金融資安人才職能地圖

金融監督管理委員會
中華民國 113 年 4 月

修訂紀錄			
版次	承辦者	摘　　要	發行/修訂生效日期
V1.0		訂定金融資安人才職能地圖	110/6/23
V1.1		修正附錄二及附錄三部分課程內容 1. 附錄二「資安管理」及「風險管理」領域新增基礎課程「S207」 2. 附錄二「程式設計」領域新增進階課程「S303」、「資安防護」領域新增進階課程「S305」 3. 附錄三「資安管理」領域新增基礎課程「S201」、「風險管理」領域新增基礎課程「S218」 4. 附錄三「事件應變」領域刪除進階課程「S402」	110/7/7
V1.2		修正附錄一至附錄四部分課程內容 1. 附錄一： (1) 修正 S203、S204、S206、S214、S218、S404 之內容大綱 (2) 新增 S220、S221、S405、S406 之課程及內容大綱 2. 附錄二：依領域責任需求新增「S220」、「S405」、「S221」及「S406」課程 3. 附錄三： (1) 依領域（職務）需求新增「S220」、「S405」、「S221」及「S406」課程 (2) 「程式設計」領域新增「S404」課程 4. 附錄四： (1) 修訂 ISO 27001 Lead Auditor 版本 (2) 資安維運 A. 刪除 EC-Council Certified Security Analyst(ECSA) B. 新增 EC-Council Certified Penetration Tester(CPENT)	113/4/12

目 錄

壹、 前言

一、設計說明

為發展兼具涵蓋性及可行性之金融產業資安人才培訓架構及學習地圖，參考國家資通安全研究院[1]所規劃之公務人員資安職能訓練，美國國家標準暨技術研究院（National Institute of Standards and Technology，簡稱NIST）[2]於 2017 年發布之「Special Publication 800-181：National Initiative for Cybersecurity Education Framework（簡稱 NICE Framework）」，以及歐洲網路安全局（European Union Agency for Cybersecurity，ENISA）於 2022 年發布之「European Cybersecurity Skills Framework」（簡稱 ECSF），擬具培訓架構；並參考國內外資安訓練資源設計相關課程，包括國家資通安全研究院、台灣金融研訓院[3]、英國標準協會(BSI)[4]、國際電子商務顧問(EC-Council)[5]、環球銀行金融電信協會(SWIFT)[6]、 雲端安全聯盟(Cloud Security Alliance,CSA)[7]、系統網路安全協會(SANS Institute)[8]及金融資安資訊分享與分析中心(F-ISAC)等。

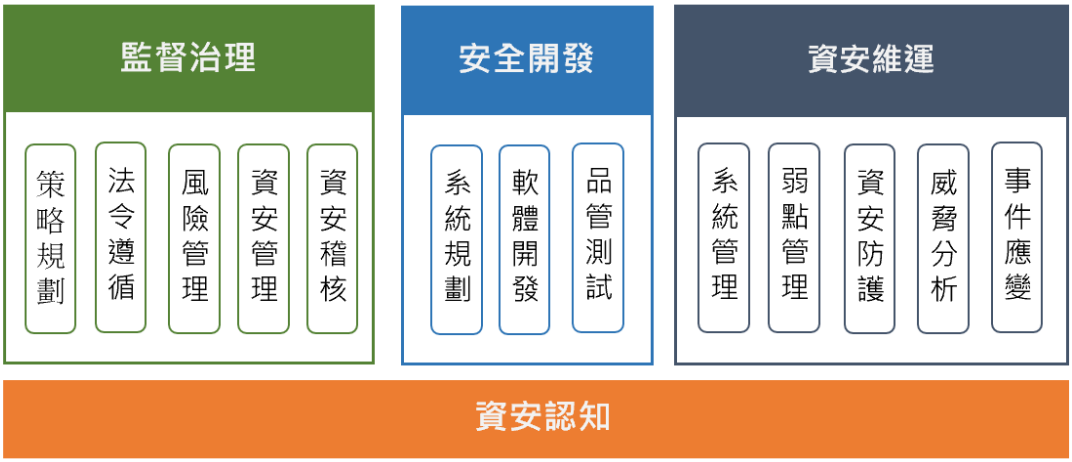

圖 金融資安人才培育架構

二、適用對象

金融產業從事資安實務工作之在職人士、有志從事金融資安產業人士。

貳、架構說明

一、 架構組成

架構類別包括監督治理、安全開發及資安維運等三項，各類別項下分由資安認知領域及專業領域組成，進而對應至相關單位及所需之工作職能（詳如下表）。

類別	領域	對應單位	核心職能
監督治理 *負責管理、稽核、風控及法遵等工作，俾組織有效處理資訊安全相關作業。*	資安認知	規劃單位	CA001：具備基本資訊安全概念 CA002：熟悉資訊安全管理制度 CA003：瞭解資訊安全相關法律 CA004：瞭解個人資料保護議題 CA005：瞭解新興科技資安威脅
	資安管理		CM001：具備資安策略制定能力 CM002：具備資安管理決策能力 CM003：具備跨部門協調能力 CM004：具備資安人力評估能力 CM005：具備危機管理能力
	資安稽核		CU001：具備資安系統查核技巧 CU002：瞭解網路標準相關知識 CU003：瞭解網路威脅和漏洞
	風險管理		CR001：瞭解風險管理流程及架構 CR002:具備資安風險及威脅評估能力
	法令遵循		CL001：確認作業符合法令規定
安全開發 *負責系統開發及品管測試工作，俾概念化、設計、採購及*	資安認知	執行單位	CA001：具備基本資訊安全概念 CA002：熟悉資訊安全管理制度 CA003：瞭解資訊安全相關法律 CA004：瞭解個人資料保護議題
	程式設計		CD001:具軟體安全架構規劃或開發安

類別	領域	對應單位	核心職能
建置安全之系統。			全軟體能力
	品管測試		CT001：瞭解軟體安全架構及工具能力 CT002：具分析、蒐集、確認及驗證測試資料能力
資安維運 *負責識別、分析及減輕組織面臨的威脅，並提供必要的支援、管理及防護。*	資安認知	規劃及執行單位	CA001：具備基本資訊安全概念 CA002：熟悉資訊安全管理制度 CA003：瞭解資訊安全相關法律 CA004：瞭解個人資料保護議題 CA005：瞭解新興科技資安威脅
	系統網路管理	執行單位	CS001：瞭解網路及系統安全機制 CS002：具備發展及維護資安機制能力 CS003：具備執行網路應用工具能力 CS004：具備雲地整合架構規劃能力
	弱點管理		CV001：瞭解弱點及相關系統設定等資訊，識別系統安全議題 CV002：具備執行弱點掃描及弱點修復管理作業能力
	資安防護	規劃及執行單位	CP001：瞭解網路及系統安全機制 CP002：瞭解資安防護技術 CP003：瞭解資安威脅及漏洞 CP004：瞭解加密法 CP005：瞭解駭客入侵技術與危機處理
	事件應變		CI001：瞭解事件回應及處理方法 CI002：具備網路威脅情資蒐集及分析能力 CI003：具備各系統之數位鑑識能力

二、 課程設計

因應架構所設計的課程區分為通識、基礎及進階等三個等級，內容由淺至深，期以循序漸進的方式培育人員具備各領域所需職能（課程總表請參閱附錄一）。各級課程說明分述如下：

（一）通識：資訊安全基本理論、管理作業架構及相關資安法規介紹，期能培養人員基本資安知識，達成認知資訊安全重要性之目標。

（二）基礎：基本資安能力養成，期能培養人員日常資安維運作業能力，達成資安防護技術導入及建置、開發安全應用程式、網路攻擊及防禦技術應用等目標。

（三）進階：針對各類資安主題深入探究，期能培養人員專業分析及規劃能力，達成理論與實務整合應用之目標。

參、 發展建議

一、 學習地圖

鑒於資安領域涵蓋範圍甚廣，相關專業知識與課程眾多，本會規劃學習地圖供金融業者、培訓機構、資安人員及有意願投入金融資安領域之民眾參考（學習地圖請參閱附錄三）。

二、 資安證照

考量完成全套課程所費不貲，且需花費相當時間。為協助業者降低培訓成本，鼓勵資安人員考取證照，本會定期依據數位發展部資通安全署公布之資通安全專業證照[9]，衡酌證照評鑑項目，研擬持有證照可免除培訓課程清單(資通安全專業證照對照表詳附錄四)。

三、 培訓機構

初期先以本會所轄周邊研究訓練機構(如台灣金融研訓院、保險事業發展中心、證券暨期貨市場發展基金會)及金融資安資訊分享與分析中心(F-ISAC)為主，並得洽邀專業訓練機構合作開設訓練課程。

四、 資安人員

鼓勵金融資安人員參考學習地圖，考取資安專業證照，建立個人資安專業學習歷程，並開放有意願投入金融資安領域之民眾報名參訓，充實金融資安專業人才庫，供金融機構攬才參考。

肆、 參考資料

[1] 國家資通安全研究院， https://www.nics.nat.gov.tw/.htm#。

[2] 美國國家標準暨技術研究院(NIST) National Initiative for Cybersecurity Education Framework，https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework。

[3] 台灣金融研訓院教育訓練課程，http://service.tabf.org.tw/Training/CourseClassify.aspx。

[4] 英國標準協會(BSI)資安課程，https://www.bsigroup.com/zh-TW/Our-services/training-courses/。

[5] 國際電子商務顧問(EC-Council)資安認證課程，https://www.uuu.com.tw/Course/Partner/ec-council。

[6] 環球銀行金融電信協會(SWIFT)Security Bootcamp Training，https://www.swift.com/our-solutions/services/training/tailored-training/security-bootcamp。

[7] 雲端安全聯盟(Cloud Security Alliance,CSA)課程，https://cloudsecurityalliance.org/。

[8] 系統網路安全協會(SANS Institute)網路安全課程，https://www.sans.org/courses。

[9] 數位發展部資通安全署專業證照清單，https://moda.gov.tw/ACS/laws/certificates/676。

附錄一：課程總表

一、通識課程

編號	名稱	內容大綱
S101	資訊安全概論	1. 資訊安全架構 2. 資訊安全威脅及防護 3. 資訊安全管理系統簡介
S102	ISMS 資訊安全管理系統	1. ISMS 管理系統架構介紹 2. ISO 27001 介紹
S103	資安法規介紹	1. 資安法 2. 個人資料保護法 3. 金融資安法規及自律規範

二、基礎課程

編號	名稱	內容大綱
S201	辦公室作業安全	1. 系統及網路操作安全 2. 電子郵件安全 3. Internet 安全
S202	系統及網路安全	1. Windows 系統安全 2. Linux 系統安全 3. 有線網路安全 4. 無線網路安全
S203	程式開發安全	1. 生命週期安全管理 2. 軟體安全要求 3. 軟體安全設計及開發 4. API 安全要求、API OWASP Top 10 介紹及安全建議
S204	網頁/行動應用程式安全	1. OWASP Top 10、Mobile Top 10 介紹及安全建議 2. 行動 APP 安全 3. API 安全要求、API OWASP Top 10 介紹及安全建議 4. 身分認證安全
S205	網路探測實務	1. Google Hacking 網路搜尋技術 2. NMAP 網路探測工具 3. Nessus 弱點掃描工具 4. 其他工具及技術
S206	基礎系統及網站滲透測試	1. 系統滲透測試簡介 2. 網頁滲透測試簡介 3. 紅隊、紫隊及 BAS(Breach Attack Simulation)演練 4. Kali Linux 系統介紹 5. Metasploit 系統介紹 6. 密碼破解工具 7. Exploit DB 介紹

編號	名稱	內容大綱
S207	基礎資安防禦	1. 縱深防禦 2. 防火牆及入侵偵測系統原理 3. Iptables 及 Snort 4. 其他防禦工具
S208	網路流量分析與檢測實務	1. 網路資料擷取 2. 網路流量分析 3. 網路封包分析
S209	基礎惡意程式分析	1. 惡意程式基本知識 2. 靜態特徵及動態行為分析
S210	APT 攻擊及防範	1. APT 攻擊方式介紹 2. APT 防禦方式介紹
S211	軟體測試除錯	1. 軟體測試理論 2. 軟體安全測試 3. 自動化測試
S212	金融行動支付安全	1. 行動支付安全議題 2. 行動 APP 安全 3. 身分認證安全
S213	物聯網安全	1. 物聯網簡介 2. 物聯網安全議題 3. 物聯網防禦措施
S214	資安威脅情報蒐集及分析	1. 資安日誌蒐集 2. 網路威脅資訊蒐集工具 3. 網路爬蟲工具 4. 偽冒網站或行動應用程式偵測實務
S215	數位鑑識	1. 鑑識程序 2. 電腦系統鑑識(作業系統、網路、資料庫)
S216	電腦稽核	1. 資訊系統稽核 2. 稽核分析能力建置 3. 個資稽核 4. 舞弊稽核
S217	FinTech 應用與科技風險	1. 金融科技導入之風險與效益評估 2. 金融科技之資安管理重點
S218	資安治理	1. 資訊安全治理 2. 資訊風險管理 3. 資訊安全計畫開發與管理 4. 營運持續管理 5. 資訊安全事故管理 6. AI 科技管理 7. 深偽(Deepfake)技術因應策略 8. 供應鏈安全管理 9. 零信任安全策略
S219	資安防護基準(各業別)	1. 金融、證券、期貨、保險各業別資安防護基準說明
S220	雲端安全	1. 雲端系統架構與維運管理 2. 雲端安全基礎

編號	名稱	內容大綱
S221	資安監控聯防	1. 日誌分析實務 2. 金融資安監控組態基準實務 3. 金融電腦系統安全組態基準實務

三、 進階課程

編號	名稱	內容大綱
S301	人工智慧於金融資安應用	1. 人工智慧與機器學習介紹 2. 資安發展應用介紹
S302	金融業密碼學應用實務	1. 密碼學原理(對稱、非對稱加密、雜湊函數、數位簽章) 2. 數位憑證應用 3. 利用 HSM 進行資料加解密 4. 跨行業務及 SWIFT 業務資料安全架構說明
S303	區塊鏈安全	1. 區塊鏈原理 2. 區塊鏈安全性 3. 金融業實務應用及發展
S304	進階程式及網站安全	源碼檢測及修正實務
S305	進階系統及網頁滲透測試	1. 滲透測試工具操作 2. 新攻擊手法介紹 3. 防禦方法介紹
S306	進階惡意程式分析	1. 逆向工程 2. 自動化分析工具
S307	資安資料大數據分析	1. Python 或 R 語言分析 2. 大數據資料庫介紹
S308	資安決策與管理	資安管理個案教學
S309	數位鑑識實務	1. 電子郵件鑑識 2. 惡意程式鑑識 3. 行動裝置鑑識
S401	晶片卡及 ATM 安全	1. 晶片卡原理介紹 2. 晶片卡安全性及防護 3. EMV/晶片金融卡安全機制 4. ATM 整體防護架構 5. ATM 惡意程式檢查與偵測 6. ATM 安全稽核規畫
S402	SWIFT Security bootcamp	SWIFT 安全機制及實務作業
S403	信用卡 PCI DSS 資安合規政策	信用卡 PCI DSS 規範及遵循要求
S404	網路攻防演練	1. 資安攻防演練 2. 重大資安事件應變情境演練
S405	進階雲端安全	1. 雲端數據及日誌分析 2. 雲端安全技術 3. 雲端事件鑑識技術
S406	進階資安監控聯防	1. 威脅獵捕實作 2. 資安監控機制成熟度評估

附錄二：領域核心職能與課程對照表

類別	監督治理/安全開發/資安維運		
領域	資安認知		
核心職能	**CA001：具備基本資訊安全概念** **CA002：熟悉資訊安全管理制度** **CA003：瞭解資訊安全相關法律** **CA004：瞭解個人資料保護議題** **CA005：瞭解新興科技資安威脅**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004
	基礎	S201：辦公室作業安全	CA001

類別	監督治理		
領域	資安管理		
核心職能	**CM001：具備資安策略制定能力** **CM002：具備資安管理決策能力** **CM003：具備跨部門協調能力** **CM004：具備資安人力評估能力** **CM005：具備危機管理能力**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004
	基礎	S201：辦公室作業安全	CA001
		S207：基礎資安防禦	CS001、CS002
		S218：資安治理	CM001、CM002、CM005
		S219：資安防護基準(各業別)	CM001、CM002
		S217：FinTech 應用與科技風險	CM002
		S220：雲端安全	CM001、CM002、CM004
	進階	S308：資安決策與管理	CM002、CM003、CM004
		S404：網路攻防演練	CP002、CP005

類別	監督治理		
領域	資安稽核		
核心職能	**CU001：具備資安系統查核技巧** **CU002：瞭解網路標準相關知識** **CU003：瞭解網路威脅和漏洞**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004
	基礎	S201：辦公室作業安全	CA001
		S202：系統及網路安全	CU002、CU003
		S203：程式開發安全	CD001
		S204：網頁/行動應用程式安全	CD001
		S212：金融行動支付安全	CD001
		S213：物聯網安全	CP002
		S216：電腦稽核	CU001
		S219：資安防護基準(各業別)	CM001、CM002
		S220：雲端安全	CM001、CM002
		S221：資安監控聯防	CA001、CS001、CS002、CS003、CS004、CP001、CP002、CP003、CP005、CI001、CI002、CI003
	進階	S403：信用卡 PCI DSS 資安合規政策	CD001

類別	監督治理		
領域	風險管理		
核心職能	**CR001：瞭解風險管理流程及架構** **CR002：具備資安風險及威脅評估能力**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002、CR001、CR002
		S103：資安法規介紹	CA003、CA004

		S218：資安治理	CM001、CM002、CM005
		S219：資安防護基準(各業別)	CM001、CM002
		S207：基礎資安防禦	CS001、CS002
		S217：FinTech 應用與科技風險	CR002
		S220：雲端安全	CM001、CM002、CR001、CR002
	進階	S301：人工智慧於金融資安應用	CI002
		S402：SWIFT Security bootcamp	CD001
		S403：信用卡 PCI DSS 資安合規政策	CD001

類別	**監督治理**		
領域	**法令遵循**		
核心職能	**CL001：確認作業符合法令規定**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004、CL001
	基礎	S219：資安防護基準(各業別)	CM001、CM002
	進階	S301：人工智慧於金融資安應用	CI002
		S403：信用卡 PCI DSS 資安合規政策	CD001

類別	**安全開發**		
領域	**程式設計**		
核心職能	**CD001：具軟體安全架構規或開發安全軟體能力**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004

	基礎	S201：辦公室作業安全	CA001
		S203：程式開發安全	CD001
		S204：網頁/行動應用程式安全	CD001
		S211：軟體測試除錯	CT002
		S212：金融行動支付安全	CD001
		S219：資安防護基準(各業別)	CM001、CM002
		S220：雲端安全	CM001、CM002
	進階	S302：金融業密碼學應用實務	CD001
		S304：進階程式及網站安全	CD001
		S401：晶片卡及 ATM 安全	CD001
		S402：SWIFT Security bootcamp	CD001
		S403：信用卡 PCI DSS 資安合規政策	CD001
		S404：網路攻防演練	CP002、CP005
		S303：區塊鏈安全	CP002

類別	**安全開發**		
核心領域	**品管測試**		
職能	**CT001：瞭解軟體安全架構及工具能力** **CT002：具分析、蒐集、確認及驗證測試資料能力**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004
	基礎	S201：辦公室作業安全	CA001
		S203：程式開發安全	CT001
		S204：網頁/行動應用程式安全	CT001
		S211：軟體測試除錯	CT002
		S212：金融行動支付安全	CD001
		S220：雲端安全	CM001、CM002

	進階	S302：金融業密碼學應用實務	CD001
		S401：晶片卡及 ATM 安全	CD001
		S402：SWIFT Security bootcamp	CD001
		S403：信用卡 PCI DSS 資安合規政策	CD001

類別	**資安維運**		
領域	**系統網路管理**		
核心職能	**CS001：瞭解網路及系統安全機制** **CS002：具備發展及維護資安機制能力** **CS003：具備執行網路應用工具能力**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004
	基礎	S201：辦公室作業安全	CA001
		S202：系統及網路安全	CS001
		S205：網路探測實務	CS003
		S207：基礎資安防禦	CS001、CS002
		S208：網路流量分析與檢測實務	CS003
		S213：物聯網安全	CP002
		S219：資安防護基準(各業別)	CM001、CM002
		S220：雲端安全	CM001、CM002
		S221：資安監控聯防	CA001、CS001、CS002、CS003、CS004、CP001、CP002、CP003、CP005、CI001、CI002、CI003
	進階	S303：區塊鏈安全	CP002
		S304：進階程式及網站安全	CD001
		S307：資安資料大數據分析	CS002
		S401：晶片卡及 ATM 安全	CP002
		S402：SWIFT Security bootcamp	CP002
		S403：信用卡 PCI DSS 資安合規政	CP002

		策	
		S404：網路攻防演練	CP002、CP005
		S405：進階雲端安全	CS001、CS002、CS003
		S406：進階資安監控聯防	CA001、CS001、CS002、CS003、CS004、CP001、CP002、CP003、CP005、CI001、CI002、CI003

類別	**資安維運**		
領域	**弱點管理**		
核心職能	**CV001：瞭解弱點及相關系統設定等資訊，識別系統安全議題** **CV002：具備執行弱點掃描及弱點修復管理作業能力**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004
	基礎	S201：辦公室作業安全	CA001
		S202：系統及網路安全	CV001
		S203：程式開發安全	CT001
		S204：網頁/行動應用程式安全	CT001
		S205：網路探測實務	CV001、CV002
		S206：基礎系統及網站滲透測試	CV001、CV002
		S220：雲端安全	CM001、CM002
	進階	S305：進階系統及網頁滲透測試	CV001、CV002
		S404：網路攻防演練	CP002、CP005
		S405：進階雲端安全	CV001、CV002

類別	**資安維運**
領域	**資安防護**
核心職能	**CP001：瞭解網路及系統安全機制** **CP002：瞭解資安防護技術** **CP003：瞭解資安威脅及漏洞** **CP004：瞭解加密法**

	CP005：瞭解駭客入侵技術與危機處理		
課程	層級	課程	涵蓋職能
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002
		S103：資安法規介紹	CA003、CA004
	基礎	S201：辦公室作業安全	CA001
		S202：系統及網路安全	CP001
		S204：網頁/行動應用程式安全	CT001
		S205：網路探測實務	CP005
		S206：基礎系統及網站滲透測試	CP003、CP005
		S207：基礎資安防禦	CP001、CP002
		S208：網路流量分析與檢測實務	CS003
		S210：APT 攻擊及防範	CP002、CP005
		S212：金融行動支付安全	CD001
		S213：物聯網安全	CP002
		S214：資安威脅情報蒐集及分析	CI002
		S217：FinTech 應用與科技風險	CR002
		S219：資安防護基準(各業別)	CM001、CM002
		S220：雲端安全	CP001、CP002、CP003
		S221：資安監控聯防	CA001、CS001、CS002、CS003、CS004、CP001、CP002、CP003、CP005、CI001、CI002、CI003
	進階	S301：人工智慧於金融資安應用	CI002
		S302：金融業密碼學應用實務	CP002、CP004
		S303：區塊鏈安全	CP002
		S304：進階程式及網站安全	CD001
		S305：進階系統及網頁滲透測試	CV001、CV002
		S307：資安資料大數據分析	CI002
		S401：晶片卡及 ATM 安全	CP002
		S402：SWIFT Security bootcamp	CP002
		S403：用卡 PCI DSS 資安合規政策	CP002

		S404：網路攻防演練	CP002、CP005
		S405：進階雲端安全	CP002、CP005
		S406：進階資安監控聯防	CA001、CS001、CS002、CS003、CS004、CP001、CP002、CP003、CP005、CI001、CI002、CI003

類別	**資安維運**		
領域	**事件應變**		
核心職能	**CI001：瞭解事件回應及處理方法** **CI002：具備網路威脅情資蒐集及分析能力** **CI003：具備各系統之數位鑑識能力**		
課程	**層級**	**課程**	**涵蓋職能**
	通識	S101：資訊安全概論	CA001、CA005
		S102：ISMS 資訊安全管理系統	CA002、CI001
		S103：資安法規介紹	CA003、CA004
	基礎	S205：網路探測實務	CP005
		S207：基礎資安防禦	CP001、CP002
		S208：網路流量分析與檢測實務	CS003
		S209：基礎惡意程式分析	CI002
		S210：APT 攻擊及防範	CP002、CP005
		S214：資安威脅情報蒐集及分析	CI002
		S215：數位鑑識	CI003
		S219：資安防護基準(各業別)	CM001、CM002
		S220：雲端安全	CM001、CM002
		S221：資安監控聯防	CA001、CS001、CS002、CS003、CS004、CP001、CP002、CP003、CP005、CI001、CI002、CI003
	進階	S301：人工智慧於金融資安應用	CI002
		S306：進階惡意程式分析	CI002
		S307：資安資料大數據分析	CI002
		S309：數位鑑識實務	CI003
		S402：SWIFT Security bootcamp	CP002

類別	**資安維運**		
領域	**事件應變**		
核心職能	**CI001：瞭解事件回應及處理方法** **CI002：具備網路威脅情資蒐集及分析能力** **CI003：具備各系統之數位鑑識能力**		
		S404：網路攻防演練	CI001、CI002、CI003
		S405：進階雲端安全	CI001、CI002、CI003
		S406：進階資安監控聯防	CA001、CS001、CS002、CS003、CS004、CP001、CP002、CP003、CP005、CI001、CI002、CI003

附錄三：學習地圖

各領域(職務)培訓順序，由基礎至進階；課程層級由上至下。

領域(職務)	課程層級		
	通識	基礎	進階
資安管理	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S218 資安治理 S207 基礎資安防禦 S219 資安防護基準(各業別) S201 辦公室作業安全 S220 雲端安全 S221 資安監控聯防 S217 FinTech 應用與科技風險	S308 資安決策與管理 S404 網路攻防演練
資安稽核	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S216 電腦稽核 S219 資安防護基準(各業別) S201 辦公室作業安全 S202 系統及網路安全 S203 程式開發安全 S204 網頁/行動應用程式安全 S212 金融行動支付安全 S213 物聯網安全 S220 雲端安全 S221 資安監控聯防	S403 信用卡 PCI DSS 資安合規政策
風險管理	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S207 基礎資安防禦 S219 資安防護基準(各業別) S218 資安治理 S220 雲端安全 S217 FinTech 應用與科技風險	S402 SWIFT Security bootcamp S403 信用卡 PCI DSS 資安合規政策 S301 人工智慧於金融資安應用
法令遵循	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S219 資安防護基準(各業別)	S403 信用卡 PCI DSS 資安合規政策 S301 人工智慧於金融資安應用
程式設計	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S219 資安防護基準(各業別) S201 辦公室作業安全 S203 程式開發安全 S204 網頁/行動應用程式安全 S212 金融行動支付安全 S211 軟體測試除錯 S220 雲端安全	S302 金融業密碼學應用實務 S303 區塊鏈安全 S304 進階程式及網站安全 S401 晶片卡及 ATM 安全 S402 SWIFT Security bootcamp S403 信用卡 PCI DSS 資安合規政策 S404 網路攻防演練
品管測試	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S201 辦公室作業安全 S203 程式開發安全 S204 網頁/行動應用程式安全 S211 軟體測試除錯 S212 金融行動支付安全 S220 雲端安全	S302 金融業密碼學應用實務 S401 晶片卡及 ATM 安全 S402 SWIFT Security bootcamp S403 信用卡 PCI DSS 資安合規政策
系統網路管理	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S219 資安防護基準(各業別) S201 辦公室作業安全 S202 系統及網路安全 S220 雲端安全 S205 網路探測實務 S207 基礎資安防禦 S208 網路流量分析與檢測實務 S213 物聯網安全	S303 區塊鏈安全 S304 進階程式及網站安全 S405 進階雲端安全 S401 晶片卡及 ATM 安全 S402 SWIFT Security bootcamp S403 信用卡 PCI DSS 資安合規政策 S307 資安資料大數據分析 S404 網路攻防演練

領域 (職務)	課程層級		
	通識	基礎	進階
		S221 資安監控聯防	S406 進階資安監控聯防
弱點管理	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S201 辦公室作業安全 S202 系統及網路安全 S203 程式開發安全 S204 網頁/行動應用程式安全 S220 雲端安全 S205 網路探測實務 S206 基礎系統及網站滲透測試	S305 進階系統及網頁滲透測試 S405 進階雲端安全 S404 網路攻防演練
資安防護	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S219 資安防護基準(各業別) S201 辦公室作業安全 S202 系統及網路安全 S204 網頁/行動應用程式安全 S205 網路探測實務 S206 基礎系統及網站滲透測試 S207 基礎資安防禦 S221 資安監控聯防 S208 網路流量分析與檢測實務 S210 APT 攻擊及防範 S212 金融行動支付安全 S220 雲端安全 S213 物聯網安全 S214 資安威脅情報蒐集及分析 S217 FinTech 應用與科技風險	S302 金融業密碼學應用實務 S303 區塊鏈安全 S304 進階程式及網站安全 S405 進階雲端安全 S305 進階系統及網頁滲透測試 S401 晶片卡及 ATM 安全 S402 SWIFT Security bootcamp S403 信用卡 PCI DSS 資安合規政策 S307 資安資料大數據分析 S301 人工智慧於金融資安應用 S406 進階資安監控聯防 S404 網路攻防演練
事件應變	S101 資訊安全概論 S102 ISMS 資訊安全管理系統 S103 資安法規介紹	S219 資安防護基準(各業別) S205 網路探測實務 S207 基礎資安防禦 S220 雲端安全 S221 資安監控聯防 S208 網路流量分析與檢測實務 S209 基礎惡意程式分析 S210 APT 攻擊及防範 S214 資安威脅情報蒐集及分析 S215 數位鑑識	S405 進階雲端安全 S406 進階資安監控聯防 S306 進階惡意程式分析 S309 數位鑑識實務 S307 資安資料大數據分析 S301 人工智慧於金融資安應用 S404 網路攻防演練

附錄四：課程與資通安全專業證照對照表

說明：持有數位發展部發布之資通安全專業證照且持續維持有效者，可免除受訓本職能地圖之相關課程層級。

數位發展部資通安全專業證照			金融資安人才職能地圖		可免除之課程層級		
發證單位	類別	證照名稱	類別	領域	通識	基礎	進階
TAF	管理類	ISO/IEC27001:2022Information Security Management System(ISMS) Auditor/ Lead Auditor	資安認知	資安認知	V		
TAF	管理類	ISO 22301 Business Continuity Management System(BCMS) Auditor/Lead Auditor			V		
TAF	管理類	ISO/IEC 29100 Lead Privacy Implementer Information technology —Security techniques —Privacy framework			V		
TAF	管理類	SO/IEC 27701:2019 Privacy Information Management System Lead Auditor			V		
EC-Council	管理類	EC-Council Information Security Management(EISM)	監督治理	資安管理			V
GIAC	管理類	GIAC Security Leadership(GSLC)					V
GIAC	管理類	GIAC Strategic Planning, Policy, and Leadership(GSTRT)					V
EC-Council	管理類	Certified Chief Information Security Officer (CCISO)					V
ISACA	管理類	Certified Information Security Manager(CISM)					V
ISACA	管理類	Certified in the Governance of Enterprise IT (CGEIT)					V
(ISC)2	技術類	Information Systems Security Management Professional(CISSP -ISSMP)					V
GIAC	管理類	GIAC Systems and Network Auditor(GSNA)		資安稽核			V
ISACA	管理類	Certified Information Systems Auditor (CISA)					V
ISACA	管理類	Certified in Risk and Information Systems Control (CRISC)		風險管理			V
(ISC)2	技術類	Certified Authorization Professional(CAP)					V
GIAC	管理類	GIAC Law of Data Security & Investigations(GLEG)		法令遵循			V

數位發展部資通安全專業證照			金融資安人才職能地圖		可免除之課程層級		
發證單位	類別	證照名稱	類別	領域	通識	基礎	進階
EC-Council	技術類	Certified Application Security Engineer (CASE)	安全開發	程式設計		V	
GIAC	技術類	GIAC Secure Software Programmer-Java(GSSP-JAVA) 註：GSSP-JAVA 已無相關課程，且不再發行證照。				V	
GIAC	技術類	GIAC Secure Software Programmer-.NET(GSSP-.NET) 註：GSSP-.NET 已無相關課程，且不再發行證照。				V	
GIAC	技術類	GIAC Python Coder(GPYC)					V
GIAC	技術類	GIAC Certified Web Application Defender(GWEB)					V
(ISC)2	技術類	Certified Secure Software Lifecycle Professional(CSSLP)					V
GIAC	技術類	GIAC Web Application Penetration Tester(GWAPT)		品管測試			V
GIAC	技術類	GIAC Certified Windows Security Administrator(GCWN)	資安維運	系統管理			V
GIAC	技術類	GIAC Certified UNIX Security Administrator(GCUX)					V
(ISC)2	技術類	Systems Security Certified Practitioner(SSCP)					V
CREST	技術類	The CREST Registered Technical Security Architect Examination (CRTSA)					V
GIAC	管理類	GIAC Information Security Professional(GISP) 註：GISP 應屬技術類證照。					V
(ISC)2	技術類	Certified Information Systems Security Professional(CISSP)					V
(ISC)2	技術類	Information Systems Security Architecture Professional(CISSP -ISSAP)					V
(ISC)2	技術類	Information Systems Security Engineering Professional(CISSP -ISSEP)					V
經濟部	技術類	iPAS 資訊安全工程師中級能力鑑定		資安防護		V	
EC-Council	技術類	Certified Network Defender Course (CND)				V	
EC-Council	技術類	Certified Ethical Hacker(CEH)				V	
EC-Council	技術類	Certified Threat Intelligence Analyst (CTIA)				V	
GIAC	技術類	GIAC Security Essentials(GSEC)				V	

數位發展部資通安全專業證照			金融資安人才職能地圖		可免除之課程層級		
發證單位	類別	證照名稱	類別	領域	通識	基礎	進階
GIAC	技術類	GIAC Certified Intrusion Analyst(GCIA)	資安維運	資安防護		V	
GIAC	技術類	GIAC Information Security Fundamentals(GISF)				V	
CompTIA	技術類	CompTIA Security (CompTIA Security+)				V	
Cisco	技術類	CCNA 200-301 Implementing and Administering Cisco Solutions				V	
Cisco	技術類	CBROPS 200-201 Cisco Certified CyberOps Associate certification				V	
EC-Council	技術類	~~EC-Council Certified Security Analyst(ECSA)~~ ~~註：EC-Council 業以~~ EC-Council Certified Penetration Tester(CPENT)~~取代 ECSA。~~					V
GIAC	技術類	GIAC Certified Perimeter Protection Analyst(GPPA) 註：GPPA 已無相關課程，且不再發行證照。					V
GIAC	技術類	GIAC Critical Controls Certification(GCCC)					V
GIAC	技術類	GIAC Continuous Monitoring Certification(GMON)					V
GIAC	技術類	GIAC Mobile Device Security Analyst(GMOB)					V
GIAC	技術類	GIAC Assessing and Auditing Wireless Networks(GAWN)					V
GIAC	技術類	GIAC Cyber Threat Intelligence(GCTI)					V
(ISC)2	技術類	Systems Security Certified Practitioner(SSCP)					V
(ISC)2	技術類	Certified Cloud Security Professional(CCSP)					V
CompTIA	技術類	CompTIA Cybersecurity Analyst (CySA+)					V
CompTIA	技術類	CompTIA Advanced Security Practitioner (CASP+)					V
CREST	技術類	The CREST Registered Threat Intelligence Analyst (CRTIA)					V
CREST	技術類	The CREST Certified Threat Intelligence Manager (CC TIM)					V
CREST	技術類	The CREST Practitioner Intrusion Analyst (CP IA)					V
CREST	技術類	The CREST Registered Intrusion Analyst (CRIA)					V
CREST	技術類	The Certified Network Intrusion Analyst (CC NIA)					V
CREST	技術類	The CREST Certified Host Intrusion Analyst (CC HIA)					V

數位發展部資通安全專業證照			金融資安人才職能地圖		可免除之課程層級		
發證單位	類別	證照名稱	類別	領域	通識	基礎	進階
GIAC	技術類	GIAC Certified Detection Analyst (GCDA)	資安維運	資安防護			V
GIAC	技術類	GIAC Security Expert(GSE)					V
(ISC)2	技術類	Certified Information Systems Security Professional(CISSP)					V
GIAC	技術類	GIAC Defending Advanced Threats(GDAT)	資安維運	弱點管理			V
GIAC	技術類	GIAC Penetration Tester(GPEN)					V
(ISC)2	技術類	Systems Security Certified Practitioner(SSCP)					V
CompTIA	技術類	CompTIA PenTest (CompTIA PenTest+)					V
CREST	技術類	The CREST Practitioner Security Analyst (CPSA)					V
CREST	技術類	The CREST Certified Wireless Specialist (CCWS)					V
Offensive Security	技術類	Offensive Security Certified Professional(OSCP)					V
Offensive Security	技術類	Offensive Security Wireless Professional(OSWP)					V
GIAC	技術類	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)					V
GIAC	技術類	GIAC Security Expert(GSE)					V
(ISC)2	技術類	Certified Information Systems Security Professional(CISSP)					V
Offensive Security	技術類	Offensive Security Certified Expert(OSCE)					V
Offensive Security	技術類	Offensive Security Exploitation Expert(OSEE)					V
Offensive Security	技術類	Offensive Security Web Expert(OSWE)					V
EC-Council	技術類	EC-Council Certified Incident Handler(ECIH)	資安維運	事件應變		V	
EC-Council	技術類	Computer Hacking Forensic Investigator(CHFI)				V	
ISFCE	技術類	Certified Computer Examiner(CCE)				V	

數位發展部資通安全專業證照			金融資安人才職能地圖		可免除之課程層級		
發證單位	類別	證照名稱	類別	領域	通識	基礎	進階
EC-Council	技術類	EC-Council Disaster Recovery Professional(EDRP)	資安維運	事件應變			V
GIAC	技術類	GIAC Certified Incident Handler (GCIH)					V
GIAC	技術類	GIAC Certified Forensic Analyst(GCFA)					V
GIAC	技術類	GIAC Certified Forensic Examiner(GCFE)					V
GIAC	技術類	GIAC Reverse Engineering Malware(GREM)					V
GIAC	技術類	GIAC Network Forensic Analyst(GNFA)					V
GIAC	技術類	GIAC Advanced Smartphone Forensics(GASF)					V
(ISC)2	技術類	Systems Security Certified Practitioner(SSCP)					V
CREST	技術類	The CREST Certified Simulated Attack Specialist (CC SAS)					V
CREST	技術類	The CREST Certified Simulated Attack Manager (CC SAM)					V
CREST	技術類	The CREST Certified Malware Reverse Engineer (CCMRE)					V
CREST	技術類	The CREST Certified Incident Manager					V
GIAC	技術類	GIAC Security Expert(GSE)					V
(ISC)2	技術類	Certified Information Systems Security Professional(CISSP)					V

金融資安人才職能地圖修正重點說明

因應本會近年辦理資安攻防演練、112 年修正金融機構導入雲端服務相關法規及實務運作需求，增修相關課程內容，謹就修正重點說明如下：

一、 雲端安全

因應金融業上雲法規修正，新增「雲端安全」及資安趨勢課程，培訓金融機構規劃或維運雲端服務所需資安人才，以強化雲地系統整合安全，提升金融服務韌性。

二、 新興科技運用

因應新興科技運用(如 AI、供應鏈安全、零信任等)，新增「AI 科技管理」、「深偽(Deepfake)技術因應策略」、「身分認證安全」、「供應鏈安全管理」及「零信任安全策略」等課程內容。

三、 資安攻防演練

配合本會近年推動金融資安攻防演練及演訓合一，對參與金融機構及人員均具實效，爰調整「網路攻防演練」課程內容為「資安攻防演練」及「重大資安事件應變情境演練」，以持續鼓勵金融機構派員參與實兵對抗演練或情境演練。

四、 資安監控聯防

為強化金融機構資安監控有效性及金融資安聯防監控(F-SOC)機制，新增「資安監控聯防」課程，鼓勵金融機構參採金融資安監控組態基準及電腦系統安全組態基準。

五、 應用程式介面(API)安全

API 為系統間互通之介面，為駭客主要攻擊標的之一，為提升 API 及 Web 應用程式安全性，爰於「應用程式介面(API)安全」課程新增「API 安全要求、API OWASP Top 10 介紹及安全建議」等課程內容建議。