

網絡基建及營運之能力單元

1.名稱	釐定網絡系統的接入控制	
2.編號	ITCSNO531A	
3.應用範圍	網絡是一種用來連接設備和共用資源的普及方法。網絡系統是一個把 LAN，WAN 或 MAN 上的裝置互連之網狀結構。控制措施則能管理接入網絡系統的授權。本能力單元介紹從電訊服務營運商的角度，釐定網絡系統的接入控制之能力，即在“接入網絡”水平上的控制。	
4.級別	4	
5.學分	4	
6.能力	<p>能力要求</p> <p>6.1 具備有關知識</p> <ul style="list-style-type: none"> ● 在公司的接入和安全性原則上，擁有廣博的知識 ● 在公司的安全框架或國際安全框架的標準方面，擁有豐富的經驗，例如 ISO17799 ● 在公司的網絡基建（硬件和軟件組件）上，具備經驗 ● 在安全的原則，減災技術，控制實施和最佳做法上，擁有豐富的經驗 ● 在分析和確定各種安全風險上具專業水平，包括可能的攻擊方法、如針對訊號層、用戶資料庫、網絡元素、網關、詐騙和服務中斷等 ● 完全理解網絡接入所需的產品和服務 ● 熟知健康和安全規則以及危害 <p>6.2 釐定網絡系統的接入控制</p> <p>能夠：</p> <ul style="list-style-type: none"> ● 與網絡支援團隊合作，以確認安全風險 ● 組合並把風險排列成三個範疇。三個需要考慮的範疇包括：物理、技術和行政方面 ● 為三個範疇釐定安全控制措施： 物理控制：安全措施用來阻止未經授權的人士以物理方法接入物理網絡，如保安人員、閉路電視、鎖等 技術控制：以無需使用物理結構的方法管理接入，如加密、SIM 卡、網絡身份驗證等 行政：以人的因素釐定安全措施，確定哪些用戶可以接入哪些資源：接入級別、個人註冊和賬戶、培訓和意識、職責分解、防災準備等 ● 釐定測量控制的基準 ● 釐定監控和測量的程序/計劃。此程序應為每個控制措施，說明職責及負責人（即釐定所有權） ● 記錄控制措施、預防措施及針對安全性漏洞應採取的補救措施 ● 把有關安全控制的文檔分發給相應的持份者。安排簡介會及演示會，以確保能充分理解內容和職責 <p>6.3 展示專業能力</p> <ul style="list-style-type: none"> ● 確保釐定的防護措施符合公司的安全政策 ● 時刻注意各相關技術、環境和法律因素，並從中取得適當的平衡 	

7.評核指引	此能力單元的綜合成效要求為： i. 有效地與同事溝通，以確定接入網絡的安全性漏洞；和為風險分級 ii. 確認和制定正確的控制措施，使合法授權能夠接入網絡，並防止未經授權的接入 iii. 設計有效的監測和測量功能或程序，以測量控制措施的有效性，克服弱點和迅速作出修訂 使用適當的方法，如培訓和文檔，以確保持份者都意識到這些控制措施，及把這些控制措施納入業務使用之中
備註	