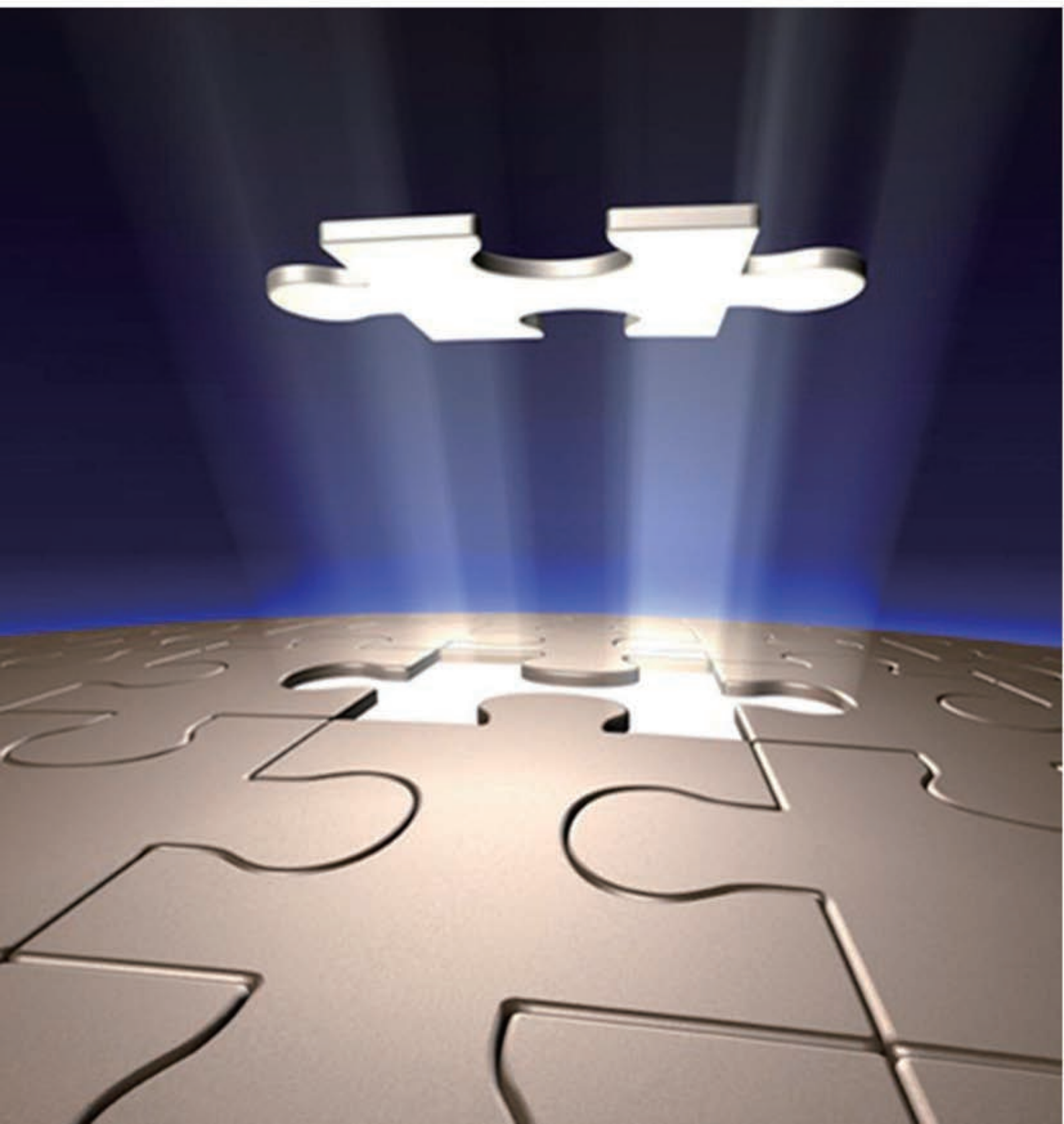


摘譯文章



電腦稽核

Vol 6, 2007 and Vol1, 2008 *Information Systems Control Journal*
摘譯文章第5期



目 錄

- 資訊科技之運作功能失調
(DYSFUNCTIONAL OPERATIONS IN IT)
作者：KENT ANDERSON, CISM
譯者：許林舜，資誠聯合會計師事務所風險管理及內部控制服務部 主持會計師.....2
- COSO 模型簡介：電腦稽核人員如何利用於評估內部控制的有效性
(THE COSO MODEL: HOW IT AUDITORS CAN USE IT TO EVALUATE THE EFFECTIVENESS OF INTERNAL CONTROLS)
作者：TOMMIE SINGLETON, CISA
譯者：楊期荔, CISA, BS7799LA, ISACA TAIWAN CHAPTER TREASURER..... 5
- COSO 模型簡介：電腦稽核人員如何用來量測內部控制的有效性
(THE COSO MODEL: HOW IT AUDITORS CAN USE IT TO MEASURE THE EFFECTIVENESS ON INTERNAL CONTROLS (PART 2))
作者：TOMMIE SINGLETON, CISA
譯者：楊期荔, CISA, BS7799LA, ISACA TAIWAN CHAPTER TREASURER..... 10
- 運用資訊科技查核舞弊
(PRACTICING INFORMATION TECHNOLOGY AUDITING FOR FRAUD)
作者：DALE JOHNSTONE AND ELLIS CHUNG YEE WONG, CISA, CFE, CISSP
譯者：陳耀崑，中央存款保險(股)公司 特別查核處 處長..... 13
- 管理內部威脅：資訊監視
(MANAGING THE INSIDER THREAT: DATA SURVEILLANCE)
作者：JOHN MOYNIHAN
譯者：張騰龍, CISA..... 19

(以上文章皆摘譯自 Information Systems Control Journal, Vol.6 2007. and Vol.1, 2008.)

資訊科技之運作功能失調 (Dysfunctional Operations in IT)

作者：Kent Anderson, CISM

譯者：許林舜，資誠聯合會計師事務所風險管理及內部控制服務部 主持會計師

資安管理人員在保護其組織資訊安全上面臨許多難題，資訊安全的威脅與日俱增，除了傳統駭客之外，資安人員必須抵擋更高明的詐騙集團、有組織的犯罪集團、身分竊盜及垃圾郵件發送、網路及系統資源的不當使用、員工盜用智慧財產權、以及應付不斷增加的管理及法規需求的壓力。國際電腦稽核協會最近針對有風險性的商業行為進行調查，顯示資安管理人員仍需解決使用者欠缺資安觀念而造成個人及組織的風險問題。

國際電腦稽核協會委由 MARC 研究調查機構，在 2007 年 8 月對任職於百人以上公司的 301 位美國白領階級進行電話調查，其結果顯示，這些員工對於風險認知及行為有很大的差別。

使用者多為低風險接受者

調查顯示多數白領階級不認為自己為高風險接受者，34%的受訪者表示他們對風險的容忍度為低或極低，僅 16%認為其願意接受中度或高度風險；約有 50%的受訪者表示，在工作場合多少會顧慮到資訊的隱私權及安全性，而超過 75%的受訪者多少會顧慮到家中電腦系統之資訊的隱私權及安全性。

92%的受訪者表示在購買手機或電子產品時，至少會考慮其安全性，而有 50%的人表示安全性會是他們購買產品時極為重要的考慮因素。

從事具風險的行為

當問及某些具風險性的網路行為時，受訪者普遍對資訊安全的嚴重認知不足，且經常造成自身及其組織的風險，例如有 35%的受訪者承認至少一次違反其組織之資訊安全政策。

此外，15%的受訪者表示在上班時會使用點對點檔案分享服務傳輸檔案，這樣的比率乍看不高，但若是公司內一百名員工就有十五人使用的話，就一個有五萬名員工的公司而言，等於有高達七千五百人使用。另 17%的受訪者表示他們不只一次使用個人手機發送公司資訊。

11%的受訪者表示他們曾將公司敏感資訊發送至錯誤的收件人(若公司有五萬名員工，則代表有五千五百件案例)。

根據調查結果，受訪者也牽涉其他具風險的行為：

- 49%的人表示他們曾點選外來的網路連結。
- 42%的人曾透過電子郵件寄送公司文件到家裡電腦。
- 33%的人在工作時曾接收朋友或家人寄來的軟體及檔案。
- 23%的人曾用隨身碟傳遞敏感資訊。

安全認知之錯覺

調查結果顯示，白領階級對於風險認知不足，因而從事高風險行為，主要是因缺乏對安全的認知及對安全認知的錯覺這二個最普遍的理由。

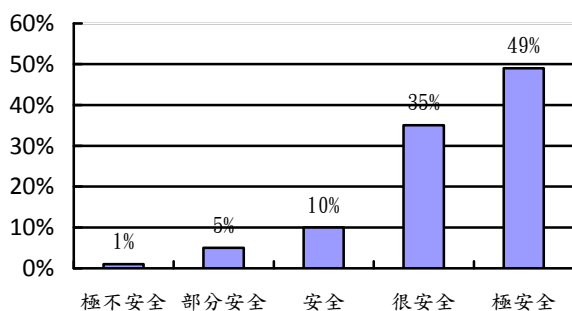
62%的人表示他們認為點對點檔案分享軟體幾乎沒有風險，令人更驚訝的是 74%的人認為下載個人軟體到公司電腦裡並幾乎無任何風險，50%的人認為不經資訊部門，使用行動設備連結公司檔案及電子郵件也幾乎沒有風險。

至於受訪者認為其他低風險或無風險的行為如下：

- 傳送機密資料至錯誤的對象(41%)。
- 使用隨身碟傳送敏感資訊(56%)。
- 使用公司電腦開啟不明郵件(56%)。
- 遺失存有公司資訊的設備，例如黑莓機或筆記型電腦(59%)。

此外，似乎大多數的白領階級對資訊安全似乎都有錯誤的認知，有 94%的受訪者相信他們的資訊環境為安全、很安全到極安全。(見圖一)

圖一 工作場所電腦及IT安全評價



這樣認知的錯覺也反映出多數白領階級在公司使用電腦時，並不注重資訊的隱私權(65%)或安全性(63%)。

結論

資安人員常把焦點放對於風險管理工具的選擇及技術性的控制，卻忽略如人員、政策及流程等重要因素，像是公司員工，政策及流程，人員通常是保護組織及重要資訊中最弱的一環，不論是管理者逾越控制而有太多的例外、缺乏專業訓練的資安人員或不了解風險行為的員工，人為因素在風險管理上不可忽略。

國際電腦稽核協會調查結果顯示，仍需要持續宣導使用者風險管理的觀念及其責任，畢竟資訊安全，人人有責。

作者簡介

Kent Anderson, CISM

is a leading authority on information security, with more than 21 years of experience in the field. He serves on ISACA's Security Management Committee and is the founder and managing director of Network Risk Management LLC. Anderson has held positions as senior vice president of IT security and investigations with an international business risk consultancy, as director in the Dispute & Analysis Investigations group of PricewaterhouseCoopers LLP, and as the European information security manager for Digital Equipment Corp. Anderson can be reached at kea@aracnet.com.

作者提醒

Questions about the ISACA survey referenced in this article may be directed to the ISACA communications department at news@isaca.org.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2010 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org

COSO 模型簡介：電腦稽核人員如何利用於評估內部控制的有效性

(The COSO Model: How IT Auditors Can Use It to Evaluate the Effectiveness of Internal Controls)

作者：Tommie Singleton, CISA

譯者：楊期荔, CISA, BS7799LA, ISACA Taiwan Chapter Treasurer

在 2006 年 Journal 的第一卷雜誌中，我們重視的是，稽核人員在履行各項職責時，如何普及使用資訊的控制目標及相關技術 (COBIT)，特別是這十年來，對如何揭露醜聞的需求。近年來，崔德威委員會 (COSO) 的內部控制模型，不僅受到關注，也越來越頻繁的適用於審計行業。本文主要討論電腦稽核人員，如何有效地運用 COSO 模型來幫助履行最新標準的要求，尤其是那些屬於美國註冊會計師協會¹訂定的風險性評估的審計標準²。

COSO 歷史簡介

在 20 世紀 80 年代，美國社會發生多起有關儲蓄和貸款協會 (儲貸) 醜聞。輿論界與立法者要求變革，以防止那些災難再次發生。因此，1985 年成立了，由詹姆斯.崔德威擔任主席，所謂的全國虛假財務報告委員會，主要研究議題就是可能導致金融詐騙的因果因素，並提出建議，供上市公司，獨立審計人員，美國證券和交易委員會 (SEC)，其他監管機構，以及教育單位參考³。

COSO 通常被稱為崔德威委員會，其主要的贊助者 (現在依然是)，分別為美國會計學會 (AAA)，管理會計師協會 (IMA)，內部審計師協會 (IIA)，美國註冊會計師協會 (AICPA) 和國際財務執

行長組織 (FEI)。

該委員會一個主要結論是，防止財務詐騙最好的方法，就是改善內部控制。

COSO 開發了一個內部控制的模型，先發佈於各種利益相關者的組織成員之間，並於 1992 年發表了一般稱為 COSO 模型的內部控制模型 (見圖 1)。這種努力立即為大眾認可，因為美國註冊會計師協會通過了採用 COSO 模型作為審計準則聲明 (SAS) 的第 78 號，“審計的財務報表時評估內部控制的意見”的內容，因此確立它成為財務審計人員一項主要技術的一部份。

最近有關事件

但是 COSO 模型的重要性，並沒有就此停止，最近的事件使模型更顯重要。

沙賓法案 404 節規定

隨著在美國 2002 年 7 月通過的沙賓法案，上市公司必須遵守第 404 節要求，管理階層每年應評估內部控制，並由稽核人員就評估結果出具意見，因而每一個需遵守沙賓法案的人，都在想如何將這一過程標準化，以應證管會 (SEC) 或上市公司會計監督委員會 (PCAOB-沙賓法案授權創設的單位)，需要一些標準模型或評估內部控制的基準的要求。

第 2 號審計標準

上市公司會計監督委員會(PCAOB)的職責包含制定財務報告標準，且該組織已開始公佈審計準則。第 1 號審計標準(AS1)，接受了所有以前美國註冊會計師協會發布的審計標準。2004 年 6 月公布的第二號審計標準(AS2)⁴，內容提及遵守沙賓法案第 404 節的議題。其中，PCAOB 建議採 COSO 的模型，以其來對內部控制進行評估和報告。AS2 接受 COSO 模型作為一種公認的審計工具，因而不論是內部和外部的稽核人員，都需要瞭解，特別是在應用到第 404 節的內部控制評估事項。

圖 1 - 內部控制的 COSO 模型



第 109 號 SAS 公報

美國註冊會計師協會 2006 年頒發的第 109 號 SAS 公報“了解實體及其環境，以及評估重大錯報的風險”，再次顯示出 COSO 模型的重要性和它在評估內部控制上的價值。本公報要求財務審計人員必須評估內部控制，特別是那些涉及 IT 組成資訊系統的成分，以及有關“實體及其環境”的項目。第 109 號 SAS 公報自 2006 年 12 月 15 日後生效。

第 109 號公報之附錄 B，內容為如何運用標準的指導，及如何使用 COSO 模型以訂定審計程序，參酌使用的問題和其他有用的制定審計程序資料。

在實務上，財務稽核需要能夠符合這個標準，此時最有可能使用電腦稽核人員或是註冊國際電腦稽核師(CISA®)。因此，電腦稽核人員需了解 COSO 模型，更重要的是，能夠將它應用在財務審計評價內部控制的程序中。

內部控制的 COSO 模型

COSO 對內部控制的定義是“一個，由企業的董事會，管理層和其他人員執行的過程，旨在提供後述目標的合理保證，(1) 作業上的有效性和效率性，(2) 財務報導的可靠性及 (3) 遵守適用的法律和法規。COSO 的內部控制模型中，使用了五大內部控制要素：控制環境、風險評估、資訊與溝通、控制活動及監督。

控制環境

什麼是錯誤報導發生在企業及其環境的重大風險？

控制環境因素是一種觀點，內部控制從企業的角度看，既包括內部環境中創建的業務流程和控制制度，也包含建立和/或保持一個有效的內部控制制度並維持它運作的能力。有時可以就其有關的風險進行控制環境的評估，如：

- 溝通和執法的誠信和道德價值
- 承諾的能力
- 治理者的參與
- 管理的理念和風格
- 組織結構
- 分配權力和責任
- 人力資源政策和做法
- 行業因素

對財務稽核人員言，當被要求必須遵守第 109 號 SAS 公報的義務，以對“企業及其環境”有所了解，確定重大錯報風險對於相關財務報表的影響時，考量 COSO 模型的元素，利用 COSO 的模型分析，會有相當的幫助，故其會是一項非常有價值的工具。

風險評估

企業是否作出了有效的努力，找出可能發生重大錯報風險的地方？

COSO 模型在風險評估方面，可以讓企業有能力，正確評估重大（“顯著”）的風險，並緩解到可以接受的水準上進行控制。一些方式可能導入到企業，幫助企業在控制範圍和/或程序的制定上，包括：

- 變化的經營環境
- 新的人事
- 新建或修改資訊系統
- 快速增長
- 採用新的資訊技術
- 新的商業模式，產品或活動
- 企業重組
- 擴展海外業務
- 新會計公報規定

如果企業的管理和/或董事會並不積極參予評估和緩解風險，這狀況下的控制系統，將會有一定程度上的缺陷。

資訊與溝通

企業是否有足夠的控制，以確保及時和妥善的通知重大錯報？

財務報告資訊，應該可靠、及時並準確地，傳達給管理人員和決策者。因此，這方面的控制，依賴有效溝通和傳遞資訊的財務報告處理制度，以使這些活動有效。下述的一些不同方法，可以用以評估資訊與溝通的風險：

- 使人員履行其職責相關的支持鑑別，捕捉和交換資訊的形式和時限的制度
- 財務報告資訊
- 內部控制資訊
- 內部溝通
- 外部溝通

控制活動

是否有足夠的控制，可以有效地降低任何重大財務報表誤報的風險，以達可接受的水平呢？

控制活動應有確實控制的能力，一些不同評估控制活動的方法包括：

- **一般控制：**
 - 有關服務/產品的政策和程序
 - 控制第三方提供服務來源的方式（特別是資訊系統和操作、網絡等。）
 - 更改核心業務系統的流程
 - 環境安全
 - 應用開發、維護和文件的規範
 - 資訊安全的要求
 - 災難回復/業務恢復的要求
- **應用控制：**
 - 測試控制
 - 控件嵌入在各種應用中，以滿足管理的政策和業務程序
- **實體控制：**
 - 服務的授權
 - 職責分工（如適用，資訊科技人員亦適用）
 - 審核制度
 - 稽核軌跡保存
 - 存取系統和資料的控制
 - 獨立驗證（績效報告、獨立審查、稽核、錯誤日誌等）

控制好壞會在三個方面上進行評估：設計、執行和運作的有效與否。

首先，設計的有效性涉及降低風險的控制能力，並在特定的或須確保政策執行的業務流程上，具有足夠的控制。控制應能及時檢測出重大錯誤陳述或錯誤。

第二，實際控制是否確實執行，它可以通逐步查核加以確定。第 109 號 SAS 公報建議採行這樣的驗證程序。

第三，是否在持續的基礎上，按設計實際執行控制（即控制的有效性）。傳統上，財務和電腦稽核人員已經使用測試以驗證控制的實際執行效果。此一項目就是模型的第五元素，監督。

企業的控制也可以分類如下：一般控制，應用控制和實體控制。一般控制是指控制實現企業功能（業務流程）會產生財務報告的相關的活動，需用到的計算機系統（資訊系統）和資訊技術。應用控制是指嵌入資訊技術和系統內，用以確保達成政策要求的控制程序。

監督

企業是否運作一個系統化的監督活動，不斷評估和改進其內部控制的效果？監督，如前所述，是指企業對他們日常的經營進行有效的監控的能力，不論是單獨或與合併其他控制活動。一些評估這些活動與相關的風險，進行監督控制是否有效的方式有：

- 持續和特地對財務報告的內部控制的評估
- 缺陷的識別和評估
- 隨著時間的推移，對報告的內部控制品質績效的評估
- 根據需要對控制系統修改（添加，更改，刪除）
- 確保對控制系統狀態進行有效的管理審查
- 時時檢查監督系統是否有執行不落實

的情況，這可以讓人們警惕需執行的控制，以減少對監督系統的弱化

- 利用相關的外部資訊，或獨立監督
- 分析控制目標及其相關的控制活動
- 檢視自前次報告後，或是過去 12 個月內的控制的變化情形

結論

今後，在稽核 IT 環境時，稽核人員知道如何運用 COSO 內部控制模型非常重要，不僅是認識其組成內容和模型對其他方面的影響，如研究單位間的跨部門的影響，更要知道如何從 COSO 的模型開發出詢問或觀察重點，發展有意義和有效的稽核程序。

【註】

- ¹ 現在泛指“風險性評估標準”，係指審計準則第 104-111 號的要求。
- ² 本文係延續 2006 年卷 1 基礎專欄，閱讀這篇文章前，請考慮重新檢閱該文。
- ³ 本款的大部分內容是來自 COSO 的網站，www.coso.org。
- ⁴ 最近，PCAOB 的公布 AS5 代替 AS2，但在遵守 COSO 的重要性上，一如 AS2，未有改變。

作者提醒

在下一次的文章，筆者將進一步就這一課題，提出一個利用 COSO 模型於風險性財務稽核上，切實可行的框架。

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2010 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

COSO 模型簡介：電腦稽核人員如何用來量測內部控制的有效性

(The COSO Model: How IT Auditors Can Use IT to Measure the Effectiveness on Internal Controls (Part 2))

作者：Tommie Singleton, CISA

譯者：楊期荔, CISA, BS7799LA, ISACA Taiwan Chapter Treasurer

2007 年第 6 卷資訊系統控制雜誌中，資訊稽核基礎知識專欄撰文談及，電腦稽核人員如何使用崔德威委員會的 COSO 內部控制模型於財務稽核工作，該次文章內容涵蓋了 COSO 模型的五大要素，本次文章將集中討論如何運用 COSO 模型評估內部控制，幫助履行美國註冊會計師協會的新風險審計標準。

如何評估風險等級

在運用 COSO 模型評估內部控制前，我們最好先再次檢視一般稽核用於評估風險的兩個步驟。電腦稽核用的審計程序，包括針對財務報告提出的問題或控制目標，其最終的目的為，在符合風險性評估標準下，評估企業整體控制的有效性和能否緩解發生重大錯誤報導的財務報告風險。

第一步驟是設計程序，以供取得資料和/或證據，協助稽核人員確定或澄清風險。這個階段的程序提供證據給稽核人員，幫助其確定關注區域所存在的風險，例如，控制環境（COSO 的），實體及其環境（第 109 號 SAS 公報）或業務流程（可能與 COSO 的模型元素的控制活動有關的流程）。

一旦已經確定了一個風險，就必須進行風險程度的評估，也就是說，有多少風險存在於這一區域，這是第二步驟。為了簡便起見，如果假設電腦稽核人員採用高，中，低來描述風險程度，是什麼因素，用以確定存在於該關注區域的風險程度，無論有多少風險及高、中、低風險程度？是什麼讓電腦稽核人員，評估控制能有效地減少風險，達到可接受的水平？內部控制有缺失或薄弱，存在的問題越多，電腦稽核人員就越有可能需就風險程度進行更深入的評估。而企業有效地採用內部控制的最佳實務做法，電腦稽核人員就越有可能無需深入的評估風險程度。

通常，稽核程序有助於執行第一步驟，界定風險，但是不一定有利於在執行第二步驟的風險程度評估，在這種情況下，稽核人員必須開發其他程序，以提供風險程度的證明（在下一節中舉例）。

如何將 COSO 模型用於稽核程序中

COSO 模型提供了一些關於內部控制中，稽核時的關注區域（或目標），這些區域共分為五項主題（既 COSO 的元素）與每個主題下可以延展的副主題¹，

例如，一個關注的內部控制主題為控制環境（COSO 的五大元素），根據該元素的一個子主題是“溝通和執法的誠信和道德價值”。

雖然本文不會說明所有的五個元素，但將舉出一些具體例證如下。

COSO 的模型，直接適用於風險性評估標準的就是控制環境²，其在風險性評估標準中稱作“實體及其環境，包括內部控制”³。正如作為風險評估程序的目標，在工作前預先設計的財務稽核計劃中，這兩者幾乎是指同樣的事情。

進行內部控制評估的總體目標，是為了確定在一個特定的控制環境下，企業有能力，建立和維持對財務報告有效的內部控制制度。風險評估程序的目標是在，同時就控制和財務報告資訊兩項，確定相關的開發，管理，監督和報告的風險程度與控制制度。而對高層管理階層的企業策略活動使用的報告中，則應包含最高級別的內容。

列在 COSO 模型控制環境元素下的第一子主題為“溝通和執法的誠信和道德價值觀”，電腦稽核人員必須確定被稽核的企業或單位在這子主題區域是否有風險。為了得到這項結論，電腦稽核人員必須設計稽核程序，以提供資訊和/或證據。因為不同企業間的特殊性，在得到該企業的具體情況和資料後，多需要設計不同的稽核程序。

舉一個例子，一項子主題的稽核程序是取得一份書面的道德準則，如果有的話；而當無法取得這項文件時，稽核人員將需要作更多的風險評估。但無論是否有書面職業道德規範存在，電腦稽核人員仍應制定其他稽核程序，以滿足他/她確定這一領域的風險是否合宜。這些程序可以包括：

- 是否員工培訓或指導內容包含道德要求
- 是否有規範違反道德倫理的文件
- 如果發生違反道德行為時，是否執行相關規範要求
- 是否有人或團體負責執行倫理要求（他/她/他們是否有效運作）

確定企業確實執行倫理要求的方法，是運用社交的方式，關注一位普通員工，隨口問他/她，如果某個特定情況下，企業是否違反道德，或問他/她如果發現了一個違反道德要求事件，他/她會做何種反應（即確認這方面溝通的有效性）。

這種模擬情況，說明了兩階段的方法來評估風險和內部控制。書面道德準則提供了一些證據，電腦稽核人員對企業已做了一些應對倫理要求風險的工作（第一步驟，確定和闡明風險）。但對評估風險水平，所提供的價值不大。如果企業沒有溝通或執行計劃，書面的道德政策可能不具什麼降低風險的成效。如果有證據表明，這項政策在員工訓練上經過討論和僱員簽署一份遵守政策的同意書，這就提供了證據，可以用來確定評估的風險程度（通常是降低風險程度）。如果有文件表明，員工誰違反了道德政策而受到行政處分的後果，即提供更大的評估風險程度價值（可能大幅降低風險程度）。換句話說，不同的稽核程序，可以有效地或多或少的確定風險程度。

在 COSO 模型的風險評估要求中，電腦稽核人員尋求證據以確定，企業管理階層正確識別和評估重大風險程度。

是否有可能當一個資訊專案失控，行政人員及/或董事會董事不能夠理解和承認，這一事件可能對財務報告的重要性或影響性？是否有可能一個大型資訊

專案會管理不善到超支數以百萬，並已經佔資產負債表非常大的比例？如果是這樣，顯然管理階層可能無法識別超支的意義。事實上，資訊人員可能不會看到這一個重大損傷，而財務稽核人員在缺少資訊背景或專案管理知識下，也有可能未加重視，這一情況在未採行專案管理最佳實務，也缺乏資訊科技治理時，是最可能發生的情況。

COSO 模型的應用還可以寫很多，希望所舉如何應用 COSO 模型在風險性評估標準和使用 COSO 模型評估內部控制的兩個例子，對各位是有用的。

結論

為了履行相關的風險性評估標準職責，電腦稽核人員將在很大程度上依賴對政策和程序的審查。電腦稽核人員想要確管理階層，就策略上正視並實際運用內部控制，由制訂政策和程序為始，並延伸到監督（COSO 的元素）和決策相關的財務報告和內部控制（如：誰是內部控制的專家，如何運用其專業知識於應用和核心業務流程）。

電腦稽核人員也將平衡考量所有的證據，利用 COSO 模型的五個元素，最後就整體內部控制完成風險評估，有時企業在模型某些元素的優勢，可能彌補其他元素的弱勢。

整體而言，電腦稽核人員能有效地運用 COSO 的內部控制模型，以供準確評估內部控制的有效性，並能夠減輕在財務報表重大錯報的風險。

【註】

- ¹ 參閱 2007 年第 6 卷雜誌，電腦稽核基礎專欄曾詳細介紹 COSO 內部控制模型。該文附圖上的項目可提供每個元素下一些可能的子主題。欲了解更多信息，請參閱 COSO 官網（www.coso.org）。
- ² 在 2007 年第 4 卷雜誌的電腦稽核基礎專欄中，介紹了幾項協助電腦稽核人員，能符合“風險性評估標準”要求的內部控制評估最佳實務。在 2007 年第 5 卷的專欄中，資訊科技治理的最佳實務被用來演示如何評價“實體及其環境”，這個名辭來自“風險性評估標準”。
- ³ 這個辭是不斷使用於指稱重大的風險性評估標準，特別是在第 109 號 SAS 公報。

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2010 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org

運用資訊科技查核舞弊 (Practicing Information Technology Auditing for Fraud)

作者：Dale Johnstone and Ellis Chung Yee Wong, CISA, CFE, CISSP

譯者：陳耀崑，中央存款保險(股)公司 特別查核處 處長

舞弊通常不易被偵測，在法庭上更難以被證明。本文在於提供稽核人員在 IT 環境中查核舞弊的普遍作法之見解。

『職業性舞弊』定義為：藉職務之便蓄意挪用受雇機構之資源或資產¹，使其個人獲得利益。本研究係以此定義作基礎，蒐集自 2004 年 1 月到 2006 年 1 月間，共 1,134 個職業性舞弊的案例資料，擷取其中重要的調查結果於 2006 年提出以下結論：

- 美國的機構每年因舞弊而造成的損失約為收益的百分之五（估算約美金 6,520 億元）。
- 職業性舞弊造成的財物損失為美金 15,900 元(取中位數)。
- 低於百分之八的犯罪者在從事舞弊行為前有被定罪的紀錄。
- 舞弊損失的金額大小與犯罪者的職位呈現高度相關。

IT 稽核人員於舞弊控制扮演之角色

不管稽核人員是否有進行過舞弊的查核，所有稽核人員都應該承擔舞弊偵查的責任，並建立一套反舞弊的機制。美國會計師協會 (AICPA)² 制定的稽核準則 (SAS) 第 99 條，強調稽核人員應就其專業，發揮懷疑精神去辨識因舞弊行為而謊報資料帶來的風險。美國上市公司會計檢察委員會 (PCAOB)³ 也要求稽核人員必須將評估舞弊相關的事項納入內部稽核查核項目。

由於資料通訊技術 (ICT) 及無線網絡的快速發展，公司行號在營運上對 IT 設備及軟體系統的依賴日益加深，是不必驚訝的。IT 稽核技術在舞弊預防、偵測及調查扮演了很重要的角色。

為了對舞弊控制作出有價值的貢獻，IT 稽核人員必須詳細瞭解各種的 IT 程序及舞弊型態，才能對其風險評估方法的研發有所貢獻。

IT 程序

資訊及相關技術控制目標 (COBIT)⁴ 完整地提供了 IT 程序的包含範圍，根據 COBIT 的定義，每一 IT 程序都可歸類至下列四種特定範疇中的一種：

- 計畫與組織 (Plan and Organize ; PO)
- 取得與建置 (Acquire and Implement ; AI)
- 交付與支援 (Deliver and Support ; DS)
- 監控與評估 (Monitor and Evaluate ; ME)

IT 程序(如表一)共 34 種，分屬於上述四種範疇中。

計畫與規劃		交付與支援	
PO1	定義策略性 IT 計畫	DS1	定義及管理服務水準
PO2	定義資訊架構	DS2	管理第三者提供的服務
PO3	決定技術方向	DS3	管理績效及容量

表一 COBIT 控制目標的 IT 程序(續)			
計畫與規劃		交付與支援	
PO4	定義 IT 程序、組織及關係	DS4	確保服務的連續性
PO5	管理 IT 投資	DS5	確保系統安全
PO6	溝通管理目標及方向	DS6	辨識及配置成本
PO7	管理 IT 人力資源	DS7	教育及訓練使用者
PO8	管理品質	DS8	管理服務台及意外事件
PO9	評估及管理 IT 風險	DS9	管理組態
PO10	管理專案	DS10	管理問題
取得與建置		DS11	管理資料
AI1	找出自動化解決方案	DS12	管理實體環境
AI2	取得及維護應用軟體	DS13	管理營運
AI3	取得及維護技術基礎架構	監控與評估	
AI4	促成運作及使用	ME1	監控及評估 IT 績效
AI5	取得 IT 資源	ME2	監控及評估內部控制
AI6	管理變更	ME3	確認遵循外部規範
AI7	安裝並確認解決方案及變更	ME4	提供 IT 治理

舞弊事件是否發生於這四種範疇中仍具爭議。為了更加了解舞弊發生的原因，稽核人員⁵應參考犯罪學家 Dr. Donald R. Cressey 所提出的「舞弊犯罪

三假說」，這些誘使舞弊事件發生的因素於表二中有扼要的描述。

表二 Cressey's 舞弊犯罪三假說	
因素	內容
無法處理的財務問題	<p>此為最初的犯罪動機。犯罪者通常都有財務問題，且無法透過正當的方法解決。財務問題可能源自於個人或工作。以下為常見的舞弊犯罪的例子：</p> <ul style="list-style-type: none"> ◆ 必須達成工作生產力的目標值 ◆ 必須達成投資者期待的利得 ◆ 藥癮或賭博
有機可趁	<p>此為舞弊者能達成作案犯罪的方法。舞弊者相信藉由職務之便來解決財務上的問題，被察覺的風險較低。例如：某員工具有決定 IT 投資的權限且對於包商的選擇有強大的影響力。</p>
合理化	<p>絕大部份的舞弊者都是初犯，且他們並不自覺為犯罪者。舞弊者會將本身的行為合理化，並將其犯行解釋成可接受或正當行為。常見合理理由如下：</p> <ul style="list-style-type: none"> ◆ 我只是“借”錢。 ◆ 我的薪資過低。 ◆ 我的雇主/主管不誠實，因此詐騙他是正當的。

任何的 IT 程序不論其自動化的程度，皆需人員參與其中，因此舞弊發生的可能性是存在的。

舞弊型態

典型的職業性舞弊有下列三種主要型態⁶：

- 盜用公司資產—任何涉及偷竊或不當運用公司資產的行為，例如：利用公司購買的有版權軟體作為個人使用或藉此牟利。
- 貪污—以個人職權上的影響力介入商業交易，從中牟取不當利益，例如：在選擇 IT 設備維修服務時，委給有提供回扣的廠商。
- 偽造財務報表—竊改公司財務報表的收益，例如：調整長途電話系統每位使用者的平均收益數。

上述每一種型態又可進一步細分成不同的舞弊手法。對不同舞弊型態和跨產業基本舞弊手法的認識，可讓企業做出更準確的舞弊風險評估。

舞弊風險評估

舞弊風險評估的第一個步驟是將 IT 程序發生舞弊行為的可能性及重要性的程度作等級區分。美國上市公司會計檢察委員會(PCAOB) 的稽核準則第二條【(AS) NO.2】即提供了風險發生的可能性和其相對重要性的區分。

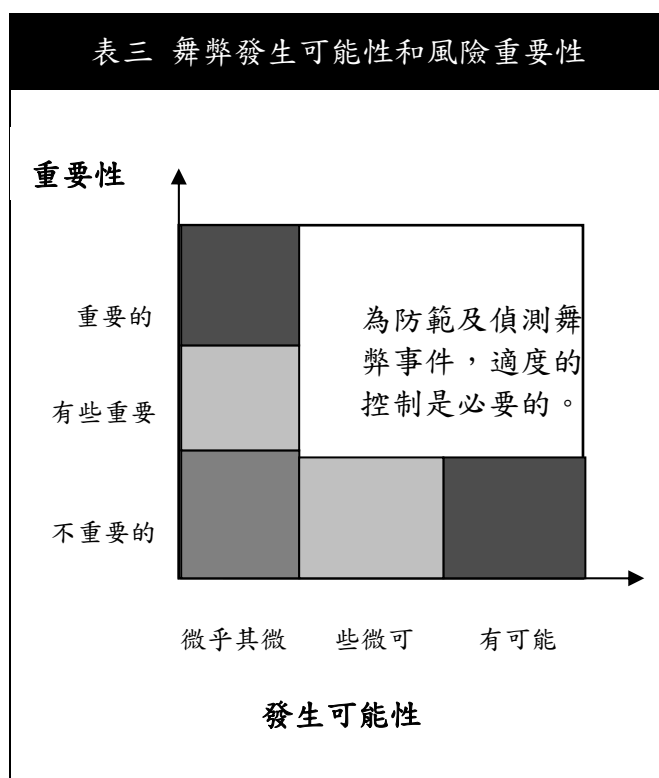
PCAOB 稽核準則定義的三種風險發生的可能性：

- 發生的可能性微乎其微
- 有些微發生的可能性
- 有可能發生的

PCAOB 稽核準則亦定義三種風險程度的重要性：

- 不重要的
- 有些重要的
- 重要的

表三為舞弊風險發生可能性和重要性的關係圖示。



當完成對 IT 程序可能發生之舞弊行為作等級區分後，舞弊風險評估可列出各種 IT 程序對應的舞弊型態及適合的控管機制，如表四。

表四 IT 程序 v.s.舞弊控制矩陣

IT 程序	舞弊的型態	舞弊的情節	內部控制
管理 IT 人力資源	貪污	IT 專案經理(預算批准者)誇示作業成果,要求增加承包商,俾從人力仲介處取得不當利益。	設立 IT 人力資源運用的管控程序。 建立人力仲介選擇標準及 IT 承包商的品質需定期監督(如:背景調查)。 定期檢視 IT 人力資源及 IT 工作量/交付量。
取得 IT 資源	資產不當挪用	採購的 IT 硬體/軟體長期未使用。相關的資產遺失或不必使用。 採購的軟體發生偽造的發票。	建立採購程序。 硬體/軟體購買證明資料的維護,且定期盤點。 建立檢查機制,以利核對軟體的實際配置使用情形。

舞弊風險評估分析可讓組織對舞弊事件可能發生的範圍顯現易見,及對防止潛在舞弊發生可運用的資源排出優先順序。有鑒於商業和 IT 環境的瞬息萬變,不論 IT 程序如何變化,舞弊風險評估應定期實行。此外,如何在舞弊風險評估中界定 IT 程序,稽核人員可運用公司過去發生的舞弊事件作為參考基準。

舞弊的預防

『預防』顧名思義就是防止事件的發生。一般而言,在商品完工後再行修改所花費的成本遠比一開始就設計對的商品來得多。舞弊的預防已成為稽核作業中重要的一環,且稽核人員早期介入商品或 IT 應用程式的開發的必要性也越來越重要。

不論風險控制的方式合適與否或是風險的程度僅達微乎其微或是些微可能,都應當設計出一套風險控管機制去預防、偵測及即時降低舞弊的發生(如表三所述)。這些機制可建置在內部控制中(BICs),並整合至特定的程序來預防

可能的舞弊,或是舞弊事件發生的早期警告訊號(EWSs)。表五提供了BICs和EWSs的一些參考例子。

舞弊的偵測

根據自 2006 年 the Nation on Occupational Fraud and Abuse 的一篇報導:約有 34%的舞弊事件是在告密者告發後才浮上檯面;有 51.4%是藉著內部稽核、內部控制和外部稽核等一連串偵查行動後才被揭露。稽核人員高度仰賴的評估與測試的控管機制能否成功揭露舞弊事件仍被存疑,但到底有多少比例的舞弊事件是由 IT 稽核人員所發現的呢?

目前,大部分的 IT 稽核程序都著重在 IT 系統及應用程式的運作是否遵循已建立的處理程序與規範,但很少使用內部控制問卷(ICQs)來偵測潛在的舞弊事件,並且確認反舞弊的控制方法是否有效地被執行。

表五 舞弊的預防分析

IT 程序	內部控制	
	BICs	EWSs
<p>專案管理/應用軟體取得及維護</p> <p>某一 IT 程式是用來簡化抵押貸款的程序。核貸的層級建立在借款的金額，因此需要將認可人員作權限的劃分。</p>	<ul style="list-style-type: none"> ● 強制要求企業實施認可功能 ● 對認可功能屬性及其相關的系統參數進行控管 ● 上述兩項的稽核軌跡 	
<p>資料管理</p> <p>在每日作業中對敏感性資料(如：客戶資料)設置太多的控管是不合實際的，但各種的早期警告訊號(EWSs)可做為潛在的濫用公司資產舞弊的指標。</p>		<ul style="list-style-type: none"> ● 於非上班時間、不正常的地點存取敏感性資料；系統/安全管理人員登入系統次數過多 ● 移除完整或部分的稽核軌跡

針對這些缺點，IT 稽核人員提出以下幾種可能的解釋：

- 太傾向於技術導向
- 認為揭露舞弊是財務稽核人員的責任
- 在進行 IT 稽核作業時，並不預期能發現任何舞弊事件

完成舞弊風險評估，連結 IT 程序及相關的偵測控制後，IT 稽核人員可建立內部控制問卷(ICQs)來評估及測試已實施的控制方法，包括反舞弊的控制方法。財務稽核人員可以從財務記錄並同營業活動來衡量目前風險控管的適當性，而 IT 稽核人員可以把焦點放在資料通訊技術 (ICT) 和與其相關的處理程序。內部控制問卷 (ICQs) 的品質和 IT 稽核人員的技術能力十分相關。IT 稽核人員須擁有 IT 方面的專業知識(如：軟體程式，資料庫管理，網路設計，網路建置，資訊安全)及同時對 IT 和業務運作有充分了解。內部控制問卷(ICQs)的設計可以參考組織內現有的處理程序、業界的實例範本和法規需求。

例如，國際長途電話在技術和業務

的複雜度讓舞弊者在財務方面有可趁之機。由於國際長途電話系統的通信費用是固定的，犯者可透過改變國際長途系統的設定來提供其他國際長途電話業者使用，此舉可以瞞過財務稽核人員的偵查。在這個案件裡，這種舞弊手法可藉由系統變更控制、檢驗系統或應用程式存取紀錄或國際長途電話邏輯安全控管等內部控制問卷 (ICQs) 機制被偵測出。

舞弊的調查

現今企業廣泛使用資料通訊技術 (ICT)，意味著如發生舞弊事件，很容易找到證據被驗證或證實。在資料通訊技術 (ICT) 系統蒐集到的證據能夠充分證實舞弊事件的發生。IT 稽核人員光靠 IT 系統的專業知識能否偵測出舞弊事件的發生呢？

以下的方法可以輔助 IT 稽核人員對舞弊案件的調查：

- 產出及/或調節報表
- 辨識/擷取電腦系統的證據及被刪除的記錄

● 導入電腦鑑識分析

當 IT 稽核人員沒有能力導入電腦鑑識分析時，稽核人員至少應該知道方法論及功能。

結語

期待 IT 稽核人員能直接和間接地參與舞弊的查核。本文提供了舞弊風險的評估方法，內容涵蓋透過 IT 稽核各種舞弊控制的範圍，包括：

- 在 IT 專案開發的早期階段整合控管機制
- 增加必要性的內部控制(BICs)和辨識早期警告訊號(EWSs)作為舞弊預防的參考
- 設計關於處理程序的內部控制問卷(ICQs)，同時包含了 IT 及商業兩個領域，而不只是聚焦於技術層面
- 透過辨識、回復直接或周邊的證據來發動或協助舞弊事件的調查

IT 稽核人員調查舞弊事件的能力，取決於對業務的嫻熟度、IT 程序及技術領域專業程度。此篇報告可提供 IT 稽核人員獲得更多實際操作方法，對在 IT 環境下舞弊案件的偵查有更進一步了解。

【註】

¹ Association of Fraud Examiners, 2006 *Report to the Nation on Occupational Fraud and Abuse*, 2007

² The Auditing Standards Board, "Consideration of Fraud in a Financial Statement Audit," SAS 99, American Institute of Certified Public Accountants, 2002

³ Public Company Accounting Oversight Board, AS No. 2

⁴ IT Governance Institute, COBIT 4.1, 2007

⁵ Cressey, Donald R; *Other People's Money: A Study in the Social Psychology of Embezzlement*, 1953

⁶ Association of Fraud Examiners, *Fraud Examiners Manual*, 2007

作者簡介

Dale Johnstone

is an information security evangelist and a leading expert in information security with more than 20 years of experience in information security management and information technology. Johnstone has been involved in various industry sectors including government, defense, law enforcement, finance, manufacturing, transportation and telecommunications. He is currently employed as the chief security consultant within the Governance and Risk Management Group of PCCW Limited, and maintains active memberships with a number of international standards bodies. He can be reached at dale.johnstone@pccw.com.

Ellis Chung Yee Wong, CISA, CFE, CISSP

is an IT audit manager in Hang Seng Bank of HSBC Group.

Wong has focused on areas such as IT operations, IT security, auditing, risk assessments and investigation. He has experience in a number of industries, including finance, telecommunications and manufacturing. He can be reached at elliswong@hangseng.com

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2010 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

管理內部威脅：資訊監視 (Managing the Insider Threat: Data Surveillance)

作者：John Moynihan

譯者：張騰龍, CISA

你的資料庫安全嗎？除了考量一些常見的預防設施如防火牆設備或實體安全措施，在回答這個問題前，請考慮以下的假設情況。一名銀行員工將他鄰居的銀行帳戶訊息揭露給另外一位鄰居。一名基金公司員工在非授權之下讀取了他岳父的帳戶訊息。出於好奇心，一名醫院的員工讀取了一位知名運動員的住院記錄。

這些假設情況不是潛伏在網絡空間的匿名駭客或身份竊賊所為。相反的，這種類型的“資料庫瀏覽”是由被信任的內部員工所為，這些員工的職責往往賦予他們於資料庫中能夠讀取客戶的金融，醫療和教育資訊的權限。

從他們的電腦工作站，員工能夠讀取越來越多的個人資訊。隨著企業持續自動化其關鍵流程和實現新資訊技術，從而賦予廣大員工讀取敏感資訊的權限，導致公司越來越難發現和預防此權限的濫用。結合積極的資訊收集策略與創新的資訊技術，公家與私人機構提高了其生產力，服務品質和營收。不幸的是，儘管這些做法產生高度的社會效益，但對於那些負責保護機密資訊的人員而言卻是一個重大的挑戰。

因此，企業需要在不限制其員工履行其工作職責的能力下，積極面對這項新的威脅並保護個人資訊。資訊監視允許企業在不影響其生產力與服務品質下來保護他們所收集的資訊。

資訊監視的定義

資訊監視是有制度性的監控被保存在一個自動化環境內的資訊。在美國麻薩諸塞州的稅收部門（MDOR），該機構負責管理及執行該州稅收與子女撫養相關的法令，該機構的內部稽核部門對於其資料庫執行持續監控機制以確保機密稅務和子女撫養費相關資訊的安全。雖然這個過程是圍繞著監控技術，MDOR的個人資訊隱私政策整合了員工宣導方案，明確的懲處規範，監視工具，以及持續的資料庫分析活動。

建立規則

在實施資訊監視方案之前，組織必須建立相關的資料保密政策，並於此政策中清楚說明相關的受管制行為及提供相關範例和懲處規範。這項政策必須適用於所有員工，不論他們的頭銜，資歷或功能。在 MDOR，所有員工都必須簽署一份年度確認申明書以證明他們已收到該機構的資訊保密政策並了解相關的懲處規範。員工在簽署確認申明書之前無法被授予讀取機密資訊的權限。

除了發放的資料保密政策，公司需執行正式的員工培訓以確保員工了解各項規定和非法讀取機密資訊的懲處規範。在 MDOR 的新進員工介紹課程中，所有的員工都會接受有關於資料保密政策的專門訓練。同時，員工在登錄任何資料庫時，系統會自動發出一個電子公告說明系統會監視他們於系統內的行

為，所有讀取必須與工作職責相關。員工在確認閱讀此電子公告之前無法登入資料庫。

監視系統

由於資訊監視是一個持續監控資料庫活動的機制，系統需要紀錄資料庫活動並保存在一個有利於分析的格式。要做到這一點，MDOR 開發了一套“交易追蹤系統”，這系統是套支援多平台，基於瀏覽器的監視技術，能運行在 Oracle，Unisys 和其他資料庫管理系統。雖然 MDOR 在 1997 年導入了初版的交易追蹤系統，在 2006 年 12 月完成加強版的升級並大大提高了資訊安全部門於資料庫中執行查詢的能力。增強的交易追蹤系統能依據不同的搜索條件而產出相關的結構化查詢語言 (SQL)。搜索結果可匯出成 Microsoft Excel，PDF 和表格檔案，並可以列印，電子郵件發送和存檔。

資訊監控

有建立正式資訊保密政策的組織應將該政策正式的告知所有員工，持續的執行員工宣導，並建制相關監控系統以便監控機密資訊的讀取。這些都是資訊監測方案必要的主要成份，而其餘的作業可能會以此作為基礎。雖然如此，組織不能單靠這些主要成份來確認資訊安全，因為這樣做可能導致組織感到不實際的安全感。如果沒有一個持續的監控機制來偵測可疑的資料庫活動和全面的調查機制以解決非授權的資訊讀取，上述的設施將無法達到其效益。

內部稽核部門扮演著監控的腳色並會積極的展開資料庫的測試和分析。內部稽核部門會使用各類型的測試方法偵測違反資訊保密策略的狀況。使用交易追蹤技術，稽核人員可以於資料庫中執

行監控測試來偵測不符合使用者職務需求之未授權讀取。例如，如果稽核人員發現員工讀取過多居住於員工家附近的個人資訊，稽核人員將認定此為可疑行為，並將會對員工的系統讀取紀錄展開更詳細的檢查。這種類型的查詢展現出交易追蹤系統的檢測功能，並提供了一個很好的例子，稽核人員如何使用的相關系統來辨識可疑的系統讀取行為。如果稽核人員無法確定這些資訊為何被讀取，資訊安全單位會發出正式信函給相關的員工要求他對於相關資訊讀取提出一個具體的業務理由。如果員工能提供合理的解釋，此事件將被視為結案。如果員工無法提供一個合理的解釋，資訊安全單位將停止與該員工任何進一步的接觸並將此事項交由內部事務部作進一步調查。

內部事務部門扮演著調查的腳色，因此，會針對調查對象展開全面的調查以得知其於資料庫內的活動，以確認調查對象是否與被讀取的個人帳戶有關聯。這樣做，內部事務部門利用鏈接分析，此分析技術通常用於執法單位在調查大型犯罪組織成員的互相關係。透過分析電話記錄，電子郵件通信和各種公開的文件，該內部事務部門往往能夠證明當事人的相關性並確認這是未經授權的讀取。MDOR 的資訊保密政策禁止員工在任何情況下讀取親戚，朋友，前配偶或熟人的機密資料。因此在任何情況下，如果有員工讀取其親戚朋友的帳戶資料就是違反資訊保密政策並該員工須受到相關的紀律處分。

責任歸屬

資訊監視機制的最後一個要件為懲處規範。故意違反資訊保密政策的員工必須受到紀律處分，其懲處性質應由組織高階主管訂定。如果沒有一套有結構

性的懲處規範，員工就會認為他們的資料庫瀏覽，即使發現，也不會導致任何後果，因此，他們不會阻止這種類型的不當行為。如果沒有一個有效的懲處規範，組織的資訊保密方案最終將會失敗。

結論

擁有機密資訊的組織需要制定相關措施，於不限制其員工履行其工作職責的能力下，來保護這一寶貴的資產並防止內部人員的濫用。在現在的環境下，那些被視為無法保護客戶託付給他們的敏感資訊的組織需承擔消費者信心降低的後果。建制資訊監視機制及同步導入明確的資訊讀取政策，持續的員工宣導，創新的監測流程，一個有效的調查功能和懲處規範是一種具有前瞻性的組織管理內部威脅所採用的方法。

作者簡介

John Moynihan

is deputy commissioner and internal control officer at MDOR and is responsible for the agency's information security, internal audit and internal affairs functions. He previously served as MDOR's director of internal audit, during which time he

designed and implemented the Transaction Tracking System, a data surveillance technology used to detect inappropriate access of confidential information. He has advised state and federal agencies, as well as international governments, on data monitoring methods. He also presents at leading industry conferences and is a published author.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2010 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org

中華民國電腦稽核協會

Information Systems Control Journal

摘譯文章第 5 期 民國 99 年 12 月 31 日發行

發行人：黃明達

總編輯：張碩毅

編輯委員：張碩毅、李順保、林宜隆、花俊傑、高進光、陳立群、陳禮炫、
黃士銘、劉其昌、歐進士、王大維、黃劭彥、孫嘉明

發行所：中華民國電腦稽核協會

Information Systems Audit and Control Association Taiwan Chapter

授權者：Information Systems Audit and Control Association

寄件處：110 台北市信義區基隆路一段 143 號 2 樓之 2

電子信箱：isaca@caa.org.tw

電話：(02) 2528-8875

傳真：(02) 2528-8876

網址：www.isaca.org.tw

(本刊圖文非經同意不得轉載)



信賴資訊系統，獲取珍貴價值

Taiwan Chapter

會 址：台北市信義區11070基隆路一段143號2樓之2
2F.-2, No.143, Sec. 1, Keelung Rd., Xinyi Dist., Taipei, Taiwan, R.O.C
Tel: 886-2-2528-8875 Fax: 886-2-2528-8876
Website: www.isaca.org.tw