網路資訊安全助理職能基準

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
v2	INM3513-006v2	網路資訊安全助理	最新版本	略	2020/12/31
v1	INM3513-006v1	資訊安全助理	歷史版本	已被《INM3513-006v2》取代	2017/12/31

職能基準代碼		INM3513-006v2			
職能基準名稱 (擇一填寫)		**職類**			
		職業	**網路資訊安全助理**		
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		依據組織網路資訊架構之特性與需要，協助配置網路相關安全防護措施、防範因網路入侵所造成相關之資安威脅。			
基準級別		3			

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配置與測試伺服器安全性	T1.1準備網路服務伺服器安全執行	O1.1.1 相關規劃文件與活動執行紀錄	P1.1.1依照場地特定安全要求以及企業職業安全衛生流程與程序準備工作事項。 P1.1.2找出安全危害並在適當人員指導下執行風險管制措施。 P1.1.3與適當人員討論以確保充分協調與現場其他人員之任務。 P1.1.4在執行配置變更前，進行伺服	3	K01稽核與滲透測試技術 K02執行備份與還原的最佳實務程序 K03加密技術 K04錯誤與事件記錄及通報程序 K05入侵偵測與修復程序 K06網路服務安全特性、選	S01溝通協調能力 S02讀寫能力 S03問題解決能力 S04應變管理能力 S05安全警覺性能力 S06研究能力 S07伺服器維護能力

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)
			器備份。		項與限制	
	T1.2依照設計配置網路伺服器安全		P1.2.1配置升級服務以提供最大安全與可靠性的升級。 P1.2.2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。 P1.2.3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。 P1.2.4依照設計要求執行加密。 P1.2.5配置網路連線服務之安全性選項以及遠端存取。 P1.2.6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。 P1.2.7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。 P1.2.8執行備份與復原方法以啟動災害時的還原功能。		K07網路服務漏洞 K08作業系統協助與支援公用程式 K09配置、監控與疑難排除技術 K10安全防護機制 K11安全性威脅與風險 K12伺服器監控與疑難排解工具與技術，包括網路監控與診斷公用程式 K13使用者驗證或目錄服務 K14協助軟、硬體更新	
	T1.3監控與測試網路伺服器安全		P1.3.1依照雙方同意的設計配置測試伺服器以評量網路伺服器安全。 P1.3.2監控伺服器記錄檔、網路流量			

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)
			與開放通訊埠以偵測可能的入侵。 P1.3.3監控重要檔案以偵測未授權的修改。 P1.3.4調查並確認可疑的伺服器或資料安全違規與隱私漏洞。 P1.3.5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。 P1.3.6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。			
T2配置與測試網路解決方案	T2.1配置與測試網路路由通訊協定解決方案	O2.1.1 配置與測試相關文件紀錄	P2.1.1配置與測試路由通訊協定解決方案。 P2.1.2以文件記錄解決方案的路由通訊協定，執行與驗證計畫結果。	3	K15與先進網際路由解決方案相關的寬頻技術 K16整合與統一組織網路的業務佐證 K17新興網路技術安全概念 K18影響網路設計的外部發展或因素 K19IPv4與 IPv6技術與解決方案概念 K20適合網路並可達成可用性與復原的維護與管理	S01溝通協調能力 S07伺服器維護能力 S09分析能力
	T2.2配置與測試以網際網路協定第6版（IPv6）為基礎之網路解決方案	O2.2.1IPv6執行與驗證報告	P2.2.1用 IPv4與 IPv6交互運作 P2.2.2以文件記錄 IPv6執行與驗證計畫的結果。			
	T2.3配置與測試以IPv4或 IPv6為基礎	O2.3.1IPv4或IPv6解決方案	P2.3.1執行並驗證網路的發佈解決方案。			

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)
	之網路再分布解決方案	執行報告	P2.3.2以文件記錄發佈、執行與驗證計畫的結果。 P2.3.3分析執行 IPv4與 IPv6發佈解決方案之間的差異。		工具與實務 K21網路拓撲 K22網路架構解決方案相關的法規、標準與認證 K23適用於複雜網路環境的風險管理策略及實務 K24路由表（routing table）、通訊協定與作業流程 K25組織環境適用之路由技術 K26組織網路安全性 K27網路環境之安全性標準與技術 K28正式或結構化網路管理方法之效益 K29虛擬私有網路（VPN）技術	
	T2.4配置與測試 OSI 第三層路徑控制解決方案		P2.4.1配置並驗證網路的第三層路徑控制。 P2.4.2執行基本遠端工作者與分層服務。 P2.4.3就存取與資料轉移方面評估與比較寬頻技術與 VPN 技術作為安全寬頻網路的解決方案。			
T3配置安全網路環境	T3.1執行網路層安全（包含虛擬化網路架構）	O3.1.1 網路安全防護配置文件	P3.1.1使用路由器作業系統（OS）指令配置以減少第二層攻擊。 P3.1.2在交換器上執行以身分為基礎之網路服務（IBNS）以提供第二層安全。	3	K30進行 VLAN 切換及切換間通訊的規劃、驗證與疑難排除程序 K31佈署方案的重要特點 K32架設與加強防火牆	S01溝通協調能力 S02讀寫能力 S03問題解決能力 S04應變管理能力 S06研究能力

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)
			P3.1.3利用存取控制系統（ACS）做為驗證伺服器執行身分管理。		K33 IOS 與 IP 網路模組 K34區域網路（LAN）以及廣域網路（WAN）執行 K35 NAT 概念與規劃 K36網路拓撲、架構與元件 K37網路標準與協定 K38規劃、驗證與解決路由器作業與路由問題的程序 K39安全連線與遠端存取通訊 K40安全性通訊協定，例如 SSL K41威脅防護策略 K42穿隧協定（tunnel portal） K43 VPN 技術	S10計算能力 S11規劃與組織能力 S12網路工具應用能力
	T3.2配置入侵防禦系統		P3.2.1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之行動處理（EAP）。 P3.2.2配置並確認 IPS 特性以找出威脅，並以動態方式阻止其進入網路。 P3.2.3維持、更新與微調 IPS 簽署。 P3.2.4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）以便動態減少找出的網路威脅。 P3.2.5配置與驗證以區域為基礎之防火牆（ZFW）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。 P3.2.6 評估 NFP 特性與功能性以提供基礎建設保護。 P3.2.7 利用路由器的功能來取得管理平面、資料平面與控制平面。			

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)
	T3.3配置虛擬私有網路（VPN）提供站台對站台以及遠端存取通訊的安全連線	O3.3.1 VPN建置文件	P3.3.1分析並評估網際網路通訊協定安全性（IPSec）與通用路由協議封裝（IPSec/GRE）特性與功能性。 P3.3.2利用憑證授權單位設定站台對站台 VPN 之安全連線。 P3.3.3分析動態多點 VPN（DMVPN）特性與功能性。 P3.3.4配置與驗證網站對網站 VPN 作業之安全連線。 P3.3.5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。 P3.3.6評估 EasyVPN 效益並以動態虛擬通道介面（DVTI）配置 EasyVPN 伺服器在虛擬通道介面上建立虛擬存取介面。 P3.3.7配置與驗證 EasyVPN 遠端以便以路由器及 VPN 軟體用戶端建立站對站連線。 P3.3.8執行群組加密傳輸（GET）VPN 特性來簡化 VPN 的供應			

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)
			與管理。			
T4安裝、配置並測試網路安全	T4.1評估網路安全威脅與弱點以找出風險	O4.1.1 網路安全測試結果報告	P4.1.1根據所需的資產安全層級，評估與回報目前的系統安全。 P4.1.2確認額外的網路、軟硬體以及系統安全威脅與弱點。 P4.1.3運用已找出之威脅與弱點資訊，確認安全風險。 P4.1.4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。	2	K44稽核與滲透測試技術驗證問題 K45客戶業務專業領域，包括客戶組織架構與業務功能性 K46網路技術特性與性能 K47隱私權問題與隱私權法規 K48安全資訊來源 K49風險分析 K50常見 VPN 問題，包括頻寬與動態安全性環境 K51規劃路由器與交換器 K52目前為業界接受之軟硬體安全產品，以及一般特性與能力的廣泛知識 K53 VPN 概念的功能與運作，包括加密、防火牆、封包與驗證 K54網路通訊協定與作業系統 K55有關安全性的組織問題	S01溝通協調能力 S02讀寫能力 S03問題解決能力 S06研究能力 S09分析能力 S10計算能力 S13網路安全執行能力 S14風險管理能力
	T4.2針對找出的弱點與威脅執行反制措施		P4.2.1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。 P4.2.2評估與執行最佳實務伺服器與網路強化技術及措施。 P4.2.3執行安全性驗證與使用者帳號管制。 P4.2.4確保資料完整性與傳輸。			
	T4.3測試與確認執行之安全系統的功能性與效能	O4.3.1系統設定文件檔	P4.3.1根據指標設計測試項目，以確認關鍵性功能與效能措施。 P4.3.2進行功能與效能測試並記錄結果。 P4.3.3依照需要修改安全系統並除			

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)
			錯。 P4.3.4研擬目前系統設定的文件與檔案以供將來參考。		K56安全性周邊網路與其功能 K57安全性通訊協定、標準與資料加密 K58安全威脅，包括竊聽、資料攔截、資料損毀與資料假造 K59 VPN 種類與相關系統程序【註1】 K60 惡意程式偵測（含蠕蟲）	
	T4.4提供系統進行安全監控與維運	O4.4.1 系統維運軌跡或紀錄	P4.4.1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。 P4.4.2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。 P4.4.3執行抽查與稽核，以確保程序不被跳過。 P4.4.4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。			
T5管理網路安全	T5.1定義設計安全的流程		P5.1.1定義網路安全設計的規劃階段。 P5.1.2定義網路安全設計的建置階段。 P5.1.3定義網路安全設計的管理階段。	3	K61稽核與滲透測試技術 K62日誌分析技術組織網路基礎建設 K63已安裝之網路基礎建設的相關弱點 K64安全技術 K65軟硬體解決方案 K66新興安全問題 K67新興安全政策的一般性	S01溝通協調能力 S02讀寫能力 S03問題解決能力 S09分析能力 S11規劃與組織能力 S14風險管理能力
	T5.2找出網路安全的威脅		P5.2.1確認為何會出現攻擊。 P5.2.2確定攻擊來自於誰。 P5.2.3分析常見網路漏洞種類。			

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)
			P5.2.4確認攻擊發生方式。 P5.2.5設計威脅模型以便將威脅分類。		特性，並強調安全程序 K68網路管理與安全流程管制 K69網路安全執行風險管理計畫與程序	
	T5.3分析安全風險	O5.3.1風險管理計畫	P5.3.1決定風險管理的工作要素。 P5.3.2決定需要保護的資產。 P5.3.3分類資產並計算其對組織的價值。 P5.3.4建立風險管理計畫。			
	T5.4建立安全設計	O5.4.1安全性原則	P5.4.1決定攻擊者情境與威脅。 P5.4.2針對網路元件設計安全性措施。 P5.4.3取得回饋，如有需要應進行調整。 P5.4.4研擬安全性原則。			
	T5.5設計與執行安全意外的應變	O5.5.1安全事故報告	P5.5.1設計稽核與事故應變程序。 P5.5.2記錄安全事故。 P5.5.3執行與事故應變程序設計一致的規劃。 P5.5.4測試與簽核。			

職能內涵（A=attitude 態度）

職能內涵（A=attitude 態度）
A01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。 A02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。 A03應對不明狀況：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，完成任務。 A04自我提升：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。

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1年以上資訊相關工作經驗。 ● 本文件內容所提之「客戶」一詞，係指接受網路專業服務之組織。 ● 【註1】相關系統程序：指網站對網站、使用者對網站網際網路流量與外部網路相關的系統與程序，包含稽核與侵入偵測系統稽核與滲透策略技術、加密技術、LAN、WLAN 與 WAN、屏障式子網、傳輸控制協定或網際網路協定（TCP / IP）與應用程式...等。