資訊及通訊科技業 《 能力標準說明 》 能力單元

「資訊保安」職能範疇

名稱	從技術和法律方面設計數碼鑑識過程
編號	111167L6
應用範圍	設計對網絡攻擊進行數碼鑑識調查的程序。該程序應遵守企業的政策，並承擔相關的管轄
級別	6
學分	3 （僅供參考）
能力	表現要求 1. 掌握該領域的知識 • 瞭解數碼鑑識的需求、重要性和局限性 • 瞭解進行數碼鑑識調查所需的工具 • 瞭解數據恢復的過程和最新的技術發展 • 認識到資訊科技技術的變化以及它們如何影響數碼鑑識 • 瞭解與企業的業務運作和數碼鑑識有關的法律 2. 設計程序 • 建立識別證據的程序，並確定它們的存儲位置 • 建立一套隔離、保護和保存數據的準則，以防止可能的篡改 • 建立數據重建/恢復和數據分析的協議，以得出攻擊的結論 • 制定一個系統來記錄所有相關的數據、證據和程序 • 建立總結數據的程序，使非資訊科技人員，例如律師和法官，能夠對事件的影響和後果有一個基本的了解 • 確保所有執行的程序都遵守企業的政策，並對相關的管轄範圍負有責任
評核指引	此能力單元的綜合成效要求為： • 設計數碼鑑識過程。該過程應包括證據識別、數據保存、數據分析和文件記錄 • 所有的程序都應遵守企業的政策，並遵守相關的管轄權
備註	