實施ISO/IEC 27001資訊安全管理系統認證

減低機構運作風險

踏入資訊時代，無論從事任何行業，都已經與互聯網密不可分，而隨之而來的資訊保安問題，便令掌握大量敏感及私隱資料的機構格外關注。機構透過推行資訊安全管理系統（Information Security Management System，簡稱ISMS），並申請ISO/IEC 27001 ISMS認證，能有效地管理資訊及應對有關的保安風險，從而達到業務目標。

ISMS是機構管理系統的一部分，目的是透過一系列風險評估，為各行各業、不同規模的機構提供有效且具針對性的管理方案，以減低敏感資料外洩的風險，從而提供可靠的服務或產品。而ISO/IEC 27001是國際標準化組織（ISO）發布有關ISMS的國際標準，為系統開發與運作提供規範性要求，透過此由第三方發出的認證，展示機構已經通過正式的合格評定程序，滿足特定的資訊安全要求。

人為因素要留意

ISO/IEC聯合技術委員會轄下負責ISMS的工作小組副召集人莊士敦（Dale Johnstone）指出，ISMS統籌機構的人員、程序與資訊科技系統三大範疇，控制業務風險，而ISO/IEC 27001所列出的標準，則幫助機構實行這三方面的統籌工作。「風險其中一個重要因素便是人，部分員工或因一時好奇、不良意圖、甚至誤墮社交工程（social engineering）陷阱，使機構的敏感資料外洩。」

所謂社交工程，即騙徒會透過電話、電郵等方式，假冒員工信任或熟悉的人，若員工警覺性低，便可能不慎把機構的重要資料洩漏。「情形就像電話騙案，對方會預先了解員工個人工作習慣、機構運作等，以獲得員工信任。」因此要實行ISMS，除了有足夠的硬件設備外，莊士敦亦建議為員工提供足夠的培訓，以及制定正式的安全指引文件讓員工跟從。

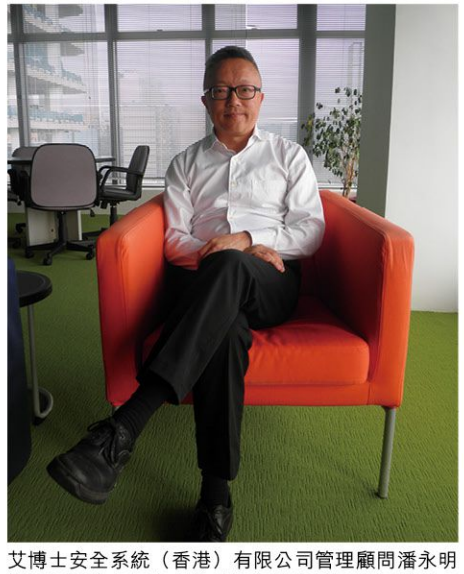
要實行ISO/IEC 27001，機構主要須完成三個步驟：辨別哪些資訊須要保護、衡量風險程度，以及訂定可行的保安措施。莊士敦建議機構由最高風險的資訊資產開始做起，逐步建立全面的保安系統。機構亦不妨尋求專業意見，例如找顧問公司協助。「獲得ISO/IEC 27001認證的機構與競爭對手產生區別，可讓其客戶知道機構能有效保護敏感資料，以獲取客戶信任。」

ISO/IEC聯合技術委員會轄下負責ISMS的工作小組副召集人莊士敦指，獲得ISO/IEC 27001認證的機構可以展示機構有效保護其敏感資料的能力，增強客戶信任。

改變管理思維成關鍵

環顧香港，不少私人公司與公營機構均有取得ISO/IEC 27001認證。提供資訊保安服務的艾博士安全系統（香港）有限公司，早於2003年便獲得此認證，成為本港最早取得認證的公司之一。該公司管理顧問潘永明表示，當時預計具備ISO/IEC 27001認證將會逐漸成為客戶服務合約的要求，所以為了爭取客戶信任，便率先申請認證。

「ISO/IEC 27001認證為我們帶來不少好處，首先是公司投標成功率提高，其次是令公司對風險管理的認識增多。」潘永明解釋，認證的過程令管理層全面審視公司的資訊安全系統管理，並就可能發生的事故制定預防政策，同時亦提高了整體員工的防範意識。早前肆虐全球的勒索軟件，該公司也能免於入侵。「若沒有申請此認證，管理層未必有此意識及會有系統地去進行資訊安全的風險管理工作。」



艾博士安全系統（香港）有限公司管理顧問潘永明說，認證令公司有系統地進行資訊安全的風險管理工作。

推行ISO/IEC 27001，最大挑戰是管理思維的改變。潘永明說：「有些中小型機構未必著重文檔建立，而為了達到認證要求，我們在這方面投放了不少資源，如制定政策指引及建立相關文件記錄。認證亦要求公司定期進行檢討及內部審計，對機構的資訊安全系統持續改善。」他認為，若機構的運作與資訊安全關係緊密，例如從事網上交易業務等，便應申請此認證，從而提升客戶信心。

考評局：員工培訓不可少

香港考試及評核局（考評局）亦為香港中學文憑考試（文憑試）系統取得ISO/IEC 27001認證，該局資訊科技部總經理曾廣納解釋，考評局須要處理大量考生個人資料、成績、試題等敏感檔案，而且在計算成績方面需要有很高的準繩度，再加上必須準時放榜，過程若有任何資料外洩或錯失，影響很大，因此考評局相當著重ISMS。

曾廣納分享實行ISO/IEC 27001的經驗：「其中一項最大的挑戰是員工培訓，由於一些保安要求如員工離開工作崗位時要把重要資料收妥，電腦閒置15分鐘便自動登出，收到可疑電郵時不要打開不明連結等，都要員工切實執行，所以我們須清楚解釋讓員工知道推行每項措施的原因，而所有新入職員工都要接受相關培訓，讓他們能自發性地保護信息資產。」

刺激思考風險管理

曾廣納續說，認證機構每年會派員進行覆檢，這是一個難得的機會審視機構的安全措施是否有效，這樣能夠持續訓練員工思考風險管理措施。「我們旗下共有兩個數據中心，每日均須將資料備份，以及運送載有資料的磁帶。過程中如何避免資料外洩？我們會不斷探討，最終制定出長遠的傳送方案。」他更表示，所有機構都會處理不同程度的敏感資料，因此鼓勵所有機構都申請ISO/IEC 27001認證。

香港考試及評核局資訊科技部總經理曾廣納認為，認證機構每年進行的檢查是一個難得的機會，讓機構審視安全措施是否有效。

(資料由客戶提供)