銀行業 - 零售銀行門類 《 能力標準說明 》

科技管理 > 5.1 資訊及網絡保安

名稱	進行審計，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	107427L4
應用範圍	為銀行管理層提供有關網絡犯罪預防、偵測和事件管理流程、政策、程序和管治活動的有效性的獨立評估
級別	4
學分	3
能力	表現要求 1. 具備新發展的知識，應用最新技術和行業中最佳實務操作來設計網絡安全審計 能夠: • 評估網絡安全的發展，並掌握最新技術和行業實務操作 • 應用最佳實務操作進行詳細評估，重點置於網絡犯罪管理標準、準則和步驟、以及該活動的實施和管治 • 領導和執行網絡安全審核，與資訊科技 (IT) 和業務單位的事件管理流程、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的其他營運審計以及和第三方的關係保持一致。 2. 分析銀行系統並識別潛在的漏洞 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 • 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. 進行整體網絡風險審計，並向銀行管理層報告 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 • 基於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： • 引導和執行全面審計，定期評估銀行網絡安全效能，並向管理團隊提交報告藉以進行改善和未來審計規劃
備註	