量測資訊安全管理系統有效性方法之研究

潘世鳴[1]　　朱惠中[2]
[1]華梵大學資訊管理系 m9845207@hfu.edu.tw
[2]華梵大學資訊管理系 hcchu@cc.hfu.edu.tw

摘要

隨著網際網路與資訊技術的快速發展，組織處於數位且資訊豐富的環境，依賴資訊的程度日趨複雜，對於資訊的安全保護與管理變得格外重要。因此，許多組織建立資訊安全管理系統，達到組織所訂定保護資訊安全與降低資訊安全事件發生風險之目標。但依照許多資訊安全或電腦犯罪等相關研究與調查報告，皆指出組織仍然因遭受來自外部資安威脅或內部發生的資訊安全事故，蒙受極大的商業損失。這使得許多管理者關注如何瞭解資訊安全管理系統實施之後，是否真正發揮其有效性的評估方法。管理學大師彼得杜拉克(Peter Ferdinand Drucker)曾說：「你不能管理你無法衡量的事情，並且認為確認有效性是檢視管理制度是否成功的根源」。這意謂在資訊安全管理領域，若組織能藉由評估資訊安全管理系統有效性的資訊安全度量，建立可量測資訊安全管理系統有效性的方法，將可協助確認資訊安全管理系統實施現狀，持續改善資訊安全管理系統。因此，本研究將探討量測資訊安全管理系統有效性的原因，以及目前有關量測資訊安全管理系統有效性方法之文獻，期望能提供有意針對資訊安全管理系統進行量測研究之參考。

關鍵詞：資訊安全、資訊安全度量、資訊安全管理系統、資訊安全管理量測

1.前言

近年來，因網際網路的普及與電子商務等資訊科技發展迅速，許多組織或政府機關都相繼使用電腦系統，將許多營運上的重要資料儲存於電腦系統或利用網際網路來傳遞。為降低組織資訊安全風險與保護有價值的資訊，組織需要具備可管理資訊安全與評估有效性之計劃(Kenneth Joseph Knapp，2005)。因此，許多組織建置資訊安全管理系統(Information Security Management System)，透過風險管理與資訊安全控制措施，以達到組織所訂定保護資訊安全之目標。依照 CSI / FBI 電腦犯罪與安全調查報告(CSI/FBI Computer crime and security survey)，各國組織在 2007 年至 2009 年間，因遭受來自外部資安威脅或內部發生的資訊安全事故，至少損失高達 100 萬美金以上，這使得許多管理者開始關注如何瞭解資訊安全管理系統是否真正發揮其有效性的評估方法。

2. 文獻探討

2.1 資訊安全管理系統介紹

資訊係指組織在營運過程中所蒐集、產生或運用的資料，利用可書寫於紙上或是以電子媒體等方式儲存，並可以用傳統郵寄或是電子信號等方式傳送。然而，無論資訊的形式為何?或是以何種方式分享或儲存，資訊已成為組織營運重要資產需要妥善保護。資訊安全則是保護資訊的機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，以確保資訊可因應使用者需求且經合法授權的程序進行存取，並且確認資訊不會被不當的修改或揭露給未經授權的使用者或組織。

為能協助組織有效保護與管理資訊資產，英國標準協會(British Standards Institution，BSI)於 1995 年制訂資訊安全管理系統，協助各國組織透過風險評鑑與管理，以及選擇適當的資訊安全政策與控制措施等管理方法，確保達成組織的營運目標與資訊安全要求 (歐陽惠華，2007)。2005 年曾提出資訊安全已成為全球組織所面臨的關鍵問題，資訊安全管理系統已經由國際標準組織(International Organization for Standardization，簡稱 ISO)引用並頒佈命名為國際標準 ISO/IEC27001:2005 資訊安全管理系統驗證要求事項(Information technology-Security techniques-Information security management systems- Requirements，以下簡稱 ISO/IEC 27001:2005)，成為資訊安全管理的國際通用語言。其實施作法為採用風險評鑑與管理、制定適切的控制目標與控制措施，建立與維護組織所需之資訊安全保護程序，以協助組織保護資訊資產的機密性、完整性及可用性。

建立資訊安全管理系統，可分為分為六個步驟:

1.制定資訊安全政策：

依照組織的營運要求及遵循相關法律規範，由管理階層設定與營運目標一致之明確的政策指示，並經由公告發布程序與文件維護等方式，說明整個組織的資訊安全政策，以展現對資訊安全的支持與承諾。

2.定義適用範圍：

組織首先要依據營運目標、核心的業務、所在位置、資產和技術等特性，定義出資訊安全應受到適當控管的範圍。

3.進行風險評鑑：

依照組織營運目標或風險接受程度，針對整個組織、或部分組織之風險進行評鑑，並識別、量化各項風險的方式及處理之優先順序。評鑑風險與選擇控制措施的過程可能需要履行數次，以涵蓋組織或個別資訊系統的不同部分。

4.進行風險管理：

組織進行風險管理或處理之前，應先建立風險是否可接受的判定準則，並適當產生文件化或記錄。當風險評鑑後識別出各項風險後，均需做風險處理決策。包括:

(1)採用適切的控制措施以降低各項風險。

(2)移相關風險至其它合作廠商或使用者。

(3)若風險處理結果滿足組織政策與準則時，則接受此風險。

5.選擇控制目標與措施與實行：

組織應針對風險評鑑結果，設計或選擇組織可接受與執行的資訊安全控制措施，以符合組織的特定資訊安全需要。組織應針對控制措施加以監視、評估與改進安全控制措施的有效性，以符合組織的資訊安全目標。

6.制定適用性聲明：

說明組織建立資訊安全管理系統，對其適用各項控制目標與控制措施的文件化聲明。

資訊安全不能單靠技術設備或產品來保護，更需要藉由適當的程序或控制措施保護組織資訊。除此之外，Thomas R. Peltier 認為保護資訊的重點，必須要可以符合組織業務目標或任務使命，以符合成本效益(Thomas R. Peltier,2001)。知名國際資訊安全專家 Bruce Schneiner 曾說過：「安全是一個過程，而不是一項產品(Security is a process , not a product.)」，這句話說明保護資訊安全不單僅是使用了哪些資訊安全防護產品所提供的安全性功能，而是針對資訊保護方式訂定明確的要求與規定，確定資訊安全人員的安全職責與義務，並測量資訊安全保護的相關要求與規定是否有效，以提供管理階層可做出明智的業務決策。

2.2 為何要量測資訊安全管理系統實施的有效性

管理學大師彼得杜拉克(Peter Ferdinand Drucker)曾說：「你不能管理，你無法衡量的事情」，並且認為確認有效性是檢視管理制度是否成功的根源。資訊安全管理系統屬於組織內部眾多管理體系之一環，如何檢視資訊安全管理系統有效性，亦是組織應重視之議題。組織建立量測(measurement)資訊安全管系統有效性的主要原因為，管理者可藉由評估資訊安全管理系統控制措施實施有效性定量數據的資訊安全度量(security metrics)，獲得組織實施資訊安全政策、過程及執行程序之客觀證據，以判定資訊安全管理系統之控制措施，是否達成所規劃預定達成之控制目標程度與有效性 (樊國禎、林樹國、黃健誠等人，2005)。

量測資訊安全管理系統實施有效性，並非僅是找出相關定量的測量(Measure)數據進行比較，而是為促進組織的發展與資訊安全管理系統實施過程可更為完善，以確保組織資訊的安全，提升組織的競爭能力。但何謂量測資訊安全管理系統實施有效性，探討相關文獻後，綜整定義如后，「量測資訊安全管理系統有效性係為組織事先定義資訊安全管控目標與預定達成的資訊安全度量，使用測量工具與測量程序，取得資訊安全度量的測量結果；並利用分析模型確認測量結果，是否符合組織當初所定義控制目標的過程」(ISO 9000：2000；ISO/IEC 3rd WD 27004；ISO/IEC 27004:2009；樊國禎、林樹國、黃健誠等人，2005；張詠翔，2005；李元全，2006)。

「安全本身並不是目的，而是達成目的的方法」(NIST SP800-12, 1995)。由此可知，組織若能確認資訊安全管理系統的有效性，達成組織體或事業體依所訂之目標與完成期限，即表示資訊安全管理系統實施是否成功的關鍵(李元全，2006)。除此之外，本研究

以三個角度說明，組織量測資訊安全管系統實施有效性的原因：

1. 資訊安全管理系統驗證要求

ISO 所制定的 ISO/IEC 27001:2005，已成為國際上使用最廣泛的使用資訊安全管理驗證標準，全球已有 85 個國家的 7,279 個組織通過驗證。而 ISO 制定的 ISO/IEC 27002:2005 資訊安全管理系統實務指南(Information technology-Security techniques-Code of practice for information security management，以下簡稱 ISO/IEC 27002:2005)，也已是全球組織若需建立資訊安全管理系統的參考指南。

在 ISO / IEC 27001:2005 與 ISO/IEC 27002:2005 標準中，多處提到組織建置資訊安全管理系統時，應建立客觀且可量測資訊安全管理系統有效性的方法，用以評估資訊安全管理系統的有效性；並可透過量測結果，持續監督與審查組織資訊安全管理系統實施之過程，以符合組織的各項安全要求。本研究整理如下：

(1) 監視與審查資訊安全管理系統：
- 依據資訊安全管理系統政策、目標及實際經驗，評鑑及在適用時測量過程績效，並將結果回報給管理階層審查。
- 組織應界定如何量測所選擇的控制措施或控制措施群的有效性，並規定如何使用這些量測去評鑑控制措施的有效性，以產生可比較與可再產生的結果。
- 量測控制措施的有效性使管理者與幕僚人員可判定控制措施達成所規劃控制目標的程度。

(2) 維持與改進資訊安全管理系統：基於客觀的測量測量資訊安全管理系統之有效性。
(3) 管理階層審查之輸入：應包括有效性測量的結果。
(4) 管理階層審查之輸出：應包括資訊安全管理系統有效性之改進與控制措施的有效性如何量測之改進。

雖然 ISO / IEC 27001:2005 與 ISO/IEC 27002:2005 標準中，均有強調測量資訊安全管系統之重要性，但卻未說明應如何蒐集與量測的方法。因此，ISO 於 2009 年 10 月公布於 ISO/IEC 27004:2009 資訊安全管理量測標準(Information technology-Security techniques-Information security management measurements，以下簡稱 ISO/IEC 27004:2009)，說明組織如何針對資訊安全管理系統有效性等量測機制與測量技術，並提供可適用任何有意要採取量測行動來保護資訊安全的組織。

2. 驗證資訊安全管理需求是否被滿足

根據國際知名資訊安全防護組織(SysAdmin, Audit, Network, Security)研究報告，組織在資訊安全需求，除須符合國際法規與經營環境的要求，且必須確保組織業務流程的資訊安全控制措施被正確的實施。但組織要如何以客觀的方式，確定所實施的控制措施符合組織或法規需求?或是要如何證明核心業務流程的資訊安全風險是被有效的降低?最佳的方式是利用資訊安全度量指標，去驗證資訊安全管理系統的實施結果，是否達到

組織的資訊安全需求 (SANS，2010) 。

雖然目前組織建立資訊安全管理系統，會先針對組織可能遭遇的資安風險進行評估，然後藉由規劃(Plan)、執行(Do)、檢查(Check)及行動(Act)等過程導向管理方法，驗證資訊安全管理系統實施的有效性。但隨著組織資訊環境愈來越複雜，資訊管理業務流程異動相當頻繁等情況下，若未能定義關鍵資訊安全度量指標與分析方式，量測結果是否得反映資訊安全管理系統實際現況，值得探討。舉例來說，某組織為保護內部的電腦，遭受蠕蟲病毒或惡意程式之攻擊，會制定電腦須安裝防毒軟體之資訊安全政策，並制定防毒軟體安裝率須達 100%的安全度量。但安裝防毒軟體固然重要，但若未能持續更新防毒碼，則會造成讓防毒軟體的防護功能大打折扣，此時，應制定防毒軟體更新比率之量測方式，以驗證資訊安全需求是否被滿足。

3. 作為資訊安全管理系統改善依據

知名國際資訊安全專家 Bruce Schneiner 曾說過：「安全是一個過程，而不是一項產品(Security is a process,not a product.)」，這句話闡述保護資訊安全不單僅是使用了哪些資訊安全防護產品所提供的安全性功能，而是應針對制定明確的資訊保護要求與規範，並依照相關回饋與建議，確認資訊安全保護的相關要求與規範是否有效，提供著高級管理階層可做出明智的業務決策，以利資訊安全管理系統持續改進。

ISO/IEC 27001:2005 共分 11 個資安保護領域，並細分 39 個控制項目與 133 個控制措施。雖然組織通常係透過資訊安全稽核找出資訊安全問題與不足之處，但管理階層應如何決定何項控制措施須優先進行改善，以及完成改善之時間(林宏昇，2008)。此時，若具備可呈現資訊安全管理系統控制措施實施有效性的資訊安全度量，將可協助管理階層決定(方仁威，2004)。同時。資訊安全度量也可藉由分析模組，反應組織資訊安全管理系統實施的趨勢，已作為後續改善之參考依據。

3. 資訊安全管理系統有效性量測方法探討

有關量測資訊安全管理系統有效性之概念，最早啟源於美國 2002 年 12 月所公布的聯邦資訊安全管理法案(Federal Information Security Management Act)中的 PUBLIC LAW 107–347 法案，此法案也成為 ISO 個會員國相繼發展量測資訊安全管理系統之重要參考指標。美國國家標準與技術研究所(National Institute of Standards and Technology，以下簡稱 NIST)，率先於 2003 年 7 月發布「資訊技術系統安全測量指南(NIST SP800-55 Security Metrics Guide for Information Technology Systems)，以下簡稱 NIST SP800-55」，而這份文件促使得澳大利亞於 2004 年新加坡 SC27 會議上，提出發展資訊安全度量與量測機制標準(Information Security Metrics and Measurement Standard)之構想。經過多年的討論，ISO 於 2009 年 10 月公布 ISO/IEC 27004:2009，提供有意建立資訊安全管理統有效性量測與分析方法的組織參考。除此之外，OISM 發展資訊安全管理成熟度模型(Information Security Management Maturity Model，簡稱 ISM3)主要以 ISO9001 品質管理系統為原

則，利用資訊安全度量(Security Metrics)與資訊安全指標，建立可針對資訊安全管理系統實施過程之評量架構，並認為認為績效指標是唯一可針對組織業務需求和現有資源是否有效的測量方法。以下將分別進行文獻回顧，並探討其共同性與差異性。

4. 資訊技術系統安全測量指南

美國聯邦政府於 2002 年 12 月公布 PUBLIC LAW 107–347 聯邦資訊安全管理法案，容載明「美國應發展，可針對政府機關所實施的資訊安全政策或控制措施的效率與有效性，訂定測量準則與指標，以確認政府機關是否遭受入侵、破壞提高政府機關資訊安全水準，訂定測量準則與指標，以確認政府機關是否遭受入侵、破壞提高政府機關資訊安全水準。標準中應包含測量的方法、架構與可支援的行動方案等」。

因此，2003 年 7 月 NIST 發布編號 NIST SP800-55 資訊技術系統安全測量指南，在這份文件裡，提供美國政府機關如何發展與透過資訊安全度量收集、分析與產出有效性量測的報告，以便聯邦政府可從而推動制定資訊安全決策、改進資訊安全管理系統有效性和責任。NIST SP800-55 亦提供組織如何通過使用資訊安全度量來鑒別一個安全控制、政策與程序式是否合適的方法(請詳見圖 1)，並以附件的方式提供包含 16 種的測量資訊安全管理系統的範例。

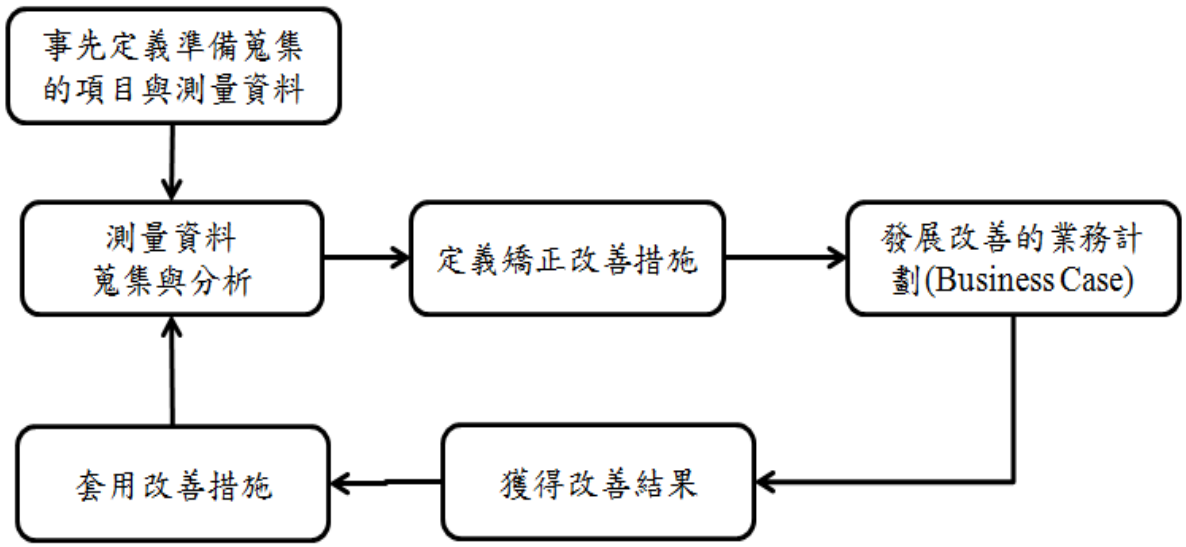

圖1 NIST SP800-55 資訊安全問題量測流程

資料來源： 本研究整理 NIST SP800-55 Security Metrics Guide for Information Technology Systems

NIST 為確保所發展之文件，可符合 2002 的 FISMA 法案，NIST 公佈 SP 800-26 資訊技術系統自我評估參考手冊(Security Self-AssessmentGuide for Information Technology Systems)，並結合資訊安全控制目標和技術結合進來的方法。NIST 於 2008 年將 SP800-26

的內容整合至 SP800-55 資訊技術系統安全測量指南中，並將 NIST SP800-55 重新命名為資訊技術系統績效測量指南(Performance Measurement Guide for Information Security)。NIST SP800-55 下的討論分為如下幾個部分：

(1)任務和責任

說明發展和執行資訊安全度量的主要任務和負責資訊安全職務之責任要求，並描述負有資訊安全職責的管理者，對於組織整個資訊安全實施成功與否有直接的關係。

(2)資訊安全度量背景

介紹安全度量的定義、各種類型的安全度量和直接影響安全度量項目成功因素及相關背景。

(3)資訊安全度量發展

介紹用於資訊安全度量發展的方法。這個方法包含度量發展過程主要是在特定時間為組織建立合適的初始的度量以及其子集的一部分。

(4)資訊安全測量專案執行

介紹可影響安全度量項目的技術執行的各種因素。度量執行過程是要運轉一個重複性的度量並保證在特定的時期度量資訊安全的某些適當的方面。

NIST SP800-55 認為有效性量測的結果，可用於確定所選定的安全控制與促進改進措施的優先順序次序，所以可能需要搭配專業的自動化檢測與評估工具，以便直接與安全控制的執行情況。其次，為使資訊安全管理系統測量方式更為完整，且可讓聯邦政府下各機關可使用，NIST 分別於 2006 年 10 月公布聯邦政府資訊系統與組織安全控制指南(Guide for Assessing the Security Controls in Federal Information Systems and Organizations)，以及於 2007 年 5 月提出資訊安全自動化計畫(ISAP)、安全內容自動化協議(Security Content Automation Protocol ，簡稱 SCAP)及針對聯邦政府桌面系統組態基準(United States Government Configuration Baseline ，簡稱 USGCB)等文件，以強化量測資訊安全管理有效性之整理完整度。

5. ISO/IEC 27004:2009 資訊安全管理量測標準

ISO 國際標準化組織與 IEC 國際電工委員會，於 2009 年 10 月公布於 2009 年 10 月公布 ISO/IEC 27004:2009 資訊安全管理量測標準(Information technology-Security techniques-Information security management measurements，簡稱 ISO/IEC 27004:2009)。ISO/IEC 27004:2009 主要說明可針對資訊安全控制措施、資訊安全過程及資訊安全管理系統有效性等測量措施技術與測量機制，並提供可適用任何有地要採取行動來保護資訊安全的組織。

ISO/IEC 27004:2009 這份國際標準原先是由澳大利亞於 2004 年新加坡 SC27 會議上提出發展資訊安全測量機制與測量措施標準之構想，並建議制訂「資訊安全測量機制與測量措施標準(Information Security Metrics and Measurement Standard)」。經 ISO／IEC、JTCl(資訊技術委員會)、SC27(安全技術小組委員會)等代表共同討論並決議啟動此標準

之新工作項目提案，並將此提案編號訂定為 ISO/IEC 24742 與專案編號 JTC 1.27.44 後納入 SC27 工作計畫書。

2005 年 1 月 10 日，SC 27 小組提出 ISO/IEC 1st WD 24742 資訊技術-安全技術-資訊安全管理測量模式與測量(Information technology - Security techniques - Information security management metrics and measurements，簡稱 WD 24742)之草案。2005 年 6 月 30 日， SC27 提出 ISO/IEC 2nd WD 24742 第二版草案，並納入 ISO/IEC 27000-ISO/IEC2009 資訊安全管理標準之中。同年 11 月 ISO/IEC 3nd WD 24742 第三版草案，並將標準名稱從「Information Security Metrics and Measurement」修訂為「Information Security Measurement」。之後，歷經多年討論後，於 2009 年 10 月由國際標準組織 ISO 正式公布。

ISO/IEC 27004:2009 說明評估實施資訊安全管理系統的有效性之量測方式，以配合 ISO / IEC 27001:2005 相關規範；包括針對資訊安全政策、風險管理、控制目標，控制措施，以確定組織是否有任何資訊安全管理系統的過程或控制需要改變或改善，同時，亦可以協助證明該組織遵守 ISO / IEC 27001:2009 相關規範。其次，ISO/IEC 27004:2009 國際標準提供組織在完成資訊安全管理系統導入完成後，同樣可藉由規劃(Plan)、執行(Do)、檢查(Check)及行動（Act）之循環，實施和運行資訊安全量測方案(請詳見圖 2)。量測方案包含制定資訊安全管理系統測量準則與事前準備、資訊安全管理系統測量數據蒐集、分析資訊安全管理系統所蒐集之數據，以及利用測量結果，以確定需要改進 資訊安全管理系統的範圍、政策、目標、控制，過程和程序。該標準具有資訊安全測量概述、管理責任、措施與測量發展、測量操作、數據分析和測量結果的報告、資訊安全量測方案的評估和改進。

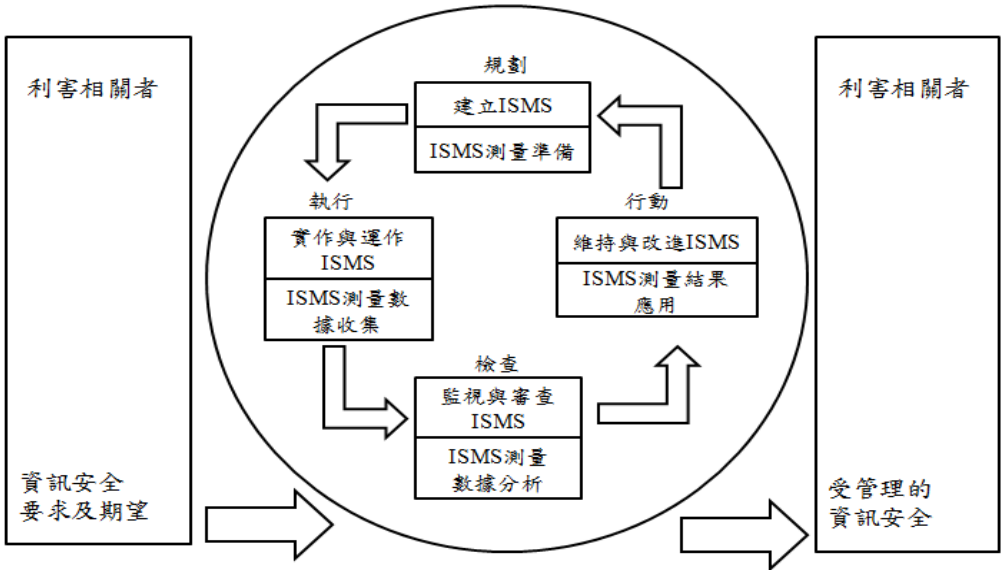

圖2　資訊安全管理量測系統與資訊安全管理系統關係圖

資料來源： 本研究整理 ISO/IEC 27001:2005 與 ISO/IEC 27004:2009

另外，ISO/IEC 27004:2009 提供一個資訊安全安全測量模型(Information security measurement model)。這個模型是當組織導入完成資訊安全管理系統後，訂定相關量化屬性，並分析測量指標與結果，是否符合原先預設定之控制目標。

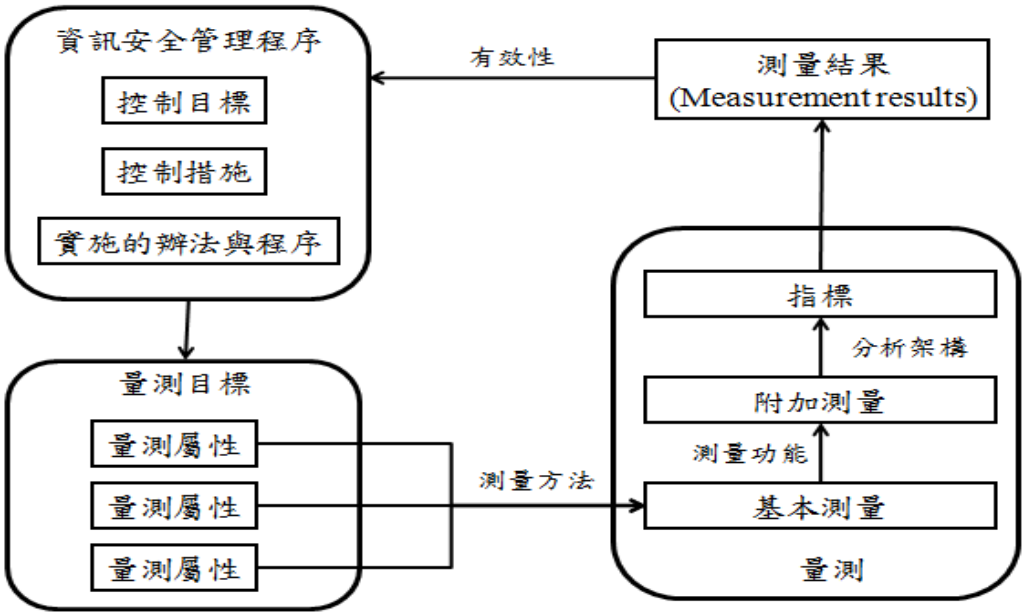

圖3　資訊安全管理系統測量模組

資料來源： ISO/IEC 27004:2009 Information technology-Security techniques-Information security management measurements

6. 資訊安全管理成熟度模型

資訊安全管理成熟度模型(Information Security Management Maturity Model，簡稱 ISM3)主要以 ISO9001 品質管理系統為原則，利用資訊安全度量與資訊安全指標，建立可針對資訊安全管理系統實施過程之評量架構，並認為認為績效指標是唯一可針對組織業務需求和現有資源是否有效的測量方法。

ISM3 認為資訊安全管理系統的目的是預防和減緩，組織可能因攻擊所造成之錯誤或和事故，危及組織資訊系統或流程。若組織實施資訊安全時具備良好的過程，各項資訊安全將會相對提升。因此，ISM3 是係針對資訊安全實施的過程(process)進行測量，而非如同 ISO/IEC 27004:2009 是以資訊安全控制措施(Control)進行測量。ISM3 認為測量的重點，在於是否可以找出資訊安全實施過程有甚麼不尋常的地方，而不用時時面對隨時在變化的風險。

ISM3 認為明確定義保護資訊安全的職責，並要求每一個資訊安全的過程有明確的管理者(Owner)，這個管理者並須具備能夠監督及修正資訊安全過程的權責。ISM3 認為定的資訊安全目標是組織進行有效管理必須需的過程，資訊安全目標必須適用於全組織

與可讓組織從上到下皆能執行，且訂定具有量化的測量指標是資訊安全管理系統是否成功的關鍵。ISM3 制定 5 個成熟度與能力評量等級。

表1　資訊安全管理成熟度模型成熟度與能力評量等級表

評量等級	評量內容說明
等級 0(未定義)	這個級別是建議組織應有限的資源下，保持資訊安全目標在最低風險環境。在這個等級並未有任何建議事項。
等級 1(已定義)	這個等級說明組織如何從技術威脅評估風險，或是如何認定風險若被降低後，是能減少組織在資訊安全流程所投入的時間、成本與效益。這些評估的過程與結果須被文件化
等級 2(管理級)	這個等級是用來定義實施資訊安全實施的過程與結果，如何進行修復與改善。並且須明確說明修復與改善的過程需要到甚麼樣的指標，才能降低資訊安全風險。
等級 3(控制級)	這個等級是組織如何藉由管理過程與里程碑，對於存在較嚴重的風險或資訊安全威脅，如何可準確預測組織為降低風險所需的資源與控制措施，已達成組織的目標。
等級 4(最佳化級)	這個等級是組織內若存在特殊需求或具有敏感資訊時，如何讓實施的控制措施與目標時，處於正常的資訊安全環境。

資料來源： Information Security Management Maturity Model

ISM3 認為安全是一個過程的結果，組織可從實施好的資訊安全過程，保護組織的可用資源。所以 ISM3 不考慮單項的資訊安全控制措施，而是從流程面去檢視所實施的資訊安全控制措施是否有益於組織的整體發展。ISM3 提供包含涉及組織廣泛的目標，協調和提供資源的戰略目標、設計可確實達成與優化管理流程的具體戰術作為，並能藉由技術手段評估有效性等方面，強化組織資訊安全的成熟度。

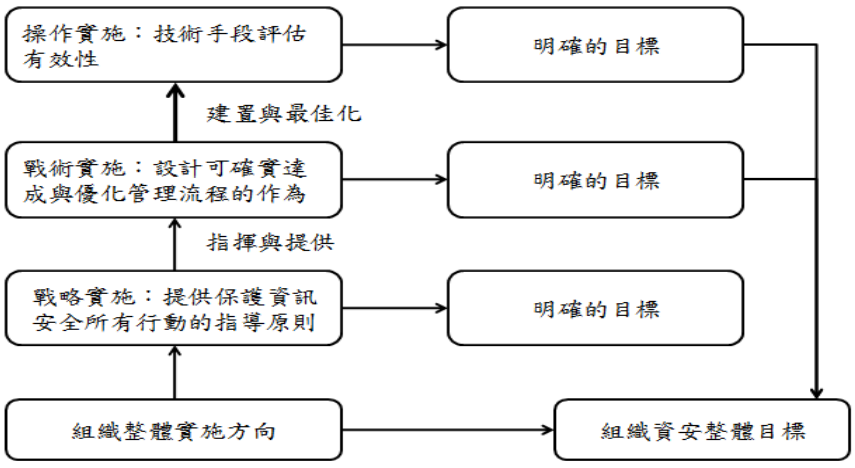

圖4　ISM3 成熟度過程評量模型

資料來源： Information Security Management Maturity Measurement

4.量測資訊安全管理系統方法之優缺點比較

資訊安全管理系統量測的目的並非是為了測量而測量，而是為了促進組織的 ISMS 發展與實施過程可更為完善，以確保組織資訊的安全，提升組織的競爭能力。組織若能經由有效性測量，將可預防與減緩，組織因自然災害或人為所造成的操作錯誤，以及外部資安攻擊可能危害資訊系統或流程。管理階層亦可針對資訊安全管理系統有效性之測量數據與安全度量，瞭解組織實施資訊安全的過程，各項資訊安全將會相對提升。本研究已別探討量測資訊安全管理系統實施有效性之方法，以下將分別針對三項量測方法的優、缺點進行比較(請詳見表 2)。

表2　量測資訊安全管理系統方法之優缺點比較表

比較方法 / 量測方法	優點	缺點
資訊技術系統安全測量指南 (NIST SP800-55)	● 提供測量資訊安全管理實施的績效的方法。 ● 提供包含 16 種的測量資訊安全管理系統的範例，有利於實際運用與操作。	● 屬開放式的方法論架構，量測方法不利適用於各國組織。 ● 僅提供如何量測之方法論，但並未提供可操作性強的測量方法，不利於資訊安全管理測量在實際工作中運用。
資訊安全管理量測標準 (ISO/IEC 27004:2005)	● 提供組織學習如何建立量測資訊安全管理系統之方法與 10 份範例。 ● 有助解決資訊安全驗證機關各自對於控制措施防範之見解，對日後組織資訊安全管理系統的量測，有一致性的指引與稽核準則。 ● 適用於已通過 ISO/IEC 27001:2005 標準驗證之組織。	● 僅提供如何量測之方法論，但並未提供可操作性強的測量方法，不利於資訊安全管理測量在實際工作中運用。 ● 僅提出資訊安全度量之定義，但未能提出如何設計資訊安全度量的方式與測量的方法
資訊安全管理成熟度模型 (ISM3)	● 提供資安成熟度評量等級，可讓組織瞭解目前資訊	● 針對資訊安全實施過程進行評量，實際執行方式過

比較方法 / 量測方法	優點	缺點
	安全問題所處的評量架構 ● 整合組織戰略與戰術目標，設計可確實達成與優化管理流程的作為，並能藉由技術手段評估有效性等方面，強化組織資訊安全的成熟度。 ● 提供建立量測成熟度參考手冊與範本，以供組織參考運用。	於複雜，不利於在組織內發展。 ● ISM3 資訊安全目標必須適用於全組織與可讓組織從上到下皆能執行與有效管理。但如何確實執行將會帶來額外的管理問題。

資料來源： 本研究自行整理

5. 結論

資訊安全管理測量的最終目的是為保障組織資訊安全，降低資訊安全風險而持續進行與改進的，然後可藉由在量測的方式取得資料、藉由數據進行分析，以發現資訊安全管理當前存在的問題，最終達到組織預定持續運行的目標。本研究發現於資訊安全管理系統量測標準建立之後，有關資訊安全管理系統量測與分析研究之相關文獻，已日益增多。顯示資訊安全管理系統有效性測量理論，測量方法與程序，以及測量數據分析方法等研究，將是資訊安全管理領域日後的研究重點。

參考文獻

1. 方仁威，「資訊安全管理系統驗證作業之研究」，國立交通大學資訊管理研究所博士論文，台北，民國九十三年五月，P75~P90。
2. 李元全，「航空站營運管理績效之研究以金門及馬祖地區機場為例」，銘傳大學公共事務學系研究所碩士論文，2006。
3. 林宏昇，「植基於 ISO 27001 標準建構資訊安全稽核決策之研究－以股務資訊系統為例」，國防大學管理學院資訊管理學系碩士論文，台北，2008，P12~16。
4. 如何制定組織安全政策(台灣通訊 NO.94 ，2001/10)，http://ssttpro.acesuppliers.com/tech/tech_1.asp?idxid=3285。
5. 佛瑞蒙德。馬利克(Fredmund Malik)著，2008「新時代的有效管理」，第一版，李芳齡譯，天下雜誌，台北。
6. 洪國興、季延平、趙榮耀等人，「影響資訊安全關鍵因素之研究」，政治大學資訊管理學系，資訊管理研究，第六期，民國 95.07，頁 1-29。

7. 張詠翔，「結合 BS7799 與資訊安全藍圖建構資訊安全評估機制之研究」，銘傳大學資訊管理學系碩士論文，台北，民國九十四年六月，P11~P13。
8. 歐陽惠華，「論文_ISO 27002 與 COBIT 4.1 控制措施之對映分析」，高雄師範大學，高雄，民國九十六年，P5。
9. 樊國楨、林樹國、黃健誠，2008.04「資訊安全管理系統驗證標準化之二：資訊安全管理系統政策集初探」，資訊安全通訊，14 期第 2 卷，頁 1-21。
10. 樊國楨、林樹國、黃健誠，「資訊安全管理系統驗證標準化初探之三：資訊安全管理系統有效性量測初探」，資訊安全通訊，14 期第 1 卷，頁 1-21，2008.01。
11. Andrew Jaquith，Security .Metrics：.Replacing.Fear.Uncertainty.and.Doubt.,US, 2007。
12. "Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson，"NIST Special Publication 800-55 Revision1，Performance Measurement Guide for Information Security" ，2008/7。
13. Hong-li Liu;Ying-ju Zhu，" Measuring effectiveness of information security management"， "IEEE Computer Network and Multimedia Technology, 2009. CNMT 2009"，18-20 Jan. 2009。
14. "ISO/IEC 27001:2005 ，Information technology-Security techniques--Information security management systems -- Requirements"，"International Organization for Standardization，ISO"，2005。
15. "ISO/IEC 27002:2005，Information technology-Security techniques-Code of practice for information security management"，"International Organization for Standardization，ISO"，2005。
16. "ISO/IEC 27004:2009，"Information technology — Security techniques — Information security management measurements"，"International Organization for Standardization，ISO)，2005。
17. "ISM3"，"Information Security Management Maturity Model，Information Security Management Maturity Model v_2_10.pdf。
18. Kenneth Joseph Knapp, "A model of mangerial effectiveness in information Security：from ground theory to empirical test"，The Graduate Faculty of Auburn University, ProQuest Information and Learning Company , December 16, 2005，P26~p30。
19. "Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo，" NIST Special Publication 800-55，Security Metrics Guide for Information Technology Systems" ，2003/7。
20. "Measuring effectiveness in Information Security Controls"，"SANS Institute InfoSec Reading Room"，April 5 2010。
21. "PUBLIC LAW 107–347—DEC 17"，"Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled"， 2002。
22. "Robert Richardson, CSI Director"，"2008 CSI Computer Crime and Security Survey，Computer Security Institute"。

23. "Robert Richardson, CSI Director"，"2009 CSI Computer Crime and Security Survey，Computer Security Institute"。
24. "Thomas R. Peltier"，"Information Security Policies, Procedures, and Standards Guidelines for Effective Information Security Management，USA，2001。

The methodology for effectiveness of information security management system measurement

Shih-Ming Pan[1] Huei-Chung Chu [2]

[1] Information Management Department of Huafan University and m9845207@hfu.edu.tw

[2] Information Management Department of Huafan University and hcchu@cc.hfu.edu.tw

Abstract

With the Internet and the rapid development of information technology, organizations in the digital and information-rich environment, dependent on the extent of information the increasing complexity of information security for the protection and management has become particularly important. Therefore, many organizations establish information security management system, set up organizations to protect information security and reduce the risk of information security incident objectives. But according to many information security or computer crime investigation and other related research and reports are that the organization continues to suffer from external or internal security threats information security incidents occur, subject to significant business losses. This has led many managers to focus on how to understand the information security management system implementation, really play their effectiveness assessments. Peter Ferdinand Drucker said: "You can not manage what you can not measure, and confirm the validity of the view that the management system is the root of success." This means that in the information security management, if the organization can assess the information security management system by the effectiveness of security measures, the establishment can measure the effectiveness of information security management system approach, will help confirm the status of implementation of information security management system, continued to improve information security management system. Therefore, this study will examine the measure the effectiveness of information security management system reasons, and the current measured on the effectiveness of information security management system approach of the literature, hoping to provide interested in information security management system for the measurement of the reference.

Keywords: Information Security、Security Metrics、Information Security Management、Information Security Management System Measurement