以標準支援風險管理並增進企業價值

英國工商業保險和風險管理者協會最新報告 揭示標準對風險管理的助益

BSI與英國風險與保險專業機構Airmic[1]共同撰寫了一份報告，文中除了介紹標準（standard），說明其發展歷程，並特別強調了標準如何支持企業組織的風險管理。

BSI 集團執行長 Howard Kerr 表示：「我們從研究中發現，標準可為英國企業創造巨大的正面貢獻，帶領企業邁向成功。舉凡提高生產力、推動創新、提高產品品質及流程效率、推廣國際貿易，都是標準的重要成效。」

Airmic 副執行長兼技術總監 Julia Graham 指出，近期發布的新版 ISO 31000:2018 風險管理國際標準，讓 Airmic 思考如何運用標準協助企業創造卓越成就，以及如何支援風險管理作業。

《標準：支援風險管理並提高企業價值》（Standards: supporting risk management and adding business value）報告全文已於 6 月在利物浦舉辦的 Airmic 年會上發表。報告主軸為兩位資深風險管理從業人員的深度對談，說明各自使用標準輔助業務風險管理工作的經驗，最後得到的結論是標準可為企業建立「系統和架構」，並促進完善的企業風險管理實務，引領企業獲致成功。

此外，英國皇家認可委員會（United Kingdom Accreditation Service, UKAS）和國際獨立驗證組織（Independent International Organisation for Certification, IIOC）在本報告中也強調，基於標準的驗證、檢驗、測試或評鑑服務，可以支援代理人和擔保人進行風險管理與評估，同時向消費者保證產品或服務已達到特定品質水準，並符合相關法律規範。

以下摘錄報告中兩位資深風險管理從業人員的深度對談，**從使用者的角度了解標準對企業風管人員的實際助益。**

[1] Airmic 是英國由風險和保險專業人員組成的非營利組織，致力於塑造風險和保險專業的未來，並支持協會會員的專業角色，同時也是英國最大的風險和保險專業人員網絡。airmic.com

標準如何協助風險管理專業人員

風險管理專業人員對談

Airmic 副執行長兼技術總監 Julia Graham 與惠康基金會[2]（Wellcome Foundation）企業風險管理師 Fiona Davidge 談論標準對企業的價值和 ISO 31000:2018 國際標準。

Julia： Airmic 正在撰寫一份文件，希望推廣以標準（standards）提高企業價值的觀點。我們認為，趁著 ISO 31000:2018 正式上路時發表是很好的時機，因為就我所知，不少人認為標準只會增加行政工作負擔。BSI 與 Cebr（現為 Gartner 旗下研究中心）攜手研究，發現遵循標準的企業能比未遵循標準的企業創造更多價值。標準可以為企業建立系統與架構。

Fiona： 標準分為很多種，有些人認為這些標準死板生硬。一聽到「標準」二字，他們往往直覺認為標準只是公式化、複雜的行事方法，過程中需要在紙上勾選很多方塊。事實上，這會依情況而有所不同。ISO 31000 旨在提供一套原則、架構和流程，勾選方塊並非重點所在。

Julia： 標準分為國際、區域、國家、地區、產業、專業技術和個別組織等許多層級。ISO 31000:2018 不僅更具策略高度，也比舊版更為精確簡鍊。目的並非作為驗證標準，而是提供一體適用的指導方針，讓各種規模及類型的企業組織都能使用。**ISO 31000:2018 提供的原則都經過策略規劃，無論是從一般的廣泛角度或高階層級的視野探討企業風險應對措施，都非常實用。**

Fiona： 那些原則在風險管理領域並不罕見，反而代表優良的管理模式。

Julia： 還有一個很重要的觀念，就是標準並不能取代良好的風險管理，兩者的關係應該是相輔相成。在我的經驗中，你的客戶和其他利害關係人很可能也同樣遵循標準，並且在合約中要求你也一併遵循。標準可為你和客戶創造一套共同語言，在彼此之間建構共同的工作方式，你可以根據企業的特質、規模和風險程度與內部加以整合。

Fiona： 說到 IT 安全和歐盟一般資料保護規範（GDPR），惠康基金會的習慣是事先知會供應商，除非他們採行 ISO 27001，並取得資訊安全驗證，否則我們不會和他們簽署任何與資料（data）有關的合約。我們認為，這麼做可以讓我們獨立客觀地看待合作廠商。**我們前陣子剛拒絕和某家大型企業續簽合約，原因就是他們沒有通過 ISO 27001 驗證。**這家國際企業會經手大量資料，我們好奇詢問他們為什麼未取得這項驗證。對方回答他們有更高的標準。我們回問：為什麼你們不取得驗證，而要把事情弄得更複雜呢？我們設立這套準則，說明我們對供應商處理機密資料的期許。總之，我們在理該續約時終止了

[2] 惠康基金會（Wellcome Foundation）是英國最大的慈善基金會之一，致力於提高公民和動物的健康福利事業。惠康基金是英國最大的生物醫藥研究贊助者之一，也是世界最大的生物醫學研究基金之一，與美國的霍華休斯醫學研究所（Howard Hughes Medical Institute）相比擬。（維基百科）

合約，他們非常驚訝。我必須說，**就算你真的很行，但你要怎麼證明？**

Julia：千萬不能低估標準附帶的語言價值。目前網路產業的一大挑戰就是缺少共同語言。標準可以提供一套分類法、實務慣例，但不會讓你感覺綁手綁腳。你可以自己決定使用方法，按照對企業有利的方式套用並維持一致性。

Fiona：我曾遇過外部稽核人員詢問我們是否使用 ISO 31000 作為風險管理政策和實務的基礎。如果我可以回答「是」，事情就會比較簡單，因為我們之間擁有共識。其實這不像有沒有通過驗證那樣非黑即白，界線分明，但對方應該都能心領神會。

Julia：但我認為，標準不必非得通過驗證，才能接受稽核。稽核和驗證並非互為充要條件。

Fiona：沒錯。如果對稽核人員初步報告時表明「我的風險管理流程符合 ISO 31000 規定」，等於在告訴對方你了解狀況。就算沒有通過驗證的那張證書也沒關係。

Julia：不過，如果你要找家通過 ISO 標準驗證的供應商，通常會希望對方的標準和驗證範圍與你的需求相符。我之前在法律事務所任職時，ISO 27001 在客戶協議中相當常見，但唯有客戶仔細確認他們對供應商指定的內容，並在業務條款中加入相對應的規範，標準才能真正發揮價值。

Fiona：你必須細心運用標準、發揮智慧，這些標準才會值得倚靠。

Julia：我喜歡你說的細心和智慧。我們都同意，標準不能取代風險管理。兩者應該相輔相成，共同促進良好的企業風險管理（ERM），最後將企業推上成功的顛峰。

Airmic 副執行長兼技術總監
Julia Graham

惠康基金會企業風險管理師
Fiona Davidge

《標準：支援風險管理並提高企業價值》報告

BSI 與 Airmic 共同撰寫此報告，文中介紹標準（standard）並說明標準如何支持企業組織的風險管理。下載報告（英文版）請按此>

› ISO 31000 風險管理國際標準 | 提供原則和框架，協助企業組織進行風險分析和風險評估，適用於大部分的業務活動。透過導入此標準，能夠提升組織營運效率、治理及強化利害關係人的信心。BSI 提供客製化教育訓練協助企業組織了解和運用 ISO 31000，立即聯絡 BSI 訓練學苑：02-26560333#133 蕭小姐