

職能單元代碼	ISD5R0730v2
職能單元名稱	設計與執行網路安全系統
領域類別	資訊科技 / 軟體開發及程式設計
職能單元級別	5
工作任務與行為指標	<p>一、評估網路基礎建設所面臨的安全威脅</p> <ol style="list-style-type: none"> 1. 評估網路攻擊與不同類型惡意軟體的解決方案。 2. 提出詳盡防禦網路架構概念。 <p>二、保護邊緣裝置（路由器）</p> <ol style="list-style-type: none"> 1. 使用軟體工具保護路由器。 2. 使用路由器作業系統，保護路由器的存取管理。 3. 保護路由器作業系統與設定檔。 <p>三、驗證、授權與帳號管理，並保護存取控制系統（ACS）</p> <ol style="list-style-type: none"> 1. 評估驗證、授權與帳號管理（AAA）的重要性，並執行其功能。 2. 使用驗證、授權與帳號管理設定路由器。 3. 分析與比較關於保護網路安全的 TACACS+ 與 RADIUS AAA 協定的特性。 <p>四、使用存取控制列表減緩對路由器與網路的安全威脅</p> <ol style="list-style-type: none"> 1. 評估存取控制列表（ACLs）功能，並記錄建立所需考量的注意事項。 2. 配置與驗證網際網路協定（IP）的存取控制列表以減緩威脅，並預防由工具產生的 IP 位置欺騙。 <p>五、執行網路安全管理與通報</p> <ol style="list-style-type: none"> 1. 使用工具配置路由器，以發送 log 訊息到日誌伺服器。 <p>六、降低常見的第二層攻擊</p> <ol style="list-style-type: none"> 1. 記錄基本交換器安全與特性的配置，以防禦第二層攻擊。 2. 進行配置交換器以防禦第二層攻擊。 <p>七、執行路由器作業系統的防火牆功能集</p> <ol style="list-style-type: none"> 1. 評估與比較不同防火牆技術的操作策略與弱點。 2. 執行區域性（zone-based）防火牆，以策略性保護群組介面。 <p>八、使用安全裝置管理員執行入侵偵測與防禦系統功能集</p>

	<p>1. 評估與比較網路型與主機型的入侵偵測與防禦系統 (IDPS)，包括辨識並通報惡意攻擊行為、log 資訊與意圖阻止/停止活動。</p> <p>2. 說明入侵偵測與防禦系統技術、攻擊反應與監控選項。</p> <p>3. 使用安全裝置管理員 (SDM) 配置路由器作業系統的入侵偵測與防禦系統，以監控網路與系統的惡意攻擊行為。</p> <p>九、使用安全裝置管理員執行點對點的虛擬私有網路</p> <p>1. 評估各種不同的加密方法。</p> <p>2. 評估網際網路金鑰交換 (IKE) 協定的功能與階段，以驗證並界定網際網路安全協定 (IPSec) 的綁定端口與安全功能。</p> <p>3. 使用預先共用金鑰 (PSK) 的驗證來配置與核實網際網路安全協定的點對點虛擬私有網路 (VPNs)，以提供安全通道。</p>
職能內涵 (K=knowledge 知識)	<p>一、風險相關之政策、法規與組織準則、程序等規範</p> <p>二、網路風險管理</p> <p>三、存取控制列表、配置及問題之解決方法</p> <p>四、驗證協定、資料加密技術、路由協定等相關基礎知識</p> <p>五、網路與系統安全性相關知識</p> <p>六、無線法規、標準及認證知識</p> <p>七、區域網路 (LAN) 與廣域網路 (WAN) 實作知識</p> <p>八、網路管理工具與虛擬私人網路設定步驟</p>
職能內涵 (S=skills 技能)	<p>一、溝通協調能力</p> <p>二、遵循風險相關之政策、法規與組織準則、程序等規範</p> <p>三、分析網路安全系統的威脅與需求</p> <p>四、規劃減緩攻擊與配置防火牆之策略</p> <p>五、調查符合需求的軟硬體資訊</p> <p>六、配置與安裝網路安全系統的技術能力</p> <p>七、使用安全裝置管理員執行虛擬私有網路</p>
評量設計參考	<p>一、評量證據</p> <p>1. 評估網路安全系統的威脅與需求。</p> <p>2. 能減緩網路威脅與配置防火牆。</p>

	<p>3. 設計與執行網路安全系統。</p> <p>4. 使用安全裝置管理員執行虛擬私有網路。</p> <p>二、評量情境與資源</p> <p>1. 評量情境須儘量符合實務工作現場環境。</p> <p>2. 相關先備條件，如可評估與加強網路安全的網站、區域網路相關軟體、組織準則與程序和政策等。</p> <p>3. 必要時提供適當的學習和評量協助。</p> <p>4. 提供特殊需求人士使用的所需設備與支援。</p> <p>三、評量方法</p> <p>1. 觀察受評者安裝、配置與測試新的或更新的網路。</p> <p>2. 評估受評者測試程序、測試結果、對網路變更的建議與完成紀錄的摘要文件。</p> <p>3. 口頭、網路或書面提問，評估受評者的必備知識。</p>
說明與補充事項	無。

更新紀錄
2021 年修訂職能內容。