

職能單元代碼	INM4R1498v3
職能單元名稱	規劃、配置與測試網路伺服器安全
領域類別	資訊科技 / 網路規劃與建置管理
職能單元級別	4
工作任務與行為指標	<p>一、 依業務需求規劃進階網路伺服器安全</p> <ol style="list-style-type: none"> 1. 與相關人員討論以確定進階網路伺服器環境的安全性要求。 2. 分析與檢討客戶安全文件並預測網路服務弱點。 3. 研究網路驗證與網路服務組態選項與執行以產生網路安全解決方案。 4. 確保網路服務安全選項的特性與性能均符合業務需求。 5. 產生或更新伺服器安全設計文件並納入新解決方案。 6. 取得適當人員對安全設計的簽核。 <p>二、 準備執行網路伺服器安全</p> <ol style="list-style-type: none"> 1. 依特定場地安全要求與企業職業安全衛生流程與程序準備工作事項。 2. 找出安全危害並依適當人員指導以執行風險管制措施。 3. 與適當人員討論以確保充分協調現場人員任務。 4. 執行配置變更前進行伺服器備份。 <p>三、 依設計配置進階網路伺服器安全</p> <ol style="list-style-type: none"> 1. 配置升級服務以提供最高安全與可靠性。 2. 配置網路驗證授權與帳號服務，以便登錄並防止未授權存取伺服器。 3. 配置基本服務安全與存取控制清單以限制使用者、群組或網路的存取。 4. 依設計要求執行加密機制。 5. 配置進階網路連線服務安全性選項與遠端存取安全。 6. 配置作業系統或第三方防火牆並依安全要求過濾流量。 7. 確認正確執行伺服器記錄檔與安全性登入伺服器以

	<p>達系統完整性。</p> <p>8. 執行備份與復原方法以啟動災難還原功能。</p> <p>四、 監控與測試網路伺服器安全</p> <p>1. 依核可的設計配置測試伺服器以評量網路伺服器安全性。</p> <p>2. 監控伺服器記錄檔、網路流量與開放通訊埠以偵測可能入侵危害。</p> <p>3. 監控重要檔案以偵測未授權修改。</p> <p>4. 調查並確認可疑的伺服器或資料安全違規與隱私漏洞。</p> <p>5. 依安全性原則與程序修復安全性漏洞並進行通報且製作文件紀錄。</p> <p>6. 評估監控結果與報告，以執行並測試維持網路服務安全性所需的改善作業。</p>
<p>職能內涵 (K=knowledge 知識)</p>	<ul style="list-style-type: none"> • 職業安全衛生風險相關規範 • 稽核與滲透測試技術 • 加密技術 • 入侵偵測與修復程序 • 網路服務安全特性與選項及限制 • 網路服務漏洞 • 安全防護機制、安全性威脅與風險 • 伺服器防火牆規劃 • 使用者驗證與目錄服務 • 執行備份與還原最佳實務程序 • 錯誤與事件記錄與通報程序 • 作業系統與公用程式於安全性的協助與支援 • 網路服務規劃相關知識【註10】
<p>職能內涵 (S=skills 技能)</p>	<ul style="list-style-type: none"> • 溝通協調能力 • 職業安全衛生風險管控能力 • 網路伺服器系統安全性風險評估能力 • 規劃進階網路伺服器安全配置流程 • 建置與測試不同組態需求配置之能力 • 資訊安全技術能力 • 撰寫安全監控日誌與稽核報告

說明與補充事項	<ul style="list-style-type: none"> • 客戶安全文件：包含風險評估報告、安全性事件報告與伺服器日誌、安全計畫、安全政策、安全程序等。 • 網路服務：包含動態主機設定通訊協定 (DHCP)、動態名稱系統 (DNS)、超文字安全傳輸通訊協定 (HTTPS)、網際網路訊息存取通訊協定 (IMAP)、遠端程序呼叫 (RPC)、網路檔案系統 (NFS)、郵件通訊協定 (POP)、簡易郵件傳送通訊協定 (SMTP)、簡易網路管理通訊協定 (SNMP)、結構化查詢語言伺服器 (SQL) 等。 • 適當人員：包含授權業務代表、用戶端、IT部門代表、主管、安全管理者等。 • 基本服務安全：包含以主機為基礎的存取管制、網路服務存取控制清單 (ACL)、網路服務驗證、網路共用的權限、安全強化Linux (SE Linux)、TCP包裹程式、Windows群組原則等。 • 加密：包含非對稱式加密、數位簽章與簽名驗證、電子郵件加密、加密檔案系統、加密網路流量、公開金鑰基礎架構 (PKI)、安全封包層協定 (SSL) 憑證等。 • 服務安全性選項：包含網路檔案服務安全性選項 (如硬碟配額、加密檔案系統)、網域名稱解析服務 (如DNS拓撲、交易簽名)、網頁伺服器與代理伺服器服務 (如驗證、SSL憑證)、郵件服務 (如電子郵件加密、郵件過濾)、FTP服務 (如FTP驗證) 等。 • 遠端存取安全：包含撥接、網際網路連線共用 (ICS)、網路位址轉譯 (NAT)、遠端驗證撥入使用者服務 (RADIUS)、路由與遠端存取服務 (RRAS)、虛擬私有網路 (VPN) 等。 • 第三方防火牆：可包含進出流量過濾、iptables、網際網路安全性與加速 (ISA) 伺服器、通訊埠與通訊協定流量過濾等。 • 備份與復原：包含利用作業系統備份與工作排程工具進行自動化備份、網路目錄服務物件的備份與復原、資料庫備份與復原、磁碟區陰影複製等。
---------	---

	<ul style="list-style-type: none">• 網路服務規劃相關知識：包括DNS、DHCP、FTP、SMB、NTP、郵件與代理等。
--	---