ISO標準助小微企開闢新出路

根據世界銀行提供的數據，中小微企(MSME)佔全球公司數量比例達到九成以上，涉及總就業人數的七成。在發展中國家，小微企更是經濟增長和創造就業機會的關鍵所在。事實上，標準不只適用於擁有數千名員工的大型企業，透過應用國際標準，中小微企同樣能夠從中獲得巨大利益，除了有助降低成本，提高公司信譽和公信力，亦能提升在國際市場中的競爭能力。

更好地開展業務

標準化讓企業獲益良多，不僅可減少與其他公司合作時產生的摩擦，亦有助於優化實踐，從而降低成本及提高生產率，這對於盈虧總額起着實質性的影響。乍看之下，或許ISO的每一項標準都令人覺得難以理解，然而，它們都是得到世界各地行業領袖一致認可的最佳方法。例如，使用ISO 50001（能源管理標準）可以顯著降低運營成本，而使用ISO/IEC 27001（信息安全管理系統）則有助於保護企業免受極具破壞性的潛在威脅。

位於瑞典的Veriscan Security總部，多年來一直致力參與ISO/IEC 27000系列標準的制訂。其首席執行官Jan Branzell也是ISO/IEC 27003的制訂者之一，他表示：“隨着網絡安全/信息安全成為了大多數組織的必要需求，使用國際標準不單可以建立良好的內部架構，還可作為與其他組織建立聯繫的基礎。若這些組織也同樣使用ISO/IEC 27000系列，則有助雙方更好地、更透明地了解如何共建良好的安全性和相互信任。”

登上世界舞台

ISO國際標準是基於一個迭代的細化循環方式，不斷持續制訂和更新，以滿足不斷變化的需求、目標和期望。標準除了可確保產品和服務的一致性和可追溯性，同時有助提升質量。

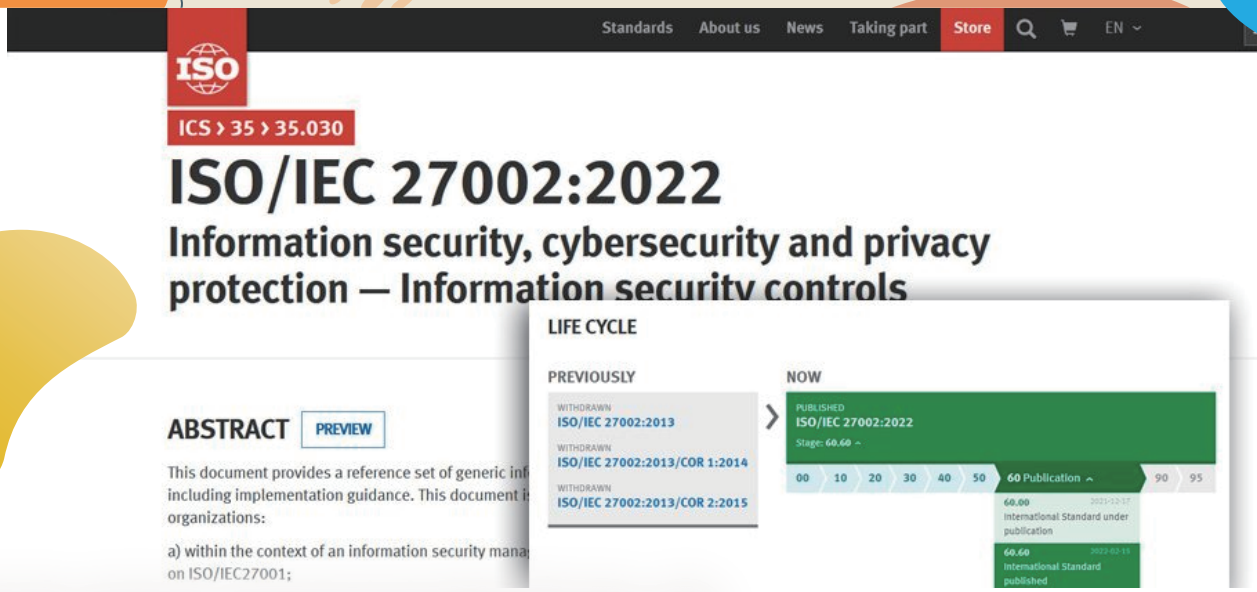
標準化實際上是“信任”的縮寫，它讓消費者、投資者和合作夥伴對企業充滿信心。許多國際客戶和組織只選擇與採用標準的企業合作，包括在環境和工作場所安全等領域。當中小微企謀求增長和競爭時，更能突顯出標準的價值——標準可確保競爭環境的公平性，使中小微企能夠與國際市場上的企業公平競爭。

此外，企業參與標準化的過程對於塑造行業的未來發揮着積極的作用，這對行業的發展極為重要，而非只把行業的未來押注在大公司的手中。

ISO標準是否適合所有中小微企業？

當然，並不是所有的標準都與中小微企有關，小型企業應仔細考慮哪些標準最有利於參與。長遠來看，參與標準制訂及應用可以讓小微企在全球市場競爭中處於更有利的地位。ISO發佈過大量和各式各樣的標準，當中許多都適用於規模較小的企業。例如，ISO 9001（質量管理）、ISO 45001（職業健康和安全）和ISO 26000（企業的社會責任），對於大部分中小微企業及大型企業都是適用的。

詳情：https://www.iso.org/contents/news/2022/06/small-businesses-keeping-up-with.html



ISO/IEC 27002修訂完成

ISO（國際標準化組織）於2022年2月15日對《ISO/IEC 27002:2013》進行改版，並發佈了《ISO/IEC 27002:2022資訊安全、網路安全和隱私保護——資訊安全控制》新版標準。所有已建置ISMS資訊安全管理系統的組織，都必須針對組織的需求與環境，根據修訂後的《ISO/IEC 27002》內容更新其控制措施。

《ISO/IEC 27002》提供了一套通用資訊安全控制措施的參考和實施指引。作為《ISO/IEC 27001》的詳細參考資訊，新版標準可幫助用戶識別和實施最適合其組織需求的資訊安全控制措施，從而加強對資訊方面的保護。

《ISO/IEC 27002:2022》的主要修訂如下：

● 刪除了“最佳實踐”的叫法，改為“資訊安全、網路安全和隱私保護——資訊安全控制”，以更好地反映其作為資訊安全控制措施的目的。
● 將一些不再適合當前環境的控制措施刪除，控制措施數量從114個減少至93個。
● 新增11項安全控制，涵蓋了威脅情報、雲端服務使用的資訊安全和資料外洩預防等方面，以確保組織能夠有能力持續控制自身的資訊安全。
● 2022版提供了對2013版控制標識符號的引用，讓企業組織更方便過渡到最新版本。

簡單來說，新版標準簡化了控制措施架構，從原來的14條款類別，調整為4大類別：組織控制、人員控制、實體控制與技術控制；而整體控制項目亦從114個減至93個，藉此強化資安管控有效性，並將不適合當前環境的內容刪除，當中更新了58個控制項目，並將多個控制項目合併為24個控制項目，同時新增了11個控制項目。

新增項目主要是為應對當前的網路攻擊手法與樣態，控制項目包含了威脅情資、雲端服務使用的資安、通訊技術營運持續整備、實體安全監控、組態管理、資訊刪除、資料遮罩、資料外洩防護、活動檢視、網站過濾與安全程式碼撰寫，以確保組織有能力持續控制自身的資訊安全。

新版同時增加了屬性標籤，包括控制類型（預防、偵測與矯正）、資安特性（機密性、完整性、可用性，CIA）、網絡安全概念（識別、保護、偵測、回應、復原，NIST CSF）、執行能力，以及安全領域，讓企業組織可從不同角度，快速過濾相關控制措施，以及執行排序呈現，令組織更方便找出相關控制要求。

相關資料：https://www.iso.org/standard/75652.html

查詢詳情，請聯絡：
澳門生產力暨科技轉移中心-標準、管理及培訓考試部
地址：澳門新口岸上海街175號中華總商會大廈六樓
網址：www.cpttm.org.mo/quality
電話：(853) 2878 1313
傳真：(853) 2878 8233
電郵：quality@cpttm.org.mo