資訊科技的一般和應用控制：內部化模型
IT General and Application Controls : The Model of Internalization

作者: **Emanuele Palmas, CISA,**

has been part of the internal audit team at Guess Europe Group, based in Lugano, Switzerland, since 2008. He has gained experience in external auditing for medium and large companies within the industrial sector at PricewaterhouseCoopers, with mandates including the US Sarbanes-Oxley Act and support to IT audit. At Guess Europe Group, Palmas has had the opportunity to improve his IT audit skills and has followed the implementation of IT general controls (ITGC) and IT application controls (ITAC) at the enterprise, supporting the external auditors when required. An important task during his practice has been the ITGC performance in Hong Kong for Guess Asia. Palmas holds the COBIT 4.1 Foundation Certificate and ITIL v3 Foundation Certificate. He can be contacted at emanuele.palmas@ch.guess.eu.

譯者: 高進光,CIA,BS7799LA, 上海商業儲蓄銀行 稽核部 資深經理

各產業公司有時會發現自己面臨著是否將電腦審計服務及資訊科技一般控制（IT general controls -ITGC）和應用控制（IT application controls - ITAC）外包的選擇。外包的決定很可能是由於被審計的企業之財務規劃、時間因素、資源不足或是公司本身技術層面上無法勝任，特別是資訊科技一般和應用控制在技術和實務上的知能需求，並不像如COBIT4.1或資訊科技基礎設施庫（the IT Infrastructure Library -ITIL）等資訊管理模型那般盡如人意，而是遠超出如沙賓法案中相關資訊科技控制目標理論範本中（*IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*）所提出的論點。事實上，導入資訊科技一般和應用控制並不僅是一種規範遵循問題而已，而會對於風險的辨識與改善提供附加價值，另在實務上也有助於即時建立適當的全年審計策略。

在實施內部稽核服務時，某種程度上的實務經驗是必須的，但很遺憾對一般公司而言這不是永遠可得的。為了彌補經驗不足的缺失，企業能選擇以外包的方式來處理，但這種為了現下實行目的的選擇也同時讓企業喪失了一個重要的學習機會，考量到外包伴隨的相當程度的風險，這種選擇可以說是相當沒有遠見的。

事實上，主要風險是很清楚的：辨識風險的過程中，很有可能是被局限於除了資訊科技以外的作業面、財務面或合規面的角度，致未能正確地識別所有的風險。此外，也代表所有辨識評估的模式已被固定化，這也意味著錯過了成熟的稽核部門擬建置“整合性審計模式”基礎的機會。

內部稽核業務外包時會錯過的機會（MISSED OPPORTUNITIES WHEN INTERNAL AUDIT IS OUTSOURCED）

內部稽核業務外包使得內部稽核沒有機會去了解他們單位的全部業務流程，所有的數據資料都是代表公司業務運作和管理的資訊，內部稽核人員如果不能了解全公司資訊流，則無法掌握所有業務流程的真正含義。能處理和了解資訊系統架構及其可用性，基本上已讓內部稽核人員更能掌控相關風險的知識，這意指內部稽核更進一步能掌握前述綜合性審計業務模式的全貌。

在企業組織中起初及最終階段，均可用數據資料本身來表示其效益，這些數據資料則經由資訊系統分門別類的有效率處理後顯現出來的。 COBIT清楚地在資訊科技和業務目標間的策略結合研究中總結了這一概念。縱然資訊部門可以視為一個獨立且完整組織，有自己的預算、客戶、內部供應商和策略目標的子公司，資訊科技可以藉由將資訊

策略、計劃、目的和目標，與公司需求目標的定位相同且支持企業，成為企業的一個成功因素，至少也能使企業體認到它的成就。因此，資訊科技所規劃的預算應花費在支持業務目標的達成，所有計劃項目都應該顯示其經營策略，並由董事會或高階管理階層批准並確定。核心業務和資訊科技策略之間不應該存有任何分歧，或可量化、識別的差異存在。最好的策略，應盡可能的減少差異。

一般和應用控制的內化作用是將資訊治理知識基礎整合到企業資產的一個重要途徑（The internalization of ITGC/ITAC is an important path to the integration of fundamental IT governance knowledge within corporate assets）很明顯也很通常，特別是外包期間，內部稽核人員會進行大量的測試工作，而常常忘記其已對一般和應用控制有完整地下定義和信賴其他審計評價結果。然而，若從對已建立的資訊一般控制機制有一定程度的體認開始著手，可以使稽核人員立即看到該公司現在及將來的經營策略、組織結構、相關業務作業流程、及資料與資訊處理過程的變化。例如，只須檢查該期間之重要程式變更的數量和內容重點就很有幫助。因此，控制測試外包會產生一個不是可以立即或不容易補救的知識落差。

資訊部門_公司內部的公司
（THE IT DEPARTMENT—A COMPANY WITHIN THE COMPANY）

從開發訂單、應付帳款到供應商和薪水線上轉帳資訊資料，所有公司都透過組織內部之作業流程處理。

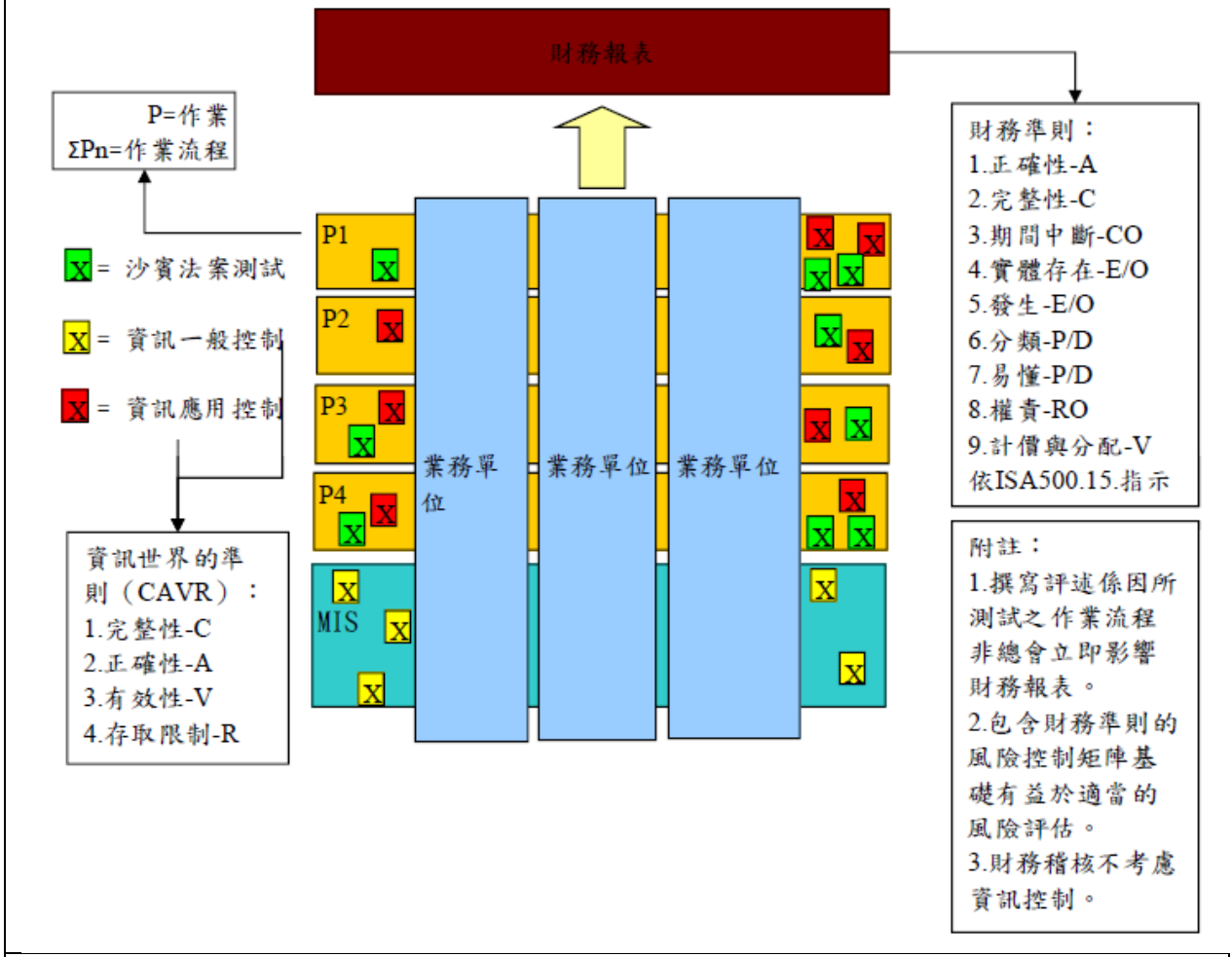
資訊部門可以定義為在公司內部的公司。資訊部門通常有它自己的供應商和顧客目錄（子公司，分公司或控股公司本身的一個部門），其中從控股公司整體來看，很少會有同一單位同時為供應商和顧客之情形發生。例如，當財務部門之協助或支援需求需要在內部自行開發新電腦程式時，該部門就可以成為資訊部門的“顧客”。意識到管理資訊系統（MIS）部門可作為公司內部的公司，提供了將該部門從舊的“資料中心”屬性轉變到有增加附加價值的業務單位，與以業務導向、效益及效率為原則的指導策略方向是一致的。

最後，依公司治理，管理階層的任務肯定是向董事會爭取批准建立一個獨立的資訊部門，以支持業務的發展。

事實上，不像外部審計和顧問公司，內部稽核部門對公司是有應具備完整企業知識的承諾，不僅僅是查核法令遵詢問題，往往把重點放在經營績效成果是否達到目標。可能只有內部稽核人員最知道也最有機會好好地評估公司全部的業務風險、控制環境、企業文化及風格以及可能的業務疏失，以履行其職責。例如：在一個特定的內部稽核中覺察到在供應鏈過程中的變化，資訊一般和應用控制的風險提高特別容易出現，事實上，這種變化的影響可能不會很明顯在IT流程的反映出來，但聯結收到的資訊是非常重要的。有時，對資訊管理部門或財務部門負責人的訪談，可能不足以偵測到其變化，因為一個人不能確認組織內部當場的溝通是有效率及有效益的。因此，訪談可能是只有當資訊和業務部門間有具體的策略結盟時，稽核人員用來充分瞭解公司（如COBIT的建議）。資訊和業務部門間的策略結盟時，是否真的根據一般和應用控制的範圍，有失敗的風險，藉由作業面基礎設施的運作，可以實際上“感覺”公司節拍，掌握其風格和文化。因此，依由上而下的方法論來建立策略結盟的誠信。如果公司的共識是藉由資訊基礎設施（即概念上等同公司的框框），則企業可以公正的確認經由企業網路的業務流程變更，可以有被具體實現的機會。如果公司的共識是不通過資訊基礎設施處理，有可能整個業務流程和風險相對不能完全理解。

在稽核人員的測試過程，資訊一般和應用控制在資訊治理知識和成熟度模型，提供了立即的價值，此外，測試資訊一般和應用控制也給企業吸收控制和相關風險的基本要求知識的機會，創造附加價值和資訊治理知識。

圖1－整合性架構：控制的結合



資料來源: Guess Europe, “ITGC & ITAC at Guess Europe Group: FY2010, July 2010,” Switzerland, 2010

資訊一般和應用控制的內部化，可以說是把資訊治理基本知識整合為企業資產一部份的一個重要途徑。公司治理和資訊治理之間的合作發展，創造了發現一個有趣的風險地圖的機會，很明顯，這些協同效應只在公司內部適用。這是一個令人難以置信的機會，嚴格限制稽核人員於審計期間使用。這種新的認知將提供立即可見的效益，即策略上建立能完全融合領會風險的年度審計計劃。

審計計劃裡，稽核人員需要驗證內部控制是有效的，以確保利益相關者能獲得財務報表能表現其真實與公平性。如圖1所描述，雖然財務報表編製要依循外部的衡量及評價主張，公司內部的所有數據資料皆係出自其經營過程，公司則是由一群不同業務單位作業流程相互交叉組成，所有作業流程整合起來就是流程週期。因為稽核人員以資訊一般控制來進行MIS部門相關的作業流程的測試，MIS部門是一個可以支援所有業務單位和作業流程的業務單位，就此而言，資訊一般控制對其他作業流程和審計來說是可靠的。

資訊應用控制（ITAC）則關注作業程序與美國的沙賓法案的測試控制，以評估作業流程控制的有效性。導入應用控制係為控管得住已被公司辨識出的風險。為能更佳認識和評估所有的風險，則必須利用一般和應用控制及業務流程來檢試資訊治理成效。最徹底深入的稽核涉及資訊控制，正確得體

的執行稽核工作，能使得企業的業務流程和相關的風險更容易相互連結。當稽核人員能遵循系統性和方法論來執行稽核業務時，同一主題相關連的資訊一般和應用控制及其他稽核作業則可視為亦屬合格，並能改善稽核品質。

結論

在內部實施資訊一般和應用控制，提供了稽核人員增進他們瞭解公司的一個很好機會；就公司而言，則為公司建立資訊治理並加強公司治理的契機。資訊一般和應用控制的內部化，可以說是把資訊治理基本知識整合為企業資產一部份的一個重要途徑，也是讓稽核人員變成專家的刺激因素，特別是當稽核人員遵照完整的稽核過程，包括了最基本及重要的資訊控制的評價時更是如此。除了缺乏專業知識的理由外，沒有什麼特別的原因需要將資訊控制作業外包。然而，每一個陰影下都有一線希望，在這種情況下，知識內部化可以是增加專門技術的投資，而不是熟練度不足的外包。

REFERENCES

ISACA, CISA® Review Manual 2010, USA, 2010

ISACA, IT Governance Implementation Guide: Using COBIT® and Val IT, 2nd Edition, USA, 2007

IT Governance Institute (ITGI), COBIT ® Control Practices, 2nd Edition, USA, 2007

ITGI, IT Assurance Guide: Using COBIT ®, USA, 2007

ITGI, IT Control Objectives for Sarbanes-Oxley, 2nd Edition, USA, 2006

KPMG; Geneva & Universität Zürich Institut für Rechnungswesen und Controlling "Objectifs de Contrôle Pour l'Information et les Technologies Associées (COBIT)," 2005

Laudon, Ken; Jane Laudon; Management of Information Systems, Prentice Hall, USA, 2006

Leleu, Eric; "Le COBIT: L'état de l'Art, Socle de la Gouvernance des SI," January 2009, http://home.nordnet.fr/~ericleleu/cours/cobit/cobit.pdf