108 年特種考試地方政府公務人員考試試題

等　　別：四等考試
類　　科：資訊處理
科　　目：資訊管理概要
考試時間：1 小時 30 分

一、隨著金融科技的發展，線上付款與線上銀行使用普及。若組織有提供客戶這類的服務，說明組織如何保護客戶資訊，避免個資外洩。（25 分）

【解題關鍵】
《考題難易》：★★★
《破題關鍵》本題以個人資料保護法施行細則授權各主管機關所訂之個人資料檔案安全維護辦法作答。

【擬答】：

根據金管會指定非公務機關個人資料檔案安全維護辦法，除要求相關非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法；依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入計畫及處理方法之範圍。評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管理機制。此外非公務機關提供電子商務服務系統，應採取下列資訊安全措施：

㈠使用者身分確認及保護機制。
㈡個人資料顯示之隱碼機制。
㈢網際網路傳輸之安全加密機制。
㈣應用系統於開發、上線、維護等各階段軟體驗證與確認程序。
㈤個人資料檔案及資料庫之存取控制與保護監控措施。
㈥防止外部網路入侵對策。
㈦非法或異常使用行為之監控與因應機制。

二、供應鏈攻擊是一種新興的威脅，一種以軟體開發人員和供應商（委外廠商）為目標，目的在於存取企業資訊系統或是內部資料。針對供應鏈攻擊之威脅，說明企業如何控管供應商（委外廠商）之資安風險。（25 分）

【解題關鍵】
《考題難易》：★★★
《破題關鍵》本題以 ISO27001 A.15 供應商關係中的控制措施即可作答。

【擬答】：

根據 ISO27001，為控管供應商資安風險，可以實行 A.15 供應商關係控制措施，包括下列：

㈠ A.15.1 供應商關係的資訊安全

其目標在確保供應商可存取之組織資產的保護。

1. A.15.1.1 供應商關係的資訊安全政策

應與供應商協議資訊安全要求，以減少供應商對組織資產存取的風險並加以文件化

2. A.15.1.2 供應商協議內的安全處理

應建立所有相關的資訊安全要求，並與每項可存取、處理、儲存、傳達組織資訊或提供 IT 基礎設施組件的供應商達成協議。

3. A.15.1.3 ICT 供應鏈

與供應商的協議，應包含因應有關資訊與通訊技術服務及產品供應鏈之資訊安全風險的要求。

㈡ A.15.2 供應商服務交付管理

其目標在維持議定等級之資訊安全及服務交付，並能與供應商協議一致。

1. A.15.2.1 供應商服務的監控與審查

應定期監控、審查及稽核供應商提供之服務。

2. A.15.2.2 供應商服務變更的管理

供應商所提供服務的變更，包含維持與改進現有的資訊安全政策、程序及控制措施均應加以管理，並考量所涉及之營運系統與過程的重要性及風險重新評鑑。

三、企業新開發的資訊系統上線後，可能才發現問題，例如客戶資料格式不符、與某些舊系統無法相容等。說明組織在開發新資訊系統時，如何避免上線後可能面臨到維運與使用上的問題。（25 分）

【解題關鍵】
《考題難易》：★★
《破題關鍵》本題以系統維護中的組態管理(Configuration management)即可作答。

【擬答】：

需要進行組態管理與變更管理（Configuration and Change Management），目的是追蹤與維護專案資產在演進過程之完整性（Integrity）。包括下列活動：

㈠型態識別：主要在訂定型態項目（CI）、型態基準線、製作型態項目的文件與編碼。目的在於建立及維持一套基準線，使其能在軟體生命週期內，對於每個型態項目做管制及狀態的彙報。因此要針對每個型態項目實施確認工作，包括定義、命名、編號等。

1. 描述型態項目之實體與功能特徵，經過核准的技術文件稱為型態文件，是在型態項目生命週期中，每一個設計審查階段，描述系統功能、接合方式與結構等。其主要目的是提供下一階段工作的正式標準以及控制任何變更的動作發生。
2. 由型態文件擷集而成為型態基準線。

㈡型態變更控制：是針對型態項目中已建基準線所提出的修改事項，進行評估、協調與核准，並且對於已核准之修改加以執行，建立有系統的管制程序以確保型態項目在專案開發過程中的一致性。通常由使用者提出變更需求申請表，經過直屬部門主管的核可以後，呈交型態控制委員會審查。若經審查發現不合乎變更的需求則立刻通知申請部門，並註明拒絕的理由，若認定有變更的必要時，則通知專案小組進行可行性分析與衝擊分析，並提出一些建議方案以及執行變更的命令。其次，經過修正完畢以後須交由型態控制委員會做確認工作，若不合規定再交由專案小組進行修改，一直到完全符合變更需求為止，因此變更工作必須加以嚴格控制，否則極易造成軟體開發工作混亂或延誤交期的情形。

㈢型態稽核：主要目的是確保軟體能夠符合規格、標準、合約規定或是其他規定準則。包括下列類型：

1. 事前稽核準備活動：包括宣布稽核的時程、位置與目的、參與人員等，制定稽核的準則、稽核使用標準表格、設計詳細檢查表、制定稽核程序等。
2. 正式稽核活動：在軟體開發的分析、設計、發展、測試階段與正式作業均設置管制點以確保軟體的品質水準。
3. 事後稽核活動。

㈣型態狀況報告：蒐集、記錄、變更型態文件、型態基準線或外包廠商繳交系統文件的狀態，針對型態項目的進度與變更提供一份完整資訊。主要內容包括：

1. 定義型態項目的功能及實體特性清單。
2. 各種預計變更與偏差的狀況表。
3. 變更進度表。
4. 專案資料庫現有型態項目的功能與實體特性清單。

四、假新聞對民眾與組織造成許多困擾，影響社會安定與企業形象等。說明如何辨別假新聞。（25 分）

【解題關鍵】
《考題難易》：★★★
《破題關鍵》本題需要注意時事，並搭配駭客攻擊手法即可作答。

【擬答】：

根據趨勢科技提供的判斷準則，若發現新聞出現以下徵兆，就很可能是假新聞：

㈠誇張聳動、讓人忍不住想點閱的標題，可能為惡意「點擊誘餌」

㈡可疑的網站地址，可能冒充真實的新聞網站

㈢內容出現拼字錯誤或網站版面不正常

㈣明顯經過刻意修圖的照片或圖片

㈤沒有附註發佈日期

㈥未註明作者、消息來源或相關資料