

資訊安全工程師職能基準

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	INM2529-001v3	資訊安全工程師	最新版本	略。	2024/12/31
V2	INM2529-001v2	資訊安全工程師	歷史版本	已被《INM2529-001v3》取代	2021/01/18
V1	INM2529-001v1	資訊安全工程師	歷史版本	已被《INM2529-001v2》取代	2019/03/07

職能基準代碼		INM2529-001v3			
職能基準名稱 (擇一填寫)		職類			
		職業	資訊安全工程師		
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	其他資料庫及網路專業人員	職業別代碼	2529	
	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	J62	
工作描述		具備相關資訊安全知識，藉由組織內部能力或尋求外部廠商、專家協助，建立符合法規與組織安全需求之資訊安全管理系統，並執行相關維運作業與協助其他單位執行資訊安全相關活動			
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 資訊安全管理系統維運	T1.1 資訊安全管理系統維運	O1.1.1 資訊安全管理系統文	P1.1.1 依據資訊安全管理系統觀念知識，撰寫管理系統文件，並協助相關紀錄產出與留存。	3	K01機密性、完整性、可用性 K02可歸責性、不可否認性、鑑別、可靠度	S01 文件撰寫能力 S02 應變管理能力 S03 系統建置與維運能力

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)
		件 O1.1.2 資訊安全管理系統維運紀錄			K03戴明循環 (Deming Cycle) Plan-Do-Check-Act, PDCA K04最小權限 (Least Privilege) K05職務區隔 (Segregation Of Duties, SOD) K22相關法規、主管機關要求 K23合約要求、業務需求 K96稽核	S04 系統安全規劃與執行能力 S07 評估與分析能力 S08 問題解決能力 S09 組織與規劃能力 S10 監督執行能力 S11 溝通協調能力 S14 文件閱讀與理解能力
T2 資產與風險管理	T2.1 建立資產清冊	O2.1.1 資產清冊	P2.1.1協助各資產負責人盤點並建立資產清冊。	3	K06資產分類 K07資產盤點	S01 文件撰寫能力 S05 資產分類與盤點能力 S10 監督執行能力 S11 溝通協調能力
	T2.2 風險識別、分析與評估	O2.2.1 可接受風險判定準則 O2.2.2 風險識別、分析與評估報告	P2.2.1參與可接受風險等級判定準則之討論。 P2.2.2協助各單位進行風險分析與評估並產製報告。	4	K08可接受風險 K22相關法規、主管機關要求 K23合約要求、業務需求 K36威脅、脆弱性 K87風險評估	S01 文件撰寫能力 S06 風險識別能力 S07 評估與分析能力 S11 溝通協調能力 S14 文件閱讀與理解能力
	T2.3 風險處理	O2.3.1 風險清單	P2.3.1協助識別不可接受風險項目。 P2.3.2協助風險高於可接受等級項目之權責單位。	4	K09剩餘風險 K10風險處理方式	S01 文件撰寫能力 S02 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)
		O2.3.2 風險處理計畫	<p>擬定風險處理計畫。</p> <p>P2.3.3協助確認風險處理計畫執行之有效性，以確認是否如預期之降低風險值。</p> <p>P2.3.4協助需進行風險處理單位，針對高於可接受風險項目，提出風險處理計畫。</p> <p>P2.3.5協助確認風險處理計畫實際執行之有效性。</p>		<p>K64監控與通報</p> <p>K77補償措施</p> <p>K82根因分析</p> <p>K100資安作業相關安全知識</p>	<p>S08 問題解決能力</p> <p>S09 組織與規劃能力</p> <p>S10 監督執行能力</p> <p>S11 溝通協調能力</p>
T3資訊安全系統防護架構規劃	T3.1 網路安全管控規劃	<p>O3.1.1 網路架構圖</p> <p>O3.1.2 網路安全設備規格文件</p> <p>O3.1.3 網路安全解決方案</p> <p>O3.1.4 VPN 網路解決方案</p>	<p>P3.1.1協助與網路管理人員，確認網路安全需求。</p> <p>P3.1.2協助網路管理單位，依據網路安全需求，設計安全網路架構。</p> <p>P3.1.3 依網路安全規範，規劃網路區隔與路由，並依需求選擇適當網路設備。</p> <p>P3.1.4 依網路安全規範，規劃不同區域的 VPN 連網架構及遠距作業模式。</p>	5	<p>K11網路拓樸 (Topology)</p> <p>K12 Transmission Control Protocol / Internet Protocol (TCP/IP)</p> <p>K13網路路由 (Network Routing)</p> <p>K14網路通訊協定與服務 (Network Protocol / Service)</p> <p>K15網路與系統弱點</p> <p>K16攻擊手法與防禦</p> <p>K22相關法規、主管機關要求</p> <p>K23合約要求、業務需求</p> <p>K44無線網路安全性</p> <p>K58了解網路、系統、設備事件意義</p>	<p>S01 文件撰寫能力</p> <p>S02 應變管理能力</p> <p>S08 問題解決能力</p> <p>S09 組織與規劃能力</p> <p>S10 監督執行能力</p> <p>S11 溝通協調能力</p> <p>S12 網路安全規劃與執行能力</p> <p>S13 安全警覺性能力</p>

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)
					K64監控與通報 K88緊急應變 K89營運持續作業方式 K90系統、網路還原與處置 K100資安作業相關安全知識	
	T3.2 系統安全管控規劃	O3.2.1 系統安全組態設定規範 O3.2.2 系統安全架構規劃 O3.2.3 系統安全解決方案 O3.2.4 系統備援解決方案 O3.2.5 遠距辦公安全解決方	P3.2.1協助系統管理人員，確認系統安全需求。 P3.2.2協助系統管理單位，依據系統安全需求，設計足夠之安全系統組態與架構。 P3.2.3 依需求選擇適當之資料、作業系統與服務(含應用程式)。 P3.2.4 依作業環境需求規劃設備與系統備援。	5	K15網路與系統弱點 K16攻擊手法與防禦 K17作業系統原理 K18資料庫原理 K19服務系統(郵件、File Transfer Protocol、網站等) K22相關法規、主管機關要求 K23合約要求、業務需求 K40弱點、漏洞之修補 K43原始碼弱點、漏洞之修補 K57系統、網路、資安與終端稽核日誌設定 K58了解網路、系統、設備事件意義 K59日誌保護機制(如：防竄改方式)	S02 應變管理能力 S03 系統建置與維運能力 S04 系統安全規劃與執行能力 S08 問題解決能力 S09 組織與規劃能力 S10 監督執行能力 S11 溝通協調能力 S13 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)
		案			K61SOC/日誌收容系統建置 K62SOC/日誌收容系統維運 K63關聯分析 K64監控與通報 K65 時間同步協定 (Network Time Protocol, NTP) K85備援機制 (含異地備援與同步) K86營運衝擊分析 K88緊急應變 K89營運持續作業方式 K90系統、網路還原與處置 K100資安作業相關安全知識 K102遠端存取及資料安全	
	T3.3 資安架構規劃	O3.3.1 網路端資安防護架構 O3.3.2 主機端資安防護架構 O3.3.3 終	P3.3.1與相關人員討論以找出網路、主機、終端設備之安全需求。 P3.3.2依據安全需求，選擇與建置合適之資安防護設備。 P3.3.3 依據安全需求，建立網路隔離規劃。 P3.3.4 依資安架構規範，規劃與配置防火牆、入侵偵測/防禦系統及惡意攻擊防護機制。	5	K11網路拓樸 (Topology) K12 Transmission Control Protocol / Internet Protocol (TCP/IP) K13網路路由 (Network Routing)	S02 應變管理能力 S04 系統安全規劃與執行能力 S08 問題解決能力 S09 組織與規劃能力 S10 監督執行能力 S11 溝通協調能力 S12 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)
		端資安防護架構	<p>P3.3.5 依據安全需求，進行多層次防禦規劃、縱深管理。</p> <p>P3.3.6 依據安全需求選擇並執行身份鑑別、裝置鑑別及微分割解決方案</p>		<p>K14網路通訊協定與服務 (Network Protocol / Service)</p> <p>K15網路與系統弱點</p> <p>K16攻擊手法與防禦</p> <p>K17作業系統原理</p> <p>K18資料庫原理</p> <p>K19服務系統 (郵件、File Transfer Protocol、網站等)</p> <p>K22相關法規、主管機關要求</p> <p>K23合約要求、業務需求</p> <p>K58了解網路、系統、設備事件意義</p> <p>K64監控與通報</p> <p>K66雲端運算架構框架</p> <p>K67雲端資料安全</p> <p>K71雲端應用程式安全</p> <p>K88緊急應變</p> <p>K89營運持續作業方式</p> <p>K90系統、網路還原與處置</p> <p>K100資安作業相關安全知識</p> <p>K102遠端存取及資料安全</p> <p>K103零信任框架及原則</p>	S13 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)
T4 系統、 網路維運	T4.1 身分 認證與存 取控制	O4.1.1 身 分認證管 理制度 O4.1.2 權 限控管機 制	P4.1.1協助設計使用者可以安全存取到適當的網 路、系統、終端設備之認證程序。 P4.1.2協助擬定權限 (含實體管控、系統、網路、 資料庫、終端、資安設備等) 之變更管理 流程。 P4.1.3協助各網路、系統、終端設備管理人員，進 行存取權限審查作業。	4	K04最小權限 (Least Privilege) K05職務區隔 (Segregation Of Du-ties, SOD) K20特權管理 K21變更管理 K22相關法規、主管機關要求 K23合約要求、業務需求 K24識別 (Identification)、鑑別 (Authentication) K25識別與存取管理 (Identifica- tion and Access Management, IAM) K26權限審查 K33物聯網身分認證 K64監控與通報 K68雲端身分認證與存取管理 K100資安作業相關安全知識 K104多重要素驗證 (Multi-fac- tor authentication, MFA)	S03 系統建置與維運能力 S04 系統安全規劃與執行能力 S10 監督執行能力 S11 溝通協調能力 S12 網路安全規劃與執行能力 S13 安全警覺性能力
	T4.2 帳號 密碼管理	O4.2.1 帳 號管理程	P4.2.1協助擬定帳號申請/異動、刪除之安全變更 程序。	3	K04最小權限 (Least Privilege) K20特權管理	S01 文件撰寫能力 S03 系統建置與維運能力

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)
		序機制 O4.2.2 密碼管理機制	P4.2.2協助擬定符合需求之密碼原則 (如：強度、長度、複雜度、變更週期、最小重複代數等)。 P4.2.3向使用者宣導密碼強度要求與重要性。 P4.2.4 建置可管理使用者符合密碼原則之管理系統。		K21變更管理 K27密碼複雜度與安全 K64監控與通報 K100資安作業相關安全知識	S04 系統安全規劃與執行能力 S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力
	T4.3 資料傳輸安全與金鑰管理	O4.3.1 資料傳輸安全機制 O4.3.2 金鑰管理機制	P4.3.1協助擬定傳輸之安全要求 (如：加密強度、方式與加密設備之使用規範)。 P4.3.2依需求協助選擇與建立安全通道機制與產品 (如：SSL、VPN)。 P4.3.3依據金鑰管理機制，協助金鑰發放、保管、更新金鑰等事項。	4	K28密碼學 K29金鑰使用與管理 K30安全通道相關知識 K64監控與通報 K100資安作業相關安全知識 K102遠端存取及資料安全	S02 應變管理能力 S03 系統建置與維運能力 S04 系統安全規劃與執行能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力
	T4.4 行動裝置與物聯網安全	O4.4.1 行動裝置安全管控機制 O4.4.2 物聯網安全管控機制	P4.4.1因應行動裝置安全議題、弱點、威脅與攻擊手法，協助建立行動裝置安全管控機制。 P4.4.2 因應物聯網安全議題、弱點、威脅與攻擊手法，協助建立物聯網管控機制。	4	K31行動裝置特性 K32行動裝置弱點與威脅 K33物聯網身分認證 K34物聯網加密技術 K35物聯網弱點與威脅 K64監控與通報 K100資安作業相關安全知識	S02 應變管理能力 S03 系統建置與維運能力 S04 系統安全規劃與執行能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力

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)
					K105 BYOD 與 MDM 相關知識	S13 安全警覺性能力
	T4.5 弱點管理	<p>O4.5.1 弱點掃描與滲透測試分析報表</p> <p>O4.5.2 弱點通報、修補與追蹤紀錄</p> <p>O4.5.3 弱點修補紀錄或補償管控措施</p> <p>O4.5.4 停止支援服務系統清冊</p>	<p>P4.5.1即時蒐集系統、網路、資安設備、終端、資料庫、行動裝置、應用程式等弱點資訊。</p> <p>P4.5.2通報相關使用者、管理員相關資訊。</p> <p>P4.5.3定期執行弱點掃描、滲透測試。</p> <p>P4.5.4協助管理人員修補與追蹤相關弱點，並對無法修補之部分採行必要之補償措施並追蹤執行結果。</p> <p>P4.5.5依據實際現況，建立並更新仍在使用但原廠已停止支援服務系統清冊，監控並執行必要之管理措施。</p>	4	<p>K36威脅、脆弱性</p> <p>K37駭客攻擊手法與對策</p> <p>K38弱點掃描工具使用</p> <p>K39滲透測試之理論、實作與工具使用</p> <p>K40弱點、漏洞之修補</p> <p>K41補償措施之選擇</p> <p>K64監控與通報</p> <p>K100資安作業相關安全知識</p>	<p>S01 文件撰寫能力</p> <p>S02 應變管理能力</p> <p>S07 評估與分析能力</p> <p>S08 問題解決能力</p> <p>S10 監督執行能力</p> <p>S11 溝通協調能力</p> <p>S13 安全警覺性能力</p>
	T4.6 程式碼弱點管理	<p>O4.6.1 程式原始碼掃描紀錄</p> <p>O4.6.2 程</p>	<p>P4.6.1協助選用原始碼掃描工具，執行程式原始碼掃描與產製報表。</p> <p>P4.6.2協助解釋程式原始碼掃描結果與追蹤修改作業，並針對無法修補之弱點與漏洞，提出</p>	4	<p>K41補償措施之選擇</p> <p>K42程式語言概念</p> <p>K43原始碼弱點、漏洞之修補</p> <p>K64監控與通報</p>	<p>S01 文件撰寫能力</p> <p>S02 應變管理能力</p> <p>S07 評估與分析能力</p> <p>S08 問題解決能力</p>

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)
		式碼修補紀錄	適當之補償措施建議。		K100資安作業相關安全知識 K106原始碼掃描方法論 (SCA、DCA)	S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力
	T4.7 無線網路管理 (含：4/5g、藍牙、Wi-Fi、其他專有無線通訊網路)	O4.7.1 無線網路定期掃描與處理紀錄 O4.7.2 系統、終端之無線網路使用檢查紀錄 O4.7.3 無線網路認證與傳輸加密機制之選擇與建立 O4.7.4 無線網路管理措施	P4.7.1定期掃描實體區域、機房、設備之無線網路使用狀況，協助產製紀錄報表。 P4.7.2定期檢查系統、終端是否連接無線網路。 P4.7.3協助擬定無線網路使用之認證方式與傳輸加密強度。 P4.7.4無線傳輸檔案安全性管理機制及處理方式	3	K44無線網路安全性 K45無線網路加密方式 K46無線網路認證方式 K47無線網路掃描工具之使用 K64監控與通報 K100資安作業相關安全知識	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S13 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)
	T4.8 協助備份之執行與有效性確認	O4.8.1 備份執行紀錄 O4.8.2 備份有效性確認紀錄 O4.8.3 異地備份媒體管理紀錄	P4.8.1協助各系統、設備管理人員，選擇合適備份方式及備份失敗之處置。 P4.8.2協助各系統、設備管理人員，建立備份機制。 P4.8.3協助確認備份執行之有效性（如：還原測試或無法直接還原測試時，進行可讀性測試）。 P4.8.4針對異地備份、備援裝置或媒體管理及存取紀錄。	3	K48備份原理 K49備份方式之特性與優缺點 K50備份工具之使用 K51備份還原測試方式之優缺點與風險 K64監控與通報 K100資安作業相關安全知識	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S15資料備份與還原能力
	T4.9 公開資訊與網頁安全	O4.9.1 網頁監控紀錄 O4.9.2 網頁安全定期掃描紀錄 O4.9.3 網頁存取記錄定期分析與稽核	P4.9.1建立網頁監控機制（如：置換與攻擊警告），並持續監控網頁並進行必要處置。 P4.9.2定期網頁弱點掃描並進行必要修補措施。 P4.9.3建立網頁存取記錄稽核機制，並執行必要之分析。	4	K36威脅、脆弱性 K41補償措施之選擇 K52網頁攻擊手法與防禦 K53網頁監控技術 K54網頁弱掃與修補 K64監控與通報 K100資安作業相關安全知識 K107網頁存取記錄稽核技術	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力 S16 Log 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)
	T4.10 委外管控	O4.10.1 委外合約 (含明文之安全要求事項) O4.10.2 委外監督紀錄	P4.10.1協助合約管理單位，於合約中納入必要之安全要求項目。 P4.10.2協助合約管理單位，針對合約之安全相關項目，監督委外廠商之合約履行並留存紀錄。	3	K22相關法規、主管機關要求 K23合約要求、業務需求 K55了解合約管理單位相關業務之安全議題 K64監控與通報 K95資通安全管理法及其子法 K96稽核	S01 文件撰寫能力 S02 應變管理能力 S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力 S14 文件閱讀與理解能力
T5 日誌收容、分析與監控	T5.1 稽核日誌設定	O5.1.1 稽核日誌設定準則 O5.1.2 稽核日誌設定紀錄	P5.1.1協助各管理人員，制定系統、網路、資安與終端設備稽核日誌啟動之準則 (如：對管理者與使用者之行為)。 P5.1.2依據準則，設定系統、網路、資安與終端設備稽核日誌。 P5.1.3協助確認維運所需注意之系統事件。	4	K22相關法規、主管機關要求 K23合約要求、業務需求 K56設備事件定義 K57系統、網路、資安與終端稽核日誌設定	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力
	T5.2 收容與保護稽核日誌	O5.2.1 日誌收容紀錄	P5.2.1建立稽核日誌保護機制，如：資安監控中心 (Security Operation Center, SOC) 或日誌伺服器，並依業務、法規需求，決定需留存紀錄之日誌時間。 P5.2.2協助各管理人員，依特性進行系統、網路、資安與終端設備稽核日誌收容 (如：	4	K58了解網路、系統、設備事件意義 K59日誌保護機制 (如：防竄改方式) K60維運與法規對紀錄留存之要求	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S13 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)
			Syslog 外拋，或主動連接 Database)。		K61 SOC/日誌收容系統建置 K62 SOC/日誌收容系統維運	
	T5.3 日誌分析與通報	O5.3.1 監控日報/月報表 O5.3.2 通報記錄	P5.3.1分析單一事件或交叉關聯分析異質事件，建立關聯分析規則。 P5.3.2依據關聯分析規則進行判斷。 P5.3.3判斷攻擊事件與事故，即時依程序通報。	4	K12 Transmission Control Protocol / Internet Protocol (TCP/IP) K13網路路由 (Network Routing) K14網路通訊協定與服務 (Network Protocol / Service) K15網路與系統弱點 K16攻擊手法與防禦 K17作業系統原理 K18資料庫原理 K19服務系統 (郵件、File Transfer Protocol、網站等) K22相關法規、主管機關要求 K23合約要求、業務需求 K63關聯分析 K64監控與通報 K73事件、事故定義 K82根因分析	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S09 組織與規劃能力 S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力 S16 Log 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)
	T5.4 時間 同步	O5.4.1 選 定時間同 步源 O5.4.2 時 間同步設 定與定期 檢查紀錄	P5.4.1協助決定共同時間同步源。 P5.4.2協助各管理人員，設定系統、網路、資安與 終端設備之時間同步。 P5.4.3協助各管理人員，定期檢視設定是否正常運 作。	3	K22相關法規、主管機關要求 K65 時間同步協定 (Network Time Protocol, NTP)	S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力
T6 雲端安 全管理	T6.1 雲端 維運安全 管理	O6.1.1 各 項雲端服 務、系統 維運安全 管控紀錄	P6.1.1了解雲端架構。 P6.1.2協助相關人員，進行雲端維運相關安全管理 及協助雲端事務應變處理。	4	K22相關法規、主管機關要求 K23合約要求、業務需求 K64監控與通報 K66雲端運算架構框架 K67雲端資料安全 K68雲端身分認證與存取管理 K69雲端服務供應商管理 K70雲端資料中心維運 K71雲端應用程式安全 K72雲端事故回應、緊急應變 K100資安作業相關安全知識	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S13 安全警覺性能力
T7 資訊安 全事故通 報、緊急	T7.1 事故 通報與期 初處理	O7.1.1 事 故通報紀 錄	P7.1.1協助各管理人員，建立事故偵測與通報機 制，即時記錄事故並進行分類。 P7.1.2協助事故期初處置，以減少中斷時間與避免	4	K22相關法規、主管機關要求 K23合約要求、業務需求 K73事件、事故定義	S01 文件撰寫能力 S02 應變管理能力 S08 問題解決能力

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)
應變及營運持續管理		O7.1.2 事故期初處置紀錄	事故擴大。 P7.1.3 了解通報應變架構。		K74事故偵測 K75事故分類與通報 K76事故期初處置 (Initial Support) K77補償措施 K88緊急應變 K93個人資料保護法與施行細則 K95資通安全管理法及其子法	S11 溝通協調能力 S13 安全警覺性能力
	T7.2 事故分析與恢復	O7.2.1 事故分析結果 O7.2.2 事故處理紀錄	P7.2.1協同事故相關人員，針對事故發生原因，進行評估與分析。 P7.2.2協助事故相關人員，進行必要處置，並盡速恢復系統運作。	4	K22相關法規、主管機關要求 K23合約要求、業務需求 K78事故分析與評估 K79事故修補與復原	S01 文件撰寫能力 S02 應變管理能力 S08 問題解決能力 S11 溝通協調能力 S13 安全警覺性能力
	T7.3 事故鑑識與證據保全	O7.3.1 事故鑑識紀錄與相關處理紀錄	P7.3.1協助事故發生單位，判斷是否需留存與保護可能之入侵、犯罪資料，必要時，協助隔離事故區。 P7.3.2協助事故發生單位保存必要之證據 (含數位與非數位) 以作為相關法律議題處理之依據。	4	K22相關法規、主管機關要求 K23合約要求、業務需求 K80數位鑑識 (Digital Forensic) K81數位證據保全	S01 文件撰寫能力 S02 應變管理能力 S08 問題解決能力 S11 溝通協調能力 S13 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)
	T7.4 由事故中學習與實施預防措施	O7.4.1 事故根因分析報告 O7.4.2 事故矯正改善紀錄	P7.4.1協助事故發生單位進行根因分析，依據根因，協助事故發生單位提出矯正與改善措施。 P7.4.2協助事故發生單位，提出矯正改善措施，並確認有效性。	4	K82根因分析 K83改善、矯正措施 K84有效性審查 K100資安作業相關安全知識	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力
	T7.5 備援機制規劃與實作	O7.5.1 備援機制	P7.5.1協助各管理人員選擇符合需求之備援方式，建立備援系統與備援機制。	4	K22相關法規、主管機關要求 K23合約要求、業務需求 K85備援機制（含異地備援與同步） K89營運持續作業方式 K90系統、網路還原與處置	S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力
	T7.6 緊急應變與營運持續	O7.6.1 緊急應變計畫書 O7.6.2 營運持續計畫書	P7.6.1依據營運衝擊分析結果，進行風險分析，協助分析可能造成需啟動緊急應變與營運持續之事故。 P7.6.2協助各管理人員，識別所有可能造成過長中斷時間之事故、威脅，並撰寫緊急應變計畫書。	4	K86營運衝擊分析 K87風險評估 K88緊急應變 K89營運持續作業方式 K100資安作業相關安全知識	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力
	T7.7 緊急應變及營運持續演	O7.7.1 營運持續演練計畫	P7.7.1協助各管理人員，撰寫各系統、設備之各情境應變作業程序及緊急應變計畫。 P7.7.2協助各管理人員依時程演練並進行檢討與改	4	K88緊急應變 K89營運持續作業方式 K90系統、網路還原與處置	S01 文件撰寫能力 S02 應變管理能力 S07 評估與分析能力

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)
	練與改善	O7.7.2 演 練紀錄 O7.7.3 演 練檢討與 改善紀錄	善。		K91營運持續演練方式	S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力
T8法規遵循	T8.1 識別 適用法規	O8.1.1 適 用法規清 單	P8.1.1了解所屬產業與日常作業需遵循的相關法規。 P8.1.2尋求法務單位協助，識別所需遵循相關法規。 P8.1.3定期更新法規資訊。 P8.1.4與各相關單位合作溝通，了解、識別利害關係人要求及合約所列之應遵循事項。	3	K22相關法規、主管機關要求 K23合約要求、業務需求 K92法規識別	S01 文件撰寫能力 S07 評估與分析能力 S11 溝通協調能力 S14 文件閱讀與理解能力
	T8.2 個人 資料保 護、資 通安 全管 理 責 任 與 智 慧 財 產 權	O8.2.1 個 資保 護作 業相 關紀 錄 O8.2.2 智 慧財 產遵 循檢 查紀 錄 O8.2.3 資	P8.2.1協助作業單位識別所有涉及個資作業之流程，確保維運作業對個人資料蒐集、處理、利用時，皆需符合個人資料保護法。 P8.2.2宣導與協助各單位，資料、音樂、圖片、軟體等使用需符合著作權法 P8.2.3 協助作業單位符合資通安全管理法及其子法施行。	4	K22相關法規、主管機關要求 K23合約要求、業務需求 K93個人資料保護法與施行細則 K94智慧財產權 K95資通安全管理法及其子法	S01 文件撰寫能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S14 文件閱讀與理解能力

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)
		通安全管理相關紀錄				
	T8.3 獨立稽核與遵循性檢查	O8.3.1 稽核作業紀錄 O8.3.2 遵循性檢查紀錄	P8.3.1協助規劃並執行稽核作業，並確保獨立性。 P8.3.2協助定期確認所有作業之法規遵循性。	4	K22相關法規、主管機關要求 K23合約要求、業務需求 K96稽核 K97法規遵循	S01 文件撰寫能力 S07 評估與分析能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力 S14 文件閱讀與理解能力
T9教育訓練	T9.1 資安意識與認知宣導	O9.1.1 資安意識與認知宣導教育訓練教材 O9.1.2 社交工程演練訓練教材 O9.1.3 教育訓練紀錄	P9.1.1協助準備資安意識與認知宣導教育訓練教材。 P9.1.2協助執行資安意識與宣導教育訓練。 P9.1.3協助執行社交工程演練（如：電子郵件測試）並留存紀錄。	3	K22相關法規、主管機關要求 K23合約要求、業務需求 K98資訊安全認知 K99社交工程手法 K101授課技巧	S01 文件撰寫能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力

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)
	T9.2 職能教育訓練	O9.2.1 協助辦理資安作業相關技能教育訓練 O9.2.2 教育訓練紀錄	P9.2.1協助準備執行資安作業所需技能教育訓練教材。 P9.2.2協助執行資安作業所需技能教育訓練。	3	K22相關法規、主管機關要求 K23合約要求、業務需求 K100資安作業相關安全知識 K101授課技巧	S01 文件撰寫能力 S08 問題解決能力 S10 監督執行能力 S11 溝通協調能力

職能內涵 (A=attitude 態度)

A01：溝通協調能力、A02：獨立、A03：細心謹慎、A04：彈性、A05：執行力、A06：正直、A07：自我管理、A08：自主學習、A09：抗壓性、A10：冷靜思考、A11：問題分析、A12：堅忍、A13：守法、A14：職業道德

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：
 - 大學或專科以上學歷，或具有資訊安全相關背景，資訊或電機相關科系尤佳。
 - 具備英文閱讀能力，具跨領域學習特質者尤佳。
 - 具相關資訊安全相關專業證照尤佳。