應用系統查核 (下)

Auditing Applications, Part 2

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,

電腦稽核協會常務監事

本文之為以流程為導向的應用系統查核架構兩部分的文章之下半段，第一部分已先詳細介紹了前三個步驟：規劃，確定目標和映射。剩下的步驟將在本卷詳細介紹。完整的應用系統查核架構包括下面的步驟：

- 規劃稽核作業
- 確定稽核目的/目標。
- 應用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。

確定關鍵控制點（IDENTIFY KEY CONTROLS）

在評估相關控制點時，電腦稽核人員首先想要將公司自己建制的控制點和那些包含在商用套裝軟體（COTS）的控制點區別開來。對於自己建制的控制點，開始評估的好方法就是「詢問」。

其中一個關鍵的問題就是要問管理者，在系統開發過程中，有那些的內部控制專業知識被嵌入到應用程式中？控制目的為何?也就是說，誰或什麼部門提供了可以確保適當的控制被嵌入在新應用程式的專業知識？是如何達到這個目標？最後，電腦稽核人員應確保這些控制點已經被妥善記錄和測試。

對於商用套裝軟體，電腦稽核人員可能會從應用程式流程之貫穿檢查開始，以確定哪些控制實際上是有在應用程式內和瞭解它們的功能。貫穿檢查將會依交易步驟，順著資料輸入人員按鍵，解釋他們在做什麼和為什麼，一步一步的進入後續交易或流程。

這樣的過程應該讓電腦稽核人員來大致了解應用程式的控制機制，控制機制的充分性和有效性。若單位第一次使用應用程式時，這種貫穿檢查是特別需要的。

電腦稽核人員應建立商用套裝軟體的控制基準底線測試，以了解其可靠性和有效性。這些將包括應用程式的作業系統，如 SAP 和 Oracle。

對於商用套裝軟體，電腦稽核人員需要確定所涉及的供應商的責任。這就是為什麼圖 1，(在應用系統查核 (上) 系統和資料流程之對照詳細說明)，列出有關於應用程式的供應商和維護者資料的本意。當應用程式出現問題時，管理者需要確認到底是誰來解決這個問題。顯然地，供應商管理實務最常運用。

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	

控制的類型可以採用傳統的系統模型：輸入、處理和輸出來進行評估。輸入控制包括：

- 存取安全
- 職責分工(SoD)
- 資料驗證
- 資料完整性
- 編碼
- 輸入錯誤更正
- 批次作業控制

傳統的處理過程控制包括：

- 自動化程度(全自動、半自動、全人工)
- 關聯工作排程(依作業處理)
- 工作排程監控
- 自動計算
- 自動對帳
- 自動通知

傳統的輸出控制包括：

- 對帳
- 複核
- 核定
- 偵錯及錯誤清單
- 實體文件控制(輔助控制)

了解應用程式的功能

(UNDERSTAND APPLICATION'S FUNCTIONALITY)

通常，有效的稽核品質功能是稽核主管的目標。稽核程序主要即驗證操作功能的有效性，這應該在應用程式開發（AppDev）過程中的需求說

明書階段即應描述清楚。除了檢視應用程式的授權文件，電腦稽核人員應檢閱最終用戶驗收報告。如果驗收報告不存在，代表應用程式開發有關的控制程序不足夠：缺乏最佳實務。

典型的查核目標與該應用程式之目的是相關的。當測試應用程式時，將考慮到該應用程式的各種情境已被妥適地測試。如果該應用程式的結果為二分法（如:是或否，批准或不批准等等）之結果，測試其中一種情形就可能就夠了。但是，如果應用程式為工資單處理之更新等類者，則要考慮到影響計算工資稅的不同因素之各種情境相關組合之測試。在測試安全性和存取控制時也是同樣的情形。

另有一些特殊的考慮，包括最終用戶和業務經理在資訊需求收集階段時往往忽視：安全性和是否取得適當範圍的數據等 2 項因素。應用程式開發時，適當水準的安全性明顯是一個關鍵的成功因素，因此，需要進行評估。通常情況下，用戶和管理者不完全掌握交易時需要被取得的數據範圍。但其實這是特別重要的，如果單位有計劃導入使用數據倉儲、資料探勘進行數據分析以實現商業價值之商業智慧(business intelligence-BI)或業務分析(business analytics)之技術，數據的豐富性成為資料探勘工具“大卸八塊多樣性詳細分析”的有用數據，以獲得採用商業智慧的最大利益。

依據應用程式的目的，操作控制及財務報表的控制機制可能要列入查核範圍內。

利用該系統的模型很可能使分析和測試該應用程式功能變得更容易和更完整。

執行應用測試

(PERFORM APPLICABLE TESTS)

當一個應用程式無法正確執行，或有錯誤產生，或嵌入到應用程式之處理進程無法正常工作，這些問題通常可以追溯到之前不當的測試階段。測試應用程式並不僅僅是行單一的測試，而其最佳實務應包括不同層次的測試。首先，通常是由主要負責開發應用程式之高級程式員或分析師負責應用程式單元測試，然後，改應用程式再經過資訊部門的一些獨立的專家進行整體測試之品質控制考驗。

接著，應用程式是由實際用戶測試。通常，這些終端用戶在應用程式正在開發階段中都會參與其中一部分。但最低限度，應用程式一旦完成，一個或多個最終用戶應該測試該應用程式，以便確定是否充分的發展它的功能性，完整性，正確性和效率性。基本上有那些最終用戶測試完成簽署最終用戶驗收報告，記錄測試結果。

然後，該應用程式應與同一模組或同一作業循環或同一性質類別交易之其他應用程式合併一起進行測試。這通常需要比早期單元測試時要更健全的環境。其中最佳作法為之一，為在另外建立一個有區隔的基礎設施，應用系統、作業系統和資料庫之模擬實體測試環境，來進行這項測試。但尚未結束。應用程式應該在企業制度的背景下進行整體測試，所有的數據傳輸和介面要模擬在實際的運營資訊系統上運作。此過程中特別是需要一個與實際營運系統區隔的測試環境作業。

避免/考慮衍生之枝節問題

(AVOID/CONSIDER COMPLICATIONS)

應用系統查核過程中需要考慮應用系統開發時所會伴隨的一些固有風險。首先，專屬的（客戶訂制）應用程式具有較高的固有風險。這實際上影響了目標，規劃，控制和風險的步驟。

若有包括資料倉儲（DWs）系統因素，固有風險相對較高。當 DW 初步建置時，幾乎是普遍性的有下列問題，導致被輸入到資料倉儲的數據幾乎有很高的風險，例如，資料不一致性（同一個字段名稱不同），數據缺失和錯誤（即錯誤）。因此，當從交易處理系統（TPS）取得數據，應注意數據對照，並使用 ETL（提取，轉換和加載）過程，以找出並改正前面提到的數據異常。

對於正在使用的資料倉儲系統，資料所有者可以更改欄位名稱和添加欄位，如果變更控制不佳，該數據資料無法成功通過接下來的提取，轉換和加載(ETL)過程。因此，對於資料倉儲的變更管理控制是非常重要的。這同樣適用於其它類似的整合功能。

資料倉儲的風險應該區分兩種類型。首先，有處理過程的完整性問題。這種完整性是牽涉處理是否成功，應用程式是否做到它應該做的功能？第二，數據資料的完整性和數據品質，其中涉及被處理，傳輸和記錄的資料的可靠性和完整性。被輸入的資料是否有效？原始資料是否有效，準確和完整？原始資料是否有效地完成傳輸而沒有錯誤？

包括財務判斷

(INCLUDE FINANCIAL ASSERTIONS)

當財務報告也在應用程式範圍時，應用程式需要發表帳戶餘額及交易類別或財務揭露等辨識判斷的宣告。應用程式是否有對帳戶餘額或交易類別的最終結果之適當控制予以辨別判斷？電腦稽核人員對該應用程式所稱之宣告應予以測試。舉例來說，如果這個宣示說法是準確度，測試可能包括的東西，如：

- 數據輸入驗證控制
- 自動驗算
- 自動調節核帳

存在性的宣告可能會是對資料輸入驗證控制機制進行測試。完整性宣告可能為工作/整批處理控制或調節表進行測試。

考慮有利的工具

(CONSIDER BENEFICIAL TOOLS)

電腦輔助審計技術(CAATs)和 ETL 是測試應用程式有用的工具。電腦輔助審計技術在引導辨理某些檢查程序是很有用的，例如資料探勘技術，以檢測應用程式產生的最終結果數據，以確定該應用程式的控制是否有用?還是有效?還是會產生錯誤。

電腦輔助審計技術在對利用分析數據達成確認數據完整性的稽核目標上也是很有用的。

ETL 技術在偵測問題資料上非常有用，追溯到應用程式產生問題資料的源頭，因此提供改正的機會。

控制測試

(TESTS OF CONTROLS)

一些可能的控制測試包括：

- 核對/調節
- 重新計算
- 重複
- 缺口差異

核對的應用例子如驗證客戶在主檔與交易檔中的客戶 ID。也就是說，交易檔中的客戶是否真的存在於授權客戶名單？另一個例子是重新計算，電腦稽核人員可能會從存貨資料庫的資料延伸，看看總庫存成本總量是否與總帳帳戶餘額相符。重複和差距在偵測資料處理的錯誤非常有用。

電腦協助查核工具

(CAATS)

電腦協助查核工具可以用在重新執行自動計算或自動核對的功能

資料探勘

(DATA MINING)

資料探勘可以支持審計目標。特別是在從事如涉及代碼是否被正確的認證或有無分類錯誤等之資訊作業相關的實質性程序測試時，非常有用。

訂購單門檻

(PURCHASE ORDER THRESHOLDS)

任何時間應用程式會涉及初始/額外採購審批門檻的需要，電腦輔助審計技術可確定該項控制是否有效運行。例如，應用程式是否不是採購訂單就是支出，是否採購和付款都是一筆對一筆（即，支出需憑發票支付和而非憑報表不支付），抓取所有超過門檻的支出的檔案資料，比對檢視這些交易批准檔案資料（如採購訂單文件），此簡單的測試會暴露任何例外控制/門檻。如果有人對審批門檻故意偷梁換柱，這也有偵測欺詐的額外好處。

庫存異常

(INVENTORY ANOMALIES)

如果該應用程式是記錄接收的存貨，電腦輔助審計技術可用於顯示應用程式是否允許零或負的數量進行記錄。顯然構成了錯誤（異常），因此，該應用程式將被視為含有一個控制缺陷，不是需要進行應用程式變更就是要有其他補償控制。其他的應用程式，可以使用這種測試。其次，如果應用程式是一個維護檔案的程式時，系統會希望盡量減少其僱員可能無核准文件而變更庫存資料的情況，可能會導致存貨資料的差異和錯誤。故需要予以控制，以防止這種異常現象。例如，使用分工牽制功能可限制負責維護檔案的員工不能隨意變更檔案資料。此外，應用程式/系統可以通過改變前和改變後的記錄資料來追踪其變化。

如果沒有這樣的追踪，員工可以偽造的變更資料，創建錯誤資料或舞弊。資料探勘可以利用期初餘額加計所有交易總和之結果，來驗證期末餘額，找出帳戶餘額差異。類似的情況存在於任何檔案維護應用程式。

完成報告

(COMPLETE THE REPORT)

顯然地，所有查核審計係以某種形式的報告來結束。這些報告通常是專有的格式。但是，他們往往包括審計目標，進行了測試，測試結果和建議。

結論

(CONCLUSION)

成功的應用系統查核有賴於一個可靠的方法。此兩部分的文章展示了一個可靠的方法和一些工具，應該是有幫助開展查核工作，尤其是系統和資料流程之對照和電腦輔助審計技術。

ADDITIONAL REAOURCES

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

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 4, 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 4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。

Copyright

版權聲明：

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。