使用 COBIT 5 於資料外洩預防
Using COBIT 5 for Data Breach Prevention

作者: Mathew Nicho, Ph.D., CEH,SAP-SA, RWSP,

is the director of the Master of Science program at the College of Information Technology at the University of Dubai (Dubai, UAE). He trains students/professionals on ethical hacking and preventive measures; teaches IT governance, audit and control; and has published papers in several international journals and conference proceedings.

Hussein Fakhry, Ph.D.,

is the dean of the College of Information Technology at the University of Dubai (Dubai, UAE). Fakhry's research in information systems research using systems dynamics, information systems security, e-commerce and e-business, decision support systems, applications of artificial intelligence, and assessment of academic programs has appeared in numerous international journals and international conferences.

譯者: 陳立群

CISM,CISA,CISSP,PMP, 電腦稽核協會理事,Taiwan CISM Coordinator,中華電信數據通信分公司政府網路處組長

受矚目的資訊安全事件已經常態地造成公司之壓力，強化其網路與對資訊安全採更積極的態度。然而哪一種安全倡議能提供公司最大的改善常常不明確。[1] 自 2003 年 [2] 起，安全和隱私仍然為資訊安全管理階層十大關鍵議題，在這方面，資訊安全變成資訊系統(information systems ,IS) 管理者 [3] 緊要的議題，且對於持續幸福的現代組織至關重要。[4] 因此組織需要保護資訊資產以對抗網路犯罪、阻斷服務攻擊、網站駭客、資料外洩、身分和信用卡偷竊、舞弊和其他形式的內部威脅 [5]。公司的資訊相關資產現在已經成為最有價值的資產之一 [6]，勞動力中不斷增加的移動性以及在組織內外透過不同可攜式與網路媒介處理公司資訊之方便性，已經將任何威脅放大到關鍵的程度。在任何組織中資訊是十分重要的資產，因此透過資訊安全的程序進行保護有很高的重要性 [7]。現行的技術性資訊系統安全框架與資訊系統控制的應用曾有效地預防從外部進入組織之網路，但組織員工與資訊資產沿著延伸網路之可移動性已經顯示對於組織資料之嚴重風險。這已經被每十名員工中有六名介於 18 至 35 歲之間於工作時使用個人裝置而公司員工平均每天收與送 112 封電子郵件之事實證實。[8]

在過去三年（2010～2012 年）CSI 電腦犯罪調查和身分竊取資源中心（ITRC）的研究報告經過詳細分析與審閱資料外洩之趨勢與統計指出，駭客迴避組織的網路防禦，針對在延伸網路內與外儲存、使用以及移動中的資料與媒體等目標攻擊。此外，在員工使用數據錯誤、問題和意外的部分，惡化這種情形因此傳統技術與社會經驗技術控制並無法適當預防。在此方面，組織將儲存、使用以及移動中的資料分類與保護為當務之急。

COBIT® 5 促成因素和管理實務可用於防止組織內與延伸網路之惡意活動與資料外洩.源自於 ITRC 資料庫詳細識別與分析 2012 年十大資料外洩與入侵事件可確認、分析與凸顯導致資料外洩之弱點與欠缺的控制。此分析顯示百分之七十之資料外洩是由於欠缺或忽視非技術性之資訊技術控制，亦即百分之三十的資料外洩可以採用技術機制避免。

對於確認的弱點，相對的 COBIT® 5 資訊技術管理實務已經選擇並對映，不僅展現已確認之弱點能使用 COBIT® 管理實務予以預防，也能使用三種 COBIT® 5 監控管理流程監督這些管理實務之有效性。本文建議依據一組 COBIT® 5 基礎管理實務的安全框架及特定行業相關框架被要求適切地保護組織避免外部和內部入侵。

2012 年十大資料外洩事件

根據 ITRC 資料庫，2012 年十大資料外洩事件經過分析以決定攻擊的特性並評估在這些侵害事件中技術與非技術性資訊科技機制的角色。這些資料呈現於表 1 以確認每一個案例中

攻擊的性質與方法。

表 1—2012 十大資料外洩事件

編號	組織	資料外洩特性	方法	攻擊特性
1	Nationwide Mutual Insurance—Allied Insurance (Columbus,Ohio, USA)	公司電腦系統的資料庫遭入侵，包括姓名、社會安全號碼及其他身分識別資訊例如駕照號碼、生日等資料外洩，某些案例還包括婚姻狀況、性別、職業、姓名與雇主的地址。此次資料外洩並未包含信用卡資訊	遭外部駭客攻擊，調查持續進行中	未確認的/假設為技術純熟的駭客所為
2	Global Payments (Atlanta,Georgia, USA)	一千五百萬名北美客戶之支付卡詳細資訊自公司伺服器被竊取，包含從 Global Payments 公司申請處理服務的商家所蒐集的個人資訊，花費美金九千三百九十萬元的收費和罰款	遭外部駭客攻擊，調查持續進行中	未確認的/假設為技術純熟的駭客所為
3	New York State Electric & Gas (NYSEG) (USA)	此個資外洩牽涉一百八十萬筆包含社會安全號碼、生日的紀錄，對某些顧客還包含銀行帳號	分包商的職員取得未經授權的顧客資訊存取	非技術性的
4	University of Nebraska (Lincoln,Nebraska, USA)	此事件牽涉入侵大學資料庫，其內包含超過 650,000 名學生、雙親及雇員之紀錄。自 1985 年就讀 Nebraska 大學的學生其社會安全號碼、姓名、地址、課程分數、就學貸款與其他資訊都遭洩漏。.	大學生使用已知的漏洞進行熟練的攻擊	未確認的/假設為技術純熟的駭客所為
5	University of North Carolina—Charlotte (North Carolina, USA)	350,000 名北卡羅來納州夏洛特大學學生與教職員的機密資料包括銀行帳號與社會安全號碼意外遭洩漏	系統設定錯誤與不正確的存取設定造成電子資料公開可以取得	非技術性的

6	South Carolina Department of Revenue (USA)	藉由遠端服務駭客存取內部系統與其他資源而竊取使用者名稱和通行碼	針對員工採目標式釣魚郵件攻擊；不恰當的控制程序。系統具有弱點不需要雙重確認即可存取納稅申報單、社會安全號碼並未加密軟體版本老舊、資訊技術控制已經過時。	非技術性的
7	California Department of Social Services (USA)	超過 700,000 居家照護業者與收件者之個人資料在郵遞過程遺失，部分居家照護業者工資發放資料也遺失	於寄送過程的意外錯誤	非技術性的
8	California Department of Child Support Services (USA)	於加州之小孩支援系統大約 800,000 人之個人資料在中轉運送時遺失	在例行的災後復原演練後，發現 4 捲備份磁帶從 IBM 位於科羅拉多州的設施運送到加州時遺失	非技術性的
9	Emory Healthcare, Inc. (Atlanta,Georgia, USA)	包含自 1990 年 9 月至 2007 年 4 月以手術方式醫療的病人資料的 10 顆硬碟遺失	由 Emory 大學醫院 (Emory University Hospital）儲存位置竊取	非技術性的
10	Utah Department of Technology Services (USA)	此次資料外洩牽涉美國醫療輔助計畫病人 (Medicaid patients) 以及小孩的健康保險計畫（Children's Health Insurance Plan) 之收據,可提供小孩不用其他健康保險之保險範圍並符合收入指導方針.有人認為 780,000 筆紀錄受影響，包括社會安全號碼、姓名、生日、住址和小孩的健康規劃數據	弱密碼	非技術性的
取材自: Shalal-Esa, A.; "Scores of US Firms Keep Quiet About Cyber Attacks," 2013 March, *www.reuters.com/article/2012/06/13/net-us-media-tech-summit-cyber-disclosur-idUSBRE85C1E320120613*				

分析和討論

雖然不可能對於資訊系統之安全完全地解決，但系統風險可以透過有效的管理實務大幅地降低。10 種電腦安全技術已經不易持續跟上運算能力跳昇的腳步，對於使用者親和度的大幅度重視已

經負面地影響某些安控機制之佈署，經常導致安全設計之遭破解並造成系統管理員與稽核員的問題。[11]

於百分之七十的上述案例，由於缺乏有效控制而非強度不足的各項安全性層次結構造成攻擊發生。雖然說明資訊安全主要是人的問題，由人進行技術設計與管理，但是人為疏失誤用而造成資安事件。[12] 在這些案例，資訊技術存取控制政策的識別是必須的，以引導組織內資訊技術安全任務的最佳實務方式。[13] 因此，這些案例證明當強化技術層面是重要的以防止資料外洩，在資訊安全方面人的介入是同等重要，而許多現存案例顯示人的活動可以連結到安全議題。[14]

資訊技術控制的角色

從技術轉向非技術的被駭客採用，導致組織瞄準的是資訊系統技術和非技術方面的最佳組合及綜合的通用資訊系統治理控制最佳實務的結合。因此，為了使資訊系統安全措施變得有效，安全不應該只建立類似結合安全措施之梯子，而是這些安全措施應該彼此互相依存。[15]

適當的控制措施是必須的，以保護組織免於因過失責任的法律訴訟並符合防止電腦誤用與資料保護的法規。[16] 內部控制措施廣泛定義為程序，受個體的董事會、管理階層和其他人員影響，設計用於提供關於達成下述分類的目標之合理的保證：維運之效率和有效性、財務報表的可靠性及符合適用的法律與規範。[17]

在這方面，COBIT® 5 框架協助企業實施健全的治理促成因素，其中的程序是七種促成因素之一，以達成企業資訊技術治理與管理（governance and management of enterprise IT ,GEIT)。[18] 目前資訊系統控制框架的實施由於不同的規章與標準之合規性與管理的要求而於世界各地興起。[19] 由於組織並非處在確保最大安全的位置，任何控制實施之關鍵的指引原則是決定安全之適當程度。在此方面，所花費的金額應正比於系統之關鍵程度、控制措施的花費與事件發生的機率，因為適當的控制措施對於保護組織免於責任疏失及符合電腦誤用與資料保護法規之法律訴訟，[20] 組織通常將資訊安全視為符合法規的作為，不必驚訝因為責任是管理階層之主要考量，然而這僅是資訊安全窄化與短視之觀點，因為法律與規章是準備好保護組織的外部利害關係人例如客戶與投資者。[22]

根據對於資訊安全專業人員之調查，企業策略集團（Enterprise Strategy Group ,ESG)發現百分之七十二超過一千名員工的北美組織已經實施一種以上的資訊技術最佳實務控制與程序模型。[23] 此外，此研究發現最廣為使用的商用資訊技術控制框架為資訊技術基礎架構庫(IT Infrastructure Library，ITIL)、ISO 27002 和 COBIT®，其中 COBIT 能提供最佳的資訊安全管理。ISO/IEC 27002、COBIT®、ISO 20000 和 ITIL 是最適用和廣為使用的管理與維持資訊技術服務的框架，資訊技術控制實踐者使用 ITIL 定義策略、規劃和流程；COBIT® 用於度量、基準與稽核；ISO/IEC 27002 強調降低風險之安全議題。[24]

資訊安全往往不強調全面性和綜合的方式。當所有的面向都考慮到，真正安全的環境才能存在，防止真正的風險。對此，提出了資訊系統安全 12 個面向，焦點放在結合治理、稽核、法律、技術、人力和測量領域以創造安全的環境。[25] 對映這 12 個面向到表 2 所詳述的資訊技術控制框架中，顯示技術和非技術的 IT 控制的綜合性質。

表2闡述了COBIT® 包含大部分的資訊安全面向，並考慮到技術和非技術方面的問題。接下來，分析COBIT® 相關程序（也稱為資訊技術控制），以看如何應用這些程序以防止如前所述的十大最受矚目資料外洩案例。

表2—資訊系統安全的維度和相關資訊系統控制框架/標準之對映	
面向	可用之框架
策略/公司治理	COBIT® 之高階聚焦
治理/組織的證據	COBIT® 之四個領域的證據
政策	在COBIT®, ISO 27002, 美國國家標準與技術研究院(National Institute of Standards and Technology (NIST)), 資訊技術基礎架構庫(IT Infrastructure Library , ITIL)認可的資訊系統安全政策
最佳實務	33 IT 治理最佳實務, 資訊技術基礎架構庫(IT Infrastructure Library , ITIL)最佳實務, COBIT®
道德	延伸的資訊系統安全互連(Extended Information Systems Secure Interconnection ,ISSI)模型著重資訊系統安全道德面向
驗證	COBIT®, ITIL 與ISO 驗證
法律	法規例如美國聯邦資訊安全管理法(US Federal Information Security Management Act (FISMA), 美國健康保險流通與責任法案(US Health Insurance Portability and Accountability Act, HIPAA)及美國沙賓法案(the US Sarbanes-Oxley Act)
保險	(只和保險公司相關）
人員/人力資源	COBIT®, 資訊技術基礎架構庫（ITIL）, ISO 27002 控制項
認知	資訊安全文化框架
技術	支付卡片工業資料安全標準(Payment Card Industry Data Security Standard ,PCI DSS 2.0) 與資訊技術基礎架構庫（ITIL）
測量/指標	COBIT®, ISO 27004 與資訊技術基礎架構庫（ITIL）提供之指引

稽核	COBIT®
取材自:IT Governance Institute (ITGI), Global Status Report on the Governance of Enterprise IT (GEIT), USA, 2011	

COBIT® 5的推薦使用

COBIT® 5合併與整合這些前述發佈的ISACA框架COBIT® 4.1, Val IT 2.0, Risk IT與資訊安全的業務模型(the Business Model for Information Security, BMIS)。它對齊其他框架和標準如ITIL、國際標準化組織（ISO）的標準知識、專案管理共用知識（PMBOK）、PRINCE2和開放群組架構框架(The Open Group Architecture Framework, TOGAF)。

許多詳細的COBIT® 5流程直接對映到資訊安全，所有前面提供的資料外洩案件對映到COBIT® 5，表3顯示如果實施每個COBIT® 5的管理實務，如何能夠防止違約。而這些對映的管理實務符合COBIT® 5的規劃（APO）和執行（DSS）領域，六個管理實務—APO01.02, 01.06, 03.02, 09.03, BAI09.01和DSS06.06—提供這些活動的輸入。

表 3-資料外洩案例弱點對映資訊系統安全-相關 COBIT® 實務

研討案例	COBIT® 管理實務		輸入	描述	輸出	到
1, 2, 4	**APO13.01 建立和維護資訊安全管理制度 (information security management system , ISMS).** (透過支援性活動傳遞)	責任指派矩陣	COBIT® 以外（企業資訊安全方法）		ISMS 政策 ISMS 範圍文件（適用性聲明）	APO01.02 DSS06.03
	DSS05.01 藉由防護惡意軟體進行保護 (透過支援性活動傳遞)			● 惡意軟體預防政策 ● 潛在威脅的評估		APO01.04 APO12.02 APO12.03
	DSS05.02 管理網路和連線安全. (透過支援性活動傳遞)		APO01.06 APO09.03		● 連線安全政策 ● 滲透測試結果	APO01.04
	DSS05.03 管理端點安全.		APO03.02 APO09.03 BAI09.01	● 資訊架構 ● 模型,維運水準	● 端點裝置的安全政策	內部的

	(透過支援性活動傳遞)		DSS06.06	協定,服務水準協定 ● 實體資產檢查結果 ● 違反政策之報告		
	DSS05.04 管理使用者身分和邏輯存取. (透過支援性活動傳遞)		APO01.02 APO03.02	● IT 相關角色和責任之定義 ● 資訊架構模型	● 核准之用戶存取權限 ● 使用者帳號與權限審查之結果	內部的 DSS06.03
	DSS05.05 管理對 IT 資產之實體存取. (透過支援性活動傳遞)			● 經核准之存取需求 ● 存取紀錄		內部的
	DSS05.06 管理敏感文件與輸出裝置. (透過支援性活動傳遞)		APO03.02	● 安全事件紀錄 ● 安全事件特性 ● 安全事件通報		
3	**APO10.05 監督供應鏈表現與合規性.** (透過支援性活動傳遞)			● 供應鏈合規監督準則 ● 供應鏈合規查核結果		
	DSS05.04 (參見上述)					
5, 10	**APO13.01; DSS05.02; DSS05.04** (參見上述之輸入與輸出)					
6	**APO13.01; DSS05.02; DSS05.04** (參見上述之輸入與輸出)					
7, 8, 9	**APO13.01; DSS05.02; DSS05.04** (參見上述之輸入					

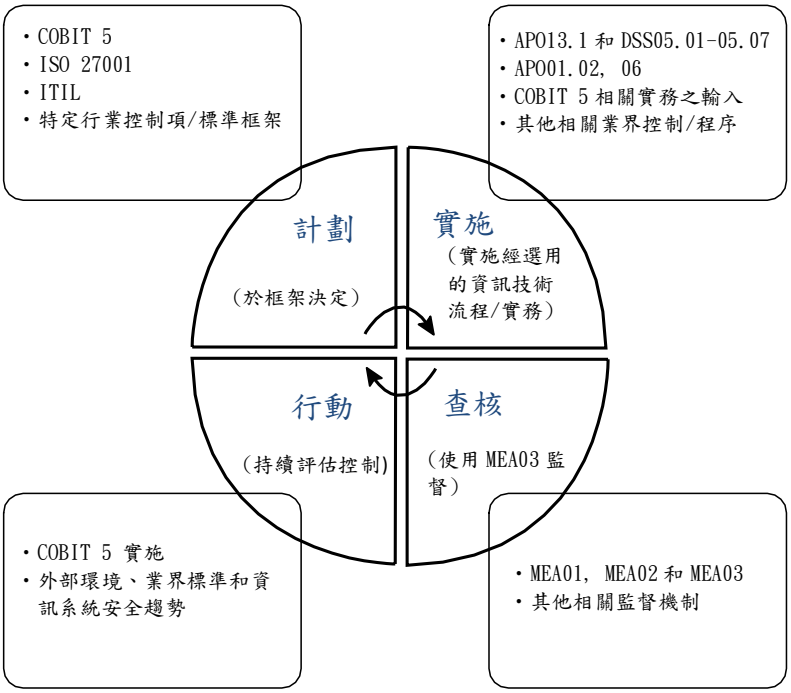
	與輸出)					

COBIT® 5 管理實務是通用的，可以對映到多個漏洞。在 10 個案例，7 個管理實務和 6 個輸入被發現是至關重要的以防止經確認的資料外洩事件。這些管理實務包括 APO13.01, DSS5.01, DSS5.02, DSS5.03, DSS5.04, DSS5.05 和 DSS5.06，其中 APO01.02, APO01.06, APO03.02, APO09.03, BAI09.01 和 DSS06.06 提供輸入。流程促成因素來自於監測，評估和評價領域（Monitor, Assess and Evaluate domain）—MEA01, MEA02 and MEA03 確保針對選用的管理實務提供有效的監督機制。實施 DSS05.07 與這些管理實務確保安全事件、紀錄和通報的監控。

COBIT® 5 其中一項優點是其通用的性質，允許更大的彈性以客製化這些促成因素，相對映實務與活動。這不僅有助於實現特定的目標，並產生一組輸出，支持實現整體 IT 相關的目標，同時也適合動態的資訊系統安全之威脅環境。注意的是資訊系統安全高度動態性質的威脅轉化為 COBIT® 促成因素的持續改善，以克服當前和新興的資訊系統安全的威脅。COBIT® 5 建置提供了指導方針，以實現一個持續改善的過程，並保持這一動能。威脅的技術和非技術性質，證明分離業務和資訊技術相關的活動不但不可能，也不是一個很好的做法。

表4描述建置框架提供如何發展預防資料外洩建置策略的指引，然而框架、最佳實務和標準只有在被組織採納與適用之情況才有用。從整體的角度來看，資訊安全控制措施的建置程序依據資訊系統安全環境、業界和強制性法規持續性的基礎上考慮相關資訊技術控制和標準的選擇、客製化對映。資訊的評估是持續性連續的過程，而安全評估為反覆的程序以檢查現行功能與和特定的標準。[26] 這些遵循使用於ISO 27001之戴明(Deming)的計劃-實施-查核-行動循環（Plan-Do-Check-Act , PDCA）。

圖 4—倡議植基於 COBIT® 5 資料外洩預防之框架



第一階段牽涉根據整體資訊系統安全角度或僅針對COBIT® 5決定相關框架/標準。第二階段

牽涉選擇和實施與資訊系統安全相關的COBIT® 5管理程序 (亦即APO13.01 and DSS5.01－5.07)，並附帶選擇和對映使用COBIT® 5資料外洩預防相關資訊安全程序與控制措施之選項。使用COBIT® 5 MEA領域的促成因素程序趨近回饋循環。結合此植基於MEA01－ MEA03的回饋循環產生精確與調整以監督和確保合規性的機制。在此階段，組織也可從相關標準/框架去選擇/對映特定行業或必要控制的選項。由於弱點和資料外洩的方式之高動態性質，在行動(Act)階段與資訊安全非常相關，因此執行連續性稽核與COBIT®程序及相關資訊技術控制的客製化以達到規劃之階段。

結論

雖然資訊系統安全技術進展以及相關框架、標準及資訊技術控制機制可資應用，於資料外洩之統計趨勢顯示對於組織之威脅持續增加。抽樣十大最受矚目案例，本文識別脆弱之範圍與矯正的行動以防制資料外洩，因此證實大部分的資料外洩事件的發生是由於省略或輕忽非技術性資訊技術控制措施。並強調管理者應於資訊系統安全實施非技術性控制措施。由實踐者的觀點，針對確認之弱點，COBIT® 5流程對映與管理實務提供資料外洩預防與偵測之實施的路線圖。

ENDNOTES

1. Johnson, E.; E. Goetz; "Embedding Information Security Risk Management Into the Extended Enterprise," *IEEE Security and Privacy*, vol. 5, 2007, p. 16-24
2. Luftman, J.; T. Ben-Zvi; "Key Issues for IT Executives 2011: Cautious Optimism in Uncertain Economic Times,"*MIS Quarterly Executive*, vol. 10, 2011, p. 203-212
3. Culnan M. J.; E. R. Foxman; A. W. Ray; "Why IT Executives Should Help Employees Secure Their Home Computers," *MIS Quarterly Executive*, vol. 7, 2008,p. 49-56
4. Kruger, H. A.; W. D. Kearney; "Consensus Ranking—An ICT Security Awareness Case Study," *Computers & Security*, vol. 27, 2008, p. 254-259
5. Smith, S.; D. Winchester; D. Bunker; "Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization," *MIS Quarterly Executive*, vol. 34, 2010, p. 463-486
6. Gordon, L. A.; M. P. Loeb; T. Sohail; "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly Executive*, vol. 34, 2010, p. 567-594
7. Thomson, K. L.; R. V. Solms; "Information Security Obedience: A Definition," *Computers and Security*, vol. 24, 2005
8. ISACA, *COBIT® 5 for Information Security*, 2012, *www.isaca.org/cobit*
9. While the findings in this study provide an understanding of data breaches from both technical and nontechnical perspectives, a number of caveats need to be noted. First, a small sample of 10 cases in one country does not represent the population and, hence, this study needs to be extended with a larger sample from different countries in order to generalize findings. Second, the cases are all taken from secondary sources, which may not always reveal the true cause or the events leading to the breach. Finally, while COBIT 5 is taken as the framework to demonstrate the mitigation of the identified vulnerabilities, further research can identify and map relevant IT controls/ processes from related industry frameworks/ standards and result in a common set of IT controls/processes for a set of commonly identified vulnerabilities.
10. Adams, D. A.; S. Y. Chang; "An Investigation of Keypad Interface Security," *Information & Management*, vol. 24, 1993, p. 53-59
11. Schultz, E.; "The Human Factor in Security," *Computer & Security*, vol. 24, 2005, p. 425-426
12. 12 Hagen, J. M.; E. Albrechtsen; J. Hovden; "Implementation and Effectiveness of Organizational Information Security Measures," *Information Management & Computer Security*, vol. 16, 2008, p. 377-397
13. Ward and Smith; "The Development of Access

Control Policies for Information Technology Systems," *Computers & Security*, vol. 21, 2002, p. 356-371
14. *Op cit*, Kruger and Kearney
15. Dhillon, G.; S. Moores; "Computer Crimes: Theorizing About the Enemy Within," *Computers & Security*, vol. 20, 2001, p. 715-723
16. Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, 22 May 2012, *http://coso.org/documents/Internal%20Control-Integrated%20Framework.pdf*
17. ISACA, *COBIT® 5: Enabling Processes*, 2012, *www.isaca.org/cobit*
18. Dutta, A.; K. McCrohan; "Management's Role in Information Security in a Cyber Economy," *California Management Review*, vol. 45, 2002, p. 67-87
19. *Op cit*, Smith, Winchester and Bunker
20. *Op cit*, COSO
21. Turner, M. J.; J. Oltsik; J. McKnigh; "ISO, ITIL, & COBIT® Together Foster Optimal Security Investment," 2009, *www.thecomplianceauthority.com/iso-itil-a-cobit.php*
22. Nicho, M.; "An Information Governance Model for Information Security Management," in Mellado, D.; L. E. Sánchez; E. Fernández-Medina; M. Piattini, Eds.; *IT Security Governance Innovations: Theory and Research*, IGI Global, 2012
23. Sahibudin, S.; M. Sharifi; M. Ayat; "Combining ITIL, COBIT® and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations," Second Asia International Conference on Modeling & Simulation, Malaysia, 2008
24. Solms, B. V.; "Information Security—A Multidimensional Discipline," *Computers & Security*, vol. 20, 2001, p. 504-508
25. *Op cit*, Nicho
26. Yadav, S. B.; "A Six-view Perspective Framework for System Security: Issues, Risks, and Requirements," *International Journal of Information Security and Privacy*, vol. 4, 2010, p. 61-92

譯者致謝

感謝同事李顯成先生對於部分名詞之中譯提供建議。

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 5, 2013 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2013,Volume 5中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。