104年公務人員升官等考試、104年關務人員升官等考試
104年交通事業公路、港務人員升資考試試題　代號：16330　全一頁

等　　級：簡任
類科(別)：資訊處理
科　　目：系統分析研究
考試時間：2小時　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

一、請就政府機關資訊業務委外常見的風險，分別就以下兩類人員的不同立場，各寫出5項風險：
㈠機關單位個案人員。(15分)
㈡承包廠商。(15分)

二、資訊系統發展中的「需求規劃」，可使用的方法包括：訪談、文件查閱、觀察、調查、問卷、抽樣及研究等。請就以下內容，寫出「訪談法」其餘執行步驟2～步驟6的步驟名稱及各步驟的作業內容。(20分)
步驟1：決定訪談對象
為了得到正確資訊，必須選擇合適的人選，以能從中收集恰當的問題與內容。
……..
步驟7：評量訪談
除了獲取資訊之外，訪談時也要注意訪談是否有所失當。

三、有關MVC（Model-View-Controller）軟體系統架構，請回答以下問題：
㈠請定義說明MVC架構，並分別說明各組成部分的作用。(15分)
㈡請以繪圖方式說明這種由MVC架構所發展的資訊系統的運作程序。(15分)

四、若機關單位的資訊系統，擬導入資訊安全管理機制(Information Security Management System，簡稱ISMS)，而以國際化資訊安全規範標準(「國際資訊安全認證ISO 27001」)檢視前揭系統控制措施之符合性，期能降低資安風險、強化有關作業的資訊安全。身為系統分析人員，您將提出那些資訊系統發展規範，以作為機關內部機敏性資訊系統的發展規範（包含需求分析至系統運作維護等階段）？(20分)
「ISO 27001」的控制目標【A.12 資訊系統獲取、開發及維護】的規範，請參考以下：許多組織不自行開發資訊系統，因此一些A.12的安全目標並不適用，可以在適用性聲明書（SoA）中予以剔除。

A.12.1 資訊系統的安全要求：確保安全是整體資訊系統的一部分。
*規劃新資訊系統或現有資訊系統升級時，應詳細敘述安全要求與規格。
A.12.2 應用系統的正確處理：防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用。
*輸入與輸出的資料應予確認，以確保該資料正確。應用系統應具備確認查核功能（validation check），以偵測有意或無意的資料損壞，例如偵測緩衝區溢位等。
A.12.3 密碼控制（cryptographic control）措施：藉由密碼方式以保護資訊的機密性、鑑別性或完整性。
*使用加解密作業來保護資訊，並提供適當的金鑰管理。
A.12.4 系統檔案的安全：確保系統檔案的安全。
*應備妥各樣程序，以控制作業系統上軟體的安裝。系統的測試資料及系統的原始碼應予保護並控制存取。
A.12.5 開發與支援過程的安全：維持應用系統軟體與資訊的安全。
*應經由正式的變更控制程序（change control procedures）來變更作業系統、應用系統及套裝軟體。
*開發過程中應防範資料洩漏的機會；委外的軟體開發應監督與監視。
A.12.6 技術脆弱性管理：降低因利用已公布的技術脆弱性所導致的風險。
*應取得使用中資訊系統之技術脆弱性的及時資訊，並評估它對組織的影響；採取適當措施以因應相關的風險。
*若有修補程式（補丁），則評鑑安裝修補程式之風險，安裝前後應測試評估。