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：ISK108

學科 100% （為單複選題，每題 2.5 分，共 100 分）

1.	「去識別化」(De-identification) 是個人資料保護安全措施近年來重要的發展方向之一，下列哪些為正確敘述？**【複選】** （A）兼顧開放分享資料與個人資料保護之間的平衡 （B）移除或模糊個人資料中任何可識別資訊 （C）讓違法搜集個人資料的企業無所遁形 （D）2017 年公布的 ISO25237，對去識別化提供了適當的標準與規範
Ans：ABD	
2.	歐盟於 2016 年通過一個隱私保護法規，預計於 2018 年上路，屆時凡是需要蒐集、處理及儲存歐盟人民個人資料的企業機構，若違犯該法規將可能被處以該公司全球營收的 4% 罰鍰。該法的出現迫使企業必須重新檢討資料處理流程以期能符合新的規範。這個法規為何？ （A）PIPA（Personal Information Protection Act） （B）PPA（Personal Privacy Act） （C）CBR（Cross Border Regulation） （D）GDPR（General Data Protection Regulation）
Ans：D	

3.	為確保資訊安全政策持續適當及有效，應定期或適時進行政策的審查，下列何者最為正確？ (A) 外部稽核開出缺失時 (B) 每三年一次 (C) 組織或業務重大變更時 (D) 公司上市時
Ans：C	
4.	機密資料在傳遞的過程當中，為避免被有心人士攔截竊取，通常採用加密的保護措施，以避免機密資料外洩。請問下列何者為正確的敘述？ (A) 機密資料外洩是資料先天性的弱點所造成，與外在威脅無關 (B) 機密資料外洩是外在威脅利用資產弱點所造成的風險 (C) 加密是在增加資訊資產的流通價值 (D) 加密可以完全排除資料傳遞時外在威脅
Ans：B	
5.	關於資訊安全政策，下列何者敘述有誤？ (A) 必須要有管理高層的支持 (B) 發佈的範圍要包含合作廠商 (C) 組織有重大變更時要進行調整 (D) 只規範公司高層與資訊安全人員之行為
Ans：D	
6.	資訊資產價值的評鑑應該包含下列哪一項面向的組合？ (A) 機密性及可靠性 (B) 完整性及不可否定性 (C) 機密性、可用性及完整性 (D) 可用性及財務性
Ans：C	

7.	下列何項敘述不是定量風險分析方法的特性？ （A）欲被保護的資產之價值是可被精確評估出來的 （B）以「情境可能發生的機率」與「可能造成的衝擊」為其主要的考量面向 （C）可估算在某個特定的威脅，因為沒有實施安全控制的年損失期望額（annualized loss expectancy）是多少 （D）可根據成本效益原則，來決定要不要投入資源去保護資產
Ans：B	
8.	某資料中心正在執行資安稽核，這時火災警報器突然無預警響起，此時在現場的所有人員應如何反應較為正確？ （A）應立即關閉主要電源，以避免設備損毀 （B）應迅速備份所有重要資料 （C）所有人應迅速撤離資料中心，以避免傷亡 （D）由於稽核範圍包括災難復原，所以應該開始觀察資料中心員工對警報的反應情況
Ans：C	
9.	針對資訊安全的三個要素，下列何者並非正確的敘述？ （A）機密性：適當保護資訊資產，確保資訊資產不會未經授權被使用 （B）完整性：維持資訊資產內容的正確與完整 （C）可用性：確保資訊資產能隨時提供使用 （D）企業之電腦機房使用 UPS（Uninterruptible Power Supply）的主要目的是為符合機密性的要求
Ans：D	
10.	公司資料庫管理人員的一台筆記型電腦被盜，其中包含資料庫密碼檔案，該公司應該採取下列那些措施以降低資安風險? **【複選】** （A）啟動應變程序，通報相關人員 （B）全面停用資料庫以避免風險擴大 （C）更改資料庫密碼 （D）全面檢討行動裝置及可攜式資訊設備的安全管理措施
Ans：ACD	

11.	關於資訊安全組織的權責區分，下列敘述何者不正確？ (A) 資訊作業主管：負責資訊安全政策的推行及實施 (B) 最高主管：核准資訊安全政策 (C) 資訊安全長：為資安的推行之總舵手 (D) 全體員工：均要遵守各項資安政策、程序與作業要求
Ans：A	
12.	有些風險因為過低但實施的成本過高，組織在評估後，選擇進行監控而未實施相對應的控制，這種風險稱之為何？ (A) 先天風險 (B) 剩餘風險 (C) 機會風險 (D) 成本風險
Ans：B	
13.	資訊安全管理的目的主要是為下列何項？ (A) 防止人員進行財務舞弊 (B) 強化對資訊資產之保護，包含資料、系統與相關設施 (C) 希望能招募到志同道合的未來工作夥伴 (D) 有利資訊資產的活化及流通
Ans：B	
14.	下列何者並不是具體的人員安全管理措施？ (A) 代理人制度 (B) 人員輪調 (C) 職務區隔 (D) 考勤管理
Ans：D	
15.	關於資訊資產清單的覆核，下列敘述何者不正確？ (A) 只能交由有權限的資訊長來執行 (B) 系統有重大異動時必須執行 (C) 為確保資訊資產清單的正確性及完整性 (D) 作業環境改變時必須執行
Ans：A	

16. 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

17. 下列哪些為資訊安全政策所應規範的範疇？**【複選】**
(A) 委外的辦公室區域清潔人員
(B) 全體員工
(C) 工讀生
(D) 往來廠商

Ans：ABCD

18. 下列哪些為「風險處理的作法」？**【複選】**
(A) 接受風險
(B) 轉移風險
(C) 迴避風險
(D) 放任風險

Ans：ABC

19. 關於資訊資產的價值、弱點及威脅的對應關係，下列何者為正確的敘述？
(A) 威脅與弱點的增加與資訊安全風險的增加是兩回事
(B) 資訊資產具有價值，並會受到資本市場波動的潛在影響
(C) 組織通過實施安全控制防範威脅，以降低資安的投入人力
(D) 威脅利用弱點對資訊資產造成影響

Ans：D

20. 資訊安全風險管理流程中，「建立全景」的目的為下列何者？
(A) 瞭解組織及其全景、瞭解關注方之需要及期望、決定資訊安全管理系統之範圍及資訊安全管理系統
(B) 盤點資訊資產清單
(C) 分析資訊資產的風險
(D) 建立安全管理整體計畫

Ans：A

21.	資安稽核人員在進行稽核時，發現檔案伺服器並未安裝最新的安全漏洞修補程式，請問此稽核人員下一步該如何處理較為正確？ （A）建議系統管理人員安裝安全漏洞修補程式 （B）先開出口頭建議，並要求期限內改善。若未改善，則開立書面缺失，並定期監控改善進度 （C）審查修補程式管理政策，並確認與這種情況有關的風險 （D）建議系統管理人員安裝安全漏洞修補程式後進行測試
Ans：C	
22.	組織應依規劃之期間施行內部稽核，以提供資訊安全管理系統之何者資訊？ （A）組織本身對其資訊安全管理系統之要求事項 （B）風險評鑑報告 （C）CNS27001 標準之要求事項 （D）是否有效實作及維持
Ans：B	
23.	關於營運持續管理之資訊安全層面，組織應考量多重備援之議題，CNS27001 附錄 A.17 標準中有何項控制措施？ （A）資訊處理設施之可用性 （B）規劃資訊安全持續 （C）實作資訊安全持續 （D）查證、審查並評估資訊安全持續
Ans：A	
24.	資訊安全風險等級評估的主要目的是在於？ （A）決定資訊資產的權責單位 （B）決定資訊資產的損失可能性 （C）訂定風險等級及決定可接受風險等級 （D）訂定數位證據的證據搜集原則
Ans：C	

25.	資訊安全管理系統（ISMS）使用之 PDCA 循環，其中 PDCA 循環是指下列何者？ （A）準備 - 執行 - 檢查 - 稽核 （B）準備 - 執行 - 檢查 - 行動 （C）計劃 - 執行 - 檢查 - 稽核 （D）計劃 - 執行 - 檢查 - 行動
Ans：D	
26.	關於資訊資產的權責單位（Owner），下列哪些是正確的定義？**【複選】** （A）僅有保管及使用的權利 （B）對資訊資產具有實質的財產權 （C）由組織指定的資訊資產擁有單位 （D）負責資訊資產的生產、發展、維護、使用及安全
Ans：CD	
27.	下列何者為風險評鑑（Risk Assessment）的定義？ （A）把預估的風險與已知的風險進行比較的過程 （B）藉由協調各項活動以控管組織相關風險 （C）選擇與實施控制措施以修正風險的過程 （D）風險分析與風險評估的整體過程
Ans：D	
28.	組織的災難復原計畫（DRP）中包含互惠協議時，是採用了以下哪一項風險對應方法？ （A）轉移（Transfer risk） （B）緩解（Control/Mitigate risk） （C）規避（Avoid risk） （D）接受（Accept risk）
Ans：B	
29.	針對機房範圍購買火災險，係屬於下列何種風險處理控制措施？ （A）接受風險 （B）轉移風險 （C）迴避風險 （D）控制風險
Ans：B	

30.	請問企業之電腦機房使用 UPS (Uninterruptible Power Supply) 的主要功能為何？ (A) 消除靜電 (B) 防止電源瞬間中斷 (C) 傳送資料 (D) 備份資料
Ans：B	
31.	在定義及應用資訊安全風險評鑑時，組織應建立及維持下列哪些資訊安全風險準則？**【複選】** (A) 誠信倫理準則 (B) 風險接受準則 (C) 履行資訊安全風險評鑑之準則 (D) 最小化準則
Ans：BC	
32.	下列何者不屬於資訊安全業務持續計畫的管理範疇？ (A) 機房備用電力規劃 (B) 備援中心的選擇 (C) 資料備份方式 (D) 程式開發測試流程
Ans：D	
33.	公司內部辦理一場資訊安教育訓練，主題是”資安事件之緊急應變”，請問下列何者不適合到場聆聽？ (A) 資安人員 (B) 一般人員 (C) 稽核人員 (D) 資安官
Ans：B	

34. 請問下列何者是不正確的資訊安全「保護措施」措施？
(A) 定期備份資料庫
(B) 機密檔案由專人保管
(C) 留下重要資料的使用記錄
(D) 資料檔案與備份檔案保存在同一磁碟機

Ans：D

35. 電腦教室藉由刷卡管制門禁，此類型之安全措施屬於？
(A) 矯正措施
(B) 實體措施
(C) 邏輯措施
(D) 預防措施

Ans：B

36. 下列何者可作為量測資訊安全「完整性」之指標？
(A) 確保關鍵服務之達成率
(B) 確保教育訓練之達成率
(C) 網頁資訊公開正確性之達成率
(D) 確保人員知悉之達成率

Ans：C

37. 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

38.	最高主管在資安組織的權責區分下，具有下列哪些主要職責？**【複選】** （A）核准並發佈資訊安全政策 （B）審核各級資安相關文件，並適時實地稽核 （C）遵守並力行各項資安要求 （D）檢視稽核軌跡
Ans：AC	
39.	風險有四種處理方式，下列哪些為正確敘述？**【複選】** （A）降低：建置「正確且適當的」安全防護措施，降低潛在風險 （B）接受：如果因某些不必要的活動而導致風險產生時，組織考慮停掉相關活動 （C）避免：無法處理的風險或者影響很小的風險，組織可選擇不處理 （D）轉移：透過保險的機制，將風險轉嫁給保險公司，一旦風險產生時，可有補償的機制降低損失
Ans：AD	
40.	下列哪些為識別資訊安全風險的目的？**【複選】** （A）識別可能的財務損失 （B）應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內與漏失資訊之機密性、完整性及可用性相關聯之風險 （C）識別風險擁有者 （D）識別具有合作潛力的協力廠商
Ans：BC	