資訊安全人員職能基準

職能基準代碼		INM3513-001			
職能基準名稱 (擇一填寫)		**職類**			
		職業	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		依據網際網路資訊系統之特性與需要，設計網路安全系統與防火牆、防範電腦病毒、偵錯、測試及安裝等工作。			
基準級別		4			

工作任務	工作活動	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、配置與測試進階伺服器安全性	T1.1 依照業務需求規劃進階網路伺服器安全	O1.1.1 網路安全解決方案 O1.1.2 伺服器安全設計文件	P1.1.1 與客戶及關鍵利害關係人討論以找出進階網路伺服器環境中的安全要求 P1.1.2 分析與檢討現有用戶端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 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	4	K1 稽核與滲透測試技術 K2 執行備份與還原的最佳實務程序 K3 加密技術 K4 錯誤與事件記錄及通報程序 K5 入侵偵測與修復程序 K6 網路服務規劃，包括DNS、DHCP、網路、郵件、FTP、SMB、NTP與代理 K7 網路服務安全特性、選項與限制	S1 與內外部人員連繫安全相關事務的溝通技能 S2 讀寫技能： ■ 解讀技術文件 ■ 依照規定格式撰寫報告 ■ 閱讀與解讀企業安全程序、政策與規格 ■ 檢視廠商網站、公告與注意事項是否有相關安全性資訊 S3 規劃與組織技能： ■ 規劃網路服務安全性與驗證的管制方法 ■ 規劃、排定優先順序與監控自

工作任務	工作活動	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)
			核		K8 網路服務漏洞 K9 作業系統協助與支援公用程式 K10 規劃、配置、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 伺服器防火牆規劃 K14 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 K15 使用者驗證與目錄服務	身工作 S4 問題解決與應變管理技能： ■ 採用符合網路服務安全性要求之程序，並根據不同的營運緊急情況、風險狀況與環境重新規劃 ■ 偵測與調查安全漏洞並從中修復 S5 安全警覺性技能： ■ 應用預防措施與所需的行動以減少、控制或消弭工作活動中可能存在的危害 ■ 遵循企業職業安全衛生程序 ■ 以系統性方式作業並隨時注意各項細節，以免造成自身或他人受傷或財物或設備損壞 S6 查詢廠商資料庫與網站建置不同組態需求以符合安全性層級的研究技能 S7 技術技能： ■ 設計網路服務與驗證安全性 ■ 針對特定客戶伺服器安全性
	T1.2 準備網路伺服器安全執行		P1.2.1 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 P1.2.2 找出安全危害並在適當人員指導下執行風險管制措施 P1.2.3 與適當人員討論以確保充分協調與現場其他人員之任務 P1.2.4 在執行配置變更前，進行伺服器備份			
	T1.3 依照設計配置進階網路伺服器安全		P1.3.1 配置升級服務以提供最大安全與可靠性的升級 P1.3.2 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 P1.3.3 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 P1.3.4 依照設計要求執行加密			

工作任務	工作活動	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)
			P1.3.5 配置進階網路連線服務之安全性選項以及遠端存取 P1.3.6 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 P1.3.7 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			要求找出技術要求、限制與可管理性問題 ■ 執行安全性策略 ■ 安裝網路服務與驗證安全性設計 ■ 監控記錄檔以確認安全資訊 ■ 選擇與使用伺服器與網路診斷 ■ 測試伺服器安全性

工作任務	工作活動	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)
	T1.4 監控與測試網路伺服器安全		P1.4.1 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 P1.4.2 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			
T2 規劃、配置與測試網路解決方案	T2.1 規劃、配置與測試網路路由通訊協定解決方案		P2.1.1 決定在網路上執行距離向量路由協定解決方案、多區域鏈結狀態路由協定解決方案與外部路由協定解決方案所需之網路資源 P2.1.2 製作各路由解決方案的協定、執行計畫與驗證計畫 P2.1.3 配置與測試路由通訊協定解決	4	K16 與先進網際路由解決方案相關的寬頻技術 K17 整合與統一企業網路的業務佐證 K18 新興的可行業務與社會技術 K19 會影響網路設計的外部發展或因素	S8 找出網路運作相關之功能性、效能與管理特點的分析技能 S9 溝通技能： ■ 以技術性方式與簡單語言傳達複雜概念與問題 ■ 與各種用戶端連繫 S10 讀寫技能： ■ 研擬並準備作業文件，例如政

工作任務	工作活動	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)
			方案 P2.1.4 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		K20 IPv4 與 IPv6 技術與解決方案 K21 適合網路並可達成可用性與回復力的維護與管理工具與實務 K22 網路拓撲 K23 與進階網際路由解決方案相關的法規、標準與認證 K24 適用於複雜網路環境的風險管理策略及實務 K25 路由表、通訊協定與作業流程 K26 企業環境適用之路由技術 K27 企業網路安全性 K28 網路環境之安全性標準與技術 K29 正式或結構化網路管理方法之效益 K30 虛擬私有網路(VPN)技術	策與程序以及技術與管理報告 ■ 解讀與準備技術文件 ■ 準備專案管理文件 S11 進行複雜與動態環境風險管理的規劃與組織技能 S12 適合高難度服務等級之複雜與動態環境的問題解決技能 S13 技術技能： ■ 依照業界標準與最佳實務設計、執行與維運複雜網路 ■ 找出可行的互補與新興技術
	T2.2 規劃、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 決定在網路上執行 IPv6 所需的網路資源 P2.2.2 針對以 IPv6 為基礎之網路解決方案建立執行計畫與驗證計畫 P2.2.3 用 IPv4 配置 IPv6 選路與 IPv6 交互運作 P2.2.4 驗證與測試 IPv6 解決方案，如有需要進行修改 P2.2.5 以文件記錄 IPv6 執行與驗證計畫的結果			
	T2.3 規劃、配置與測試以 IPv4 或 IPv6 為基礎之網路再分布解決方案	O2.3.1IPv4 或 IPv6 解決方案執行報告	P2.3.1 根據網路發佈分析建立一套 IPv4 或 IPv6 發佈執行計畫與驗證計畫 P2.3.2 規劃並驗證網路的發佈解決方案 P2.3.3 以文件記錄發佈、執行與驗證計畫的結果 P2.3.4 分析執行 IPv4 與 IPv6 發佈解決方案之間的差異			
	T2.4 規劃、配置與		P2.4.1 根據網路再分布分析結果建立			

工作任務	工作活動	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)
	測試第三層路徑控制解決方案		一套第三層路徑，控制執行計畫與驗證計畫 P2.4.2 配置並驗證網路的第三層路徑控制 P2.4.3 執行基本遠端工作者與分層服務 P2.4.4 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 執行第二層安全		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 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	3	K31 進行以下項目的規劃、驗證與疑難排除程序： ■ VLAN 切換 ■ 切換間通訊 K32 佈署方案的重要特點 K33 架設與加強防火牆 K34 IOS 與 IP 網路模組 K35 區域網路(LAN)以及廣域網路(WAN)執行 K36 NAT 概念與規劃 K37 網路拓撲、架構與元件 K38 網路標準與協定 K39 規劃、驗證與解決路由	S14 與內外部人員連繫技術、營運與業務相關事務的溝通技能 S15 讀寫技能： ■ 解讀技術文件 ■ 依照需要撰寫報告 S16 計算技能： ■ 評估網路效能與可交互運作性 ■ 解讀結果 ■ 進行測試測量 S17 規劃與組織技能： ■ 與其他人連繫協調流程 ■ 規劃、排定優先順序與監控自身工作
	T3.2 配置路由器 OS 入侵防禦系統(OS-IPS)以減輕網路資源威脅		P3.2.1 評估路由器 OS-IPS 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			

工作任務	工作活動	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 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		器作業與路由問題的程序 K40 安全連線與遠端存取通訊 K41 安全性通訊協定，例如 SSL K42 威脅防護策略 K43 穿隧協定 K44 VPN 技術	S18 問題解決與應變管理技能： ■ 依照網路要求採用規劃程序 ■ 依照不同的營運緊急情況、風險狀況與環境重新規劃 ■ 解決網路安全問題 S19 研究符合要求之適當硬體的研究技能 S20 技術技能： ■ 評量與執行安全要求 ■ 選擇與規劃網路裝置 ■ 使用網路工具
	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		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			

工作任務	工作活動	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)
			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 的供應與管理			
	T3.4 執行基礎網路保護(NFP)		P3.4.1 評估 NFP 特性與功能性以提供基礎建設保護 P3.4.2 利用路由器的 OS 功能來取得管理平面、資料平面與控制平面			
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		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	K45 驗證問題 K46 客戶業務專業領域，包括客戶組織架構與業務功能性 K47 網路技術特性與性能 K48 隱私權問題與隱私權法規 K49 安全資訊來源 K50 風險分析	S21 分析技能： ■ 分析系統評估 ■ 查閱系統的安全性記錄檔以找出漏洞 S22 與用戶端連繫的溝通技能 S23 依照組織安全性原則撰寫系統安全評估報告的讀寫技能 S24 進行成本效益比較的計算技能 S25 問題解決技能：

工作任務	工作活動	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)
	T4.2 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		K51 常見 VPN 問題，包括頻寬與動態安全性環境 K52 規劃路由器與交換器 K53 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 K54 VPN 概念的功能與運作，包括加密、防火牆、封包與驗證 K55 網路通訊協定與作業系統 K56 有關安全性的組織問題 K57 安全性周邊網路與其功能 K58 安全性通訊協定、標準與資料加密 K59 安全威脅，包括竊聽、資料攔截、資料損毀與資料假造 K60 VPN 種類，包括網站對	■ 判斷入侵偵測 ■ 疑難排除與除錯 S26 找出與分析網路安全性方法與技術的研究技能 S27 技術技能： ■ 研擬企業政策、策略與程序 ■ 執行區域網路(LAN)、廣域網路 (WAN) 、虛擬私有網路 (VPN) 及無線區域網路 (WLAN)解決方案 ■ 執行安全策略並規劃網路安全軟硬體 ■ 安裝提升網路安全性相關的軟硬體 ■ 進行網路安全性風險評估
	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錯 P4.3.4 研擬目前系統設定的文件與檔案以供將來參考			
	T4.4 提供系統進行安全監控與維運		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			

工作任務	工作活動	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)
			脅弱點與風險，向適當人員簡報以取得變更許可		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： ■ 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 ■ 病毒偵測軟體之使用	
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 軟硬體解決方案的能	S28 分析技能： ■ 分析網路資訊 ■ 規劃技術問題或管理要求的解決方法 S29 溝通技能： ■ 傳達並釐清複雜資訊 ■ 與客戶連繫
	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 P5.2.4 確認攻擊發生方式			

工作任務	工作活動	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)
			P5.2.5 設計威脅模型以便將威脅分類		力 K66 新興安全問題 K67 新興安全政策的一般性特性，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	S30 解讀與準備技術文件的讀寫技能，包括紀錄安全事故與研擬安全政策 S31 規劃管理系統安全管制方法的規劃技能 S32 問題解決技能： ■ 在複雜網路上應用解決方案，包括系統流程 ■ 快速佈署有關失效與安全事故問題的解決方案 S33 在系統安全方法與技術上應用最佳實務的技術技能
	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 P55.4 測試與簽核			
T6 規劃、管理與執行疑難排除	T6.1 規劃疑難排除與監控進階整合 IP 網路效能的策略		P6.1.1 研擬一套監控與管理 IP 網路的計畫以便將網路的效能與可靠性最佳化 P6.1.2 針對疑難排除程序規劃網路區塊的隔離 P6.1.3 規劃網路基礎建設的測試步驟與情境	3	K70 進階網路解決方案 K71 進行以下項目的規劃、驗證與疑難排除程序： ■ 路由器作業與路由 ■ VLAN 切換與切換間通訊	S34 與內部與/或外部人員連繫技術、營運與業務相關事務的溝通技能 S35 讀寫技能： ■ 解讀技術文件 ■ 依照需要撰寫報告 S36 計算技能： ■ 進行測試測量與解讀結果

工作任務	工作活動	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)
			P6.1.4 選擇適當的網路測試與監控工具與應用軟體以配合特定的網路疑難排除與監控步驟		K72 佈署方案 K73 IOS 與 IP 網路模型 K74 IOS 服務 K75 IP 網路拓撲、架構與工作要素 K76 網路標準與協定 K77 威脅減輕策略 K78 VLAN 技術	■ 評估網路效能與可交互運作性 S37 規劃與組織技能： ■ 與其他人連繫協調流程 ■ 規劃、排定優先順序與監控自身工作 S38 問題解決與應變管理技能： ■ 依照網路要求採用規劃程序 ■ 依照不同的營運緊急情況、風險狀況與環境重新規劃 ■ 解決 WLAN 問題並除錯 S39 研究符合要求之適當硬體的研究技能 S40 技術技能： ■ 選擇與規劃網路裝置並評量與執行安全要求 ■ 使用網路連線與網路測試及管理工具
	T6.2 管理與監控企業網路的疑難排除策略		P6.2.1 管理與監控網路監控結構的策略 P6.2.2 建立一套例行性網路作業系統(IOS)裝置維護計畫以納入路由協定及路由器規劃的監控 P6.2.3 在適當的開放系統連結(OSI)模型層將未最佳化的網際作業隔離 P6.2.4 建立一套計畫來為任務關鍵應用程式解決並監控 IOS 服務相關安全問題 P6.2.5 建立一套計畫來解決並監控網際網路協定第 6 版(IPv6)與第 4 版(IPv4)可交互運作性的問題			
	T6.3 執行進階網路解決方案的測試計畫		P6.3.1 針對以虛擬區域網路(VLAN)為基礎的解決方案測試交換器對交換器連線、存取埠以及迴圈預防 P6.3.2 測試私有 VLAN P6.3.3 測試交換器虛擬介面(SVI)			

工作任務	工作活動	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)
			P6.3.4 測試進階服務的交換器支援 P6.3.5 排除交換器規劃的問題			
T7 評估安全風險管理選項	T7.1 確認安全風險		P7.1.1 確認並遵守法律與組織要求中針對評量活動的適用條款以及相關標準 P7.1.2 根據針對客戶作業環境與核心業務作業，決定安全風險的種類與本質 P7.1.3 依照風險程度將安全風險排名，並將風險連結到潛在的適當處理選項 P7.1.4 評量現有與有效資料來決定風險程度	4	K79 適用的國家標準、業界實務守則與法案，包括職業安全衛生法規 K80 保險方面有關可接受之風險、保費範圍與法律責任等的基本了解 K81 客戶作業環境與業務營運 K82 整合安全措施之概念，包括實體安全、資訊科技安全以及人員與資訊安全 K83 訴訟概念 K84 現有安全系統與技術方面可用的專業知識 K85 資訊與情報的區別 K86 文件與簡報程序的準備 K87 基本統計與計算的原則 K88 有效溝通原則	S41 精確確認找出的風險與威脅 S42 在評估流程中應用推理與邏輯分析 S43 評估風險與威脅 S44 以教導與指導方式提供同事支援彙整數值資料 S45 以清楚且簡明扼要的方式溝通 S46 依照安全風險決定處理選項的適當性 S47 決定安全風險的種類與本質 S48 找出與評估資產 S49 準備與呈現口頭與書面報告 S50 排定任務的優先順序並排定期程 S51 依照安全風險程度排定處理選項的優先順序 S52 依照彙整報告與總結資訊所需之標準提供書面通訊 S53 將不同社會文化背景的人員與各種生理與心理能力者進行連結 S54 研究與分析資訊 S55 取得並存取資訊
	T7.2 找出並評估處理選項		P7.2.1 找出並確認符合定義之風險種類、本質與原因的處理選項 P7.2.2 依照文件記錄與可驗證之證據，研究並評估應用於類似背景處理選項的有效性 P7.2.3 確認處理選項之風險評估指標和業界實務及相關標準一致 P7.2.4 根據建立之標準，挑選適合全部潛在安全風險之處理選項，並排定優先順序			

工作任務	工作活動	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)
	T7.3 檢視與呈現發現	O7.3.1 網路安全風險管理報告	P7.3.1 準備說明評估之發現與建議處理選項的報告，並向相關人員簡報 P7.3.2 分析與建議須明確、具有關聯性，與參考條件一致且有可驗證之證據支持 P7.3.3 分析中須包含有說明不執行建議處理選項時，可能會發生之後果的建議 P7.3.4 採用有效人際技巧與簡報程序來加強對建議處理選項的了解與接受度		K89 AS/NZS 4360: 2004 風險管理的原則與相關指南 K90 隱私與機密性要求 K91 相關業界實務守則 K92 相關法律與規範，包括證照要求 K93 風險評量技巧 K94 適用於適合界限與業務之安全與威脅範圍的處理選項種類	S56 使用各種問題解決技術 S57 使用業務與資訊科技
T8 準備安全風險管理計畫	T8.1 評估安全風險		P8.1.1 找出並遵守有關風險評量活動之法律與組織要求之適用條款以及相關標準 P8.1.2 明確區分並確認可接受與不可接受的風險 P8.1.3 強調並詳述高優先順序的風險以確保適當管制措施的開發 P8.1.4 評估現有管制措施以確認對風	4	K95 適用之職業安全衛生證照與法律符合性要求 K96 控制層級之應用 K97 認可的通訊術語及口號 K98 可用支援單位與提供的服務種類	S58 存取與使用工作場域資訊 S59 主動聆聽 S60 在各種情況下轉變個人溝通風格 S61 分析與評估資訊與資料 S62 以教導與指導之方式提供同事支援彙整數值資料 S63 以清楚且簡明扼要的方式溝通 S64 設計處理選項與測試

工作任務	工作活動	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)
			險發生的影響，並找出所需的修改		K99 統計分析的基本方法與統計資料的呈現 K100 正面與負面語言之間的差異 K101 書寫與口說英語之間的差異 K102 如何讀取與使用肢體語言取得他人的信任 K103 如何紀錄可作為法律用途的資訊 K104 如何保護機密資訊 K105 如何使用業務設備呈現資訊 K106 談判技巧 K107 書面資訊呈現與保存	S65 談判 S66 計算資源與成本的計算技能 S67 規劃 S68 解讀複雜資訊的閱讀技能 S69 將不同社會文化背景的人員與各種生理與心理能力進行連結 S70 解決問題以處理複雜且非例行性的困難 S71 利用科技來研究、分析與回報資訊 S72 研擬複雜報告的寫作技能
	T8.2 研擬行動計畫	O8.2.1 行動計畫	P8.2.1 研擬行動計畫找出關鍵任務、活動與資源以達成安全風險管理的目標 P8.2.2 找出與安全背景相關的風險種類並將適當管制措施整合至規劃流程中 P8.2.3 建立維持現行行動計畫的溝通與通報安排 P8.2.4 研擬行動的應變安排並將之整合至計畫中			

工作任務	工作活動	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)
	T8.3 設計處理選項		P8.3.1 監控作業環境以確認潛在與實際風險、威脅及所需之處理 P8.3.2 依照可用的組織實務選擇處理選項，研究與釐清其意涵並交由相關人員認可 P8.3.3 以文件記錄可行之處理選項並估計其成本，以確保與風險本質及客戶要求兩者的相容性 P8.3.4 將處理選項連結到整個或部分安全風險，並與客戶確認安全背景的適當性 P8.3.5 進行處理選項的測試以決定現場的適用性，並將結果進行統計分析以確認處理的效果		相關的職業標準 K108 AS/NZS 4360: 2004 風險管理的原則 K109 風險管理原則與實務 K110 安全設備或系統的資源供應 K111 戰術性應變措施 K112 武力使用指南	

工作任務	工作活動	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)
	T8.4 研擬安全風險管理計畫	O8.4.1 安全管理計畫	P8.4.1 找出管理要求並納入安全風險管理計畫的研擬中 P8.4.2 研擬安全風險管理活動的監控與檢討程序以確保持續改善 P8.4.3 依照適當格式與相關標準研擬整合所有相關資訊之安全風險管理計畫 P8.4.4 依照組織程序完成計畫並向客戶簡報以便其審核與認可			

工作任務	工作活動	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)
T9 執行安全風險管理計畫	T9.1 組織功能與任務		P9.1.1 找出並遵守有關風險評量活動之法律與組織要求之適用條款以及相關標準 P9.1.2 明確定義與安全風險管理計畫執行相關的角色與責任，並與適當人員連結 P9.1.3 將活動與目標與達成專案行動計劃里程碑和結果進行連結 P9.1.4 資源、設備與素材用以協助計畫執行須符合專案目的，並可在特定時間表內取得 P9.1.5 利用建立好的溝通管道精確且即時傳遞與計畫執行相關之資訊 P9.1.6 依照客戶與組織要求確認並維持機密性要求	5	K113 具備使用專案管理軟體的能力 K114 整合安全措施之概念，包括實體安全、資訊科技安全以及人員與資訊安全 K115 現有安全系統與技術方面可用的專業知識 K116 作業環境與業務營運 K117 文件程序的準備 K118 有效溝通原則 K119 AS/NZS 4360: 2004 風險管理的原則與相關指南 K120 隱私與機密性要求 K121 安全風險管理流程 K122 相關法律與法規，包括證照要求 K123 風險評量技巧與流程 K124 安全設備或系統的資源供應 K125 適用於適合界限與業務之安全與威脅範圍	S73 分配工作任務與功能 S74 以教導與指導之方式提供同事支援 S75 彙整與分析數值資料 S76 以清楚且簡明扼要的方式溝通 S77 指派角色與責任 S78 依照安全風險決定處理選項的適當性 S79 決定安全風險與威脅的種類與本質 S80 管理專案 S81 監控執行程序 S82 監控風險背景並找出對資產的新興風險或威脅 S83 準備與進行口頭與書面報告 S84 排定任務的優先順序並排定期程 S85 依照安全風險程度排定處理選項的優先順序 S86 依照彙整報告與總結資訊所需之標準提供書面資訊 S87 將不同社會文化背景的人員與各種生理與心理能力進行連結 S88 研究與分析資料與資訊
	T9.2 監控風險背景		P9.2.1 監控並評量對資產的新興風險或威脅，以維持執行中安全風險處理選項的適當性 P9.2.2 監控作業環境的變更，並依照需要將決定修正措施，整合到計畫中 P9.2.3 根據相關標準定期檢討與評估			

工作任務	工作活動	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)
			目標與結果以確保專案目的的達成 P9.2.4 精確且完整記錄風險的存在與發生，作為提供評量種類、本質與原因之依據 P9.2.5 精確記錄應變與修正措施之應用		的處理選項種類	S89 總結資訊 S90 使用各種問題解決技術 S91 使用業務設備與科技
	T9.3 檢討處理選項的效果		P9.3.1 計算長短期選項的成本確保將精確估計的資源分配好以支援計畫 P9.3.2 監控處理選項與風險事故之間的差異並透過計畫的適當修改來解決 P9.3.3 確認執行的各階段並協調資源與選項以確保可取得與可用性 P9.3.4 研擬與測試修正措施並將其納入風險管理計畫 P9.3.5 尋求有關處理選項效果的回饋並提供給適當人員			

職能內涵（A=attitude 態度）
A03 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。
A05 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。
A07 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。
A08 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。
A12 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。

說明與補充事項
● 此項職能基準乃參考國外職能資料發展並經國內專家本土化及檢視完成。 ● 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。 ● 基準更新紀錄 • 因應 2017/05/25 公告職能基準品質認證作業規範修訂版，將原「入門水準」內容移至「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】。