

資訊科技及通訊業標準說明  
能力單元

1. 名稱	進行營運保安的風險評估和審計
2. 編號	ITSWOS530A
3. 應用範圍	為機構資訊科技操作提供保安管理服務時，執行定期的營運保安的風險評估及內部保安審計，並落實基於保安風險評估及審計結果的建議 [營運與支援 - 保安管理服務]
4. 級別	5
5. 學分	2
6. 能力	<p style="text-align: right;"><u>表現要求</u></p> <p>6.1 熟悉公司的保安要求和業務流程 有能力</p> <ul style="list-style-type: none"> <li>▪ 理解規定的保安控制計劃</li> <li>▪ 顯示對用戶管理和系統管理流程的瞭解</li> </ul> <p>6.2 計劃風險評估和保安審計 有能力</p> <ul style="list-style-type: none"> <li>▪ 遵守保安風險評估和內部保安審計時間表的要求</li> <li>▪ 與目標營運單位溝通，並協議時間表</li> </ul> <p>6.3 執行定期的保安風險評估及內部保安審計 有能力</p> <ul style="list-style-type: none"> <li>▪ 識別和分類影響保安環境的風險</li> <li>▪ 執行定期的保安風險評估</li> <li>▪ 執行定期的內部保安審計，以確保符合既定的指引和程序</li> <li>▪ 推薦跟進行動以加強保安控制</li> </ul> <p>6.4 落實基於保安風險評估及審計結果的建議 有能力</p> <ul style="list-style-type: none"> <li>▪ 評估建議的成本、效益和效率</li> <li>▪ 尋找管理層對有關建議的支持</li> <li>▪ 落實這些建議</li> </ul> <p>6.5 以專業方式執行定期的保安風險評估及內部保安審計，並落實基於保安風險評估及審計結果的建議 有能力</p> <ul style="list-style-type: none"> <li>▪ 在進行風險評估和內部審計時，減少對目標營運單位的干擾</li> <li>▪ 遵從機構內部指引和程序以及任何適合的(本地及國際)法律和監管要求</li> </ul>
7. 評核指引	上述能力單元之綜合能力要求為 (i) 執行定期的保安風險評估及內部保安審計；並且

	(ii) 落實基於保安風險評估及審計結果的建議
備註	<ol style="list-style-type: none"><li>1. 假設參與者具備廣泛的資訊科技及其應用的知識</li><li>2. 上述能力單元包含 ITIL 保安管理服務的基礎建設環境的保安計劃和營運</li></ol>