銀行業 《 能力標準說明 》 能力單元

職能範疇- 6. 科技管理

(主要職能 – 6.2 資訊科技系統保安/網絡安全)

名稱	評估網絡安全風險保護的有效性，並進行事件監測和報告
編號	109375L4
應用範圍	評估銀行網絡安全風險保護和報告架構的總體有效性;包括向銀行提供管理資訊，並就防止網絡犯罪、偵查和事件管理流程、政策、程序和管治活動的有效性進行獨立評估。 這職能包括評估人工智能 （AI）、區塊鏈、大數據收集和分析等不同系統等。
級別	4
學分	3 （僅供參考）
能力	表現要求 1. 職務範圍的知識 能夠: • 掌握最新技術知識並將其應用於評估網絡安全的發展; • 瞭解網絡安全的行業實務操作方法，並運用最佳實務操作對網絡犯罪管理的標準、準則指引和程序以及這些活動的實施和管治進行詳細評估。 2. 應用 能夠: • 分析由於系統配置不良或不正確，已知和/或未知的硬件或軟件缺陷或操作弱點導致的潛在漏洞的系統; • 識別具體的漏洞，並提供詳細的說明來緩減或消除每種風險; • 執行網絡安全審核，配合其他營運審計如：資訊科技事件管理流程、網絡和伺服器的配置管理和安全性、保安管理和意識、業務延續性管理，信息安全管理，管治和管理實務操作等，並和業務單位及第三方保持一致的協作關係; • 設計和實施“網絡防禦”對安全措施和表現進行獨立檢討，評估和確定加強企業安全的機會。 3. 專業行為及態度 能夠: • 對銀行進行全面的網絡風險評估，並將調查結果簡化為審計委員會和管理團隊的簡要摘要，從而推動以風險為本的網絡安全審計計劃; • 評估完整的網絡安全框架;將目前的狀況與銀行的目標框架特徵和銀行業預期的網絡安全實務操作進行比較; • 根據網絡風險評估的結果，誠實地報告現有系統的缺陷和不足，接受具建設性的反饋，積極尋求改進措施。
評核指引	此能力單元的綜合成效要求為: • 遵循銀行的標準程序，進行全面審計，定期評估銀行的網絡安全有效性，並提交報告給管理團隊，藉以改進未來的審計規劃。
備註	