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：ISK-110

【注意事項】

一、本測驗為單面印刷試題，共計 12 頁。第 2 至 12 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）

001. 時間校正發生錯誤，應加強哪一項控制措施？

(A)事件存錄

(B)日誌資訊之保護

(C)管理者及操作者日誌

(D)鐘訊同步

Ans：D

002. 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

003. 建立資訊安全管理機制的最主要目的是：

(A)降低組織在資訊安全的風險

(B)符合法令或法規的要求

(C)通過 ISO 27001 的驗證

(D)防止駭客入侵

Ans：A

004. 下列何者最適合作為量測資安事件應變（Incident Response）的風險指標？
(A)資安事件在規定的時間內完成通報的比率
(B)資安事件發生的數量
(C)資安人員完成年度資安教育訓練的比率
(D)未經授權的遠端存取次數

Ans：A

005. 制定資訊安全管理政策時應考量以下哪些事項？**(複選)**
(A)營運的要求
(B)法令或法規的要求
(C)是否需要設置入侵偵測設備
(D)防火牆的設定

Ans：AB

006. 有關資通安全管理法的敘述何者正確？
(A)資通安全管理法納管對象包含公務機關及所有非公務機關
(B)公務機關可視組織規模及業務屬性決定是否設置資通安全長
(C)C 級機關的資通系統檢測目前以 IT 設備為主，OT 設備不必納入
(D)委外開發之資通系統如屬委託機關之核心資通系統，或委託案件金額在 1,000 萬元以上，委託機關應自行或另行委託第三方進行安全性檢測。

Ans：D

007. 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

008. 有關稽核的敘述，以下何者有誤？
(A)稽核的準則應包含組織資訊安全標準的內容
(B)內部稽核時所紀錄、蒐集的資料應該在稽核完成後立即銷毀
(C)稽核時應確認資訊安全管理系統是否有效實作
(D)組織應建立資訊安全稽核計畫

Ans：B

009. 資訊安全除應考慮保存資訊的機密性、完整性及可用性；此外，亦能涉及以下哪些性質？**(複選)**
(A)鑑別性
(B)可歸責性
(C)不可否認性
(D)可靠度

Ans：ABCD

010. 營運衝擊分析（Business Impact Analysis）最主要的用途是？
(A)取得認證
(B)找出那些軟體系統有需要進行修補的弱點
(C)決定採用哪種備份機制
(D)鑑別用以支援產品與服務供應的活動

Ans：D

011. 資訊安全政策文件應公布傳達給所有員工與相關各外部團體，其最主要的目的是：
(A)讓抗拒的員工更願意接受管理
(B)降低資訊安全最弱一環的風險
(C)通過 ISO 27001 驗證
(D)符合法令或法規對資訊安全的要求

Ans：B

012. 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

013. 組織應依據營運、組織所在位置、資產及技術等特性，界定 ISMS 政策，該政策應該由哪個職務核決，請由選項中找出最適當的答案？
(A)法務長
(B)總經理
(C)資安長
(D)資訊長

Ans：B

014. 以下哪些內容較適合放在一般層面的資訊安全教育訓練中？**(複選)**
(A)聲明管理階層對全組織資訊安全之承諾
(B)個人之作為及不作為的個人可歸責性
(C)惡意軟體控制措施
(D)通行碼安全

Ans：ABCD

015. 減少重要資訊資產暴露在外是一種有效降低風險的方法，主要是因為降低了：
(A)被攻擊成功後產生的損失
(B)被攻擊的機會
(C)弱點
(D)需要復原的時間

Ans：B

016. 資料的機密等級應該由誰來決定最恰當？

(A)資訊長（CIO）

(B)資安長（CISO）

(C)資料的保管者（Data Custodian）

(D)資料的擁有者（Data Owner）

Ans：D

017. 以下人員哪一位最適合擔任資訊安全管理委員會的委員？

(A)系統分析師

(B)採購人員

(C)風險管理部門主管

(D)網路管理員

Ans：C

018. 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

019. 以下哪些有關雲端服務的敘述為真？**(複選)**

(A)當組織使用雲端的 IaaS（Infrastructure as a Service）時，硬體設備及場地環境的安全由雲服務供應商提供

(B)當發生資安事件時雲服務提供者必須承擔最終的責任

(C)雲端服務的可用性一般而言低於組織自己系統的可用性

(D)當組織使用雲端的 SaaS（Software as a Service）時，虛擬平台的安全由雲服務供應商提供

Ans：AD

020. 下列何者最適合作為量測資訊安全「可用性」之風險指標？
(A)防火牆檔下的連線次數
(B)網站內容未經授權被修改的次數
(C)非計劃內的服務中斷累計時數
(D)防毒軟體部署成功的百分比

Ans：C

021. 以下哪些是資訊安全風險管理的範疇？**(複選)**
(A)人員
(B)技術
(C)流程
(D)委外廠商

Ans：ABCD

022. 以下哪一項工具或技術不適合用來找出威脅及弱點？
(A)腦力激盪
(B)查檢表
(C)企業衝擊分析（BIA）
(D)蒙地卡羅模擬

Ans：D

023. 資訊資產在進行分級時主要考量以下哪個因素？
(A)重要性及機敏性
(B)風險發生的機率及衝擊程度
(C)資訊資產的建置成本
(D)威脅

Ans：A

024. 組織應決定資訊安全管理系統之邊界及適用性，以建立其範圍。於決定範圍時，應考量哪些事項？**(複選)**

(A)內部及外部議題

(B)關注方之需要及期望

(C)組織履行之活動與其他組織履行之活動間的介面及相依性

(D)範圍應以文件化資訊提供

Ans：ABCD

025. 於互連世界中，其營運、處置及保護所涉及之資訊及以下的哪些項目均屬資產，對組織之營運具價值？**(複選)**

(A)相關的過程

(B)系統

(C)網路

(D)人員

Ans：ABCD

026. 以下何者有關風險處理的描述有誤？

(A)當風險高於可接受風險水準時應進行處理

(B)可以透過購買個資險的方式避免產生風險

(C)風險進行處理後，應重新檢視殘餘風險

(D)接受風險是處理風險的選項之一

Ans：B

027. 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哪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

028. 有關風險評鑑的作法，以下敘述哪些有誤？**(複選)**

(A)風險評鑑應該一律以定量的方式進行

(B)進行定量分析時宜列出面臨之威脅與可能存在的脆弱性

(C)資訊資產的價值應該由系統管理者決定

(D)資訊資產的價值應考慮到機密性、完整性和可用性

Ans：AC

029. 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

030. 當進行營運衝擊分析（Business Impact Analysis）時，首先應考慮以下哪個選項？

(A)重建資訊系統的成本

(B)備援場地的地點及成本

(C)災害復原團隊的人員配置及職責

(D)若系統無法提供服務時每天將造成的損失

Ans：D

031. 以下哪些選項屬於資訊安全的威脅？**(複選)**

(A)資訊安全人員專業能力不足

(B)DDOS 攻擊

(C)APT

(D)啟動不必要的服務

Ans：BC

032. 以下哪種方式可以及時、有效的發現組織內部跟技術無關的資安違規事項，請選出最佳選項？

(A)定期的由第三方執行事件紀錄稽核作業

(B)建立組織內部各類型通報管道

(C)建議自動化資訊安全合規監控系統

(D)在組織內建立意見箱

Ans：B

033. 有關實體安全的控管，以下的描述何者有誤？

(A)機房出入口應設置門禁系統、受監視並於火災時自動上鎖

(B)無人的保全區域，宜實體上鎖並定期檢查

(C)除非經授權，不宜允許使用拍製、錄影、錄音及其他紀錄設備

(D)裝卸區之進貨及出貨宜於實體上隔離

Ans：A

034. 機房宜使用以下哪些消防設施？**(複選)**

(A)乾粉滅火設備

(B)FM-200

(C)二氧化碳滅火設備

(D)自動灑水設備

Ans：BC

035. 根據行政院資通安全會報公布的資通系統風險評鑑參考指引，風險評鑑（Ri Assessment）可分成以下三個作業：1. 風險分析、2. 風險評量、3. 風險識別，三者的執行順序為何？

(A)1,2,3

(B)2,3,1

(C)3,1,2

(D)2,1,3

Ans：C

036. 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

037. 根據行政院公布的【資通安全責任等級分級辦法】，以下哪些敘述為真？**(複選)**

(A)【資通系統防護需求分級原則】的構面可分為機密性、完整性、可用性及法律遵循性

(B)根據【資通系統防護需求分級原則】，防護需求等級可分為高、中、低、普

(C)當發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。這類的資通系統的需求防護等級是中等。

(D)公立醫學中心的資通安全責任等級為 B 級

Ans：AC

038. 有關人力資源安全，以下哪一項敘述有誤？

(A)為確保員工及承包者瞭解其將承擔之責任，且適任其角色，在聘用前、聘用期間及聘用終止應進行控管

(B)因個人資料保護法相關規定，各類型組織對所有可能被聘任者所進行背景調查時，均不得要求應徵者提供「警察刑事紀錄證明書」

(C)對所有可能被聘任者所進行背景調查時，宜確認應徵者所宣稱之學歷及專業資格

(D)對所有可能被聘任者所進行背景調查時，宜進行獨立之身分查證(身分證、護照或類似證件)

Ans：B

039. 「衝突之職務及責任範圍應予以區隔，以降低組織資產 遭未經授權或非蓄意修改或誤用之機會。」前述為 CNS 27001 何項控制措施之要求？

(A)職務區隔

(B)資訊安全之角色及責任

(C)聘用條款及條件

(D)管理階層責任

Ans：A

040. 一般而言，控制措施可提供以下之一種或多種形式保護，包含矯正、消弭、預防、衝擊最小化、制止、偵測、復原、監視及認知。資安事件管理平台（Security information and event management）屬於哪一類控制措施？

(A)偵測

(B)認知

(C)復原

(D)矯正

Ans：A