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-109

【注意事項】

一、本測驗為單面印刷試題，共計 14 頁。第 2 至 14 頁為 40 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 分，共 100 分）

001. 資通安全管理法的主管機關為何？

(A)國家安全會議

(B)國家資通安全會報

(C)行政院

(D)國家安全局

Ans：C

002. 主管機關應衡酌公務機關及特定非公務機關業務下列哪些條件，訂定資通安全責任等級之分級？**(複選)**

(A)重要性與機敏性

(B)機關層級

(C)機關首長職等

(D)保有或處理之資訊種類、數量、性質、資通系統之規模及性質

Ans：ABD

003. 為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：

(A)資通安全管理法相關子法

(B)國家資通安全發展方案

(C)國家資通安全政策

(D)國家資通安全管理及技術規範

Ans：B

004. 公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。依據資通安全管理法，下列哪些機關不必訂定並實施資通安全維護計畫？**(複選)**

(A)台北市政府警察局

(B)三軍總醫院

(C)海洋委員會海岸巡防署

(D)國家安全局

Ans : BD

005. 公務機關應置資通安全長，負責推動及監督機關內資通安全相關事務。應由機關首長指派下列哪些人員擔任此一職務？**(複選)**

(A)資訊單位主管

(B)副首長

(C)適當人員兼任

(D)外聘資訊安全專家

Ans : BC

006. 各機關依資通安全管理法施行細則第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項，何者不正確？

(A)受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證

(B)受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗有資通安全專業證照或具有類似業務經驗之資通安全專業人員。之資通安全專業人員

(C)受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣二千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測

(D)受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施

Ans : C

007. 資通安全責任等級 A 級之公務機關應辦事項中，初次受核定或等級變更後一年內，需配置資通安全人員幾名？

(A)專責 1 人，兼任 3 人

(B)專責 2 人，兼任 2 人

(C)專責 4 人

(D)兼任 4 人

Ans : C

008. 資通安全責任等級 B 級之特定非公務機關應辦事項中，資通安全專責人員以外之資訊人員，下列哪些為應受課程、時數及頻率為何？**(複選)**

(A)每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練

(B)每人每三年至少接受六小時以上之資通安全專業課程訓練或資通安全職能訓練

(C)每年接受四小時以上之資通安全通識教育訓練

(D)每年接受三小時以上之資通安全通識教育訓練

Ans：AD

009. 公務機關就其所屬人員辦理業務涉及資通安全事項之獎懲，得 依「公務機關所屬人員資通安全事項獎懲辦法」之規定自行訂定獎懲基準。以下何種情形得予獎勵？

(A)辦理 A 級機關資通安全管理業務，符合資通安全責任等級分級辦法附表一應辦事項，沒有缺失

(B)主動發現零時差弱點，獲得 CVE 編號

(C)考取公務人員資安職能證照

(D)訂定年度資通安全維護計畫

Ans：B

010. 資通安全責任等級 A 級之公務機關應辦事項在下列哪些要件成立下，得採用危害國家資通安全產品？**(複選)**

(A)機關首長核可

(B)因業務需求且無其他替代方案

(C)全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置

(D)沒有任何例外可以購置

Ans：BC

011. 資通安全責任等級 A 級之特定非公務機關應辦事項中，每年需辦理至少 2 次的技術面項目有那些？

(A)網路架構檢視

(B)核心資通系統網站安全弱點檢測

(C)核心資通系統滲透測試

(D)網路惡意活動檢視

Ans：B

012. 在資通安全責任等級 B 級之公務機關應辦事項中，哪些項措施是 可以增強政府資訊資產脆弱性管理水準？**(複選)**

(A)防火牆

(B)防毒軟體

(C)政府組態基準

(D)系統滲透測試

Ans：CD

013. 公務及非公務機關針對全部核心系統需進行「業務務持續演練」的依據係在資通安全管理法及其相關子法中那一份法規中？

(A)資通安全管理法

(B)資通安全管理法施行細則

(C)資通安全責任等級分級辦法

(D)資通安全事件通報及應變辦法

Ans：C

014. 關於資訊安全業務持續計畫(BCP)，下列何者為正確？

(A)由資訊部門依服務能量決定最大可容忍中斷時間（MTPD）

(B)可以用營運持續演練腳本來取代 BCP

(C)BCP 的啟動時機，必需小於「最大可容忍中斷時間（MTPD）減去目標回復時間（RPO）

(D)資料回復目標點（RTO）是由業務單位單獨決定

Ans : C

015. 關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，應送下列何權責單位審查？

(A)董事會

(B)行政院資通安全處

(C)中央目的事業主管機關

(D)地方政府

Ans : C

016. 資通安全責任等級 A 級之特定非公務機關應辦事項中，初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，需於幾年內完成公正第三方驗證？

(A)1 年

(B)2 年

(C)3 年

(D)4 年

Ans : C

017. 在資通安全責任等級分級辦法附表+資通系統防護基準中，等級「高」者，在稽核與可歸責性中，除了滿足所有「普」及「中」等級外，應辦事項中，下列何者為非？

(A)應定期審查稽核事件

(B)應稽核資通系統管理者帳號所執行之各項功能。

(C)機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。

(D)系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。

Ans：B

018. ISO31000 的風險管理的核心與關鍵成功因素為下列何者？

(A)領導與承諾

(B)整合與設計

(C)建置

(D)評估與持續改善

Ans：A

019. 鑑別資訊及資通系統「機密性」、「完整性」及「可用性」資產價值，主要係依下列何準則？

(A)組織全景

(B)後果準則

(C)80 / 20 法則

(D)衝擊準則

Ans：B

020. 在詳細風險評鑑作法中，在風險識別階段的順序，以下列何者為先？

(A)後果識別

(B)威脅與脆弱性識別

(C)現有控制措施識別

(D)資產識別

Ans：D

021. CNS/ISO/IEC 27005 所描述之資安風險管理過程與「行政院風險管理與危機處理作業手冊」所陳述之管理架構，均源自於下列那一份國際標準？

(A)ISO 22301

(B)ISO 27001

(C)ISO 31000

(D)ISO 27701

Ans：C

022. 「資通安全責任等級分級辦法」所描述之「安全等級設定原則」，其所採用技術類似 ISO 31010 之企業衝擊分析，評鑑對於機關之衝擊程度，並未考量其發生之可能性(亦可視為衝擊發生是必然的)，以評定資通系統之安全等級，是下列何種風險評鑑作法？

(A)一般風險評鑑做法

(B)敏捷風險評鑑作法

(C)高階風險評鑑作法

(D)詳細風險評鑑作法

Ans：C

023. 全球資訊網由於廠商維護人員更動頻繁，經常安排經驗不足人員到場維護，依此情況識別出的威脅及脆弱性分別是？

(A)威脅：未授權存取(C)；脆弱性：身分與權限設定不當

(B)威脅：故障(A)；脆弱性：維護不當

(C)威脅：軟體異常或錯誤(I)；脆弱性：定期更新或升級

(D)威脅：未授權變更(竄改) (I)；脆弱性：缺乏監控與警示機制

Ans：B

024. 全球資訊網維護廠商由於廠商開發人員眾多，並非所有人均了解委外契約中有規範「廠商所交付程式碼，不得有惡意程式碼或高風險漏洞」，且所交付程式碼經源碼檢測後，程式碼經常含許多高風險漏洞與弱點，依上述情況識別出的威脅及脆弱性分別是？

(A)威脅：違反合約或協議(A)；脆弱性：未釐清委外協議的權責

(B)威脅：故障(A)；脆弱性：維護不當

(C)威脅：軟體異常或錯誤(I)；脆弱性：定期更新或升級

(D)威脅：未授權變更(竄改) (I)；脆弱性：未依照變更管理規範執行

Ans：A

025. 在計算風險值的公式中，下列那一項非計算因子？

(A)資訊及資通系統資產價值

(B)威脅發生可能性

(C)脆弱性利用難易度

(D)現有控制措施的強度

Ans：D

026. 下列哪些為「風險接受準則」考量因素？**(複選)**

(A)業務需求及目標

(B)資源分配狀況

(C)經費預算

(D)控制措施實施難易度

Ans：ABC

027. 依 CNS27005 風險決策點有 2 個點，第 1 個是在實施風險評鑑結果之後，第 2 個決策點是在哪一個時間點？

(A)擬訂風險處理計畫前

(B)擬訂風險處理計畫後

(C)執行風險處理計畫前

(D)執行風險處理計畫後

Ans：D

028. 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，於控制措施選擇期間，應權衡控制措施的哪些因素？**(複選)**

(A)高階主管的指示

(B)獲取、實作、行政管理、運作、監視及維護之成本

(C)基層操作人員的看法

(D)受保護之資產價值加以比較

Ans : BD

029. 因應法律、法令、規章及合約方面要求的改變，組織應對已經完成年度風險評鑑報告進行何種處理？

(A)原封不動

(B)明年再納入風險評估範圍

(C)進行風險評鑑變更

(D)重做風險評鑑

Ans : C

030. 在 ISO27701 隱私資訊管理制度，係基於下列哪些標準發展出來？**(複選)**

(A)ISO/IEC 27001

(B)ISO/IEC 27002

(C)ISO/IEC 29100

(D)ISO/IEC 27017

Ans : ABC

031. 瞭解關注方之需要及期望，組織應決定哪些事項？**(複選)**

(A)與資訊安全管理系統有關之關注各方

(B)關注方對資訊安全之要求事項

(C)關注方之要求事項可能包括法律及法規要求，以及契約義務

(D)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

Ans：ABC

032. 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

033. 「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

034. 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

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. 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

037. 定期辦理資訊設備報廢作業，係符合 CNS 27001 何項要求？

(A)資訊之分級

(B)資訊之標示

(C)資產之處置

(D)資產之歸還

Ans : C

038. 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

039. CNS27001 對「監督、量測、分析及評估」之要求，何者敘述有誤？

(A)需要監督及量測之事項，包括資訊安全過程及控制措施

(B)所選擇之方法不需產生適於比較及可重製視為有效之結果

(C)監督、量測、分析及評估之適用方法，以確保有效的結果

(D)執行監督及量測之時間及人員

Ans：B

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