ISO 27001「資訊安全管理系統要求」在圖書館的應用

The Applications of ISO 27001 in Libraries

吳政叡
Cheng-Juei Wu
輔仁大學圖書資訊系專任教授
Prof. of Department of Library & Information Science, Fu-Jen University

【摘要 Abstract】

本文從圖書館的角度來分析 ISO 27001，以了解其對圖書館可能產生的衝擊。首先，介紹國際 ISO 27001（或國內 CNS 27001）「資訊安全管理系統要求」標準的主要內容。其次，藉由一件圖書館資訊安全事件來分析 ISO 27001 的應用。

In this work, we analyze the impacts of ISO 27001 from the library's point of view. Firstly, the principles and structure of ISO 27001, which is Information technology – Security techniques – Information security management systems – Requirements, are introduced. Then, an information security event is analyzed to see how the ISO 27001 standard can be used in libraries.

【關鍵詞 Keyword】

資訊安全；資訊安全管理系統

ISO 27001; Information Security; Information Security Management System; ISMS

壹、前言

現代的組織在運作上是非常依賴資訊系統，組織的各種資訊（含機密資料）基本上也是存放在資訊系統中，再加上各不同組織間往來非常密切和頻繁，例如一個商業公司須要與各式各樣的供應商和客戶往來，其間往往會有大量的資料相互流通。這使得如何預防機密資料的不當洩露，成為一個非常重要的課題，甚至是攸關組織生死存亡的課題；又如一個高科技廠商的研發產品機密被競爭對手提早獲知，往往會蒙受非常巨大的損失。另一方面，由於各國大都制訂有智慧財產權或個人資料機密保護等相關法律，因此，機密資料的不當洩露也可能衍生為法律事件，造成組織非常大的困擾或損失。由以上的分析可

知，建立一個有效的資訊安全管理機制來確保資訊系統的安全和持續運作，是現代社會組織生存不可或缺的一環。

為了制定一個有效的管理機制來確保資訊系統的安全和持續運作，國際標準 ISO/IEC 27001「Information Technology – Security Techniques – Information Security Management Systems – Requirements」乃應運而生（註 1），其前身為英國國家標準 BS7799 – 2，而國內根據 ISO/IEC 27001（以下簡稱 ISO 27001）也制定了 CNS 27001「資訊技術 – 安全技術 – 資訊安全管理系統 – 要求事項」（以下簡稱「資訊安全管理系統要求」）（註2）。

正如前述，由於數位資訊的普及，可保護機密資料的一個資訊安全管理系統（Information Security Management System，簡稱 ISMS），成為許多重視機密資料保護組織生存不可或缺的一環，因此，紛紛依據 ISO 27001 的規範，建立資訊安全管理系統（ISMS），並尋求資訊安全認證。例如：金融機構（註 3）、企業（註 4-5）、醫院（註 6）、電信業（註 7）、壽險業（註 8）、行政機關（註 9）、主機代管業（註 10）。

隨著行政院與教育部對於資訊安全的重視，各大學也追隨商業公司或製造商的腳步，紛紛著手進行資訊安全認證的相關準備工作。大學圖書館為大學內不可或缺的一環，同時也是資訊收集、處理與傳播的主要機構之一，自然無法置身事外，必須要正視此一課題或時代趨勢。

透過 ISO 27001 的資訊安全認證即可確保資訊系統的安全和持續運作，因此，以下將先介紹 ISO 27001「資訊安全管理系統要求」的基本觀念和主要內容，然後以一件圖書館資訊安全事件（或資安事件）來分析 ISO 27001 的應用。

由於國內有 CNS 27001「資訊安全管理系統要求」標準，以下文章中關於 ISO 27001 的名詞及其解釋，將以 CNS 27001 中所使用（或翻譯）的詞彙為主，且不再一一指明其在 CNS 27001 中的出處。

貳、ISO 27001 整體架構

以 ISO 27001 對資訊安全管理系統（ISMS）的整體架構規劃而言，是採用「規劃 – 執行 – 檢查 – 行動」（Plan – Do – Check – Act，簡稱 PDCA）的模式來設計，其正文內容的主要章節（第 4 - 8 節）基本上就是以 PDCA 的模式來安排（註 11）：

一、建立 ISMS（規劃）：第 4 節「資訊安全管理系統」。

二、實作與運作 ISMS（執行）：第 5 節「管理階層責任」。

三、監視與審查 ISMS（檢查）：第 6 節「ISMS 內部稽核」與第 7 節「ISMS 之管理階層審查」。

四維持與改進 ISMS（行動）：第 8 節「ISMS 之改進」。

這裡要特別強調的是，ISO 27001 非常重視持續改進的精神，因此，要求針對每個發生的資安事件擬定矯正措施（而非危機處理完畢就落幕），以防止類似的資安事件再次發生。

再者，為了協助落實資訊安全管理系統（ISMS），在 ISO 27001 附錄 A 針對 11 個控制面相（A5 – A15）制訂了 39 個控制目標（與相對應的 133 個控制措施），由於這些控制面相與控制目標具體呈現資訊安全管理系統（ISMS）的預防與查核重點，為使讀者對資訊安全管理系統（ISMS）全貌有更清楚的認知，以下根據 CNS 27001 的翻譯列舉如下（註 12）：

（A. 5）安全政策：A.5.1 資訊安全政策。

（A. 6）資訊安全的組織：A.6.1 內部組織、A.6.2 外部團體。

（A. 7）資產管理：A.7.1 資產責任、A.7.2 資訊分類。

（A. 8）人才資源安全：A.8.1 聘僱之前、A.8.2 聘僱期間、A.8.3 聘僱的終止或變更。

（A. 9）實體與環境安全：A.9.1 安全區域、A.9.2 設備安全。

（A. 10）通訊與作業管理：

- （A. 10.1）作業之程序與責任
- （A. 10.2）第三方服務交付管理
- （A. 10.3）系統規劃與驗收
- （A. 10.4）防範惡意碼與行動碼
- （A. 10.5）備份
- （A. 10.6）網路安全管理
- （A. 10.7）媒體的處置
- （A. 10.8）資訊交換
- （A. 10.9）電子商務服務
- （A. 10.10）監視

（A. 11）存取控制：

- （A. 11.1）存取控制的營運要求
- （A. 11.2）使用者存取管理
- （A. 11.3）使用者責任
- （A. 11.4）網路存取控制
- （A. 11.5）作業系統存取控制
- （A. 11.6）應用系統與資訊存取控制
- （A. 11.7）行動計算與遠距工作

（A. 12）資訊系統獲取、開發及維護：

- （A. 12.1）資訊系統的安全要求
- （A. 12.2）應用系統的正確處理
- （A. 12.3）密碼控制措施
- （A. 12.4）系統檔案的安全
- （A. 12.5）開發與支援過程的安全
- （A. 12.6）技術脆弱性管理

（A. 13）資訊安全事故管理：A.13.1 通報資訊事件與弱點、A.13.2 資訊安全事故與改進的管理。

（A. 14）營運持續管理：A.14.1 營運

持續管理的資訊安全層面。

（A. 15）遵循性：A.15.1 遵循適法性要求、A.15.2 安全政策與標準的遵循性以及技術遵循性、A.15.3 資訊系統稽核考量。

由上述的 11 個控制面相（與 39 個控制目標）清單，可知資訊安全管理系統（ISMS）涵蓋了與資訊相關的所有層面：政策、組織、人員、實體環境、作業管理、資訊系統開發及維護、危機處理、法律。

ISO 27001 的附錄 A 雖然詳列了 133 個控制措施以供參考，不過都還祇是原則式的敘述，為了進一步協助實際運作，另外有一個與 ISO 27001 相搭配的標準 – ISO 27002（原先為 ISO 17799）「資訊安全管理作業要點」（Code of Practice for Information Security Management）（註 13）。

為了便於對照參考，ISO 27002 資訊安全管理作業要點的章節安排，乃以第 5 節到第 15 節來一一對映 ISO 27001 附錄 A 的 A.5 到 A.15。同時每節內的條文編號也完全對映，例如：ISO 27001 有 A.10.7.1「Management of removable media」的控制措施，在 ISO 27002（或 ISO 17799）中即有條款 10.7.1「Management of removable media」，其中詳列許多有關可移除式媒體管理的實作建議。

參、ISMS 的實作規劃

ISO 27001 對資訊安全管理系統（ISMS）的實作規劃，是以資產（Asset）為出發點，透過適當的風險評鑑（Risk Assessment）和風險處理（Risk Treatment）（註 14-15），使剩餘風險（Residual Risk）皆在可接受的範圍內，藉以達到效益和成本的最佳平衡，並完成資訊安全的三個最主要目標：機密性（Confidentiality）、完整性（Integrity）、可用性（Availability），這三個最主要的目標，一般簡稱為 CIA。

根據 ISO 27001（或 CNS 27001），「資訊安全管理系統」（ISMS）的正式定義為 – 「整體管理系統的一部分，以營運風險導向（作法）為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全。」

至於資訊安全的三個主要目標 CIA，其正式定義分別如下：

一、機密性：「使資訊不可用或不揭露給未經授權之個人、個體或過程的性質」。

二、完整性：「保護資產的準確度 (Accuracy) 和完全性 (Completeness) 的性質」。

三、可用性：「經授權個體因應需求之可存取及可使用的性質」。

這裏要特別提出說明的是，一般人在提及資訊安全時，祇會直覺聯想到機密性，這並不正確，其實資訊安全至少應同時包含機密性、完整性和可用性才算完整。

以圖書館為例，做為一個資訊傳播

的主要機構之一，一向較強調或重視資訊的公開與普及，因此，圖書館內的資訊系統較少機密性資料，所以機密性相對來說較不重要，但是完整性和可用性對圖書館仍然是很重要的。

以完整性來說，我們不希望提供給讀者的資訊是不完整的，甚至是錯誤的。舉例來說，我們必須注意公告的事項是否與實際情況一致，像開閉館時間或是樓面分布圖等；另外我們也須要防範駭客非法入侵來篡改網頁內容或毀損資訊系統內的資料。以上所舉的例子，皆是完整性所涵蓋的範圍，由此可知完整性的重要。

就可用性而言，對圖書館也是很重要的。現代圖書館做為一個資訊的處理機構，是非常倚賴館內各式各樣的資訊系統來維持日常運作和提供服務，事實上，圖書館大多數的資訊系統都是全年全天無休的透過網路提供服務給讀者，一旦系統當機，勢必對圖書館的營運造成極大的影響，也會招致讀者很多的抱怨。

如前所述，資訊安全管理系統（ISMS）的整體架構規範是以資產為出發點，那何謂資產？ISO 27001 將資產（asset）正式定義為 – 「對組織有價值的任何事物」（註 16）。

雖然這是一個範圍很廣泛的定義，不過，對處於現在資訊時代（或知識經濟時代）的大多數組織而言，其最主要的資產是 – 與資訊（或資料）有關的人員、場所、設備、軟體、儲存媒體等。以圖書館為例，其資產是以書籍、資料庫、書目紀錄與其他參考資源所組成的資料群（或資訊系統）為核心，以及與此核心有關的

㈠人員：如館員。

㈡場所：如圖書館建築物。

㈢設備：如電腦硬體設備、門禁系統設備。

㈣儲存媒體：如硬碟、CD。

也都是圖書館的重要資產，因為缺少這些資產，圖書館的核心資訊系統將無法順利運作。

因此，組織高層在安全政策上劃定資訊安全管理系統（ISMS）的範圍（或界限）後，最重要的起步工作就是要鑑別出此範圍（或界限）內所涵蓋的資產有那些。鑑別資產的主要目的在：確定個別資產的擁有者（Owner），和分析個別資產的價值（Value）、弱點（Vulnerability）、威脅（Threat）。

確定個別資產擁有者（Owner）的目的，在識別對個別資產安全負保護責任的人員，所以，這裡的資產擁有者，並非法律認知或一般認知的財產擁有者。以圖書館為例，圖書館自動化系統的擁有者，可能是負責管理該系統的館員。因此，根據 ISO 27001（或 CNS 27001），擁有者（owner）的正式定義為 – 「負有被認可管理責任的個人或個體，其控制資產的生產、發展、維護、使用及安全，擁有者一詞並非意指該人員實際上對該資產有任何財產權。」（註 17）

另一方面，任何資產皆有其弱點（Vulnerability），藉由弱點分析，可以識別出與該弱點相對應之威脅（Threat）與其可能性（Likelihood）。以圖書館自動化系統為例，可能的威脅有

㈠駭客入侵。
㈡人為操作錯誤。
㈢館員密碼設定不當遭破解。
㈣系統管理館員離職。
㈤天災：如地震、火災。
㈥硬碟毀損。
㈦系統更新程式有臭蟲（Bug）。
㈧備份失敗。
㈨備份資料遺失或毀損。

由此可知，資訊系統的威脅可能來自各方面 – 人員、場所、設備、軟體、儲存媒體等，人為或非人為、有意或無意都有可能。

另一方面，各式各樣的可能威脅，其發生的可能性或機率各異，對資訊機密性、完整性、和可用性所可能產生的衝擊也大不相同，再加上個別資產的價值往往相差甚大，因此，某個可能威脅對某個特定資產的風險值（Risk Value）是綜合資產價值、威脅可能性和衝擊等因素而來。

上述的整個過程，從識別資產及其價值、分析弱點與威脅、評估威脅可能性與衝擊，到最後產生風險值（Risk Value）的過程，即稱為風險評鑑（Risk Assessment）。透過適當的風險評鑑，可以較準確知道那些高風險威脅須要優先處理。經過處理後剩下的風險就稱為剩餘風險（Residual Risk），祇要在組織資訊安全管理系統政策可接受的範圍內，並經組織管理階層核准即可。因為風險處理經常須要成本，所以在成本效益的考量下，並不是所有的風險都要排除或降到 0。

肆、一個圖書館資訊安全事件分析

以下藉由一件大學圖書館的資訊安全事件，來分析 ISO 27001 資訊安全管理系統（ISMS）中的規定是否能對此資訊安全事件的預防與處理有所幫助，這起資訊安全事件的導火線是圖書館自動化系統的硬碟毀損。

一般電腦（整天開機）硬碟的使用壽命大約 2-3 年，不過硬碟的故障通常是無預警的，圖書館自動化系統為了克服此問題，基本上設計了二個安全機制：一是資料定期備份，一是硬碟的 RAID（磁碟陣列）架構。這間圖書館目前採用的是較通行的 RAID 5 架構，在此架構下，如果祇有一顆硬碟損壞，在更換新的硬碟後，系統可以自動恢復毀損的資料；但是，如果超過一顆硬碟同時損壞，就無法自動恢復，必須要靠備份資料來回復。

在 3 月 2 日（星期五）早上，某大學圖書館的館長接到通知，圖書館自動化系統有二顆硬碟同時損壞（雖然機率非常低，但仍會發生），館長接著詢問

備份情況，才赫然發現資料的完整備份作業從 2 月初以來就一直有問題而無法成功，上一次成功備份是 1 月 31 日（後來得知在此次成功備份後，負責管理系統的館員安裝了系統的更新程式），換言之，整個 2 月的資料皆不見，包括採購和新編的書目紀錄，以及這段期間內的所有借還書紀錄。

稍後，館長詢問負責管理系統的同仁為何沒及時反映資料備份問題，才發現在第一時間他確實有跟其業務上司（組長）反映，但是，此位組長卻沒意會到事態的嚴重性而未跟館長報告，以致於在跟美方技術人員交涉不順利的情況下，事情拖延過久，造成圖書館可能的重大損失。

系統當機當天，為不影響師生借閱書籍，圖書館已採取人工方式進行流通作業。另一方面，在下午 1:30 館長本來要召集館內相關同仁開緊急危機處理會議來討論善後事宜，很幸運的，在硬體承包商趕來更換硬碟前，負責管理系統的館員抱著姑且一試的心理，在中午嘗試啟動系統最後一次，沒想到居然成功了，於是館長開始坐鎮圖書館監督，並要求在當天無論如何要完成備份工作。

由於圖書館自動化系統廠商在台祇有業務代表，並無技術人員，因此，都是透過網路從美國遙控整個系統。雖然館內同仁及廠商在台業務代表皆盡心盡力交涉，但該公司（在美國）第一線技術人員太過堅持己見，以致拖延到晚上 7:30 仍無所進展，不得已，館長對廠商下最後通牒，要求美國技術人員在 8:00 前退出系統，館長決定先冒險關機嘗試更換受損硬碟，因為館長不知道那二個硬碟還能支撐多久，再加上適逢週末，美方人員過幾小時後也將休假，而如果先更換其中一顆硬碟後又能重新啟動系統，此時系統會自動開始進行資料重建與修護，完成後可以有充裕時間繼續來克服備份的問題。

也許是受到館長最後通牒的影響，美國技術人員終於開始願意嘗試其它方式，很快發現系統有些檔案損壞以致於無法進行備份，在隔離受損檔案後，備份工作終於可以順利進行，並且在晚間 9 點多完成完整備份，館長在交待要妥善保存備份磁帶和開始更換硬碟後離開學校。

由於更換硬碟後的系統重建與修護工作甚為耗時，而且一次祇能更換一顆硬碟，在週日與負責管理系統的館員聯繫後，得知硬碟更換工作順利完成，但是嘗試備份仍然失敗。

因此，在星期一（3 月 5 日）召開會議，館長一方面要求同仁檢查 2 月份資料是否有遺失，一方面要求隨時跟他會報系統的狀況。初步發現資料並無遺失，祇是書籍流通容易發生異常而鎖住系統。

在 3 月 6 日下午，書籍流通異常鎖住系統的現象已大幅減少，不過仍比正常情況稍高，發生原因仍在探究中。在資料備份方面，（3 月 6 日）上午，館

長接到美國技術支援部門經理的Email，宣稱已修復系統中所有損壞檔案，並且成功完成備份工作，於是館長請負責管理系統的同仁在晚上圖書館關門後，再嘗試進行正常完整備份作業來驗證廠商的說法。在3月7日上午，負責管理系統的館員回報已能成功備份資料，至此整起資訊安全事件暫告落幕。

綜合來看，此次嚴重的資訊安全事件是混合多種因素而來：

㈠廠商更新程式可能有臭蟲（Bug）：雖然負責管理系統的館員已經採取較謹慎的作法，並未在第一時間就安裝廠商的更新程式，而是觀察一段時間看其他大學圖書館安裝後的狀況後才進行更新，可惜有些臭蟲（Bug）是在某些特殊情況下才會發作。

㈡電腦硬體設備故障：雖然在系統的架構設計上已採用 RAID（磁碟陣列）來防止硬碟的故障，但並無百分之一百的保證。更慘的是，有些時候硬碟的故障並不會使系統立刻停擺，在拖延的過程中，常導致系統效能降低、某些機制失常（如備份）、和增加第二顆硬碟故障的機率而使 RAID（磁碟陣列）機制失效。

㈢自動化系統廠商第一線技術人員專業訓練不足：不但未能明瞭備份的重要性，在屢次交涉過程中一直堅持既定程序，不斷質疑是館員操作有誤，居然可以延宕客戶無備份情況長達一個月，實屬罕見，也讓人對此自動化系統廠商的專業聲譽打上大問號，這可以說是引發此次資訊安全事件的最主要因素。

㈣部分館員專業訓練和資訊素養能力不足：未能了解備份的重要性，不但未在第一時間通知館長，在與自動化系統廠商第一線技術人員交涉未成後，又沒立刻通報館長來拉高談判層級，以致延宕過久而引發嚴重的資訊安全事件。

㈤圖書館本身沒建立完善的資訊安全事件通報機制。

如果我們檢視 ISO 27001 附錄 A 的 11 個控制面相、39 個控制目標、133 個控制措施，就可以發現上述五項資訊安全事件的因素都有被涵蓋到（註18）。

㈠系統軟體的更新：ISO 27001 A.10.1.2「變更管理」和 A.12.4.1「作業軟體的控制」都對系統軟體的更新有所規範。ISO 27002（或 ISO 17799）10.1.2 規定作業系統和應用軟體應該有嚴格的變更管理，其中也建議（a）變更應有計畫和測試（b）評估可能的衝擊（c）應有適當的回復程序（Fallback Procedure）。以此案例來看，由於自動化系統的主機相當昂貴，無法有備用主機以供事前測試，但是可以擬定變更後的事後測試與回復程序，來測試系統的重要功能（包含備份機制），以提早發現可能的問題和回復系統成變更前狀態，但是在此案例中，負責管理系統的館員忽略了更新後對完整備份機制的立即測

試。另外在 ISO 27002 條文 12.4.1 中，也建議在能移除或減少系統安全漏洞情況下才考慮更新，以減低更新的可能風險。

㈡電腦硬體設備故障：ISO 27001 A.9.2.4「設備維護」中提及要確保硬體設備持續的可用性和完整性，在此案例中，硬碟的不穩定其實是有跡可尋且持續了一段時間，可能是館員太信任 RAID（磁碟陣列）的安全機制，以致於忽略了某些徵兆。另一方面，雖然在維護合約中有可更換新品的規定，不過廠商一般為了節省成本，往往堅持在硬碟確定損壞後才更換新品，而不肯在硬碟出現不穩定徵兆時即更換新品，因此，也加大設備故障時的影響範圍和增加 RAID（磁碟陣列）安全機制失敗的機率。所以圖書館最好在採購系統時，就在合約內就此部分的維護加入適當條文來保障自身的權益。

㈢與自動化系統廠商的安全協議：ISO 27001 A.6.2.3「第三方協議中之安全說明」是規範與來往廠商相關的安全規定與作法，ISO 27002（或 ISO 17799）6.2.3 中有建議（a）要針對硬體和軟體的安裝和維護訂定明確規定；（b）要規定目標服務水準和無法接受的服務水準為何。如上所述，引發此次資訊安全事件的最主要因素，固然是自動化系統廠商第一線技術人員專業訓練不足，且未能明瞭備份的重要性所致，但是，如果在採購與維護合約中有規定重要系統功能（含備份機制）的最長修復期限，則廠商第一線技術人員也斷然不敢堅持己見而延宕客戶無備份情況長達一個月。

㈣員工的資訊安全教育及訓練：ISO 27001 A.8.2.2「資訊安全認知、教育及訓練」有規範應給予所有組織員工適當的資訊安全教育及訓練。這樣一來就不致於會發生部分館員因資訊素養能力不足而未能了解備份重要性的情形。

㈤資訊安全事件通報機制：ISO 27001 A.13.1.1「通報資訊安全事件」規範組織員工應循適當管道盡速通報資訊安全事件給管理階層。在此案例中，負責管理系統的館員在第一時間有跟其業務上司（組長）通報，但是該組長卻未繼續跟其業務上司（館長）報告，就是違反了 ISO 27001 A.13.1.1 條款的規定。另一方面，組織也應該對各種類資訊安全事件的通報流程和層級訂出明確的規範，使組織員工有所依循。

伍、結語

由於現代組織在運作上非常依賴資訊系統，因此，資訊安全管理系統（ISMS）近年來在國際間越來越受到重視。在國內，行政院也通令各級行政機構應盡快依據 ISO 27001 的相關規定，來建立資訊安全管理系統（ISMS）和取得資安認證。

由於ISO 27001對資訊安全的目標是希望能同時兼顧機密性 (Confidentiality)、完整性(Integrity)、可用性(Availability)，而圖書館做為一個傳播資訊的主要機構之一，雖然一向較強調或重視資訊的公開與普及，因此，圖書館內的資訊系統較少機密性資料，所以機密性相對來說較不重要，但是完整性和可用性對圖書館仍然是很重要的，這也正是ISO 27001應用在圖書館的切入點。

本文首先介紹了 ISO 27001 資訊安全管理系統（ISMS）的整體架構，和其所採用的「規劃 – 執行 – 檢查 – 行動」（PDCA）模式，使讀者對 ISO 27001 能有較全面性的掌握，其間也解釋了 ISO 27001 和 ISO 27002（或 ISO 17799）的相互關係。

再者，就 ISO 27001 對資訊安全管理系統（ISMS）的實作規劃而言，是以資產（Asset）為出發點，透過適當的風險評鑑（Risk Assessment）和風險處理（Risk Treatment），使剩餘風險（Residual Risk）皆在可接受的範圍內，藉以達到效益和成本的最佳平衡，並完成資訊安全的三個最主要目標：機密性、完整性、可用性。其間也以圖書館的角度或例子，來詮釋一些主要的概念、過程、作法。

最後，以一件大學圖書館的資訊安全事件為例，先詳細描述整個資訊安全事件發生和處理的過程，再列舉出引起資訊安全事件發生的 5 個（可能）因素，然後針對這些因素來一一分析，看 ISO 27001 資訊安全管理系統（ISMS）中的規定，如何能對此資訊安全事件的預防與處理有所幫助。

綜合來說，雖然圖書館由於其服務與運作的特性，其資訊系統中較少機密性資料，因此，在成本與效益的考慮下，是否應以 ISO 27001 來做全面的資訊安全認證仍須思量。但是，ISO 27001 和 ISO 27002（或 ISO 17799）的 11 個控制面相、39 個控制目標、133 個控制措施，幾乎涵蓋了保護資訊系統完整性和可用性的所有層面，就此點而言，圖書館即使不做資訊安全認證，仍應參考 ISO 27001 和 ISO 27002 內的相關規定來保護資訊系統，以使圖書館能持續不斷的來服務讀者。

附　註

註 1　ISO/IEC 27001 的官方網頁在 <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103>（2007/09/14）。

註 2　CNS 27001 的官方網址在 <http://www.cnsonline.com.tw>（2007/09/14）。

註 3　胡文騰，「金融機構 ISO 27001 換證作業：一個案公司之研究」（長庚大學資訊管理研究所，碩士論文，民國 95 年）。

註 4　鄭進興，「企業資料安全機制導入之研究」（高雄第一科技大學資訊管理研究所，碩士論文，民國

96 年 6 月）。

註 5　蔡重成、彭家亮、敖先義，「從企業營運的觀點探討 ISO 27001 資訊安全管理系統的產業價值」 **品質月刊** 43 卷 2 期（2007 年 2 月），頁 67-70。

註 6　「行政院衛生署玉里醫院通過 ISO 27001:2005 國際資訊安全管理制度認證」<http://www.training.tw.sgs.com/zh_tw/sa_news-1224?viewId=10005873>，(2007/09/14)。

註 7　「中華電信取得 ISO 27001 資安認證」 <http://www.ithome.com.tw/itadm/article.php?c=45123>，(2007/09/14)。

註 8　「國華人壽導入 ISO 27001 告別草莽時期」 <http://www.ithome.com.tw/itadm/article.php?c=36529>，（2007/09/14）。

註 9　「全機關獲 ISO27001 資安驗證 新聞局拔頭籌」<http://www.cna.com.tw/top10/20070913cap0360.html>，(2007/09/14)。

註 10　「主機代管業者爭相取得 ISO 27001 認證」 <http://www.ithome.com.tw/itadm/article.php?c=38073>，(2007/09/14)。

註 11　CNS 27001 第 4 頁。

註 12　133 個控制措施由於條款過多，請讀者自行參閱 ISO 27001 或 CNS 27001。

註 13　ISO 17799 後來調整為 ISO 27002，國內也有 CNS 17799 來呼應 ISO 17799，此外 ISO 17799 來自英國國家標準 BS 7799-1。

註 14　張美月，「風險評鑑 123：符合 ISO 27001 規範的資訊安全風險評鑑」 **證券櫃檯** 128 期 （2007 年 4 月），頁 109-115。

註 15　李慧蘭，「國際資訊安全標準 ISO 27001 之網路架構設計－以國網中心為例探討風險管理」，<http://yang.nhlue.edu.tw/tanet2006/ D000/D00018.pdf>，(2007/09/14)。

註 16　此定義取自 ISO/IEC 13335-1:2004。

註 17　此定義見 ISO/IEC 27001（或 CNS 27001）4.2.1(d)。

註 18　條文詞彙將採用 CNS 27001 中的翻譯文字。