資訊安全管理系統 ISO27001:2013與ISO27001:2005差異說明

聞美晴／金融聯合徵信中心 資安部

國際標準化組織（International Organization for Standardization；以下簡稱ISO）於2013年10月正式公佈將原ISO27001:2005更新爲ISO 27001:2013資訊安全管理系統標準，此爲ISO 27001自2005年正式成爲國際標準之後的首次改版，對於原先已持有ISO27001:2005標準證書之組織，於公佈後24個月爲轉版過渡期，已導入之組織需於這段期間完成轉版，若超過轉換期，原ISO 27001:2005證書就將自動失效，因此於2015年9月30日前須使用新版標準進行審查作業，取得新版證書。

近年來資訊安全的威脅與過去相比無論在議題複雜性、管理難度與範圍涵蓋面向，皆有重大的變化，如：行動支付(Mobile Payment)、行動裝置(BYOD)、社群媒體(Social Media)、巨量資料(Big Data)、雲端運算 (Cloud computing)、物聯網(Internet of Things)等安全管理，組織未來如何有效地展現在資訊安全面向的有效治理將會扮演著日趨重要的角色。聯徵中心向來以資安最高標準承諾社會大眾，全體員工除落實「資訊安全，人人有責」之理念，更持續推動資訊安全管理制度與個人資料保護管理制度之運行，展現聯徵中心保護信用資料之決心與承諾，亦為善盡企業社會責任具體表現，針對新版ISO27001:2013之驗證作業，聯徵中心已完成現行制度與新版要求之差異分析，全面檢視內部各項作業規範與工作手冊，新版SOA各控制項目要求於現行制度之合適性，並辦理風險評估作業，預期於

今年9月前通過資訊安全管理體系驗證，順利取得ISO 27001:2013版證書。ISO27001:2013版標準要求與2005版之主要差異，概略說明如下：

(一) 採用Annex SL結構

ISO27001:2013新版採用Annex SL結構，制訂ISMS管理制度面的要求，原2005版本文

0-8條款調整為0-10條款(參見表一)，與其他管理系統更易於整合。ISO過去制定不同的管理標準要求，其涵蓋主題從品質、資訊安全、營運持續管理、食品安全至能源管理等等，儘管所有的ISO管理系統有著共同的要素，然而各管理系統於標準要求之結構、文字、用語釋義與定義等皆有所差異，對於導入多種管理系統標準之組織於執行時，容易造成混淆與整合困難等情形，因此ISO/IEC Directives在2012年決定所有的管理系統標準將使用包括高階結構(High Level Structure, HLS)、通用形式和術語的通用架構，以提昇標準的相容性及標準化和標準發展的有效性，讓不同的管理系統標準易於接軌、整合。

(二) 引用ISO31000風險管理要求

新版於風險評鑑方法，引用ISO31000風險管理要求(參見圖二)，允許組織針對不同的管理系統採用相同風險管理方法論，不再特別強調識別資訊資產、威脅與弱點等項目，降低整體風險評鑑作業之複雜度，主要著重於規劃及執行風險評估與風險處理程序之要求，此一改變賦予組織於風險管理上有較多的空間。

(三) 移除2005年版中的用語釋義

承如第一點說明，為促進整個ISO管理系統之整合及標準術語與定義的一致性，新版於「2.引用標準(Normative references)」與

表一　ISO27001:2013版與2005版標準

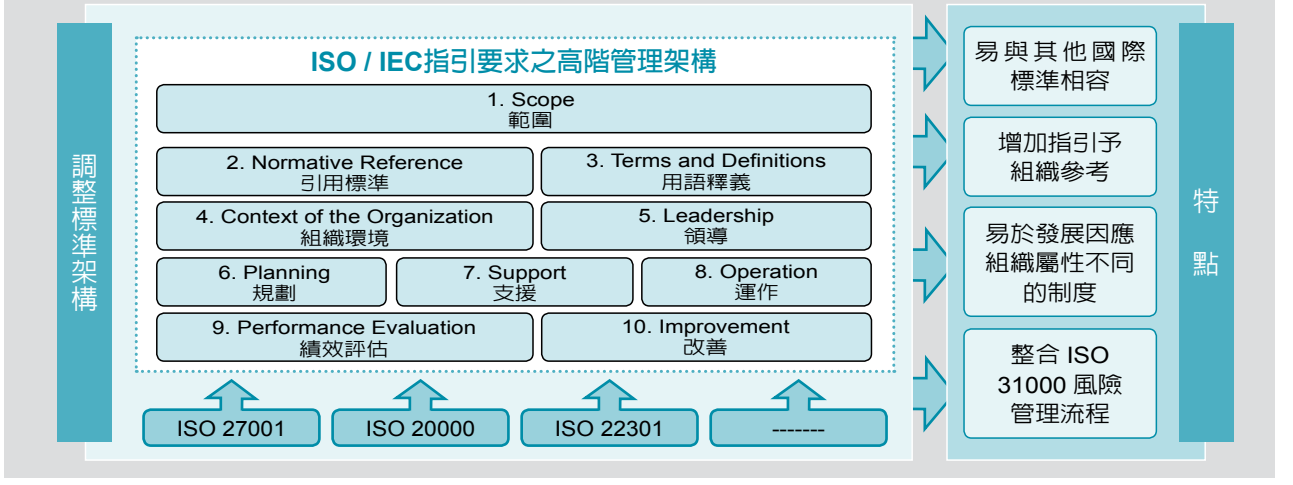
27001:2013版本條款	27001:2005版本條款
0 Introduction 介紹	0 Introduction 介紹
1 Scope 範圍	1 Scope 範圍
2 Normative references 引用標準	2 Normative references 引用標準
3 Terms and definitions 用語釋義	3 Terms and definitions 用語釋義
4 Context of the organization 組織環境	4 ISMS 資訊安全管理系統
5 Leadership 領導	5 Management responsibility 管理階層責任
6 Planning 規劃	6 Internal ISMS audits 資安管理內部稽核
7 Support 支援	7 Management review of ISMS 資安管審會
8 Operation 營運	8 ISMS improvement ISMS之改進
9 Performance evaluation 績效評估	
10 Improvement 改善	
Annex A (normative) Reference control objectives and controls A.5-A.18(14 domains, 35 objectives, 114 controls)	Annex A (normative) Control objectives and controls A.5-A.15(11 domains, 39 objectives, 133 controls)
	Annex B (informative) OECD principles and this international standard
	Annex C (informative) Correspondence between ISO 9001:2000; ISO 14001:2004; this international standard

「3.用語釋義(Terms and definitions)」直接參照ISO27002。

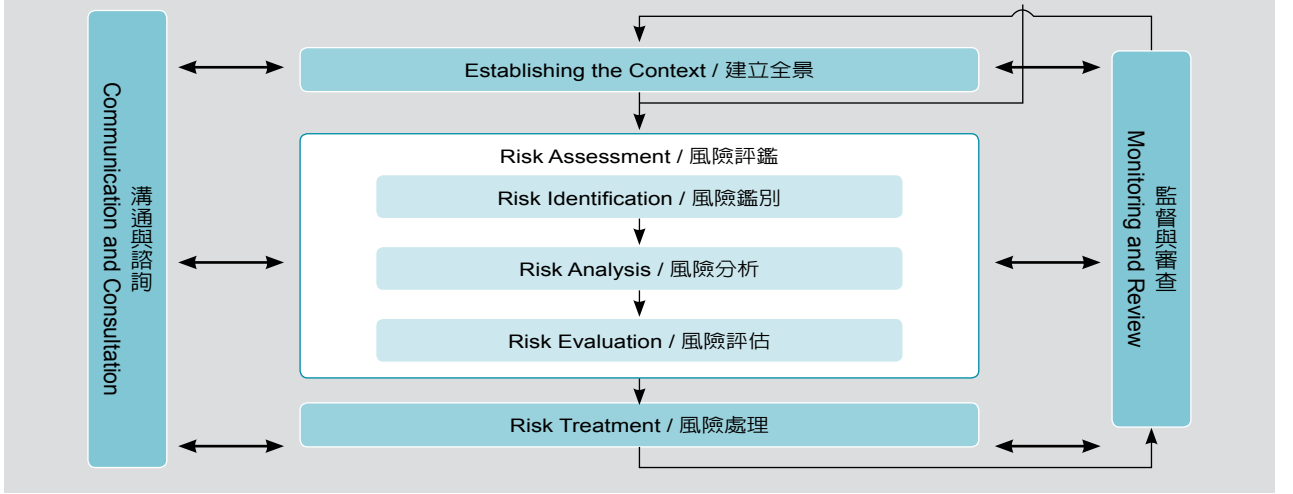
(四) 移除重複要求及以短語的方式陳述要求

新版為避免要求中可能造成的抵觸，移除控制措施中重複要求的部分，如原「A.10.10.1稽核日誌(Audit logging)」、「A.10.10.2監控系統的使用(Monitoring system use)」及「A.10.10.5失誤日誌(Fault logging)」於新版合併為「A.12.4.1事件存錄(Event Logging)」，同時於敘述各要求上改以較精簡之文字表達，允許組織有更大自由選擇實施要求。

圖一、新版之標準架構



圖二、風險管理方法論 (ISO 31000)



(五) 明確管理階層之支持及承諾要求

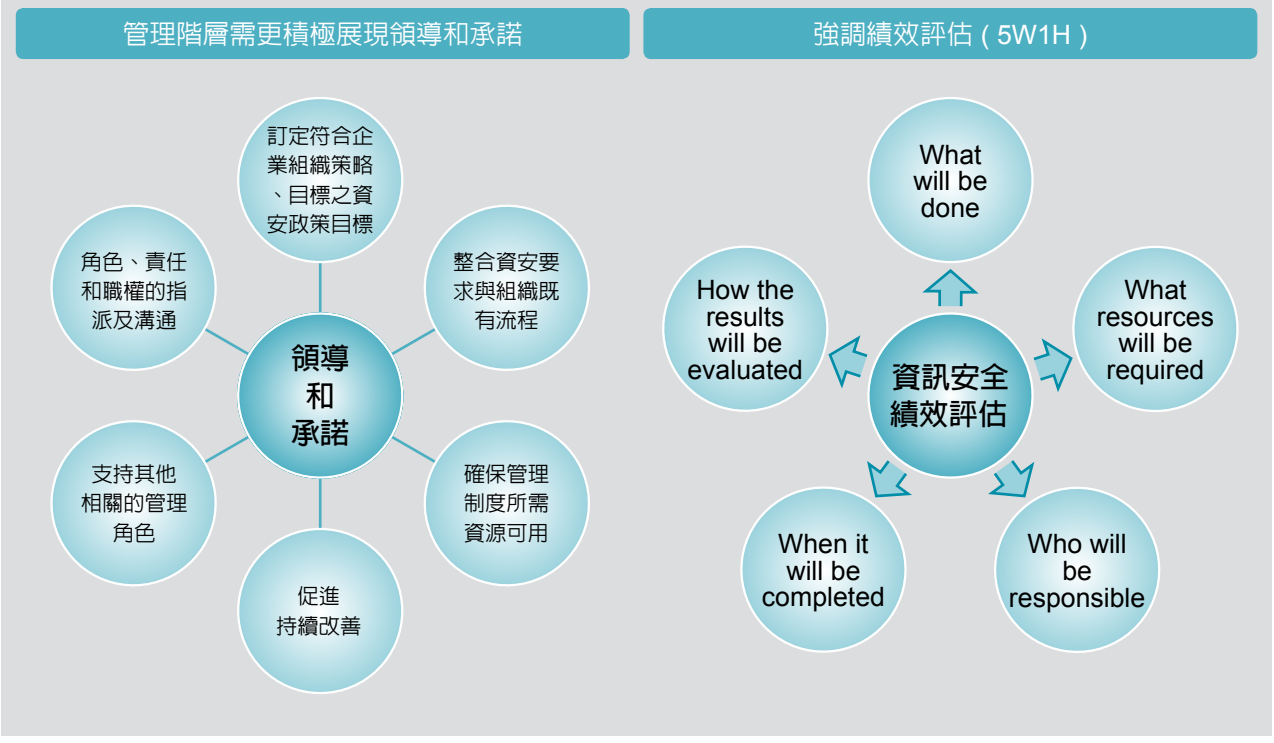
新版「5.領導(Leadership)」要求管理階層之支持及承諾，為有效展現領導力，須確保各資訊安全相關角色、責任及職權，並特別強調下列兩事項之責任及職權：確保ISMS符合ISO27001要求；對最高管理階層報告ISMS績效。

(六) 移除預防措施之要求

新版移除原「8.3預防措施(Preventive action)」，以新版「6.1因應風險與機會的行動(Actions to address risks and opportunities)」要求取代，而本項要求亦為與新版「4.1瞭解組織及其全景(Understanding the organization and its context)」與「4.2瞭解關注方之需要及期望(Understanding the needs and expectations of interested parties)」之要求一致，亦即組織於決定ISMS驗證範圍時應先了解組織全景，對於組織內外部環境有所認識，辨識出相關內外部議題與利害關係者，並由此提出相對應之風險與機會所需採取之作為，才能更為落實資訊安全管理制度。

(七) 強調績效展現，監控績效及訂定量測指標

圖三、明確管理階層之支持及承諾要求

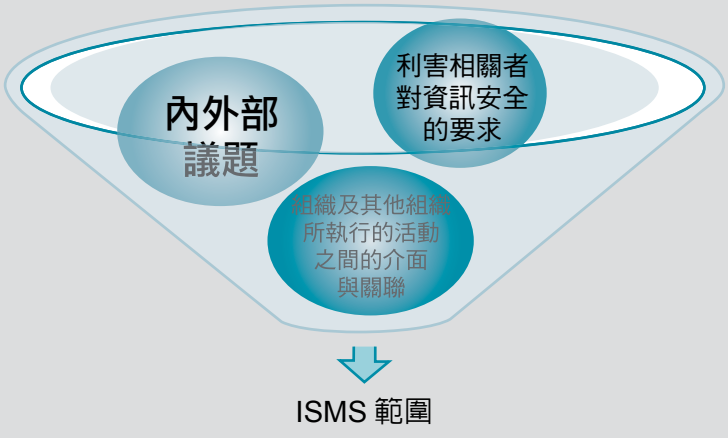


此外，新版強調績效展現，須突顯績效之有效性量測；適用性聲明書(Statement of Applicability，SOA)要求與2005版雖相似，但在控制措施的選擇要求應藉由風險處理過程來決定；ISMS不再特別強調「計劃、執行、檢查、行動（Plan-Do-Check-Act，PDCA)」，以「建立、實施、維護、持續改進(Establish、Implement、Maintain and continually improving)」為ISMS管理架構。

在條文要求之改變，除本文調整為0-10條款，考量組織環境對於新興議題與科技之挑戰，將密碼學與供應商關係管理獨立為新領域，原先同領域之通訊與作業管理分開成兩個獨立領域，並合併重複控制措施，使得標準要求由原本的11個領域、39個管理目標、133項控制措施，新版調整為14個領域、35個管理目標、114項控制措施。

資料來源：BSI、PwC

圖四、資訊安全管理系統範圍



圖五、新舊版安全控制措施之比較