

## 談整合管理系統(ISMS & ITSMS)以強化 IT 治理之績效

謝君豪 (Joe Hsieh)

joe.hsieh@bsigroup.com

BSI 英國標準協會

驗證部協理

ISO 27001/ ISO 20000 產品經理及主導稽核員

在全球化及資訊化的時代下，組織的競爭力及優勢會因各種環境之變化及事件而有所改變(如金融風暴、資安事件、事故之發生等)。所以強化組織在各個面向的競爭力一定是個不可避免之趨勢，如果從整個國際標準之發展方向來看，組織強化競爭力的重點可從 "Performance – 績效"，"Risk – 風險" 及 "Sustainability – 永續性" 等三個大面向來進行考量。不論從哪一個面向來考量，IT治理都是一個越來越受重視的主題。從國際間的研究報告的數據中也可發現，有效的管理IT所面臨的治理(Governance)、風險(Risk)、符合性(Compliance) – IT GRC的議題可協助組織在營運面強化管理階層對風險及符合性的理解、改善營運績效、保護敏感資料及降低符合性所花費的成本等。但組織面臨到的最大挑戰則是如何在IT GRC的相關活動中於成本、風險及報酬率取得一個平衡點。所以有效的展現出IT治理的績效(從Governance、Risk、Compliance等角度)，必是一關鍵成功要素。

如何有效強化 IT GRC 的績效呢？根據國際研究報告指出：國際標準之導入為組織最常採用的方法之一(如 ISO 27001-資訊安全 & ISO 20000-1-IT 服務管理)。但許多組織也發現許多控制措施之執行是不容易展現其有效性及績效

的。但如果組織能夠適當的整合相關之管理系統的要求及精神，是可達到互補之效的。舉例來說，ISO 20000 或 ITIL 中有許多要求就與 ISO 27001 的控制措施有互補之效。因為在 IT 服務管理系統中其最主要之目標為展現組織所提供之 IT 服務的績效、品質、成本等。所以在標準中之要求完全是以服務的角度出發(End to End Service)。其中有多個服務管理流程皆可與資訊安全管理系統做適當的整合；如可用性管理、營運持續/IT 服務持續管理、容量管理、事故管理、變更及發行管理等。從筆者之觀察及稽核經驗，組織如能適當藉由上述所提及的服務管理流程強化既有之資安控制措施，除了可顧及到安全之考量，相信同時也可兼顧到品質、正確性等議題。



以變更管理為例，許多讀者應會發現近來越來越多的資安事件、事故皆與組織在對其應用系統或 IT 服務進行日常之維護/變更時處理不當所造成的。如委外廠商因執行日常之系統變更活動而造成極高數量的民眾資料外洩、關鍵系統服務中斷、網站漏洞等。分析相關原因後，有極大比例的原因應可歸納在組織執行相關之變更流程不夠周延所導致。ISO 27001 標準中其實針對變更管理有多項要求，如在：

**A.10 通訊與作業管理章節：**

A.10.1.2之要求：對資訊處理設施與系統的變更應受控制。

**A.12 資訊系統之獲取、開發及維護章節：**

A.12.5.1之要求：應藉由使用正式的變更控制程序，以控制變更的實作。

雖然在ISO 27001及相關指引中針對相關要求已訂定相關之要求，但如果藉由ISO 20000中的要求予以強化，組織應會發現其既有之變更管理流程應可展現各個面向的績效 (如安全、品質、效率等)。下列為ISO 27001及ISO 20000間有關變更管理的要求進行比較 (例)：

ISO 27000標準	ISO 20000標準
<p><b>ISO 27001 – A.10.1.2 Change Management</b> 對資訊處理設施與系統的變更應受控制。</p> <p><b>ISO 27002 – 實作指引</b> 運作之系統和應用軟體宜受到嚴格的變更管理控制。宜特別考量下列事項：</p> <ul style="list-style-type: none"> <li>(a) 重大變更之識別與記錄。</li> <li>(b) 規劃與測試變更。</li> <li>(c) 評鑑此類變更的潛在衝擊，包括安全衝擊。</li> <li>(d) 對所提議之變更的正式核准程序。</li> <li>(e) 向所有相關人員通報變更細節。</li> <li>(f) 後撤程序，包括由不成功的變更和意料之外事件的中止和復原之程序與責任。</li> </ul>	<p><b>ISO 20000-2 Cl.9.2 Change Management - 實作指引</b></p> <p><b>規劃與實作</b> 變更管理流程及程序宜確保</p> <ul style="list-style-type: none"> <li>(1) 變更有一明確定義且文件化之範圍。</li> <li>(2) 僅提供營運利益的變更被核准。</li> <li>(3) 變更基於優先次序與風險排序。</li> <li>(4) 在必要時，實作變更的時間要予以監視及改善</li> <li>(6) 能夠展示變更如何             <ul style="list-style-type: none"> <li>(a) 提出、記錄及分類。</li> <li>(b) 就變更對於服務、客戶及發行計畫的衝擊、急迫性、成本、利益及風險評鑑。</li> <li>(c) 若不成功之撤銷或補救。</li> <li>(d) 文件化。</li> <li>(e) 被變更權責單位核准或駁回，視變更的型式、規模及風險而定。</li> <li>(f) 被負責將變更之組件的小組內，受指派的擁有者所實作。</li> <li>(g) 測試、查證及簽署。</li> <li>(h) 結案及審查。</li> </ul> </li> </ul>

	<p>(i) 被排程、監視及提報。</p> <p><b><u>變更要求之結案與審查</u></b></p> <p>所有的變更宜在實作及任何有記錄之改善後，就成功或失敗予以審查。以查核</p> <p>(1) 變更符合其目標。</p> <p>(2) 客戶滿意其結果。</p> <p>(3) 沒有意外的副作用。</p> <p><b><u>變更管理報告、分析、與行動</u></b></p> <p>變更紀錄宜予以定期分析，以發現變更升高的層級、經常復發的型式、浮現的趨勢及其他相關的資訊。變更分析的結果與所獲結論，宜予以記錄，並採取行動。</p>
--	---

從上面之比較讀者應可發現，組織如果善用及整合不同管理系統的要求。不僅可提升原管理系統相關活動的符合性及有效性，更可以有效的展現出該活動的績效進而強化 IT 治理成功的可能性。舉例來說，組織可針對相關活動如變更管理制定績效指標或是有效性量測指標。一旦訂定出相關指標並定時監控量測，就能鑑別及分析出該活動目前之達成狀態並進行必要之改善。如：



1. 變更成功的比例不可低於 XX%
2. 因 Coding 異常而造成的系統中斷不可超過 XXX 件
3. ....

**結語：**

在本文中筆者主要從組織在IT治理活動中如何透過管理系統之整合達成可能的效益。一旦相關的效益能適當的被展現(如透過量化指標之訂定與展現)。組織就可鑑別出需改善的面向並進而改善。那組織在IT GRC (Governance、Risk、Compliance)的成熟度也會相對的提升，並達到滿足各方團體之要求。