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：ISK103

學科 100% （為單複選題，每題 2.5 分，共 100 分）

1. 關於近期的資訊安全管理趨勢與說明，下列哪些為是？**(複選)**
   （Ａ）APT，全寫為 Access Protection Technology，泛指一切用以保護存取軌跡紀錄的資訊技術
   （Ｂ）DLP，全寫為 Data Loss Protection，泛指一切用以防堵組織重要資料外洩的套裝軟體或設備
   （Ｃ）BYOD，全寫為 Bring Your Own Device，指為回應員工以私有行動運算設備處理公務，所產生的資訊安全管理趨勢
   （Ｄ）Social Media，泛指具備社交功能的應用軟體或平台，例如：Twitter、Line、Skype、Facebook 等
   Ans：**BCD**
2. 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**
3. 在制定資訊安全政策時，應包括下列哪些事項？**(複選)**
   （Ａ）資訊安全之定義、目標及範圍
   （Ｂ）資料交換的通訊協定
   （Ｃ）訪客動線的安排
   （Ｄ）業務永續運作計畫
   Ans：**AD**

4. 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**

5. 下列何者為社交工程攻擊方式？
（Ａ）針對網站主機執行目標漏洞掃瞄
（Ｂ）利用電子郵件誘騙使用者開啓含有惡意程式之圖片
（Ｃ）利用網站已知弱點實作漏洞攻擊
（Ｄ）寄送大量電子郵件，以癱瘓攻擊目標郵件信箱
Ans：**B**

6. 關於日常作業應注意事項，下列敘述哪些正確？**(複選)**
（Ａ）帳號密碼不得寫在紙本資料上，而應以明碼方式置於電子檔案中，以利安全存取
（Ｂ）使用隨身碟前，應先掃毒，才可以安心使用
（Ｃ）休假期間，必須要將帳號密碼告知職務代理人，以利業務繼續推動，同時也落實代理人制度
（Ｄ）應定期掃描電腦病毒並更新病毒碼
Ans：**BD**

7. 下列關於人員聘雇安全的管理方式，哪些正確？**(複選)**
（Ａ）確認應徵者所宣稱的學經歷與資格
（Ｂ）為遵循個資法，不得要求應徵人員提供畢業證書
（Ｃ）電子郵件帳號應於人員報到前開通啓用
（Ｄ）新進同仁應施予資訊安全教育宣導
Ans：**AD**

8. 身為資訊資產的擁有者（Owner），下列管理責任中，最適合指派其他人代為執行的是？

（A）定義該資訊資產的保護要求

（B）執行每日檢核與維護作業

（C）核可存取或使用資訊資產的申請

（D）核可設備報廢申請

Ans：**B**

9. 下列哪些為導入風險改善措施後還剩下的風險？**(複選)**

（A）殘餘風險

（B）固有風險

（C）內部控制風險

（D）查核風險

Ans：**AB**

10. 在資訊安全管理的實務中，定義資產的擁有者（Owner）之目的在於下列何者？

（A）只有擁有者（Owner）才負有資產保護的權責

（B）識別所有資產的擁有者（Owner），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**

11. 下列哪些為資產價值的正確描述？**(複選)**

（A）不可否認性 - 避免資料未經授權之使用

（B）可用性 - 確保資料隨時皆可使用

（C）機密性 - 避免未經授權使用者有意或無意地揭露資料

（D）完整性 - 確保資料只能被所有人存取

Ans：**BC**

12. 下列哪一項非資訊風險管理系統導入範圍之範例？
（Ａ）一個 IT 應用系統
（Ｂ）一個企業品牌
（Ｃ）一項營運過程
（Ｄ）一項 IT 基礎建設
Ans：**B**

13. 關於有效性量測的敘述，下列哪些是錯誤的？**(複選)**
（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**

14. 下列何者為資訊安全實地查核時的詢問技巧？
（Ａ）營造緊張氣氛讓受查人員恐懼
（Ｂ）應先詢問與受查區域無關的問題，以混淆受查人員
（Ｃ）應使受查人員感到自在
（Ｄ）不論時間長短仍應堅持進行全範圍查核
Ans：**C**

15. 關於評估資訊安全風險的三大考量，以下何者有誤？
（Ａ）價值
（Ｂ）弱點
（Ｃ）威脅
（Ｄ）發生頻次
Ans：**D**

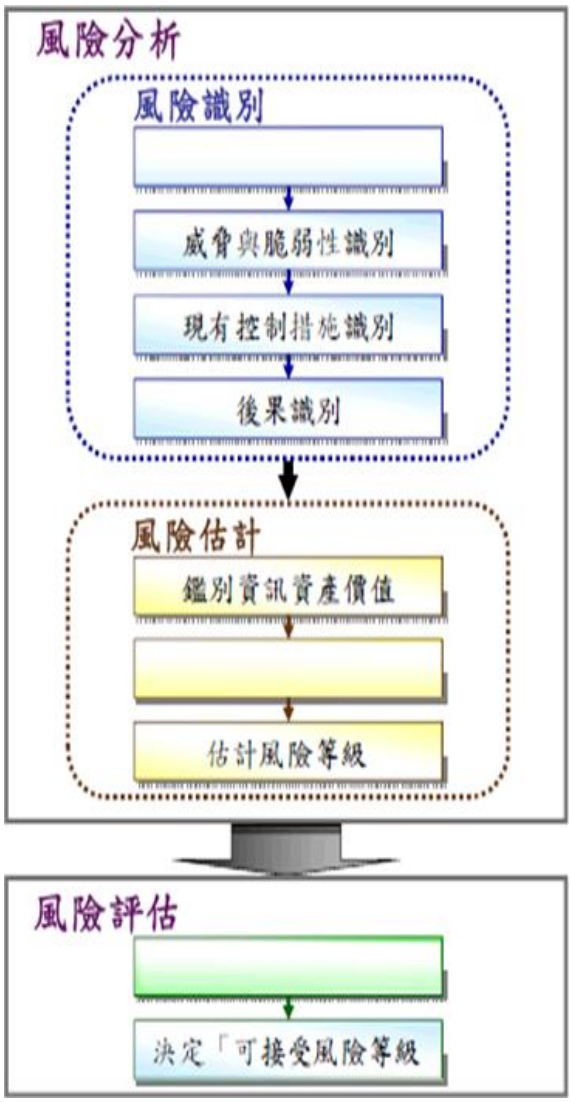
16. 下列為近期受矚目的資安議題，與其對應的處理方針進行配對，何者不適當？
（Ａ）雲端儲存 - 禁止同仁將資料傳輸至雲端資料夾
（Ｂ）社交工程攻擊 - 限制內部網路電腦，只能與公務相關的特定網站連線
（Ｃ）行動商務 - 通訊一律使用有線電話，禁用行動電話
（Ｄ）零時差攻擊 - 強化與資安組織聯繫，加速修復弱點
Ans：**C**

17. 下列何者為資安組織的最佳組成？
（Ａ）總經理、股東代表、資訊長
（Ｂ）總經理、資訊長、人資長、主要資安服務供應商
（Ｃ）總經理、各部門副主管、稽核人員
（Ｄ）獨立監事、財務長、資訊長、資安設備管理人員
Ans：**C**

18. 有關威脅性與脆弱性之描述，下列何者正確？
（Ａ）識別威脅性與脆弱性主要是為了鑑別資訊資產在使用或處理過程中，各項威脅運用於資訊資產脆弱性對「機密性」、「完整性」及「可用性」造成之衝擊
（Ｂ）威脅會因為自然災害而產生風險
（Ｃ）威脅性主要為評估管理防護機制是否完備
（Ｄ）弱點能利用威脅對組織造成衝擊
Ans：**A**

19. 當定義資訊安全風險管理範圍與邊界時，下列哪一項目非最優先考量的重點？
（Ａ）組織之資訊安全政策
（Ｂ）相關利害關係者之期望
（Ｃ）資訊資產價值
（Ｄ）作業之方便性
Ans：**D**

20. 請將以下三個作業活動，依序正確填入附圖中的空格部份：(1) 評鑑事故可能性，(2) 資產識別，(3) 訂定風險等級。（請參閱附圖作答）



（A）(2)-(1)-(3)

（B）(3)-(1)-(2)

（C）(1)-(2)-(3)

（D）(3)-(2)-(1)

Ans：**A**

21. 在風險處理與控制措施進行過程中，下列敘述哪些有誤？**(複選)**

（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**

22. 經風險評鑑及內部稽核後，發現組織未針對單位內的人事調整訂定權限，及流程檢核機制，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的資料取走，故組織增加了組內人員異動時權限檢核機制，是以下列哪個量測方式來量測此控制措施的有效性最佳？

（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**

23. 下列何者屬於資訊安全的威脅性事項？

（Ａ）離開工作站時，未登出

（Ｂ）電信設備故障

（Ｃ）不良的通行碼管理

（Ｄ）錯誤的存取權限分配

Ans：**B**

24. 下列關於資訊資產管理的敘述，何者最不適當？

（Ａ）建立資訊資產管理規範，主要目的是確保資訊資產受到良好保護

（Ｂ）定義資訊資產擁有者（Owner），主要目的是明訂管理權責及資產價值

（Ｃ）資訊分類（Classification）主要目的是對其實施合理的管控強度

（Ｄ）資訊資產標示（Labeling）主要目的是確保資產不會被外部駭客攻擊

Ans：**D**

25. 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？**(複選)**

（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

（Ｄ）應於可控制的範圍內進行

Ans：**ACD**

26. 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**

27. 下列哪一項不是營運衝擊分析階段應了解的項目？

（Ａ）範圍內有哪些業務流程

（Ｂ）重要業務流程復原時間的要求

（Ｃ）重要業務流程會對應的資源項目

（Ｄ）計畫的演練與實施的落實

Ans：**D**

28. 下列關於資訊安全組織的敘述，何者正確？

（Ａ）是管理階層對資訊安全的承諾

（Ｂ）要擔負起組織內未來資安滲透測試的重責大任

（Ｃ）工作上必須要獨立，不得同時兼任他職

（Ｄ）主要處理內部敏感事務，不應與組織外部人員有所聯繫

Ans：**A**

29. 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**

30. 在數種身份驗證的機制中，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**

31. 下列哪些為進行資訊安全查核的程序？**(複選)**
（A）查核規劃
（B）查核底稿製作
（C）實地查核
（D）人員懲處
Ans：**ABC**

32. 關於資訊安全營運持續計畫，下列敘述哪些有誤？**(複選)**
（A）推動營運持續管理體系應以 IT 單位前導，其他單位全力配合
（B）復原時間目標（RTO）應大於或等於最大可容忍中斷時間（MTPD）
（C）風險評鑑的目的，在於找出有哪些可能的事件會影響到關鍵資源，進而造成業務中斷
（D）營運衝擊分析與風險評鑑是了解與分析業務現況的核心步驟
Ans：**AB**

33. 關於辦公室環境安全注意事項，下列何者不正確？
（ A ）電腦應設置需密碼開啓之螢幕保護程式
（ B ）委外人員也應申請及佩戴工作證
（ C ）如需報廢設備，需遵循報廢程序及主管覆核
（ D ）已經處理過的機敏紙本文件可直接回收
Ans：**D**

34. 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**

35. 下列有關資訊安全查核基本觀念之敘述，下列何者有誤？
（ 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**

36. 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**

37. 下列關於資訊安全政策的敘述，何者有誤？
（ A ）資訊安全政策是組織與成員間一種權利義務關係的定義
（ B ）資訊安全政策只能以正式書面表達
（ C ）資訊安全政策是對人員的資安責任予以獎懲的重要依據
（ D ）資安政策最好可以公佈給組織內外的所有人都知道
Ans：**B**

38. 有關組織的人員資訊安全管理與說明，下列哪些有誤？**(複選)**

（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覈的繁複程序外，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：**ACD**

39. 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**

40. 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**