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
V4	INM3513-001v4	網路資訊安全人員	最新版本	略	2025/12/15
V3	INM3513-001v3	網路資訊安全人員	歷史版本	已被《INM3513-001v4》取代	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		INM3513-001v4			
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、配置與測試網路伺服器安全	T1.1依照業務需求規劃網路伺服器安全	O1.1.1網路安全解決方案 O1.1.2網路伺服器安全設計	P1.1.1與使用者討論，以找出網路伺服器環境中的安全要求。 P1.1.2分析與檢討使用者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配置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

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）
		文件	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產生或更新網路伺服器安全設計文件以納入新解決方案。 P1.1.6向使用者取得安全設計的簽核。		K07網路服務漏洞 K08規劃、配置、監控與疑難排除技術 K09安全防護機制 K10安全性威脅與風險 K11伺服器防火牆及相關網路防護系統規劃 K12伺服器監控（錄製）與疑難排解工具與技術 K13使用者驗證或目錄服務	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
	T1.2準備網路伺服器安全執行	O1.2.1網路配置文件	P1.2.1與使用者討論以確保充分協調與現場其他人員之任務。 P1.2.2在執行配置變更前，進行網路伺服器備份。	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網路服務安全概論 K07網路服務漏洞 K08規劃、配置、監控與疑難排除技術 K09安全防護機制 K10安全性威脅與風險 K11伺服器防火牆及相關網路防護系統規劃	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 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伺服器監控（錄製）與疑難排解工具與技術 K13使用者驗證或目錄服務	
	T1.3依照設計配置網路伺服器安全	O1.3.1網路伺服器配置文件	P1.3.1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網路伺服器。 P1.3.2配置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。 P1.3.3依照設計要求執行加密。 P1.3.4配置網路連線服務之安全性選項以及遠端存取。 P1.3.5配置作業系統或第三方防火牆以便依照安全要求過濾流量。 P1.3.6確認網路伺服器記錄檔與登入網路伺服器的安全，均能適當執行以求系統完整性。 P1.3.7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網路服務安全概論 K07網路服務漏洞 K08規劃、配置、監控與疑難排除技術 K09安全防護機制 K10安全性威脅與風險 K11伺服器防火牆及相關網路防護系統規劃 K12伺服器監控（錄製）與疑難排解工具與技術 K13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
	T1.4監控與測試網路伺服器	O1.4.1監控紀錄	P1.4.1依照與使用者同意的設計配置測試網路伺服器，以評量網路伺服器安全。	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	S01溝通協調能力 S02讀寫能力 S03規劃與組織能力

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）
	安全		P1.4.2監控網路伺服器記錄檔、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，以檢視未經授權的修改。 P1.4.4調查並確認可疑的網路伺服器或資料安全違規。 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。		K04錯誤與事件記錄及通報程序 K05入侵偵測與修復程序 K06網路服務安全概論 K07網路服務漏洞 K08規劃、配置、監控與疑難排除技術 K09安全防護機制 K10安全性威脅與風險 K11伺服器防火牆及相關網路防護系統規劃 K12伺服器監控（錄製）與疑難排解工具與技術 K13使用者驗證或目錄服務	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配置安全網路環境	T2.1執行網路安全（包含虛擬化網路架構）	O2.1.1網路安全防護計畫與配置文件	P2.1.1規劃、配置與測試以 IPv4或 IPv6為基礎之網路路由通訊協定解決方案。 P2.1.2使用路由器作業系統指令配置以減少被攻擊。 P2.1.3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，提供網路安全。	3	K14網路服務相關技術規劃 K15網路安全相關風險識別 K16網路安全相關防護機制規劃 K17網路通訊協定 K18OSI 通訊網路架構應用 K19遠端連線、遠端存取及虛擬私有網路（VPN）加密技術協定 K20網路通訊安全監控技術 K21路由通訊協定 K22NAT 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

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）
	T2.2配置網路防禦系統		P2.2.1評估路由器及入侵偵測防禦系統特性進階能力，納入網路資源之威脅事件即時處理。 P2.2.2配置並確認入侵偵測防禦系統特性以找出威脅，並以動態方式阻止其進入網路。 P2.2.3維持、更新與微調入侵偵測防禦系統佈署。 P2.2.4配置與驗證以背景為基礎之存取控制（CBAC）以及網路位址轉譯（NAT）以減少網路威脅。 P2.2.5配置與驗證防火牆來納入新進應用程式檢查並通知統一資源標識符（URI）過濾，以達到網路安全的提升。 P2.2.6利用路由器功能來取得管理、資料與控制資訊。	3	K14網路服務相關技術規劃 K15網路安全相關風險識別 K16網路安全相關防護機制規劃 K17網路通訊協定 K18OSI 通訊網路架構應用 K19遠端連線、遠端存取及虛擬私有網路（VPN）加密技術協定 K20網路通訊安全監控技術 K21路由通訊協定 K22NAT 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配置虛擬私有網路（VPN）	O2.3.1 VPN 建置與管理文件	P2.3.1分析並評估通訊協定安全性與通用路由協議封裝特性與功能性。 P2.3.2利用憑證授權設定站台對站台 VPN 之安全連線。 P2.3.3配置與驗證網站對網站 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。	3	K14網路服務相關技術規劃 K15網路安全相關風險識別 K16網路安全相關防護機制規劃 K17網路通訊協定 K18OSI 通訊網路架構應用 K19遠端連線、遠端存取及虛擬私有網路（VPN）加密技術協定 K20網路通訊安全監控技術 K21路由通訊協定	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

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）
			P2.3.5以動態虛擬通道介面（DVTI）建置 VPN 伺服器，在虛擬通道介面上建立虛擬存取介面。 P2.3.6建置與驗證 VPN 遠端以便能以路由器及 VPN 軟體用戶端建立站對站連線。 P2.3.7執行群組加密傳輸（GET）VPN 特性來簡化 VPN 的供應與管理。 P2.3.8 製作 VPN 建置與管理文件。		K22NAT 機制、概念與規劃	
T3測試並監控網路安全	T3.1評估網路安全威脅與弱點	O3.1.1網路安全測試結果報告 O3.1.2安全風險建議文件	P3.1.1根據所需的網路伺服器安全層級，評估與回報目前的系統安全，建立測試程序，以確認額外的網路、軟硬體以及系統安全威脅與弱點。 P3.1.2運用已找出之威脅與弱點資訊，確認安全風險。 P3.1.3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	K14網路服務相關技術規劃 K15網路安全相關風險識別 K16網路安全相關防護機制規劃 K23VPN 概念的功能與運作 K24風險分析稽核與滲透測試技術 K25封包分析與安全威脅評估	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修正弱點與威脅		P3.2.1根據安全風險建議文件，執行所需的網路安全等級。 P3.2.2執行安全性驗證。 P3.2.3確保資料完整性與傳輸。	4	K14網路服務相關技術規劃 K15網路安全相關風險識別 K16網路安全相關防護機制規劃 K23VPN 概念的功能與運作 K24風險分析稽核與滲透測試技術 K25封包分析與安全威脅評估	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

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）
						S14網路安全規劃與執行能力
	T3.3確認安全系統的功能與效能	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。 P3.3.2進行功能與效能測試。 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	K14網路服務相關技術規劃 K15網路安全相關風險識別 K16網路安全相關防護機制規劃 K23VPN 概念的功能與運作 K24風險分析稽核與滲透測試技術 K25封包分析與安全威脅評估	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監控與維運系統安全	O3.4.1 系統安全文件	P3.4.1運用第三方監控軟體，設定關鍵安全指標並即時監控網路安全。 P3.4.2運用威脅情報與行為分析技術，主動搜尋潛在進階持續性威脅，並透過機器學習演算法分析安全日誌，識別異常行為模式。 P3.4.3針對發現的威脅事件進行根因分析，建立完整的事件時間軸與影響評估報告。 P3.4.4針對相關配置與設定的變更需求，建立變更程序，並取得適當授權。 P3.4.5實施最小權限原則與即時存取控制，並建立身份治理與管理流程，定期執行存取權限審查與認證。	4	K14網路服務相關技術規劃 K15網路安全相關風險識別 K16網路安全相關防護機制規劃 K23VPN 概念的功能與運作 K24風險分析稽核與滲透測試技術 K25封包分析與安全威脅評估	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）
T4管理網路安全	T4.1分析資訊安全風險	O4.1.1資產清冊與分類表 O4.1.2風險管理計畫	P4.1.1識別內外部威脅來源，評估威脅發生可能性並計算風險值並制定風險處理優先順序。 P4.1.2建立組織資訊資產清冊，進行資訊資產分類與價值評估。 P4.1.3建立風險管理計畫與建立風險紀錄並定期更新風險狀態。 P4.1.4制定風險監控指標與報告機制。	3	K01稽核與滲透測試技術 K26日誌分析技術及組織網路基礎建設 K27已安裝網路基礎建設弱點 K28網路管理與安全流程管制及風險管理計畫與程序 K29外部資訊安全情資 K30 ISO31000風險管理原理及指導綱要 K31 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識別網路安全的威脅		P4.2.1蒐集並分析威脅情報，建立威脅資料庫。 P4.2.2執行攻擊面識別與威脅建模分析 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評估威脅對組織的潛在影響程度。	3	K01稽核與滲透測試技術 K26日誌分析技術及組織網路基礎建設 K27已安裝網路基礎建設弱點 K28網路管理與安全流程管制及風險管理計畫與程序 K29外部資訊安全情資 K30 ISO31000風險管理原理及指導綱要 K31 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）
	T4.3建立安全設計	O4.1.1網路安全政策與程序準則 O4.3.2風險分析評估報告	P4.3.1決定攻擊者情境與威脅。 P4.3.2針對網路元件設計安全性措施。 P4.3.3取得回饋，如有需要應進行調整。 P4.3.4研擬設計網路安全政策與程序準則，包括安全政策、安全程序、安全標準與安全指引等，並確保政策內容具備可操作性與可稽核性。 P4.3.5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。 P4.3.6協調跨部門安全設計整合與溝通，確保所有利害關係人充分理解安全設計的必要性與效益。	3	K01稽核與滲透測試技術 K26日誌分析技術及組織網路基礎建設 K27已安裝網路基礎建設弱點 K28網路管理與安全流程管制及風險管理計畫與程序 K29外部資訊安全情資 K30 ISO31000風險管理原理及指導綱要 K31 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）
	T4.4建立資安事件意外應變措施	O4.4.1處理流程圖及案例說明的事件分類分級作業手冊。 O4.4.2安全事故報告	P4.4.1建立資安事件分類與分級處理機制，結合組織業務特性與風險承受度，分級調整與及應變流程。 P4.4.2制定事件初步分析與影響評估之標準程序，設計隔離、阻斷及修復機制。 P4.4.3依據事件類型與影響程度，執行圍堵措施，進行攻擊路徑分析與影響範圍確認。 P4.4.4執行威脅根除作業包含惡意程式清除、後門移除、弱點修補及配置強化。 P4.4.5制定系統復原優先順序與復原時程規劃，及執行資料復原、系統重建及服務恢復作業，並進行復原後的安全驗證與功能測試。 P4.4.6撰寫資安意外處理執行記錄、復原作業報告及驗證測試文件等安全事故報告。 P4.4.7建立事件後分析與持續改善機制，制定預防性安全措施與監控強化方案。	3	K01稽核與滲透測試技術 K26日誌分析技術及組織網路基礎建設 K27已安裝網路基礎建設弱點 K28網路管理與安全流程管制及風險管理計畫與程序 K29外部資訊安全情資 K30 ISO31000風險管理原理及指導綱要 K31 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。

職能內涵（A=attitude 態度）
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：** • 網路服務，包括 DNS、DHCP、網路、郵件、FTP、SMB、NTP 與代理等。 • 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。 • 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。