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：SK101

【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. 如果要將含有機密資料的設備汰換掉時，請問其中的舊硬碟應如何處置較為合適？

(A) 連續 5 次執行 Windows 7 的格式化工具
(B) 利用最高級的硬碟加密技術加密後，送資源回收處理
(C) 使其潮濕後產生銹蝕
(D) 用特殊機器絞碎

Ans：D

2. 組織必須要有能力針對其各項安全要求進行辨識，各項安全要求有三個主要來源，下列何者為正確的組合？

(A) 人、程序、科技
(B) 風險評鑑、組織（包括交易夥伴、承包商等）的法律契約的要求、組織的目標及營運要求
(C) 高階主管的要求、法律規定、人的自我約束
(D) 科技的限制、組織的成長、內控的強化

Ans：B

3. 某公司的主要伺服器遭受電腦病毒攻擊，造成運作中斷，依資訊資產的價值、弱點、威脅及風險的相對應關係來看，下列敘述何者有誤？

(A) 伺服器上的防毒程式未定期更新是弱點
(B) 電腦病毒是威脅
(C) 電腦病毒是風險
(D) 伺服器本身具有價值

Ans：C

4. 為確保資安風險的改善能持續進行，組織必須要實施合理的風險量測機制，用量測工具來針對量測項目作目標水準的評估，以作為管理的依據。下列的量測工具及量測項目的對應，何者有誤？

(A) 工具：訓練記錄；項目：人員安全管理與教育訓練
(B) 工具：事件記錄；項目：連外網路斷線次數
(C) 工具：管理審查會記錄；項目：業務永續運作管理
(D) 工具：事件通報單；項目：資訊安全事件之處理

Ans：C

5. 請參閱附圖作答：

電源的供應目的在於支援重要營運作業設備，而使運作不中斷，
其所使用的措施有下列幾種不同的選擇：
1. 不斷電系統（UPS）
2. 備援發電機
3. 獨立的小發電站
請問下列敘述何者正確？

(A) 若長時間停電而業務需要持續時，宜考慮不斷電系統（UPS）
(B) 建議使用備援發電機以支援正常關機或持續運作
(C) 不斷電系統與備援發電機宜定期檢查以確保有充分的容量
(D) 不斷電系統在平時應關閉電源，以備不時之需

Ans：C

6. 資產分類的目的在於該資產在被處置時，組織可以掌握下列哪些？

(A) 資產的市場可流動性
(B) 保護措施的必要與否
(C) 資源投入的優先順序
(D) 保護等級的適切與否

Ans：BCD

7. 為確保資訊安全政策持續的適當性、充分性、及有效性，應於下列何時進行政策的審查為最佳？

(A) 每五年一次
(B) 更換承包商
(C) 公司的組織及業務有重大變更
(D) 公司面臨外部稽核

Ans：C

8. ”個人資料保護法”第六條所定義的特種資料，除依規定外，雖經當事人同意，亦不得蒐集、處理或利用。請問下列何者不屬於特種資料？

(A) 基因
(B) 性特徵
(C) 犯罪前科
(D) 健康檢查

Ans：B

9. 防止資訊處理設施被誤用的控制措施，主要目的在制止使用者未經授權而使用資訊處理設施。在實作上應注意下列哪些？

(A) 管理階層宜核准資訊處理設施的使用
(B) 所有使用者宜認知其被允許的確切存取範圍
(C) 執行監控程序前宜徵詢法律建議
(D) 授權使用者使用資訊處理設施，可以書面、口頭的方式進行

Ans：ABC

10. 為確保「業務持續性管理」的有效性，以下哪一作為應該加以避免？

(A) 應分析各種災難、安全缺失和損失服務對業務所可能產生的後果，並用保險方式移轉部份風險
(B) 全組織持續營運措施之制訂與維護作業，有明確管理之過程
(C) 業務持續運作的測試應以未預警的方式施行，才可得知規劃的有效與否
(D) 應維持單一營運持續計畫之框架，避免混淆

Ans：C

11. 在與承包商訂定合約時，關於資訊安全方面的要求，必須注意到承包商對組織內部的資訊及資訊處理設施存取的形式，下列何者並非最佳的控制方式？

(A) 規劃稽核的時點及方式
(B) 承包商必須要於現場（on-site）執行所有工作
(C) 限定連線及資料的方式，並採取必要控制措施
(D) 進入管制區域須有人陪同

Ans：B

12. 王大明擔任組織內資訊安全委員會的召集人一職，在規劃資訊安全協調人員時，除了相關角色與工作功能不同部門的代表外，尚有具備特殊領域的專業代表，這些代表的專業背景最好應包括下列哪些？

(A) 保險、法律
(B) 資訊技術
(C) 人力資源
(D) 風險管理

Ans：ABCD

13. 使用者對於系統的不當操作及對於系統、資料庫的非法存取或破壞，發生的原因經常為下列何者？

(A) 未對員工做正確的教育訓練及權限控管不當
(B) 外在環境的誘惑
(C) 政策制訂的不當
(D) 預算不足

Ans：A

14. 在資訊安全管理的實務中，定義資產的所有人之目的在於何者？

(A) 只有所有人才負有資產保護的權責
(B) 識別所有資產的所有人，並指派維護該資產適切控制措施的責任
(C) 保險理賠上的要求
(D) 財務管理上的要求

Ans：B

15. 請參閱附圖作答：

控制的類型主要可分成偵查性控制（detective controls）、預防性控制（preventive controls）、矯正性控制（corrective controls）。下列敘述哪些正確？
1. 定期的員工資安認知教育訓練為矯正性控制
2. 機房的偵煙器為預防性控制
3. 大門警衛具有偵查性控制、預防性控制及矯正性控制三種特性
4. 矯正性控制用來矯正偵查性控制所發現之異常

(A) 34
(B) 24
(C) 13
(D) 234

Ans：A

16. 某一組織要在內部成立跨部門的風險評鑑小組，但在成員的安排上傷透腦筋，請問下列的成員組合何者為最佳？

(A) 主要業務部門、IT 部門、公司管理階層
(B) 風險管理部門、稽核部門、人事部門
(C) IT 部門、風管部門
(D) 主要業務部門、公司管理階層

Ans：A

17. 某公司的主機房發生電源供應中斷的情形，雖欲啓動備援電力設備，但因總供電量有限，所以必須針對下列的設備或設施做出恢復供電的優先順序，請問下列何者應先優先考量？

(A) 主要伺服器
(B) 門禁系統
(C) 空調系統
(D) 照明設備

Ans：D

18. 風險處理（改善）計畫的建構，目的在於識別適當管理措施、資源、責任及優先順序以降低風險，在實作時必須要能確保下列哪些？

(A) 有效改善資產管理上的弱點
(B) 利用保險方式以避免風險
(C) 資產本身的價值不得高於投入風險改善的成本
(D) 避免資產的弱點為威脅所利用

Ans：AD

19. 請參閱附圖作答：

資訊系統稽核工具應有適切的保護措施及儲存位置，下列哪些為合適的儲存位置？
1. 開發區
2. 運作區
3. 測試區
4. 防火牆
5. 一般使用者電腦
6. 稽核人員電腦並有額外保護

(A) 1, 3, 4
(B) 3, 6
(C) 4, 6
(D) 6

Ans：D

20. 傳送資料或支援資訊服務之電源與電信纜線應予以保護，以防止竊聽或損害，纜線安全宜考慮下列指導綱要，何者敘述為非？

(A) 電源線應置於牆內，網路線應置於牆外
(B) 電源纜線宜與通訊纜線分隔
(C) 如果可能，接入資訊處理設施的電源與電信線路宜設於地下
(D) 宜使用清楚可識別的纜線與設備標示，以儘量減少處理錯誤

Ans：A

21. 當員工有違反資訊安全的具體行為,組織開始懲處過程時,下列敘述何者有誤？

(A) 確保違反的員工受到公平公正的對待
(B) 懲處可用以嚇阻其他員工
(C) 考量對組織的影響，情節重大時，應即刻解除其職務
(D) 為避免其他員工仿效，所有相關內容均不應公布

Ans：D

22. 資訊安全政策中必須簡要說明安全政策、原則、標準以及符合性要求，應包括下列哪些？

(A) 符合法令和合約的要求
(B) 安全教育要求及營運持續管理
(C) 系統安全設定的組態參數
(D) 違反安全政策的後果

Ans：ABD

23. 下列何者並非資訊安全組織設立的目標之一？

(A) 找出資料外洩事件的負責人員
(B) 核准資訊安全政策、指派安全角色及協調與審查全組織安全措施的實作
(C) 建立資訊安全專家建議的管道，供整個組織使用
(D) 發展與包括有關當局等外部安全專家或團體的聯繫，以跟上業界趨勢、監控標準與評鑑方法

Ans：A

24. 風險分析方法大致可區分成定量（Quantitative）與定性（Qualitative）兩種風險分析方法。請問下列敘述何者正確？

(A) 定性風險分析方法是指，以計量方式並使用實際的數據來描述影響
(B) 定量風險分析方法是指，使用文字的形式或是敘述性的分類等級來描述可能影響的程度，以及影響發生的機率
(C) “人員的死亡、重傷及輕傷會分別對組織產生非常嚴重、嚴重及輕微的衝擊”，此為定性風險分析的陳述
(D) 定性與定量這兩種方法不可同時使用

Ans：C

25. 風險控管的方式有避免、轉移、降低及接受四種方式，從組織投入控管的成本角度來分析，一般來說成本最高及最低者分別為何？

(A) 降低、接受
(B) 避免、接受
(C) 避免、轉移
(D) 轉移、接受

Ans：B

26. 下列哪幾種執行記錄可作為量測組織是否針對資訊資產定期作風險評鑑的積極證據？

(A) 管理審查會議記錄
(B) 資安政策修訂記錄
(C) 資產威脅及弱點評估表
(D) 資訊資產清單

Ans：CD

27. 企業要能夠永續經營，須針對資料的可用性做完善的規劃，除了基本的備份之外，異地備援也是重要的一環。在規劃時務須先評估兩項指標－RPO（Recovery point objective）以及 RTO（Recovery time objective）。請問下列敘述哪些正確？

(A) RPO 指的是當災難發生時，企業能夠接受資料遺失的多寡
(B) 需要愈少時間的 RPO 代表所需花費在異地備援的成本愈低
(C) RTO 指的是當災難發生時，將資料完全復原所需花費的時間
(D) 需要愈少時間的 RTO 代表所需花費在異地備援的成本愈高

Ans：ACD

28. 請參閱附圖作答：

資產的型式有許多種，大致分類為：
1. 資訊
2. 軟體資產
3. 實體資產
4. 服務
5. 人員
6. 無形資產
其中，公用程式、自來水、USB 隨身碟、客戶服務專員，依序分別是屬於上列哪些類別？

(A) 1、2、4、5
(B) 2、4、3、5
(C) 2、3、6、5
(D) 2、2、4、5

Ans：B

29. 請參閱附圖作答：

王大明被要求為公司的主要機房門口製作一個標示，標示的內容如下：
第一行：XXX 公司之主機房
第二行：此為管制區域
第三行：非授權人員不得擅入
第四行：亦不得飲食及吸煙
請問若身為資訊安全從業人員，應建議移除上述哪一行字？

(A) 第一行
(B) 第二行
(C) 第三行
(D) 第四行

Ans：A

30. 下列關於資訊安全政策的敘述，哪些正確？

(A) 是管理階層針對資訊安全的承諾及意向聲明
(B) 為內部使用，不得公開
(C) 等同於外部法令的位階
(D) 用以設定各項控制目標與控制措施的框架

Ans：AD

31. 資訊安全往往經由實作一組適當的控制措施來達成，下列何者並非為控制措施之一？

(A) 政策
(B) 程序
(C) 業務目標
(D) 組織結構

Ans：C

32. 企業在導入雲端運算後，會增加資料保護上新的安全風險，請問下列何者屬於雲端科技對資訊安全所形成的新挑戰？

(A) 虛擬環境安全
(B) 系統中斷風險
(C) 身分認證
(D) 資料存取安全

Ans：A

33. 請參閱附圖作答：

關於資訊安全衝擊分析的描述，下列敘述哪些正確？
1. 發生機率為威脅利用弱點對資產造成影響的機率
2. 發生機率為弱點利用風險對資產造成影響的機率
3. 影響程度為風險利用弱點對資產造成影響的程度
4. 影響程度為威脅利用弱點對資產造成影響的程度

(A) 1234
(B) 24
(C) 14
(D) 123

Ans：C

34. 滲透測試（penetration testing）或弱點掃瞄，應該謹慎為之，該類行動可能引發系統安全的危害，為降低風險，應有下列哪些控制措施？

(A) 限由合格、經過授權的人員執行，或在其監督下執行
(B) 只能以手動方式執行，嚴禁使用任何自動化的工具協助
(C) 宜經規劃、文件化並可重覆
(D) 應於可控制的範圍內進行

Ans：ACD

35. 請參閱附圖作答：

下列是關於安全區域的敘述， 1. 安全區域必須完全由人員駐守來確保資訊及設施受到保護 2. 安全周界的界定要由承包商作完整的評估 3. 要先作風險評鑑 4. 建議在出入口安裝防盜及監控的設備 5. 依消防法規要求，不可對逃生門進行任何管制 請問上述哪些不正確？

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

Ans：D

36. 在針對員工或承包商作任用前的背景查證檢核時，應優先考量下列何者？

(A) 獨立的身分核對
(B) 查證應徵者學歷與專業資格
(C) 信用核對或犯罪紀錄核對
(D) 隱私權及相關法令

Ans：D

37. 請參閱附圖作答：

在授權承包商存取任何組織的資訊資產之前，必須要執行下列工作： (1) 針對承包商所派出人員的專業能力進行調查 (2) 制訂資訊資產一旦遭受破壞（例如遺失或毀損）時的處理程序 (3) 制訂資訊外洩時的通報調查程序 (4) 風險評鑑 請問上述何者應首先被執行？

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

Ans：D

38. 建置資訊安全管理系統之前，必須先決定其邊界（或範圍），下列何者為邊界（或範圍）最佳的選擇？

(A) 單一系統
(B) 實體設施
(C) 主要作業流程
(D) 作業人員

Ans：C

39. 請參閱附圖作答：

風險評鑑作業的循環包括下列工作，請依正確執行順序作排列：
1. 資安風險評鑑之行動
2. 資安風險評鑑之建置與實施
3. 規劃資安風險評鑑
4. 資安風險評鑑之檢查作業

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

Ans：D

40. 下列敘述何者不能確保「應用系統之安全」？

(A) 輸出入資料應進行格式及內容確認
(B) 為增進資料傳輸時之速度，降低系統反應時間，也避免因系統負荷過重而造成服務中斷，資料儘量使用明碼傳輸
(C) 對於有保護訊息內容完整性之安全要求的應用程式，應採用訊息鑑別機制
(D) 要有適當之稽核紀錄或活動日誌

Ans：B