以資訊韌性協助金融服務面對挑戰

金融科技隱憂 您有對策了嗎？

撰文：

BSI 台灣
吳晟熙 客戶經理
peter.wu@bsigroup.com

BSI 台灣
花俊傑 客戶經理
jack.hua@bsigroup.com

隨著「金融科技（FinTech）」一詞被廣泛的討論及使用，包括電子支付、P2P 網路放貸、機器人理財、大數據核保理賠、大數據分析與預測、區塊鍊等技術已逐漸應用於創新的金融服務，將給予企業及消費者與過往截然不同的使用經驗。但是，金融業於推展業務時也須留意金融服務應遵循的法令法規義務，避免因違反遵循義務而產生來自於主管機關的行政裁罰或財務上的損失。因應上述的發展趨勢，BSI 提出了資訊韌性（Information Resilience），協助金融服務業者在面對金融科技、法令法規遵循和甚至未知的挑戰時，能藉由資訊韌性協助企業提供安全、穩定且持續運作的金融服務。資訊韌性是組織韌性(Organizational Resilience) 的一環，是指組織能夠預測、準備和應對可能突發的營運危機，擁有充份的能力可以因應變化，最後得以持續生存並且繁榮興盛。

組織韌性的敲門磚：國際標準

英國標準 BS 65000 針對韌性的本質給予清楚的描述，也提到了發展組織韌性的方法，也就是透過整合現有的作業流程，讓複雜的組織運作能夠透過協同運作的方式，建立組織因應各項問題的能力。基本上，組織韌性已是現代企業邁向成功的驅動力，它主要包括了以下三大領域：

- 營運韌性（Operational Resilience） - 聚焦於提升組織的營運能力，強化產品、服務與流程的績效和永續性，進一步防範組織在財務與聲譽方面受到損害。

- 資訊韌性（Information Resilience） - 管理組織的實體與數位資訊，強調資訊的生命週期管理，從資訊的產生到終止，讓各方的利害關係人都能安全且有效率地取得、儲存及使用資訊。
- 供應鏈韌性（Supply Chain Resilience） - 它是量化與緩和供應鏈風險的能力，包含了採購、製造、運輸、銷售的生命週期，以適當的管理機制將供應鏈中斷的衝擊減至最小，並且保護組織免於財務和聲譽的損害。

具有組織韌性的企業將較其他組織更為健康、更具適應力，即便經營環境變得複雜難測，也能克服長期成長的考驗，挽救或避免營運上的失誤，並防範經濟浪潮的波動對企業帶來致命威脅。

組織韌性是企業成功的驅動力
包含 3 大重要領域：

金融業資訊韌性的第一步：基礎標準

金融服務業者可以藉由建置資訊科技治理的各項基礎標準來發展組織的資訊韌性，包括各類管理系統的核心精神 ISO 31000 風險管理、ISO/IEC 27001 資訊安全管理系統、BS 10012 個人資訊管理系統、ISO 20000-1 IT 服務管理系統與 ISO 22301 營運持續管理系統。

金融業資訊韌性的第二步：特定議題標準

在充分佈署資訊韌性的基礎標準後，金融服務業者可再根據所屬產業的重要趨勢與議題（如下頁圖一）來延伸並擴大資訊治理範圍。其中在推展金融科技服務時被高度關注的議題包含行動金融服務、新興科技安全控管、ICT 供應鏈安全等。同時，金融服務業者也需要兼顧金融科技服務的法規遵循，包括未來將施行的關鍵基礎建設保護（CIB）、金融科技創新法規等。

因此在以基礎標準作為框架，完成建立資訊韌性的第一步之後，可以進一步參考及應用與其產業重要議題相關的國際標準，例如 ISO 12812（行動金融服務安全）、PCI DSS（行動支付安全）、ISO/IEC 27017 與 27018（雲端安全）、PAS 7000（供應鏈風險管理）等，讓客戶都能安全且有效率地取得、儲存及使用資訊。（如下頁圖二）

「整合」為發展資訊韌性的必要條件

伴隨科技的發展，金融服務業者面臨的議題不但多樣化、複雜且未知性高。建置資訊安全管理系統（ISMS）等基礎標準已成為發展資訊韌性的必要基礎，在基礎標準的治理框架上收納其關注的各式議題（包括管理、技術及法規遵循層面），參考及應用其他國際標準、作業規範及業界最佳實務，更有效來預測、準備和應對可能突發的資訊安全危機，為金融服務業者展現其資訊韌性能力的關鍵因素。●

圖一、資訊韌性的基礎標準及進階議題/風險

1 打樁 固基礎

5 大資訊韌性基礎標準

- ISO/IEC 27001 資訊安全管理
- BS 10012 個人資料管理系統
- ISO/IEC 20000-1 IT服務管理系統
- ISO 22301 營運持續管理系統
- ISO 31000 風險管理

2 鑑別 議題與風險

找出重要議題，例如：

- ☑ 關鍵資訊基礎建設保護 (CIIP)
- ☑ 國際支付卡產業 資料安全規範
- ☑ 新興科技安全控管
- ☑ ICT供應鏈安全

3 借鑑 最佳實務

學習應用相關進階標準

- → 資通安全管理法 及其他標準
- → PCI DSS、FinTech相關標準及其他
- → FinTech相關標準、雲端安全標準及其他
- → ISO 27036、PAS 7000 及其他標準

名師指引，快速上手

點超連結看相關課程

圖二、金融業資訊韌性 Step by Step

聯繫 BSI 取得**更多**議題與風險的關聯標準及相關課程資訊

BSI英國標準協會
T: +886 2 2656 0333 | E: infotaiwan@bsigroup.com | www.bsigroup.tw