職能單元代碼	INM2R1412v3
職能單元名稱	測試並監控網路安全
領域類別	資訊科技 / 網路規劃與建置管理
職能單元級別	3
工作任務與行為指標	一、 評估網路安全威脅與弱點以找出風險 1. 依所需資產安全層級，評估與回報目前系統安全情況。 2. 確認額外的網路、軟體、硬體與系統的安全威脅與弱點。 3. 運用已知威脅與弱點資訊確認安全風險。 4. 依商業與業務要求，向管理階層提出建議以解決安全不足之處。 二、 針對找出的弱點與威脅執行反制措施 1. 依業務需求執行所需的周邊網路安全機制。 2. 評估與執行伺服器最佳實務與網路強化技術及措施。 3. 執行安全性驗證與使用者帳號管制機制。 4. 確保資料完整性與傳輸。 三、 測試與確認執行的安全系統功能性與效能 1. 依指標設計測試項目以確認關鍵性功能與效能。 2. 進行功能與效能測試並記錄結果。 3. 依需要修改安全系統並進行除錯。 4. 建立目前系統設定的文件與檔案以供將來參考。 四、 提供系統進行安全監控與維運 1. 於適當時機運用第三方測試軟體進行網路安全監控，包括實體層面。 2. 檢視日誌與稽核報告，以找出並記錄網路安全意外、入侵或嘗試入侵事件等。 3. 執行抽查與稽核行動以確保程序不被跳過。 4. 以文件記錄新發現的安全威脅、弱點與風險，並向適當人員簡報以取得變更許可。
職能內涵 (K=knowledge 知識)	• 資通安全管理法與隱私權等問題相關規範 • 客戶業務專業領域 • 網路技術特性與性能

	• 組織風險分析 • 路由器與交換器規劃相關知識 • 網路通訊協定與作業系統 • 業界使用的軟硬體安全產品及其特性與能力 • 驗證問題類型 • 安全性通訊協定與標準及資料加密方法 • 安全性周邊網路與其功能 • 安全威脅概論 • VPN專業知識【註6】 • 不同類型的區域網路相關解決方案
職能內涵 (S=skills 技能)	• 溝通協調能力 • 資通安全管理法與隱私權等問題相關規範之風險管控 • 資訊科技應用能力 • 企業安全政策相關之研擬能力 • 網路系統安全性風險評估能力 • 分析網路安全技術與效能 • 網路安全軟硬體規劃能力 • 安全系統功能與效能測試及除錯能力 • 撰寫安全監控日誌與稽核報告
• 說明與補充事項	• 資產：如資料與資訊、智慧財產、實體資產等。 • 弱點：如應用程式錯誤、韌體瑕疵、防火牆規劃不當、作業系統漏洞、以純文字傳輸資料等、不必要的服務與通訊協定、安全性不足的驗證技術、權限控管弱、實體安全性弱等。 • 周邊網路安全：如存取管制、稽核、驗證、授權、硬體或軟體防火牆、身分辨認、網路位址轉譯（NAT）、監視等。 • 強化技術：如非軍事區（DMZ）、加密、入侵偵測系統（IDS）、作業系統修補與管理、嚴密共享資源權限、阻擋未使用通訊埠、加強實體安全、加強驗證技術、停用未使用服務與通訊協定等。 • 文件記錄：如稽核追蹤、國際標準組織、命名標準、專案管理範本、報告撰寫原則、安全性分析報告、版本管

	制、系統日誌等。 • VPN專業知識：如頻寬與動態安全性環境、VPN功能與運作（如加密、防火牆、封包與驗證）、VPN種類如網站對網站及使用者對網站的網際網路流量與外部網路相關的系統與程序等。