



# 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：SK99

**【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. 下列哪些是資訊安全的範圍？

- (A) 網路安全
- (B) 電腦與資料安全
- (C) 資訊安全政策
- (D) 資訊安全管理

Ans : ABCD

2. 下列何者在 NSTISSC Security Model 下是不同維度的？

- (A) 機密性
- (B) 完整性
- (C) 可用性
- (D) 儲存區域

Ans : D

3. 下列何者非資訊安全管理系統評估的目標？

- (A) 判斷資訊資產的價值
- (B) 確認組織資訊資產面臨的風險
- (C) 判斷目前組織實務之現有風險
- (D) 確保實體安全

Ans : D

4. 下列何者非關於資訊安全管理系統的標準？

- (A) ISO 17799
- (B) ISO 27799
- (C) ISO 37799
- (D) ISO 27001

Ans : C



5. 下列工具何者可以找出網路上的資產？

- (A) Snort
- (B) OpenNMS
- (C) Nessus
- (D) Nmap

Ans : B

6. 下列工具哪些可以協助找出資產現有風險？

- (A) Snort
- (B) Nessus
- (C) Nmap
- (D) OpenNMS

Ans : ABC

7. 下列哪項技術與 Access Control 無關？

- (A) Secure ID
- (B) Fingerprints
- (C) Hardware Firewall
- (D) Iris scan

Ans : C

8. 下列哪些技術可以讓無線傳輸更加安全？

- (A) Wired Equivalent Privacy
- (B) Wi-Fi Protected Access
- (C) Ad-hoc
- (D) PMP

Ans : AB

9. 下列何者非伺服器所應考慮的實體安全問題？

- (A) 火災
- (B) 停電
- (C) 進出管制
- (D) SQL Injection

Ans : D



10. 企業內全體員工應需負以下何種責任？

- (A) 規劃資安控制措施
- (B) 遵守資安政策
- (C) 規劃、協調、執行、審查與改進資訊安全管理系統
- (D) 審查重要資安措施

Ans : B

11. 要如何有效的編列安全預算給高階主管？

- (A) 整理出目前遭受威脅的資產，照資產成本編列
- (B) 整理出資產遇到攻擊所會損失的成本以茲證明
- (C) 整理出資產遭受攻擊時，可採取的手段之成本，並選擇最佳方案編列
- (D) 整理出資產遭受攻擊時，可採取的手段之成本，並選擇最貴的方案編列

Ans : BC

12. 下列何者與 ISO/IEC 27001:2005 無關？

- (A) 提供組織制訂安全政策與標的
- (B) 定義資訊安全管理程序
- (C) 辨認與說明已存在的資訊安全管理程序
- (D) 可當作資訊安全管理系統實作的框架

Ans : D

13. 下列何者不屬於 BS7799:2 PDCA 下的 Plan 之行為？

- (A) 定義資訊安全管理系統的範疇
- (B) 定義風險評估的方法
- (C) 制訂風險威脅計畫
- (D) 評估風險

Ans : C

14. 下列哪些工具可以檢測程式原始碼的弱點？

- (A) CodeSecure
- (B) Fortify SCA
- (C) Snort
- (D) Codescan

Ans : ABD



15. 下列哪些是文件稽核的內容？

- (A) 資訊安全政策
- (B) 資訊安全管理系統範疇(Scope)
- (C) 同意書
- (D) 適用性聲明

Ans : ABD

16. “確認改善有達到目標”這項目是屬於 PDCA 的哪一階段？

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

Ans : D

17. 下列哪些會造成資訊安全的威脅？

- (A) 使用者操作疏失
- (B) 委外開發軟體
- (C) 火災
- (D) 異地備援

Ans : ABC

18. SecSDLC 包含下列階段：(A)調查、(B)實體設計、(C)邏輯設計、(D)維護、(E)實作、(F)分析；請問執行順序為何？

- (A) CBADEF
- (B) DCAFEB
- (C) CEFBDA
- (D) AFCBED

Ans : D

19. 下列哪個方法無法達到訊息的完整性？

- (A) 雜湊函數
- (B) 對稱式加密
- (C) 數位簽章
- (D) RSA

Ans : B



20. 下列何者非對技術人員訓練所應採取的方法？

- (A) 根據工作種類
- (B) 根據工作所需操作的功能
- (C) 根據技術產品
- (D) 一視同仁

Ans : D

21. 威脅的因素不包含以下哪項？

- (A) 目標
- (B) 病毒
- (C) 起因
- (D) 事件

Ans : B

22. 風險是下列哪些因素的結合？

- (A) 威脅
- (B) 重點
- (C) 弱點
- (D) 起因

Ans : AC

23. 在 CSI/FBI 2009 年調查中，最嚴重的前兩名威脅為何？

- (A) DoS
- (B) 電腦/行動設備失竊
- (C) 惡意程式感染
- (D) 密碼竊聽

Ans : BC

24. 資產價值包含以下哪些項目？

- (A) 機密性
- (B) 完整性
- (C) 可用性
- (D) 不可否認性

Ans : ABC



25. 下列哪些為資訊資產的類別？(A)文件、(B)資料、(C)硬體、(D)軟體、(E)人員、(F)水電、(G)網路

- (A) ABCD
- (B) ABCDE
- (C) ABCDEG
- (D) ABCDEFG

Ans : D

26. 組織面臨未準備好的科技服務，資訊會面臨哪些威脅？

- (A) 病毒、蠕蟲和木馬
- (B) 密碼破解
- (C) 系統誤用
- (D) 軟體缺陷利用

Ans : ABD

27. 單一損失期望為 10,000，年度發生率為 0.3，則年度損失預期值為？

- (A) 30,000
- (B) 300
- (C) 3,000
- (D) 33,333

Ans : C

28. 當資產成本為 1,000，每次遭受風險的受損率為 50%，每年發生的次數為 0.3，花費 30 採取防護措施，請問受損率至少要降低多少才符合成本效益？

- (A) 40%
- (B) 9%
- (C) 9.9%
- (D) 10.1%

Ans : D

29. 當資產成本為 200,000，每次遭受風險的受損率為 50%，每年發生的次數為 0.3；但在花費 10,000 採取防護機制後，受損率降為 10%，請問下列敘述哪些是正確的？

- (A) 採取防護機制前的 ALE 為 30,000
- (B) 採取防護機制後的 ALE 為 5,000
- (C) 年損失降低 24,000
- (D) 採取該防護機制不符合成本效益

Ans : AC

30. (A)衡量方案的有效性、(B)實施控制、(C)進行決策支援、(D)估算風險。請問安全風險管理的執行順序為何？

- (A) DABC
- (B) BACD
- (C) ADBC
- (D) DCBA

Ans : D

31. 請參閱附圖作答：

COBIT IT 成熟等級分為：  
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為何？

- (A) ABCDEF
- (B) AFDECB
- (C) ACBFED
- (D) AFEDCB

Ans : D



32. 下列哪一種機制在理論上災難復原時間最短？

- (A) 異地備援(Active/Standby)
- (B) 異地互援(Active/Active)
- (C) 磁帶備份
- (D) 硬碟備分

Ans : B

33. 災難將發生於哪兩個因素下？

- (A) 組織無法掌握災難的影響
- (B) 沒有防火牆
- (C) 沒有防震裝置
- (D) 災難或傷害讓組織無法快速回復運作

Ans : AD

34. 下列哪項不是磁碟備份的方法？

- (A) RAID 0
- (B) RAID 5
- (C) Disk Shadowing
- (D) RAID 1

Ans : A

35. 測試應變計畫的方式有下列哪幾種？

- (A) 模擬
- (B) 平行測試
- (C) 硬碟檢查
- (D) 完全中斷

Ans : ABD

36. 應變計畫不包含以下哪個元件？

- (A) BIA
- (B) IR
- (C) DR
- (D) BD

Ans : D



37. 下列哪一項不在應變計畫的程序中？

- (A) 建構企業營運衝擊分析
- (B) 發展復原策略
- (C) 規劃維護計畫
- (D) 風險分析

Ans : D

38. 下列何者與資產權重評估無關？

- (A) 防護方式最貴
- (B) 對組織成功來說是關鍵的
- (C) 產生最大的收益
- (D) 使用的人

Ans : D

39. Win 7 的高安全性將帶來什麼樣的問題？

- (A) 駭客更願意尋找系統漏洞
- (B) 社交工程將更加盛行
- (C) 不會有任何改變
- (D) Windows 將趨弱勢

Ans : B

40. 下列哪些威脅在 OWASP Top 3 for 2010 內？

- (A) Injection
- (B) Insecure Cryptographic Storage
- (C) Cross-Site Scripting (XSS)
- (D) Cross-Site Request Forgery (CSRF)

Ans : AC