IT Audit Basics

應用系統查核 (上)
(Auditing Applications, Part 1)

作者：**Tommie W. Singleton, Ph.D.,CISA, CGEIT, CITP, CPA**
Is an associate professor of information systems (IS) at Columbus State University (Columbus, Georgia, USA). Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, valueadded dealer of accounting using microcomputers. Singleton is also a scholarin-residence for IT audit and forensic accounting at Carr Riggs & Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications.

譯者：高進光,CIA,BS7799LA

應用系統查核是在對中、大型企業進行稽核工作時常見的類型，特別是當一些應用程式係由內部開發的情形之下。

電腦稽核人員需要知道和了解應用系統查核的一些基本原則。本文之兩部分的文章即描述了一個用於有效的執行應用系統查核之架構。

架構(A FRAMEWORK)

以流程為導向的架構大致包括下面的步驟：

- 規劃稽核作業
- 確定稽核目的/目標。
- 系統和資料流程之對照。
- 確定關鍵控制點。
- 了解應用程式的功能。
- 執行應用測試。
- 避免/考慮衍生之枝節問題。
- 包括財務判斷。
- 考慮有利的工具。
- 完成報告。

前述的步驟有一些步驟是全面的，如應用系統和資料流程之對照。對照應該在查核開始時即進行，它會影響大多數的其他查核步驟。其它如財務判斷，則可能會或可能不會與其他步驟相關適用。然而，本架構之步驟應該可以表達對應用系統查核有效性的公允框架。

在本文先詳細介紹了前三個步驟：規劃，確定目標和映射。剩下的步驟將在下卷詳細介紹。

規劃稽核作業(PLAN THE AUDIT)

規劃稽核作業時，其考慮範圍應包括到所有與本次稽核目的相關的因素。想要妥善規劃稽核作業，則這種考慮是必要的。

考慮稽核目的 (Consideration of Purpose)

發生需要查核的條件或情況是在整個應用系統查核過程中的關鍵驅動因素。也就是說，什麼是推動了此查核需求？它是一個例行的/正規的查核？還是一個臨時的/專案的(*ad hoc*)查核？

查核需要通常是直接與查核首要目標相關聯。

例如，如果管理層希望確認新的應用系統是否能滿足原規劃設計的要求，此一情況將驅動該查核目標和計劃。

考慮風險(Consideration of Risk)

基於前一步驟所確定的查核目的，第二個關鍵驅動因素是考慮與此特定查核的相關風險。電腦稽核人員或查核組，需要識別與應用系統及其關連

的數據資料、原始程式、基礎架構和系統的相關風險。依前述例子，可能出現的風險情況包括：應用系統缺乏的原規劃功能（即實際上並沒有滿足資訊需求），應用系統有錯誤或漏洞，不能恰當地與其他應用程序或系統整合/連接，數據資料不正確，及其他類似的風險。

當然，一旦正確地識別風險情景時，電腦稽核人員需要評估該風險對查核目標、查核計劃、查核範圍和查核程序的影響。舉例來說，如果缺乏功能性的風險，電腦稽核人員應檢查原來的資訊需求，檢閱測試、用戶驗收文件（如果有的話），測試應用程式並執行其他類似的程序。

考慮控制環境
(**Consideration of the Control Environment**)

通常查核計劃應依查核目的之情況，考慮到應用系統周圍控制環境。如果查核的主要目的是查核系統功能的正確性，則其控制活動可能是應用程式開發或系統開發生命週期（SDLC）控制。其中對於應用程式測試的控制是特別重要的。

考慮系統導入安裝前後控制差異
(**Consideration of Pre/Postimplementation**)

電腦應用系統稽核有時候涉及系統導入前的控制，但最常見的是系統導入安裝後的查核。一個安裝前的查核往往涉及特定目的所規劃的特有應用系統稽核目標、範圍和程序。系統導入後的查核往往遵循一般例行性目標（參見確定稽核目標一節）。

考慮查核範圍(**Consideration of Scope)**

規劃稽核作業另一個非常重要的考慮因素是建立範圍的界限。這意味著要確定與查核的應用系統相關聯的有關技術和控制，例如:

- 介面接口到其他應用系統
- 原始程式系統
- 目標/目標系統
- 基礎架構/設施或其組成部分
- 資料庫
- 暫存區/測試設施

考慮查核人員能力**(Consideration of Scope)**

正如在所有查核，查核組的領導者或經理人會需要評估員工對本項查核需求的能力。例如，如果接口介面包括甲骨文(Oracle)，適當的查核程序中將有可能需要懂甲骨文的專家。

確定稽核目的
(DETERMINE AUDIT OBJECTIVES)

稽核目的常會與系統導入前/後控制查核之不同而不同。如前所述，系統導入前的查核往往涉及特定目的而專有的稽核目標。當然該專有目的可適用某些查核。對於其他查核而言，下列目的往往是各式各樣查核的典型目的之一：

- 效率（涉及開發成本，運營績效等）
- 有效性（與滿足資訊系統需求/功能，原來的授權目的，與其他資訊系統之整合，運營績效等）
- 遵循性（法律，法規，合同等）
- 預警（如果應用系統包括預警報）
- 財務報告的影響

系統和資料流程之對照
(MAP SYSTEMS AND DATA FLOWS)

電腦稽核人員執行電腦查核時，系統和資料流程之對照(mapping)是最有效的查核工具之一。在應用系統查核中，了解該應用系統影響到的其他資訊系統或受其他資訊系統影響的正確範圍是非常重要的。專家認為，對照(mapping)可以協助電腦稽核人員在這個過程中，深入了解相關的技術、程序、控制和它們是如何結合在一起的。在本文從查核規劃到報告架構的步驟中，本步驟會加強電腦稽核人員的表現，也就是說，它會全面影響電腦查核的品質。

在應用系統查核中，適當的對照項目應包括但不限於：

- 相關資訊架構元件（說明介紹）
- 業務權責/所有權人或業務指揮系統
- 變更管理的政策和程序
- 供應商的角色和影響
- 業務流程
- 一般控制

存取控制和安全管理

這些因素可以引導電腦稽核人員建立查核地圖，確定哪些應該放入查核地圖或決定哪些要列在電子表格中描述，供對照使用。圖表 1 顯示了應用系統查核地圖的一種方式。

記錄和測繪風險，可能涉及諸如風險、風險領域、目的、底稿索引、程序、查核天數、完成百分比、完成期限日數、系統範圍和備註等項目。圖表 2 顯示了一個電子表格文件，對映射風險(mapping risk)可能會有所幫助，並顯示了如何這樣的查核地圖可以在整個查核是有用的，可以協助管理查核。電腦稽核需要對照(mapping)處理過程、傳統的資料數據流向圖（DFD）、案例、系統流程圖或統一建模語言（UML）。

非傳統的圖表可作為描述一個更好的處理流程和數據流模型。例如，矩陣圖 3 可作為一個更好的模型，因為它結合了時間/交付以及系統、程序和數據流。
在圖 3 所示的特定概要圖表，描繪了讓他們清晰易懂的控制點的一種方式，例如，自動對賬、錯誤檢查系統（IT 相關）及資料上傳之前的 CRM 資料的數據和處理過程之人工審核控制流程。

相對與僅用時間軸和處理流程，如果使用的是系統模型，這一處理流程/數據流框架，可能會更有效。輸入包括原始資料，諸如用於中介應用程式(middleware application)的原始數據，並且包括中間數據(intermediate data)。來源包括內部數據庫（DBS）和外部數據，例如資料倉儲外部供應商（DWS）。處理流程部分包括應用程式的處理功能（見圖 3，包括自動對賬和檢錯/糾錯程序）。

它還包括用於描述處理功能所撰寫的任何程序文件。與資料倉儲(DWs)某些過程是相似的，如 ETL（提取，轉換和下載），它基本上描述了處理從各種來源之數據資料進入資料倉儲之過程。在圖 3 的應用案例與 ETL 相當一致。在查核應用系統時，對處理邏輯(Processing logic)是特別感興趣，因為它們通常是判斷數據的完整性和可靠性的主要因素。輸出包括報表、螢幕資料及其他印刷文件。輸出也包括需要評估被用來建制這些報表、螢幕資料工具和模組。

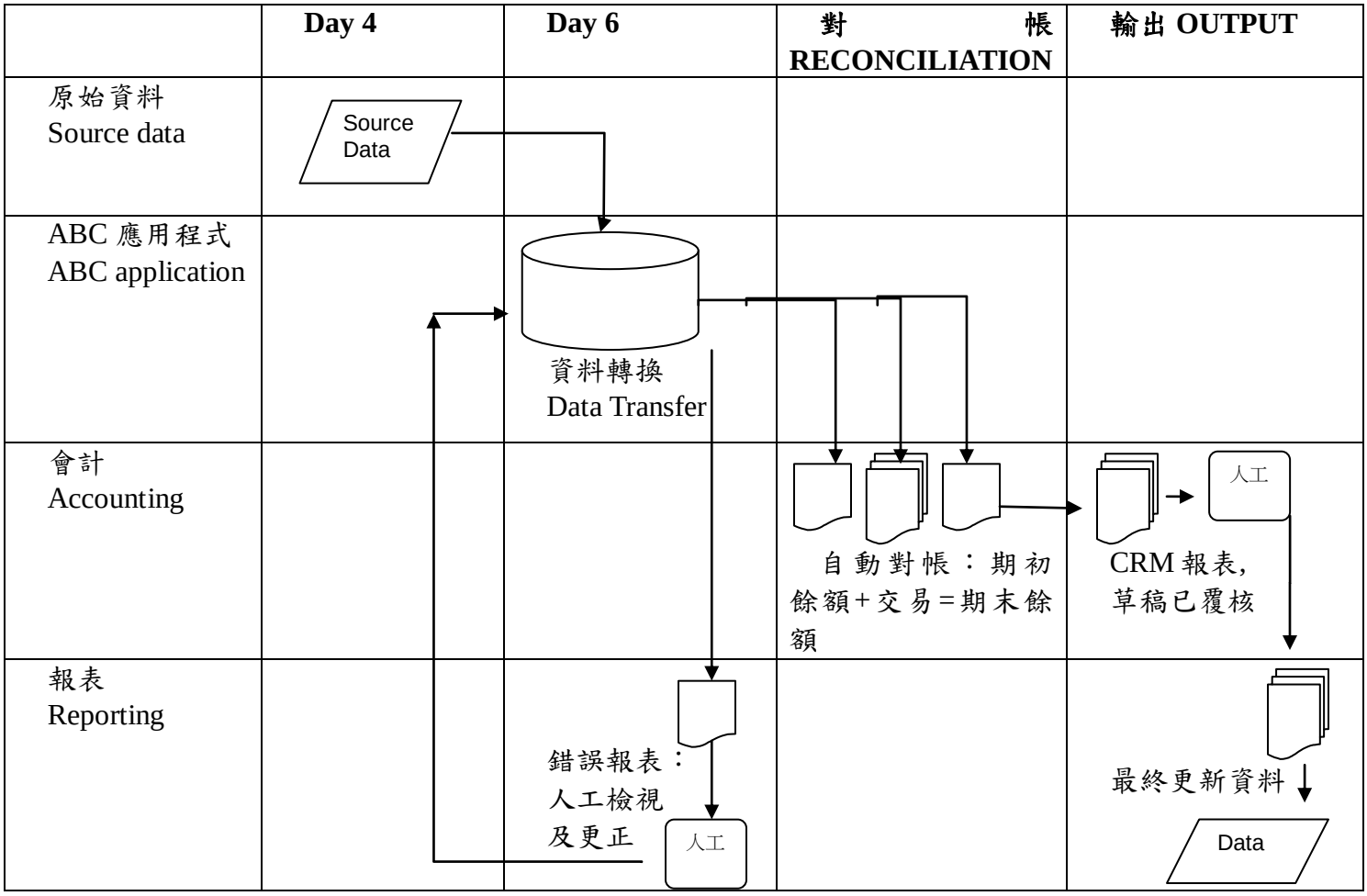
結論

本文介紹了本架構的第一部分。其中一個在這部分的應用系統查核的關鍵步驟，有利的是產生全面和準確的地圖或圖表。在下一期，對該架構的其餘步驟進行說明。大部分的實際查核程序和測試在這些後面的步驟進行。

參考資料

Bitterli, Peter R., et al; "Guide to Audit of IT Applications,"
ISACA Switzerland Chapter, 2010
ERP Seminars, "Auditing Application Controls," 2008,www.auditnet.org/docs/Auditing_Application_Controls.pdf
SANS Institute, "The Application Audit Process," InfoSec
Reading Room, www.sans.org/reading_room/whitepapers/auditing/application-audit-process-guide-informationsecurity-professionals_1534

表 3 處理程序和資料流程之對照(**Mapping Processes and Data Flows**)



圖表 1 利用表格應用系統查核對照案例 1(Mapping Example Using Spreadsheet, Part I)

系統名稱 IT	說明 Description	作業系統 O/S	資料庫 DBMS	伺服器 DB Server	存放場所 Data Location
ABC App	Middleware designed to…	N.A.	N.A.	XYZ	Birmingham
DEF App	CRM, target ...	Z/OS	DB2 Z	mainframe	Nashville

圖表 1 利用表格應用系統查核對照案例 2 (Mapping Example Using Spreadsheet, Part II)

開發者 Developed	維護者 Maintained	負責人 Owner	存取權限管理 Access Admin	變更管理 Change Control	備註 Notes
In-house	In-house	Sue	Active directory…	Controls include	
Vendor	Vendor SOC1/2available	John	Security admin…	Vendor	

圖表 2 風險對照與紀錄 1(Documenting and Mapping Risks, Part I)

Ref.	風險 Risk	風險領域 Risk Area	目的 Objective	底稿索引 W/P Ref.	程序 Procedures
1	無效，不準確或不完整的資料可能導致報表或會計資料錯誤 Invalid, inaccurate or incomplete data may cause errors in reports or accounting.	資料完整性 Data integrity	評估輸入與輸出間資料完整性檢查及控制。 Evaluate data integrity checks and controls between inputs and outputs.	CO.1.1	
2	未經授權或意外變更中間應用軟體可能導致報表或會計資料錯誤 Unauthorized or unintended changes to middleware may cause errors in reports/accounting.	變更管理 Change management	評估變更申請作業是否經適當的批准、測試和職責分工。 Evaluate changes to the application for appropriate approvals, tests and segregation of duties (SoD)	CO.1.2	
3	未經授權存取可能導致中間應用軟體或目標數據資料的非法變更，進而導致報表或會計資料錯誤 Unauthorized access may cause unauthorized changes to middleware or target data, causing errors in reports/accounting.	安全性 Security	評估應用系統之邏輯存取控制妥適性。 Evaluate logical access controls to the application and its folder.	CO.1.3	
4	無效，不準確或不完整的處理程序可能導致報表或會計資料錯誤 Invalid, inaccurate or incomplete processing may cause errors in reports/accounting.	操作面 Operations	評估應用系統發展與維護、錯誤識別與問題解決的處理程序與文件是否妥適控制。 Evaluate processing and documentation for appropriate controls on development and support, and error identification and resolution.	CO.1.4	

圖表 2 風險對照與紀錄 2(**Documenting and Mapping Risks, Part II)**

Ref.	**查核天數 Audit Days**	**完成百分比 Percent Done**	**完成期限日數 Days to Complete**	**系統範圍 Scope of Systems**	**備註 Notes**
1	0.5	100%	0	Middleware, stored procedures, views, CRM, DB2	
2	1.5	33%	1	Middleware	
3	1.0	0%	1	Active directory, middleware	
4	2.0	0%	2	INPUT: Source file PROCESS: Middleware OUTPUT: Target file/DB2, error report	

圖表 2 風險對照與紀錄 3(**Documenting and Mapping Risks, Part III)**

Ref.	**固有風險 Inherent Risk**	**控制風險 Control Risk**	**剩餘風險 Assessed Risk**	**Notes**
1	High	Medium	Medium–High	To date, facts are ..
2	Medium	Low	Low	
3	High	Medium	Medium–High	
4	Medium	Low	Low–Medium	

Quality Statement:
This Work is translated into Chinese Traditional from the English language version of Volume 3, 2012 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 2012,Volume 3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。

Disclaimer:
The ISACA 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 ISACA Journal.

Opinions expressed in the ISACA 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. ISACA Journal does not attest to the originality of authors' content.

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, MA 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.

免責聲明：
ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

若為非商業用途之課堂教學，則允許教師免費複印單篇文章。若為其他用途之複製，重印或再版，則必須獲得ISACA的書面許可。如有需要，欲複印ISACA Journal 者需向Copyright Clearance Center(版權批准中心，地址：27 Congress St., Salem, MA 01970) 付費，每篇文章收取2.50元美金固定費用，每頁收取0.25美金。欲複印文章者則需支付CCC上述費用，並說明ISACA Journal 之ISSN 編碼(1526-7407)、文章之出版日期、卷號、起訖頁碼。除了個人使用或內部參考之外，其他未經ISACA或版權所有者許可之複製行為則嚴明禁