資安檢測工程人員職能基準

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	INM2529-003v2	資安檢測工程人員	最新版本	略	2025/12/15
V1	INM2529-003v1	資安檢測工程人員	歷史版本	已被《INM2529-003v2》取代	2022/12/07

職能基準代碼		INM2529-003v2			
職能基準名稱（擇一填寫）		**職類**			
		職業	資安檢測工程人員		
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		負責規劃執行組織資訊系統之弱點掃描、滲透測試並協助修補弱點之工作。			
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 系統安全檢測	T1.1 擬定檢測計畫	O1.1.1 系統安全檢測計畫	P1.1.1訪談需求單位，收集欲檢測標的之相關資訊，以及檢測目的與要求，擬定系統安全檢測項目，包含環境、工具、人員、時程、檢測計畫風險管理、緊急應變等，產出系統安全檢測計畫。	4	K01資訊安全法規 K02系統安全防護 K03風險系統管理 K04網路與資訊安全 K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務	S01閱讀與撰寫能力 S02資訊科技應用能力 S03外部環境認知與評估 S04問題分析與解決能力 S05規劃與組織能力 S06溝通協調能力 S07資安情資蒐集能力

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）
	T1.2 執行檢測	O1.2.1 系統安全防護強度檢測報告	P1.2.1選擇適當工具與蒐集標的系統已知之弱點資訊，進行有效作業系統弱點掃描，對產生的結果進行有效的解說。 P1.2.2檢測相關系統與伺服器的權限管理、備份與還原，是否受到妥善管理與保護。 P1.2.3對安全機制（如身分識別）進行各種測試。 P1.2.4產出系統安全防護強度檢測報告如掃描出之弱點或密碼管理之弱項等測試內容。	4	K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務 K08弱點掃描 K09密碼學 K10備份與還原 K11作業系統操作指令	S02資訊科技應用能力 S03外部環境認知與評估 S04問題分析與解決能力 S05規劃與組織能力 S06溝通協調能力 S08防火牆與密碼安全能力 S09網路安全工具操作能力 S10作業系統指令操作能力
T2網路與網站安全檢測	T2.1 網路安全設備檢測	O2.1.1 網路安全設備測試計畫書 O2.1.2 網路安全設備檢測報告	P2.1.1選擇適當工具與蒐集標的系統已知之弱點資訊，檢測防火牆、入侵偵測系統、虛擬私有網路（VPN）等功能及組態與日誌檔、並評估現有網路安全設備之有效性。 P2.1.2產出網路安全設備測試計畫書並取得受測單位之同意。 P2.1.2結合上述組態與日誌檔案，與各種網路安全設備進行功能驗證，並產出網路安全設備檢測報告。	4	K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務 K08弱點掃描 K09密碼學 K12防火牆防護 K13網路安全設備	S02資訊科技應用能力 S03外部環境認知與評估 S04問題分析與解決能力 S05規劃與組織能力 S06溝通協調能力 S07資安情資蒐集能力 S08防火牆與密碼安全能力 S09網路安全工具操作能力
	T2.2 網路安全協定檢測	O2.2.1 網路安全協定檢測報	P2.2.1選擇適當工具與蒐集標的系統已知之弱點資訊，檢測各種網路安全協定軟體的組態、功	4	K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務	S02資訊科技應用能力 S03外部環境認知與評估 S04問題分析與解決能力

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）
		告	能、版本稽核、密碼強度、密碼管理政策是否適當、功能是否完整等。 P2.2.2產出包含上述項目的網路安全協定檢測報告。		K08弱點掃描 K09密碼學 K12防火牆防護 K13網路安全設備	S05規劃與組織能力 S06溝通協調能力 S08防火牆與密碼安全能力 S09網路安全工具操作能力
	T2.3 網站安全檢測	O2.3.1 網站安全檢測報告	P2.3.1以適當工具與蒐集標的系統已知之弱點資訊，對網站進行弱點掃描，包含 OWASP 十大風險，或其他組織公佈之弱點指標。 P2.3.2檢測網站的管理權限、身分識別、資料傳輸、遠端存取是否受到妥善管理與保護。 P2.3.3產出網站安全檢測報告，包含網站或使用元件存在之已知弱點、不安全之網頁程式語法、特權帳號、資料傳輸加密、限制遠端存取政策內容等。	4	K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務 K08弱點掃描 K09密碼學 K12防火牆防護 K13網路安全設備 K14程式語言	S02資訊科技應用能力 S03外部環境認知與評估 S04問題分析與解決能力 S05規劃與組織能力 S06溝通協調能力 S08防火牆與密碼安全能力 S09網路安全工具操作能力
T3 滲透測試	T3.1 規劃與執行	O3.1.1 滲透測試計畫書 O3.1.2 執行步驟紀錄表	P3.1.1蒐集欲檢測標的之相關資訊，以及檢測目的與要求，擬定滲透測試範圍、環境、工具、人員、時程、風險管理、緊急應變等，產出滲透測試計畫書並取得受測單位之同意。 P3.1.2執行滲透測試計畫，產出執行步驟紀錄表。	4	K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務 K08弱點掃描 K09密碼學 K12防火牆防護 K13網路安全設備 K14程式語言	S04問題分析與解決能力 S05規劃與組織能力 S06溝通協調能力 S07資安情資蒐集能力 S08防火牆與密碼安全能力 S09網路安全工具操作能力 S11滲透測試操作

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 結案報告撰寫	O3.2.1 滲透測試分析報告 O3.2.2 資訊安全修復建議報告書	P3.2.1進行滲透測試或協助第三方團體執行，留存過程紀錄並產出結果彙整與分析報告。 P3.2.2產出包含檢測標的存在之已知弱點（包含其所連動之元件，如資料庫）、不安全之程式語法、程式 / 流程邏輯異常等其他可能之脆弱點以及修復改善建議報告書。	4	K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務 K08弱點掃描 K09密碼學 K12防火牆防護 K13網路安全設備 K14程式語言	S04問題分析與解決能力 S05規劃與組織能力 S06溝通協調能力 S08防火牆與密碼安全能力 S09網路安全工具操作能力 S11滲透測試操作
T4 弱點修補與管理	T4.1 弱點資訊蒐集與提供	O4.1.1 弱點公告資訊	P4.1.1定期蒐集組織資訊元件之相關弱點資訊，提供即時新型弱點訊息並分析後提供組織弱點修補之建議。	4	K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務 K08弱點掃描 K09密碼學 K12防火牆防護 K13網路安全設備	S04問題分析與解決能力 S05規劃與組織能力 S06溝通協調能力 S07資安情資蒐集能力 S09網路安全工具操作能力 S11滲透測試操作
	T4.2 弱點修補記錄與管理	O4.2.1 弱點修補與改善紀錄	P4.2.1定期進行弱點檢測並提供後續修補記錄分析與資安改善，並確定系統正常運作，產出弱點修補分析與資安改善紀錄。	4	K05資安防護監控 K06事故應變處理 K07資安相關技術安全標準或實務 K08弱點掃描 K09密碼學 K12防火牆防護	S04問題分析與解決能力 S05規劃與組織能力 S06溝通協調能力 S09網路安全工具操作能力 S11滲透測試操作

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）
					K13網路安全設備	

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。
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：** OWASP：是由「開放式 Web 應用程式安全專案（OWASP）基金會」，針對 Web 應用程式漏洞和攻擊趨勢進行深入研究，建立了一套軟體安全行業指南和標準。其中，OWASP Top10是最受歡迎和使用最廣泛的 Web 應用程式安全意識指南。