

資訊科技及通訊業標準說明

能力單元

1. 名稱	制定偵查、確定和分析保安事件的過程
2. 編號	ITSWIS613A
3. 應用範圍	制定和執行偵查、確定和分析與保安相關的事件的過程，支持機構的正常營運及遠離安全威脅 [資訊保安 - 應變管理]
4. 級別	6
5. 學分	2
6. 能力	<p align="right">表現要求</p> <p>6.1 瞭解支援的過程 有能力</p> <ul style="list-style-type: none"> <li>▪ 確定用戶報告的保安事件(有能力確定某事件是假設了能夠由其他事件區別某事件)</li> <li>▪ 解釋為什麼一些支援問題是保安事件，而其他並不是</li> </ul> <p>6.2 熟悉資訊保安事件的偵查和報告的政策和過程 有能力制定過程，偵查和確定資訊保安事件</p> <p>6.3 制定處理保安事件的過程 有能力制定和執行過程，偵查、確定和分析與機構保安相關的事件，</p> <p>6.4 以專業方式制訂過程，應付保安事件 有能力制定和執行過程，偵查、確定和分析與機構保安相關的事件，並符合機構內部指引及任何適用的(包括本地及國際)法律與監管要求</p>
7. 評核指引	<p>上述能力單元之綜合能力要求為</p> <p>(i) 為機構制定和執行過程，偵查，確定和分析與保安相關的事件；並且</p> <p>(ii) 確保已制定的和已執行的過程符合機構內部指引以及任何適用的(本地和國際)法律和監管要求</p>
備註	