ITE 資訊專業人員鑑定

資訊安全類-資訊安全管理系統與風險管理試題

試卷編號：SK105

【注意事項】

一、本測驗為單面印刷試題，共計十二頁。第二至十二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. ISO 27001:2013 的控制措施數量與 ISO 27001:2005 相較，共減少多少控制措施？
   (A)20
   (B)19
   (C)17
   (D)15

Ans：A

2. 事故週期的順序為何？1.事故 2.損害 3.威脅 4.復原
   (A)1234
   (B)2134
   (C)3124
   (D)3214

Ans：C

3. 在識別資訊安全風險評估時，應考量項目有哪些？（請參閱附圖作答）

(1) ISMS 範圍內各項資產的財務流動性
(2) ISMS 範圍內各項對組織有價值的事物
(3) 對於 ISMS 資產的各項威脅與此等威脅可能利用之各項脆弱性
(4) 對於 ISMS 範圍內各項資產可能造成機密性、完整性與可用性之損失的衝擊
(5) ISMS 範圍內各項資產的擁有者

   (A)2345
   (B)12345
   (C)1345
   (D)234

Ans：A

4. 電腦教室藉由刷卡管制門禁，以卡片識別身分屬於哪種因子
(A)something you are
(B)something you have
(C)something you know
(D)something you use

Ans：B

5. 經由網路感染電腦的惡意碼為下列哪些？
(A)Storm Worm
(B)Botnet
(C)Trojan
(D)Spyware

Ans：AB

6. 在無授權或未被監測時，最嚴格的使用資產限制為何？
(A)不能存取
(B)不能修改
(C)不能刪除
(D)不能新增

Ans：A

7. 針對物聯網的資訊安全敘述何者為非？
(A)安全強度已可抵抗現存的威脅
(B)受限於硬體的規格，可能無法提供較安全可靠的通訊機制
(C)最小化所蒐集的資料，避免擔負越多的風險
(D)終端裝置的存取控制機制不當，便會導致其他使用者可以任意修改終端裝置的設定

Ans：A

8. 符合法律的前提下，以何種方式監管網際網路的使用行為是最佳的？
(A)安裝軟體工具，不能存取某些網站
(B)訂定使用守則，明訂雇主和員工雙方的權利與義務
(C)落實隱私法規
(D)安裝防毒軟體

Ans：B

9. 風險管理的目的是什麼？
(A)判定將發生的特定風險之機率
(B)判定可能的安全事故所造成的損害
(C)指出暴露於威脅的 IT 資源
(D)採取措施以降低風險到可接受的水準

Ans：D

10. 下列哪一項不是稽核時應遵守的指引？
(A)技術稽核測試的範圍應商定並被控制
(B)稽核測試應限於對軟體與資料的唯讀存取
(C)可能影響系統可用性的稽核測試應最先完成
(D)應與合適的管理者商定對系統與資料存取的稽核要求

Ans：C

11. ISO 27001:2013 與 ISO 27001:2005 相較，新增的獨立領域有下列哪些？
(A)供應商關係
(B)資產管理
(C)密碼學
(D)存取控制

Ans：AC

12. 下列有關資訊安全查核基本觀念之敘述何項有誤？
(A)所謂自行查核即查核員可為方便而查核本身所負責之工作
(B)進行查核前須先經過適當規劃
(C)使用查核工具時應避免造成營運中斷
(D)查核員應遵循職業道德規範

Ans：A

13. 可以使用哪些密碼技術達成完整性的安全目標？
(A)金鑰交換
(B)數位簽章
(C)訊息鑑別碼
(D)加密

Ans：BC

14. 資訊分類的目標是什麼？
(A)建立應用系統的說明書
(B)應用標籤，使資訊更容易識別
(C)根據其敏感性，建立分級
(D)根據其可用性，建立分級

Ans：C

15. 要持續確保資訊安全政策的適宜性、充分性和有效性，應於哪些期間進行資訊安全政策的審查？
(A)按計畫的定期時間
(B)發生重大變化
(C)發生稽核缺失時
(D)機密資料外洩時

Ans：AB

16. 為什麼有必要維持災害復原計畫是最新的並且需要定期測試？

(A)為了在辦公室以外的地方能存取備份資料

(B)為了避免業務中斷時，所採取的措施可能是不夠的或可能已經過時

(C)為了能夠應付日常發生的故障

(D)因應個人資料保護法的要求

Ans：B

17. 在風險處理與控制措施進行過程中，下列敘述哪些有誤？

(A)風險處理與控制措施擬定後即為改善完成

(B)應確實留存相關改善紀錄

(C)必須經過管理階層之授權

(D)因應法規法令要求所設計的控制項目，與風險無關，無需擬定風險處理計畫即可執行

Ans：AD

18. 有關組織的人員資訊安全管理與說明，下列哪些有誤？

(A)個人電腦禁止人員使用行動裝置同步傳輸軟體，如 iTunes、HTC Sync Manager 等，僅開放充電功能，可確保資料不會透過行動裝置洩露

(B)正職員工、約聘人員、工讀生、委外廠商及合作單位，皆應全面遵守組織內部規範之人員資訊安全要求

(C)使用同一系統之人員應共用同一帳號密碼，除降低帳號設定與定期檢覆的繁複程序外，也可避免因登入資訊過多造成系統效能降低

(D)隨身硬碟容易感染電腦病毒，或不當取用造成資料外洩，組織必須全面禁止使用，才能確保資料安全

Ans：ABD

19. 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

20. 資訊安全政策的目的，下列何者是最佳的描述？
(A)記載風險分析與尋找對策
(B)提供資訊安全管理的方向與支持
(C)提供必要的細節，使安全計畫能具體化
(D)洞察威脅與可能產生的後果

Ans：B

21. 提升資訊安全認知應讓員工了解下列哪些？
(A)做什麼
(B)如何做
(C)為什麼做
(D)何處做

Ans：ABC

22. 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

23. 關於有效性量測的敘述，下列哪些是錯誤的？

(A)設計指標衡量時可考量管理控制措施、技術控制措施、作業管理流程...等

(B)具有彈性，因此不同人計算會有不同的結果

(C)有依據、可操作、能比較

(D)針對未達成目標值的人員應進行懲罰性措施

Ans：BD

24. 整個組織實施與資訊安全相關的法律為下列哪些？

(A)智慧財產權

(B)ISO/IEC 27001：2013

(C)ISO/IEC 27002：2013

(D)個人資料保護法

Ans：AD

25. 組織與專業安全論壇或專業團體保持適當聯繫的目的為何？

(A)最新相關安全資訊的瞭解

(B)確保對當前資訊安全環境的瞭解是最近與完整的

(C)分享與交換新技術、產品、威脅或脆弱性的資訊

(D)可保證資訊安全無虞

Ans：ABC

26. 下列何者並非是風險處理與控制措施選擇所應考量的因素？

(A)業務運作的合理效率

(B)組織資源限制

(C)引用最新的控制技術

(D)可執行性

Ans：C

27. 誰有權更改文件的分類？
(A)該文件的作者
(B)該文件的使用者
(C)該文件的擁有者
(D)該文件的管理者

Ans：C

28. 對於風險處理，您的單位可能採行控制、迴避、轉移與接受風險等措施，請問在何種情況下，您的單位會選擇接受風險？
(A)該風險一旦發生受損害者非本單位
(B)已採取基本的控制措施
(C)其明顯符合組織政策與可接受風險準則
(D)單位已無足夠的資金可以投入

Ans：C

29. 下列何者較不適合作為量測安全管理有效性之指標？
(A)資安中斷次數
(B)網路設備異常次數
(C)教育訓練次數
(D)電腦中毒次數

Ans：C

30. 電纜自然鬆動、資料意外被變更、資料被私自使用、資料被偽造，前述例子中哪些屬於完整性的威脅？
(A)電纜自然鬆動
(B)資料意外被變更
(C)資料被私自使用
(D)資料被偽造

Ans：BD

31. 進行滲透測試或脆弱性評估，應完成下列哪些要求後，才能確保系統不受損害？
(A)預先計畫
(B)形成文件
(C)可再重現
(D)產生日誌

Ans：ABC

32. 最嚴重的科技風險為下列何者？
(A)網路攻擊風險
(B)資料詐騙和資料外洩風險
(C)關鍵基礎建設中斷風險
(D)科技濫用風險

Ans：A

33. 資訊安全之持續性控制措施最好的驗證方式為何？
(A)與組織業務持續與災害復原測試進行整合
(B)與一般控制措施的驗證方式相同
(C)採不定時驗證
(D)業務中斷時方可進行驗證

Ans：A

34. 某個寄送訊息的人否認有該行為，此舉有違下列何者？
(A)機密性
(B)完整性
(C)可用性
(D)不可否認性

Ans：D

35. 應用資訊安全風險評鑑過程，以識別 ISMS 範圍內的資訊喪失哪些風險？

(A)機密性

(B)完整性

(C)可用性

(D)可靠性

Ans：ABC

36. 有關人員安全管理的管理者，未包括下列何種職責？

(A)激勵人員履行組織的資訊安全政策

(B)不能提供匿名舉報安全違反的管道

(C)擔當一個角色模範

(D)遵守任用的條款與條件

Ans：B

37. 有關資訊安全組織，下列敘述何者不正確？

(A)應明確界定相關人員之資訊安全責任

(B)資安協調工作宜納入資訊人員及管理者

(C)新的資訊處理設施必須經過管理人員授權

(D)具有已配置安全責任之個人，不可將安全任務委派給其他人

Ans：D

38. 電腦教室藉由刷卡管制門禁，此類型之安全措施屬於何者？

(A)矯正措施

(B)實體措施

(C)邏輯措施

(D)預防措施

Ans：B

39. 金鑰管理包括金鑰之下列哪些？

(A)歸檔

(B)分送

(C)銷毀

(D)汰換

Ans：ABCD

40. 何項不是風險分析的主要目標之一？

(A)識別資產及其價值

(B)實施反制措施

(C)建立事故成本與安全措施成本之間的平衡

(D)確定相關脆弱性與威脅

Ans：B