資安管理人員職能基準

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
V2	INM2529-002v2	資安管理人員	最新版本	略	2025/12/15
V1	INM2529-002v1	資安管理人員	歷史版本	已被《INM2529-002v2》取代	2022/12/07

職能基準代碼		INM2529-002v2			
職能基準名稱（擇一填寫）		**職類**			
		職業	**資安管理人員**		
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	其他資料庫及網路專業人員		**職業別代碼**	2529
	行業別	專業、科學及技術服務業/其他專業、科學及技術服務業		**行業別代碼**	M7609
工作描述		依據組織政策方向，推動組織資安管理制度相關業務。			
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（ISMS）制度建立	T1.1 擬定資訊安全管理計畫	O1.1.1資訊安全制度導入計畫 O1.1.2適用性聲明書	P1.1.1依據資訊安全管理系統或國際相關資安標準及法規、主管機關要求、組織需求等，產出資訊安全制度導入計畫。 P1.1.2建立風險管理全景，確認管理制度的導入範圍，規劃資訊安全組織管理程序、資訊風險評鑑管理程序、人員資安保密管理程序，產出對應管理表單。	4	K01資訊安全管理系統 K02網路安全架構 K03系統安全架構 K04端點安全架構 K05資訊安全管理相關控制項 K06國際相關資安標準 K07法規遵循	S01外部環境認知與評估 S02策略性思考 S03價值判斷 S04文書閱讀與撰寫能力 S05資訊科技應用能力 S06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）
		O1.1.3資訊安全制度各階文件（含資訊資產清冊）	P1.1.3依據上述原則及導入需求，建立管理辦法等管制文件（如資訊設備維護管理、帳號密碼與存取控制管理資訊備份管理等）。		K08資訊資產安全等級分類	
	T1.2 風險識別、分析與評估	O1.2.1風險評鑑工作表 O1.2.2風險評估報告	P1.2.1協助各資訊資產負責人進行資訊資產清冊盤點，風險分析與評估並產製高風險清冊。 P1.2.2依據組織相關利害關係人、相關法規及管理程序等產出管理表單，建立可接受風險評鑑的過程。 P1.2.3查核上述相關程序表單進行風險識別、分析與評估，產出風險評估報告。	4	K09風險評鑑方法論 K10剩餘風險	S06溝通協調能力 S07正確傾聽 S08分析與解讀能力 S09規劃與組織能力
	T1.3 風險處理	O1.3.1風險處理計畫表 O1.3.2剩餘風險評鑑計畫表	P1.3.1參與風險等級判定準則之討論。 P1.3.2協助風險高於可接受等級項目之單位，識別不可接受風險項目，針對不可接受風險項目，擬定風險處理計畫。 P1.3.3確認風險處理計畫執行之有效性，是否如預期之降低風險值。	4	K09風險評鑑方法論 K10剩餘風險	S06溝通協調能力 S07正確傾聽 S08分析與解讀能力 S09規劃與組織能力 S10時間管理 S11問題分析與解決 S12衝突管理

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）
	T1.4 營運持續管理	O1.4.1營運持續管理計畫 O1.4.2關鍵營運業務/系統分級表 O1.4.3業務持續計畫演練報告	P1.4.1依組織營運項目之業務及組織內外部重大議題，盤點組織重要業務項目及所支援之資通訊系統，依其重要性分列，匯整核心業務項目及其支援之核心資通訊系統清單（關鍵服務項目清單）。 P1.4.2針對上述清單之業務或資通訊系統，定義其最大可容忍之中斷時間、復原時間目標（RTO）以及復原點目標（RPO）等等，並依其要求訂定各業務、資通訊系統之營運持續計畫或災難復原計畫，並執行演練。	4	K06國際相關資安標準 K11系統備份備援架構 K12系統復原要求 K13業務持續運作要求	S06溝通協調能力 S07正確傾聽 S08分析與解讀能力 S09規劃與組織能力 S11問題分析與解決 S12衝突管理
T2資訊安全管理系統維運	T2.1 資訊安全維運	O2.1.1資安管控紀錄表單 O2.1.2修訂紀錄	P2.1.1依據資訊安全管理系統要求，完成各項表格、相關紀錄，產出維運紀錄。 P2.1.2針對現有的管理制度及文件定期檢視與調整。	4	K01資訊安全管理系統 K05資訊安全管理相關控制項 K14資安稽核	S06溝通協調能力 S07正確傾聽 S08分析與解讀能力
	T2.2 執行內部稽核計畫	O2.2.1稽核計畫 O2.2.2稽核底稿 O2.2.3稽	P2.2.1依據資訊安全管理系統要求，制定明確的內部稽核計畫，以評估資訊安全管理系統的有效性	4	K01資訊安全管理系統 K05資訊安全管理相關控制項 K14資安稽核	S09規劃與組織能力 S10時間管理 S11問題分析與解決 S12衝突管理 S13稽核技巧

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）
		核報告 O2.2.4矯正措施文件	P2.2.2確保稽核項目均有文件佐證並產出詳細、組織化的稽核底稿，以呈現內部稽核過程中的所有發現和結論。 P2.2.3針對稽核過程中發現的問題，提供可行的建議，以直接解決資訊安全管理系統中的弱點，並撰寫清晰、易於理解的稽核報告呈現稽核結果。 P2.2.4確保所有內部稽核中發現的缺失或弱點，均有相應的矯正預防措施，並完整填寫相關表單。			
	T2.3 配合執行外部稽核計畫		P2.3.1依據外部或相關稽核單位之要求，配合進行相關稽核作業。	4	K01資訊安全管理系統 K05資訊安全管理相關控制項 K14資安稽核 K15委外監督管理程序 K16資訊安全認知	S06溝通協調能力 S14受稽核技巧
T3 資安教育訓練	T3.1 資安意識與認知宣導	O3.1.1資安保密相關協議文件 O3.1.2宣導計畫	P3.1.1 建立各職務之資安認知規劃，使組織人員遵守相關「資安政策」及管理規範，並了解與本身所執行業務相關之資安責任並簽署相關協議。 P3.1.2 針對組織相關利害關係人，進行資安相關宣導，確保落實「資安政策」及管理規範並簽署相關協議。	3	K06國際相關資安標準 K16資訊安全認知 K17社交工程演練 K18標準與法規識別 K19個人資料保護法與施行細則 K20資安作業相關職能教育訓練	S01外部環境認知與評估 S02策略性思考 S03價值判斷 S04文書閱讀與撰寫能力 S05資訊科技應用能力 S06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）
	T3.2 資安職能教育訓練	O3.2.1訓練計畫 O3.2.2訓練簽到表 O3.2.3訓練評估表	P3.2.1 訪視資安人員訂定資訊安全訓練需求擬定訓練計畫，訓練內容應包括「資安政策」、資安管理規範及相關法規等。 P3.2.2 執行各單位次年度資安訓練需求的調查，以規劃次年度之訓練計畫，同時研擬次年度之「訓練計畫表」，使其瞭解資訊安全之重要性及各種可能的安全風險、違反資訊安全可能的法律責任。 P3.2.3制定教育訓練管理方向，依需求提出規劃相關資安教育訓練課程，或派員接受外單位辦理之專業資安課程。	3	K06國際相關資安標準 K16資訊安全認知 K18標準與法規識別 K19個人資料保護法與施行細則 K20資安作業相關職能教育訓練	S06溝通協調能力 S07正確傾聽 S08分析與解讀能力 S09規劃與組織能力 S10時間管理 S11問題分析與解決 S12衝突管理
T4 法規遵循	T4.1 識別適用法規與法規遵循	O4.1.1適用法規清冊 O4.1.2資通安全管理相關紀錄	P4.1.1瞭解所屬產業與日常作業需遵循的相關法規。 P4.1.2尋求法務單位協助，識別所需遵循相關法規。 P4.1.3定期更新法規資訊。 P4.1.4針對法規規範調整管理辦法，協助作業單位符合相關法規要求。	4	K06國際相關資安標準 K18標準與法規識別 K19個人資料保護法與施行細則 K21資通安全管理法	S04文書閱讀與撰寫能力 S05資訊科技應用能力 S06溝通協調能力 S08分析與解讀能力 S09規劃與組織能力 S10時間管理
	T4.2 個人資料與智慧財產權	O4.2.1個資保護作業相關紀	P4.2.1作業單位識別並記錄所有涉及個資作業之資料與流程，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。	4	K06國際相關資安標準 K07法規遵循 K14資安稽核	S05資訊科技應用能力 S06溝通協調能力 S11問題分析與解決

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）
	保護	錄 O4.2.2智慧財產遵循檢查紀錄	P4.2.2檢查各單位之資料、音樂、圖片、軟體等使用需符合著作權法，並留存紀錄。		K18標準與法規識別 K19個人資料保護法與施行細則 K20資安作業相關職能教育訓練 K21資通安全管理法 K22智慧財產權	S12衝突管理 S15資料蒐集、處理、利用
	T4.3組織外部單位稽核與遵循性檢查	O4.3.1稽核作業紀錄 O4.3.2遵循性檢查紀錄	P4.3.1規劃並執行稽核作業，並確保其獨立性，產出稽核計畫及作業紀錄。 P4.3.2定期確認所有作業之法規遵循性，並留存檢查紀錄。	4	K06國際相關資安標準 K07法規遵循 K14資安稽核 K18標準與法規識別 K19個人資料保護法與施行細則 K20資安作業相關職能教育訓練 K21資通安全管理法	S05資訊科技應用能力 S06溝通協調能力 S12衝突管理 S15資料蒐集、處理、利用 S16獨立稽核作業能力

職能內涵（A=attitude 態度）
A01主動積極：不需他人指示或要求能自動自發做事，面臨問題立即採取行動加以解決，且為達目標願意主動承擔額外責任。
A02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。
A03持續學習：能夠展現自我提升的企圖心，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。
A04自我管理：設立定義明確且實際可行的個人目標；對於及時完成任務展現高度進取、努力、承諾及負責任的行為。
A05自信心：在表達意見、做決定、面對挑戰或挫折時，相信自己有足夠的能力去應付；面對他人反對意見時，能獨自站穩自己的立場。
A06團隊意識：積極參與並支持團隊，能彼此鼓勵共同達成團隊目標。
A07彈性：能夠敞開心胸，調整行為或工作方法以適應新資訊、變化的外在環境或突如其來的阻礙。

職能內涵（A=attitude 態度）
A08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。 A09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／經驗／或能力條件： 大專以上畢業且具有2年以上資訊安全相關工作經驗。 **其他補充說明：** 資訊安全管理系統（ISMS）：資訊安全管理系統（Information Security Management System，簡稱：ISMS）是一套有系統分析和管理資訊系統的方法，現今 ISO 標準是 ISO/IEC27000系列。