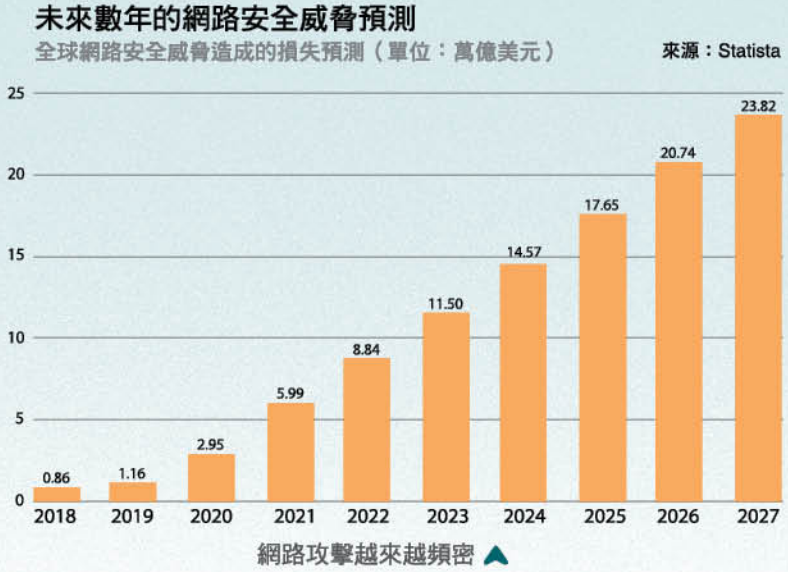
IT合規

資訊科技辦公室

為甚麼 IT 合規性很重要

網路安全威脅不斷演變，越來越複雜並且攻擊會越來越頻密。每個機構必須保持警惕，應對威脅，以最大限度地減少成為受害者和新聞頭條的機會。



市場上有不少基於科技的解決方案以應對網路安全威脅。然而，在保障安全方面，人是最薄弱的環節。

防火牆等科技解決方案主要是防範外來入侵，但員工來自內部，系統一般信賴員工誠信而不會監管。正因如此，大部分資訊事故都是由員工引起。丟失 USB、採用強度較弱的電腦密碼和發送電子郵件到錯誤的收件者……都是常見的人為錯誤。

為了加強員工聯繫，機構應制定和發佈 IT 安全政策，以確保員工可以在特定的隱私和安全要求、指南和最佳實踐的範圍內工作。這些政策提供了指令、規則和實踐的基礎，規範機構如何管理、保護和分發資訊。

IT 安全政策可以幫助機構避免聲譽受損。如果機構被發現違反法律時，可能會對其公眾形象產生負面影響，進而導致客戶和收入的流失。因此，IT 合規性對於機構識別和避免業務中可能出現的安全相關問題非常重要。

檢討合規程度

資訊科技辦公室 (ITO) 自 2020 年底成立以來，發佈了多項資訊科技政策。

為評估服務單位的資訊科技政策合規程度，ITO 於 2023 年展開資訊科技政策合規檢討，並與 10 個明愛服務單位會面。合規檢討的主要目標包括：(1) 了解服務單位如何從其角度看待政策，及 (2) 評估不同服務單位遵守政策要求的程度。透過檢討，ITO 試圖找出各單位在遵守政策上所面臨的困難，以及可以做出哪些改善。此外，ITO 希望能夠發現一些單位的良好做法，並與其他單位和部門分享。

檢討的主要目的不是要找出有關單位的問題，而是要與他們一起了解政策所須及作出改進。其實，ITO 將項目命名為檢討而不叫審核，就是為了讓服務單位在檢討時放鬆一些，以便進行更深入坦率的討論。

檢討的內容是保密的，不便在此透露。總體而言，單位與其 IT 支援之間存在密切的工作關係，並且他們可以遵守大多數政策。單位對檢討表示歡迎，並在檢討過程中與 ITO 合作。

ITO 為各服務單位提出了改善安全的建議，服務單位也希望做出改進。檢討工作有助於服務單位縮小差距以實現合規性，這是一項每年都值得做的練習。