網路資訊安全人員職能基準

版本	職能基準代碼	職能基準名稱	狀態	更新說明	發展更新日期
V3	INM3513-001v3	網路資訊安全人員	最新版本	略	2021/12/31
V2	INM3513-001v2	網路資訊安全人員	歷史版本	已被《INM3513-001v3》取代	2019/12/31
V1	INM3513-001v1	資訊安全人員	歷史版本	已被《INM3513-001v2》取代	2016/12/31

職能基準代碼		INM3513-001v3		
職能基準名稱（擇一填寫）	**職類**			
	職業	**網路資訊安全人員**		
所屬類別	**職類別**	資訊科技 / 網路規劃與建置管理	**職類別代碼**	INM
	職業別	電腦網路及系統技術員	**職業別代碼**	3513
	行業別	出版、影音製作、傳播及資通訊服務業 / 電腦程式設計、諮詢及相關服務業	**行業別代碼**	J6202
工作描述		依據組織網路架構之特性與需要，設計網路服務伺服器相關安全防護措施，防範因網路入侵所造成的相關安全威脅。		
基準級別		4		

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵（K=knowledge 知識）	職能內涵（S=skills 技能）
T1 規劃、組態與測試網路服務伺服器安全性	T1.1 依照業務需求規劃網路服務伺服器安全	O1.1.1 網路安全解決方案 O1.1.2 網路服務伺服器安全設計文件	P1.1.1 與客戶及關鍵利益關係人討論，以找出網路服務伺服器環境中的安全要求。 P1.1.2 分析與檢討現有客戶（避免被誤解為使用者端）的安全性文件並預測網路服務弱點。 P1.1.3 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	K01 稽核與滲透測試技術 K02 執行備份與還原程序 K03 加密技術程序 K04 錯誤與事件記錄及通報程序 K05 入侵偵測與修復程序 K06 網路服務相關知識【註 1】 K07 網路服務安全概論	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S05 應變管理能力 S06 安全警覺性能力

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵 （K=knowledge 知識）	職能內涵 （S=skills 技能）
			P1.1.4 確保網路服務安全選項的特性與性能均符合業務需求。 P1.1.5 產生或更新伺服器安全設計文件以納入新解決方案。 P1.1.6 向適當人員取得安全設計的簽核。		K08 網路服務漏洞 K09 作業系統支援公用程式 K10 規劃、組態、監控與疑難排除技術 K11 安全防護機制 K12 安全性威脅與風險 K13 伺服器防火牆及相關網路防護系統規劃 K14 伺服器監控（錄製）與疑難排解工具與技術 K15 使用者驗證或目錄服務	S07 研究能力 S08 程式撰寫能力 S09 伺服器架設與應用能力
	T1.2 準備網路服務伺服器安全執行	O1.2.1 網路組態文件	P1.2.1 與適當人員討論以確保充分協調與現場其他人員之任務。 P1.2.2 在執行組態變更前，進行伺服器備份。	4	K01 稽核與滲透測試技術 K02 執行備份與還原程序 K03 加密技術程序 K04 錯誤與事件記錄及通報程序 K05 入侵偵測與修復程序 K06 網路服務相關知識 K07 網路服務安全概論 K08 網路服務漏洞 K09 作業系統支援公用程式 K10 規劃、組態、監控與疑難排除技術 K11 安全防護機制	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S05 應變管理能力 S06 安全警覺性能力 S07 研究能力 S08 程式撰寫能力 S09 伺服器架設與應用能力

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵 （K=knowledge 知識）	職能內涵 （S=skills 技能）
					K12 安全性威脅與風險 K13 伺服器防火牆及相關網路防護系統規劃 K14 伺服器監控（錄製）與疑難排解工具與技術 K15 使用者驗證或目錄服務	
	T1.3 依照設計組態網路服務伺服器安全	O1.3.1 網路組態文件 O1.3.2 伺服器組態文件	P1.3.1 提供最大安全與可靠性升級服務。 P1.3.2 組態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。 P1.3.3 組態基本服務安全性與存取控制清單以限制授權使用者、群組或網路的存取。 P1.3.4 依照設計要求執行加密。 P1.3.5 組態網路連線服務之安全性選項以及遠端存取。 P1.3.6 組態作業系統或第三方防火牆以便依照安全要求過濾流量。 P1.3.7 確認伺服器記錄檔與登入伺服器的安全，均能適當執行以求系統完整性。 P1.3.8 執行備份與復原方法以啟動災害時的還原功能。	4	K01 稽核與滲透測試技術 K02 執行備份與還原程序 K03 加密技術程序 K04 錯誤與事件記錄及通報程序 K05 入侵偵測與修復程序 K06 網路服務相關知識 K07 網路服務安全概論 K08 網路服務漏洞 K09 作業系統支援公用程式 K10 規劃、組態、監控與疑難排除技術 K11 安全防護機制 K12 安全性威脅與風險 K13 伺服器防火牆及相關網路防護系統規劃 K14 伺服器監控（錄製）與疑難排解工具與技術	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S05 應變管理能力 S06 安全警覺性能力 S07 研究能力 S08 程式撰寫能力 S09 伺服器架設與應用能力

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵（K=knowledge 知識）	職能內涵（S=skills 技能）
					K15 使用者驗證或目錄服務	
	T1.4 監控與測試網路服務伺服器安全	O1.4.1 監控結果報告	P1.4.1 依照雙方同意的設計組態測試伺服器，以評量網路伺服器安全。 P1.4.2 監控伺服器記錄檔、網路流量與開放通訊埠以偵測可能的入侵。 P1.4.3 監控重要檔案以偵測未授權的修改。 P1.4.4 調查並確認可疑的伺服器或資料安全違規與隱私漏洞。 P1.4.5 依照安全性原則與程序將安全性漏洞修復、通報並製作文件紀錄。 P1.4.6 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動作。	4	K01 稽核與滲透測試技術 K02 執行備份與還原程序 K03 加密技術程序 K04 錯誤與事件記錄及通報程序 K05 入侵偵測與修復程序 K06 網路服務相關知識 K07 網路服務安全概論 K08 網路服務漏洞 K09 作業系統支援公用程式 K10 規劃、組態、監控與疑難排除技術 K11 安全防護機制 K12 安全性威脅與風險 K13 伺服器防火牆及相關網路防護系統規劃 K14 伺服器監控（錄製）與疑難排解工具與技術 K15 使用者驗證或目錄服務	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S05 應變管理能力 S06 安全警覺性能力 S07 研究能力 S08 程式撰寫能力 S09 伺服器架設與應用能力
T2 組態安全網路環境	T2.1 執行 OSI 網路層安全（包含虛	O2.1.1 網路架構配置文件 O2.1.2 測	P2.1.1 規劃、配置與測試網路路由通訊協定解決方案。 P2.1.2 規劃、配置與測試以 IPv4 或 IPv6 為基礎之網路再分布解決方案。	3	K16 網路服務相關技術規劃 K17 網路安全相關風險識別 K18 網路安全相關防護機制規劃 K19 網路通訊協定	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵（K=knowledge 知識）	職能內涵（S=skills 技能）
	擬化網路架構）	試相關規劃文件 O2.1.3 網路安全防護計畫與組態文件	P2.1.3 使用路由器作業系統指令組態以減少第二層攻擊。 P2.1.4 以存取控制機制在交換器上執行以身分識別為基礎之網路服務，提供第二層網路安全。		K20OSI 通訊網路架構應用 K21 遠端連線、遠端存取及虛擬私有網路（VPN）加密技術協定 K22 網路通訊安全監控技術 K23 路由通訊協定 K24NAT 機制、概念與規劃	決能力 S05 應變管理能力 S10 計算能力 S11 研究能力 S12 網路設計能力
	T2.2 組態入侵防禦系統		P2.2.1 評估路由器，IPS 及防火牆特性進階能力納入網路資源之威脅事件因應。 P2.2.2 組態並確認 IPS 特性以找出威脅，並以動態方式阻止其進入網路。 P2.2.3 維持、更新與微調 IPS 佈署。 P2.2.4 組態與驗證以背景為基礎之存取控制（CBAC）以及網路位址轉譯（NAT）以便動態減少找出的網路威脅。 P2.2.5 組態與驗證以區域為基礎之防火牆來納入新進應用程式檢查並通知資源定位器（URL）過濾以達到網路安全的提升。 P2.2.6 評估 NFP 特性與功能性以提供基礎建設保護。 P2.2.7 利用路由器功能來取得管理平面、資料平面與控制平面。	3	K16 網路服務相關技術規劃 K17 網路安全相關風險識別 K18 網路安全相關防護機制規劃 K19 網路通訊協定 K20OSI 通訊網路架構應用 K21 遠端連線、遠端存取及虛擬私有網路（VPN）加密技術協定 K22 網路通訊安全監控技術 K23 路由通訊協定 K24NAT 機制、概念與規劃	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S05 應變管理能力 S10 計算能力 S11 研究能力 S12 網路設計能力
	T2.3 組態虛擬私有	O2.3.1 VPN 建置	P2.3.1 分析並評估網際網路通訊協定安全性與通用路由協議封裝特性與功能性。	3	K16 網路服務相關技術規劃 K17 網路安全相關風險識別	S01 溝通協調能力 S02 讀寫能力

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵（K=knowledge 知識）	職能內涵（S=skills 技能）
	網路（VPN）提供站台對站台以及遠端存取通訊的安全連線	與管理文件	P2.3.2 利用憑證授權單位設定站台對站台 VPN 之安全連線。 P2.3.3 組態與驗證網站對網站 VPN 作業之安全連線。 P2.3.4 以安全封包層協定（SSL）VPN 提供高度安全網路存取以達到遠端存取連線特性與效益。		K18 網路安全相關防護機制規劃 K19 網路通訊協定 K20OSI 通訊網路架構應用 K21 遠端連線、遠端存取及虛擬私有網路（VPN）加密技術協定 K22 網路通訊安全監控技術 K23 路由通訊協定 K24NAT 機制、概念與規劃	S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S05 應變管理能力 S10 計算能力 S11 研究能力 S12 網路設計能力
T3 安裝、組態並測試網路安全	T3.1 評估網路安全威脅與弱點以找出風險	O3.1.1 網路安全測試結果報告 O3.1.2 問題處理追蹤改善文件	P3.1.1 根據所需的資產安全層級，評估與回報目前的系統安全，建立測試程序。 P3.1.2 確認額外的網路、軟硬體以及系統安全威脅與弱點。 P3.1.3 運用已找出之威脅與弱點資訊，確認安全風險。 P3.1.4 依現行與未來的商業與業務要求，向管理階層提出建議以解決安全不足之處。	4	K16 網路服務相關技術規劃 K17 網路安全相關風險識別 K18 網路安全相關防護機制規劃 K25VPN 概念的功能與運作【註2】 K26 風險分析稽核與滲透測試技術 K27 封包分析與安全威脅評估【註3】 K28 隱私權問題與隱私權法規	S01 溝通協調能力 S02 讀寫能力 S04 軟硬體網路安全技術問題解決能力 S10 計算能力 S11 研究能力 S13 分析能力 S14 網路安全規劃與執行能力
	T3.2 針對找出的弱點與威脅執行反制措施		P3.2.1 根據目前與未來的業務需求，執行所需的周邊網路安全等級。 P3.2.2 評估與執行最佳實務伺服器與網路強化技術及措施。 P3.2.3 執行安全性驗證與使用者帳號管制。	4	K16 網路服務相關技術規劃 K17 網路安全相關風險識別 K18 網路安全相關防護機制規劃 K25VPN 概念的功能與運作 K26 風險分析稽核與滲透測試技	S01 溝通協調能力 S02 讀寫能力 S04 軟硬體網路安全技術問題解決能力 S10 計算能力

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵（K=knowledge 知識）	職能內涵（S=skills 技能）
			P3.2.4 確保資料完整性與傳輸。		術 K27 封包分析與安全威脅評估 K28 隱私權問題與隱私權法規	S11 研究能力 S13 分析能力 S14 網路安全規劃與執行能力
	T3.3 測試與確認執行之安全系統的功能性與效能	O3.3.1 系統設定文件檔	P3.3.1 根據指標設計測試項目，以確認關鍵性功能與效能措施。 P3.3.2 進行功能與效能測試並記錄結果。 P3.3.3 依照需要修改安全系統並除錯。 P3.3.4 研擬目前系統設定的文件與檔案以供將來參考。 P3.3.5 定期驗證相關安全防護機制之有效性並予以適當修正。	4	K16 網路服務相關技術規劃 K17 網路安全相關風險識別 K18 網路安全相關防護機制規劃 K25VPN 概念的功能與運作 K26 風險分析稽核與滲透測試技術 K27 封包分析與安全威脅評估 K28 隱私權問題與隱私權法規	S01 溝通協調能力 S02 讀寫能力 S04 軟硬體網路安全技術問題解決能力 S10 計算能力 S11 研究能力 S13 分析能力 S14 網路安全規劃與執行能力
	T3.4 提供系統進行安全監控與維運	O3.4.1 系統維運管理文件	P3.4.1 於適用時運用適當的第三方測試軟體監控目前的網路安全，包括實體層面（SOC）。 P3.4.2 檢視日誌與稽核報告，以找出並記錄網路安全意外事件、入侵或嘗試。 P3.4.3 執行抽查與稽核，以確保程序不被跳過。 P3.4.4 報告文件記錄新發現的安全威脅弱點與風險，向適當人員簡報以取得變更許可。 P3.4.5 針對相關組態與設定的變更需求，應建立變更程序進行，並應取得適當授權。 P3.4.6 相關網路權限與設定應依最小權限原則執行。	4	K16 網路服務相關技術規劃 K17 網路安全相關風險識別 K18 網路安全相關防護機制規劃 K25VPN 概念的功能與運作 K26 風險分析稽核與滲透測試技術 K27 封包分析與安全威脅評 K28 隱私權問題與隱私權法規	S01 溝通協調能力 S02 讀寫能力 S04 軟硬體網路安全技術問題解決能力 S10 計算能力 S11 研究能力 S13 分析能力 S14 網路安全規劃與執行能力

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵 （K=knowledge 知識）	職能內涵 （S=skills 技能）
			P3.4.7 應針對組態、安全設定及權限定期檢視其合宜性。			
T4 管理網路安全	T4.1 定義設計安全的流程		P4.1.1 定義網路安全設計的規劃階段。 P4.1.2 定義網路安全設計的建置階段。 P4.1.3 定義網路安全設計的管理階段。	3	K01 稽核與滲透測試技術 K29 日誌分析技術及組織網路基礎建設 K30 已安裝網路基礎建設弱點 K31 網路管理與安全流程管制及風險管理計畫與程序 K32 外部資訊安全情資 K33 ISO31000 風險管理原理及指導綱要 K34 ISO27001 資訊安全管理系統制度與相關指引	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S13 分析能力 S15 風險管理能力
	T4.2 找出網路安全的威脅		P4.2.1 確認攻擊的原因。 P4.2.2 確定攻擊來源。 P4.2.3 網路弱點分析。 P4.2.4 滲透測試，以確認攻擊發生方式。 P4.2.5 設計威脅模型分析以便將威脅分類。	3	K01 稽核與滲透測試技術 K29 日誌分析技術及組織網路基礎建設 K30 已安裝網路基礎建設弱點 K31 網路管理與安全流程管制及風險管理計畫與程序 K32 外部資訊安全情資 K33 ISO31000 風險管理原理及指導綱要 K34 ISO27001 資訊安全管理系	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S13 分析能力 S15 風險管理能力

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵 （K=knowledge 知識）	職能內涵 （S=skills 技能）
					統制度與相關指引	
	T4.3 分析安全風險	O4.3.1 風險管理計畫	P4.3.1 決定風險管理的工作要素。 P4.3.2 決定需要保護的資產。 P4.3.3 分類資產並計算其對組織的價值。 P4.3.4 建立風險管理計畫。	3	K01 稽核與滲透測試技術 K29 日誌分析技術及組織網路基礎建設 K30 已安裝網路基礎建設弱點 K31 網路管理與安全流程管制及風險管理計畫與程序 K32 外部資訊安全情資 K33 ISO31000 風險管理原理及指導綱要 K34 ISO27001 資訊安全管理系統制度與相關指引	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S13 分析能力 S15 風險管理能力
	T4.4 建立安全設計	O4.4.1 安全性原則	P4.4.1 決定攻擊者情境與威脅。 P4.4.2 針對網路元件設計安全性措施。 P4.4.3 取得回饋，如有需要應進行調整。 P4.4.4 研擬安全性準則，包括安全政策、安全程序、安全標準與安全指引等。 P.4.4.5 根據安全威脅之特性以及風險分析結果，選擇合適的安全防護機制因應並執行，並觀察是否消除安全威脅並降低至可接受之程度。	3	K01 稽核與滲透測試技術 K29 日誌分析技術及組織網路基礎建設 K30 已安裝網路基礎建設弱點 K31 網路管理與安全流程管制及風險管理計畫與程序 K32 外部資訊安全情資 K33 ISO31000 風險管理原理及指導綱要 K34 ISO27001 資訊安全管理系統制度與相關指引	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S13 分析能力 S15 風險管理能力

主要職責	工作任務	工作產出	行為指標	職能級別	職能內涵（K=knowledge 知識）	職能內涵（S=skills 技能）
	T4.5 設計與執行安全意外應變措施	O4.5.1 安全事故報告	P4.5.1 設計稽核與事故應變程序。 P4.5.2 記錄安全事故。 P4.5.3 執行所規劃的事故應變程序。 P4.5.4 測試並完成簽核。	3	K01 稽核與滲透測試技術 K29 日誌分析技術及組織網路基礎建設 K30 已安裝網路基礎建設弱點 K31 網路管理與安全流程管制及風險管理計畫與程序 K32 外部資訊安全情資 K33 ISO31000 風險管理原理及指導綱要 K34 ISO27001 資訊安全管理系統制度與相關指引	S01 溝通協調能力 S02 讀寫能力 S03 規劃與組織能力 S04 軟硬體網路安全技術問題解決能力 S13 分析能力 S15 風險管理能力

職能內涵（A=attitude 態度）
A01正直誠實：展現高道德標準及值得信賴的行為，且能以維持組織誠信為行事原則，瞭解違反組織、自己及他人的道德標準之影響。
A02持續學習：能夠展現持續學習的企圖心，利用且積極參與各種機會，學習任務所需的新知識與技能，並能有效應用在特定任務。
A03壓力容忍：冷靜且有效地應對及處理高度緊張的情況或壓力，如緊迫的時間、不友善的人、各類突發事件及危急狀況，並能以適當的方式紓解自身壓力。
A04謹慎細心：對於任務的執行過程，能謹慎考量及處理所有細節，精確地檢視每個程序，並持續對其保持高度關注。
A05應對不確定性：當狀況不明或問題不夠具體的情況下，能在必要時採取行動，以有效釐清模糊不清的態勢。

說明與補充事項
● **建議擔任此職類/職業之學歷/經歷/或能力條件：** • 專科以上，資訊相關科系畢業或具備2年以上資訊相關工作經驗。 ● **其他補充說明：**

說明與補充事項
• 【註1】網路服務相關知識，包括 DNS、DHCP、網路、郵件、FTP、SMB、NTP 與代理等。 • 【註2】VPN 概念的功能與運作：包括加密、防火牆、封包與驗證、頻寬與動態安全性環境等。 • 【註3】封包分析與安全威脅評估：包括竊聽、資料攔截、資料損毀與資料假造等。