藉由禁止會導致風險發生的行動以避免風險
(D) 轉移相關風險至他者，例如：承保者或供應者

Ans：ABCD

30. 控制措施宜考量下列哪些因素確保風險降低至可接受程度：

(A) 國家、國際之法律與法規的要求與限制條件
(B) 各項組織目標
(C) 各項運作容易施行程度
(D) 與被降低之風險相關的實作與運作成本，並保持和組織之要求與限制條件相稱

Ans：ABD

31.「聚合效應（Aggregation Effect）」指下列何者？

COBIT IT 成熟等級分爲：
A 0
B 最佳化的
C 有管理的
D 有定義的
E 可重覆的
F 隨意的
請問依等級低至高的順序爲何？

(A) 大量累積之事故可能造成資安的衝擊
(B) 大量累積之事故可能造成組織的脆弱性
(C) 由非敏感資訊推導出敏感資訊
(D) 預估所需的硬體設備為何

Ans：C

32.「由一電腦轉移至另一電腦，自動執行的軟體程式碼，並以很少或不需使用者的互動執行特定功能。」是指下列何者？

(A) 行動碼
(B) 邏輯炸彈
(C) 特洛伊木馬
(D) 網路釣魚

Ans：A

33. 作業系統的登入程序應將未經授權存取的機會降到最低，下列哪一項不屬於良好的登入程序？

(A) 在登入程序未成功完成前，不顯示系統或應用程式的識別畫面
(B) 移除所有不必要的軟體公用程式與系統軟體或使其失能
(C) 限制失敗的次數(例如三次)
(D) 限制登入程序之最長與最短的時間

Ans：B

34. 下列何者不屬於資安監視(Monitoring) 之控制措施？

(A) 建立資訊處理設施使用的監視程序，並定期審查監視活動的結果
(B) 保護存錄設施與日誌資訊，不受竄改與未經授權的存取
(C) 限制與控制特權的配置與使用
(D) 失誤應予以存錄、分析，並採取適當措施

Ans：C

35. 下列敘述何者不正確？

(A) 若評鑑為低風險或處理風險的成本對組織不符成本效益時，風險可能被接受
(B) 風險評鑑依風險接受和與組織相關的目標等準則，識別、量化各項風險，並排定其優先順序
(C) 風險評鑑包括估計風險大小的系統性作法(風險分析)，及將預估風險與風險準則作比較以決定風險的顯著性(風險評估)之過程
(D) 風險評鑑應依據風險處理計畫進行風險分析與風險評估

Ans：D

36. 「考慮購買適當的保險，作為整體營運持續流程的一部分」是營運持續策略中的何種策略？

(A) 接受風險策略
(B) 避免風險策略
(C) 轉移風險策略
(D) 降低風險策略

Ans：C

37. 營運持續規劃框架中，「描述將採取哪些行動將絕對必要的營運活動或支援服務移轉到替代的臨時地點，並在所要求時間內恢復營運過程。」是為下列何項程序？

(A) 緊急程序
(B) 後撤程序
(C) 備援程序
(D) 再續程序

Ans：B

38. 下列何項不是用來分析營運中斷之衝擊與風險的方法？

(A) 識別能導致營運過程中斷的事件
(B) 風險評鑑
(C) 風險處理計畫
(D) 營運衝擊分析

Ans：C

39. 下列哪些屬於「個人資料保護法」規範之個人資料？

(A) 健康檢查報告
(B) 職業
(C) 婚姻
(D) 教育

Ans：ABCD

40. 下列哪些是資訊外洩的威脅管道？

(A) 鍵盤側錄程式
(B) 後門程式
(C) 網頁漏洞
(D) 金鑰加密

Ans：ABC