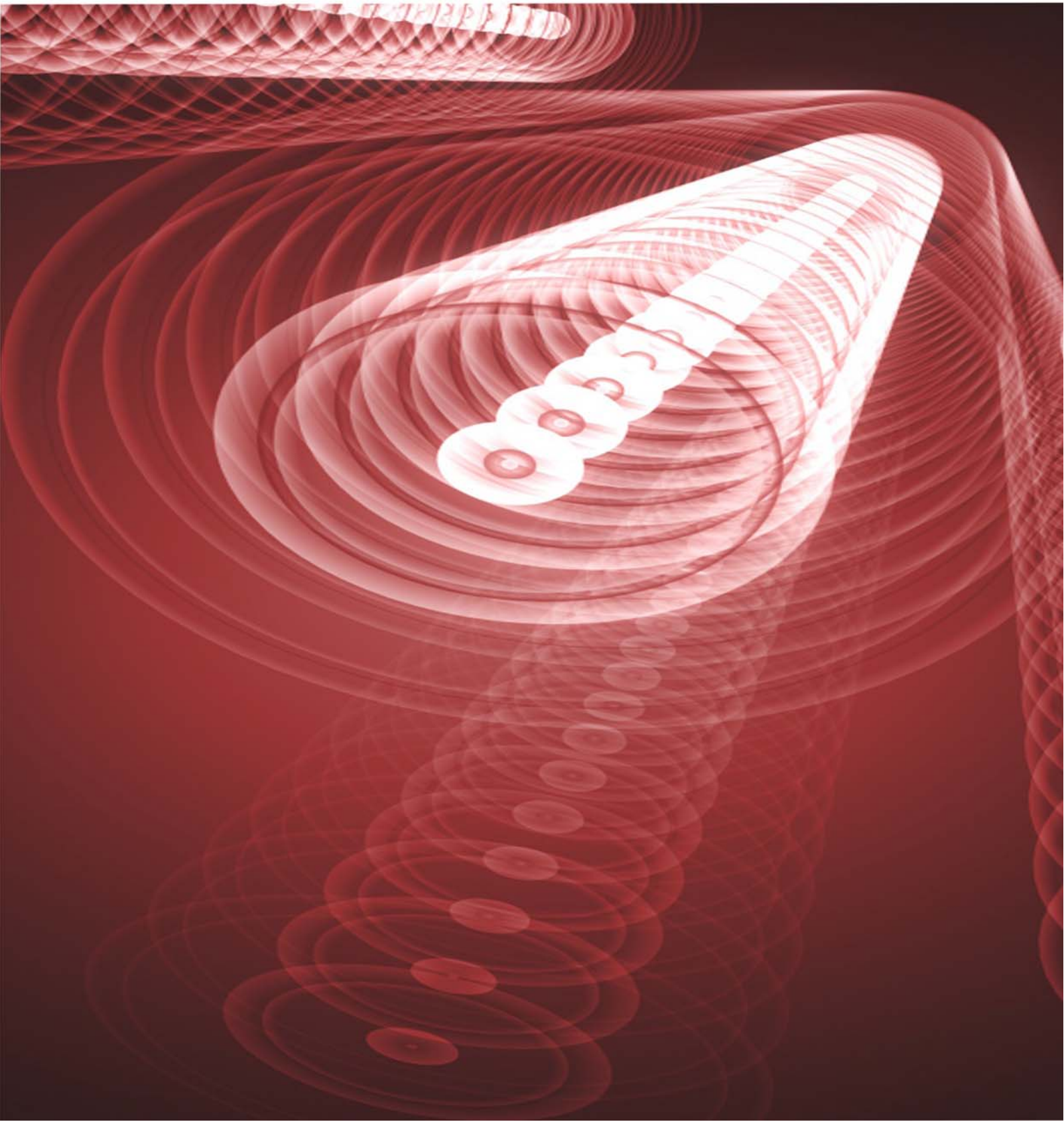
摘譯文章

# 電腦稽核

ISACA
Trust in, and value from, information systems

Vol 1 and Vol 3, 2010
摘譯文章第7期

ISACA Journal



# 目　　錄



(以上文章皆摘譯自 ISACA Journal. Volume 1, 2010. and Volume 3, 2010.)

# 開創資訊科技風險管理新價值
# Driving New Value From IT Risk Management

作者: **George Westerman, DBA**

is a research scientist at the Massachusetts Institute of Technology Sloan Center for Information Systems Research (MIT CISR) and faculty chair for the IT for the Non-IT Executive course. His research and executive level teaching examine management challenges at the interface between IT and business units such as risk management, innovation and communicating about value. He is coauthor (with Richard Hunter) of *IT Risk: Turning Business Threats Into Competitive Advantage* and *The Real Business of IT: How CIOs Create and Communicate Value.* He can be reached at *georgew@mit.edu.*

**Brian Barnier, CGEIT,** advises business and IT executives on getting better business results from IT through improved risk-return balance—whether cost cutting or building capabilities for recovery. He is also a teacher, writer and member of multiple best practices committees, including ISACA's IT Enterprise Risk Management Task Force, which oversaw the development of ISACA's Risk IT: Based on CobiT® framework. His writing includes contributing to the recent Wiley & Sons book *Risk Management in Finance*.

譯者:張碩毅, 國立中正大學會計與資訊科技學系教授

近年的經濟衰退已為資訊科技組織帶來雙重問題。資訊科技(IT)風險管理比起以往更為重要；然而面臨資金短缺，組織需在資訊科技風險管理上發掘更能吸引企業高階主管的議題，使高階主管在有限的資金下產生投資的動機。正當組織費盡心思找出所有投資中最具價值的項目時，他們同時也開始思考如何從風險管理活動中得到更多價值，包括運用風險管理的洞察特性改善資訊科技及企業流程管理；而此議題的重要性遠大於企業縮減風險管理成本。

遺憾的是，提升資訊科技風險管理價值一事在企業間進行得並不順遂。資訊科技風險管理涉及廣泛層面，不同部門的管理者(如安全、營運持續、專案管理及法規遵循)在這一方面通常以獨立作業居多。

長久以來，企業總無法明確將資訊科技風險管理歸類在企業風險或資訊科技風險。科技風險管理者需先適應所有從一般到特定領域資訊科技的風險管理指南，或者嘗試統整出特定領域的指南。這兩種方式對企業都有些許幫助，但這兩種方式卻都無法呈現一完整概念：在數位化及全球資訊互通日漸頻繁的商業環境下，資訊科技風險便等同於企業風險，其重要性與日俱增。而近日國際電腦稽核協會(ISACA)以 COBIT 框架為基礎發布之 Risk IT 為跨部門之風險管理，在資訊科技風險管理層面上，提供各部門更多執行方案上的選擇。如此專家便提出這樣的疑問：『我們該針對哪些層面來增進資訊科技風險管理效率及提升其價值？』

本文以下將針對資訊科技風險管理之三大原則、此三大原則與風險管理價值及 ISACA 框架之關係加以論述。在此三大原則的發展及應用上臻至成熟的公司不僅風險管理得當，同時也可運用資訊科技風險管理來改善內部資訊科技管理與經營成果。他們的風險管理投資為企業資訊科技風險管理創造四個新價值：更少的意外、更有效率的資訊科技流程、更高的企業一致性及靈活度。

## 資訊科技風險管理三大原則

在許多組織中，資訊科技風險管理上的目標皆是確保公司不會因導入資訊科技而遭受意外事件的波及，如預期外的停機、駭客入侵、過量的專案或法規遵循等問題。事實上，許多組織皆已初步採用不同層面的資訊科技風險管理。然而組織通常只著重於保護面而非改善面，即使花費甚鉅，仍未真正提升其價值。此外，他們通常未能察覺這些保護機制可能會妨礙風險管理上的靈活度。

麻省理工學院(MIT)最近一項研究發現結合三大資訊科技風險管理原則便可有效對應阻擾企業達成主要四大

目標之風險[1]。

此四大目標為可靠性、安全性、準確性及靈活性。在資訊科技風險管理投資上獲取較高價值的公司在此三大原則皆已發展成熟：

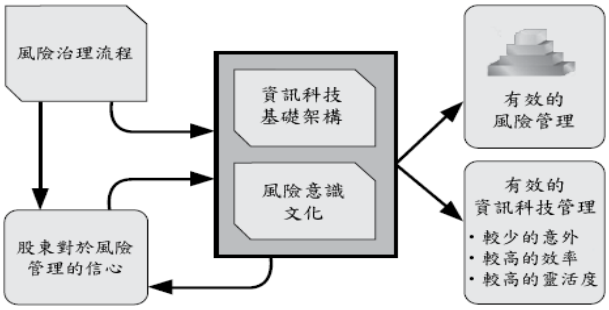
- 企業內部有一管理完善之**資訊科技基礎架構(IT foundation)**，並可視不同狀況調整其複雜度。
- 企業內部有一**風險治理流程**來辨識企業將面臨哪些風險並決議其因應之道。
- 企業內部已建立起**風險意識文化**，在此風氣下員工皆可適時適地察覺風險存在，且不需避諱談論這些議題。

此三大原則共同運行將有助組織查覺當下面臨之風險，適時做出因應決策並降低風險對組織造成的危害。

2008 年中，此文章作者群針對來自六個不同國家的 258 位資深主管進行問卷調查(其中 100 位來自資訊科技部門，158 位來自非資訊科技部門)[2]。受訪者皆代表該組織中最資深之資訊科技主管，或所從事之業務與資訊科技有關聯之主管。問卷題目皆來自先前相關研究清楚定義之概念，包含先前麻省理工資訊系統研究中心所做過之資訊系統相關研究[3]。問卷上各個項目經統計性檢測後合併發展成主要研究架構，用以檢視組織風險管理成熟度與重要組織營運成果間的關係。

研究分析發現，此三大原則在提升組織資訊科技風險管理價值上，皆各別有所貢獻(如下圖 1)。組織確實需要成熟的風險治理，但這一部分明顯不足。成熟的風險治理提升了組織對風險的關注，也提高了股東參與風險管理投資的意願，同時也在組織決策上提供更多的資訊。然而，若要真正改善組織的資訊科技風險管理，就必須從改變資訊科技基礎架構及風險意識文化開始。據統計，上述兩者發展越成熟的公司，相較於其他公司，不但意外發生的機率較低，所獲得的利益更是多出許多。而統計資料也指出，這些公司的組織效益較高，與商業資訊化的一致性與靈活度也較高。

圖1—資訊科技風險管理三大原則與企業績效之關聯性




針對258位資訊科技與非資訊科技主管所進行之資訊科技風險管理調查中發現基礎架構及風險意識文化(不僅只有風險治理流程)較成熟的公司也會有較高的企業績效，而非僅降低意外發生的機率。

資料來源：麻省理工資訊系統研究中心 & IBM

雖保護基礎架構與建立風險意識對於 COBIT[4] 使用者來說已再熟悉也不過，但資訊科技風險管理者們仍須關注更深遠的議題。

在風險治理程序上，管理者們應將目標放在改善資訊科技基礎架構及建立風險意識文化，而非僅僅守住不穩固的基礎或僅在組織間舉辦風險意識相關訓練課程。舉個非資訊科技領域的例子來說，長久以來風險治理已成功降低商業航空上的人員死亡率。這樣的成果並不止歸功於良好的風險治理程序，也歸功於良好的機身設計與維護，以及員工間風險意識文化的建立。在資訊科技領域上，COBIT 提供各組織於資訊科技基礎建構上，包含降低風險投資，一套規劃、建置、投資監控及操作的準則。在許多資訊科技環境下，企業會針對資訊科技的基礎維護添增一層保護，但這些都是不夠的。企業通常只能在風險管理上獲得有限的價值，因為他們只將投資重點放在保護鬆散的基礎架構，而非讓整體基礎架構變得更容易運行。若以上述航空業的案例來解釋，便是在駕駛艙中添加更多機具來讓駕駛員更容易察覺飛航狀況及問題，但卻沒有解決引擎設計上的問題。

**何謂在此三大原則上更加熟練？**

風險治理程序乃指一包含政策、流程及角色定位之套裝規劃，讓組織可監控資訊科技風險並針對資訊科技風險做出更好的因應決策。在大多數公司裡會有一中央團隊為企業建構企業風險相關政策及處理流程。當公司內部管理者們意識到並著手處理存在之風險時，便會同時告知中央團隊哪些屬於最高風險。一全面之企業管理委員會會優先投入緩解組織最高風險的工作；企業內部管理者們則著重於處理層級較低之風險。風險治理較成熟的公司擁有明確的風險分類與指南來依序評估風險，同時也有制式的例外處理程序及關鍵風險指標。他們同時也落實資訊科技與企業風險管理程序上的整合。

若組織內部沒有一位流程擁有者，組織流程便無法改善。根據本文作者群調查指出，僅半數左右（百分之四十八）的公司有指派流程擁有者來負責資訊科技風險管理事宜；僅約三分之一的公司擁有正式的風險分類或例外處理程序。正式的風險分類可幫助公司逐一辨識及比較各類風險。例外處理程序更為重要，組織可因處理例外事件得到成長。由於例外事件會導致組織程序複雜化，因此例外事件也會提高資訊科技基礎架構運行上的風險。有鑑於此，無論在專案執行期間及執行後，企業組織皆需格外重視例外事件的管理。

僅百分之二十八的受訪者表示能有效運用關鍵風險指標（KRIs）[5]。要達成企業分析儀表板上完整整合之關鍵風險指標並非易事，但企業仍可從較簡單的項目開始執行。金融服務業者 PFPC（現為 PNC 全球投資服務公司）便是從追蹤問題單量與員工流動率開始做起[6,7]。而其他公司也開始執行諸如密碼重設、專案達成率、帳務調節失敗、恢復時間、入侵嘗試等項目。在當今環境中，企業組織必需更熟悉如何依據現狀彙整及執行各項關鍵風險指標，並將彙整後的關鍵風險指標運用在控制設計上。

此外，另一個重要議題是尚有百分之六十六的公司未有效將資訊科技風險納入企業風險管理（ERM）當中。一般企業風險管理通則如風險管理標準（ARMS）[8]、澳洲/紐西蘭風險管理標準（AS/NZS 4360）[9]或 COSO 企業風險管理架構[10]，並無明確指示如何處理資訊科技風險，但 Risk IT 風險框架可擴大各公司自企業風險管理框架到企業流程間技術先後關係上的規劃層面。

資訊科技基礎架構是一套基礎設施，用以支援各項資訊科技技術及支援確保流程順利運作之技術人員。資訊科技基礎架構發展成熟的公司擁有管理良好的基礎設施、清楚定義的企業持續營運計畫、並對於技術與企業流程間的連結有清楚的認知。除此之外，他們更擁有完善的企業架構來確保資訊科技基礎架構符合組織所需，且不會太過複雜。

不成熟的資訊科技基礎架構—過度複雜或管理太鬆散—都會引發風險。軟體間升級不一致及依存過度複雜皆會時常導致設施運行失敗，難以復原，更難以轉變，浪費維護資源且設施靈活度也遭受限制。

雖五分之三的受訪者皆表示他們的基礎設施維護良好且公司內部皆有完善的企業持續營運計畫，企業仍需防範未然。某一公司三間辦公室分別在六個月內遭受同一種電腦病毒入侵，因資訊科技人員並未第一時間通報公司內部各處關於此病毒的相關訊息及因應方式；而在另一家公司，資訊科技人員在安裝更新檔時，則是例行性忽略了其中一組伺服器。因此，維護資訊科技基礎架構最好的方式，便是良好的設計與控管，像是運用 CobiT 所提及的內容，及像是信息技術基礎構架庫（ITIL）[11]中所提到的作業管理程序。在 CobiT 術語中，這些是屬於交付與支持（Deliver and Support，DS）及監測與評估（Monitor and Evaluate，ME）部分的程序。

雖然多數的公司對於自身資訊科技基礎架構設施維護上都感到滿意，但並非大多數的公司都能簡化資訊科技基礎架構。僅百分之四十的公司確信自身資訊科技基礎架構並未過度複雜，或者，僅百分之四十的公司確定其內部員工了解資訊科技與企業流程間的關聯性。Risk IT 中的風險

評估（RE）流程對此議題相當有幫助，尤其是RE3.1（資訊科技資源到企業流程間的規劃）及其後的流程。管理者們可運用風險收益的方式來平衡某些報酬率可能較低的投資，也可利用風險評估流程中所提及的方式來改善企業流程，而非只是保護或控制它。此外，也可採用專案層級的資訊科技治理機制（像是 CobiT 中的獲得與實施[AI]流程及 Val IT[12] 中的投資管理[IM]流程）來減少資訊科技基礎架構長久以來過度複雜的問題。

舉例來說，在需優先執行或執行中的專案中，有些公司會將企業架構標準與複雜度列入決策議題。英特爾公司在需優先執行的專案上，不僅以策略聯盟及預期財務報酬為基準，同時也配合公司的架構標準方向。一家消費食品製造商指出，若某些專案可降低企業架構上的複雜度，那麼這些專案在優先順序的排定上將會被優先考量。另外，金融服務業者 PFPC 則是針對專案所需管理及傳送過程採用風險導向之查核點。

風險意識文化為第三項原則。這並不是風險規避文化，也不是僅需要公司舉辦意識訓練課程；不同於風險規避文化，在風險意識文化下，員工皆了解自身行為會帶來哪些風險，不避諱公開討論風險相關議題且願意共同解決公司所面臨之風險或意外。成熟的風險意識文化可讓公司更安全也更為靈活，員工皆了解如何避開風險過高之行為，也了解如何解決引發不必要風險之意外狀況。然而，在持續維持該文化的同時，員工也了解過度的保護會引發組織靈活度上的危機（意即過度死板）。當員工了解何種風險值得投資，也了解何種狀況與行為會引發不必要的風險時，公司便可冒更多的風險來追求更大的報酬。

成熟風險意識文化的建立並非偶然，而是需公司全體自覺地建立，並由領導階層來強化。在風險意識文化成熟的公司中，員工皆會了解自身工作上的風險及如何控管，也可在公開的情況下針對風險議題侃侃而談，並將風險納入自身商業談話的議題當中，而員工也會在領導階層強化建立風險意識文化及不斷的提醒下受到鼓舞。

五分之三的受訪企業表示公開談論資訊科技風險在員工間是很自然的事，但僅三分之一左右的員工受過有效的風險相關訓練，或可經旁人指點加強風險控管事宜。而僅百分之二十七的受訪企業表示在討論資訊科技商務議題時會包含風險這一區塊，顯示運用風險意識來改善資訊科技決策方式的人仍占少數。探討資訊科技風險議題，如組織內部既有資訊科技資產整合上的緊密程度，或是否要在專案中使用非標準化的技術等等，對於企業找出可同時達成預期目標又可降低作業風險的方法相當有幫助。此外，比起因「這樣太危險」的想法而停滯不前，清楚去了解一新無線行動裝置所暗藏的風險，可帶給企業更長遠的利益，不只可讓企業做出更適切的決策，也可提升企業風險意識及改善企業校準。

此項原則的目的是要讓風險意識文化在資訊科技領域中普及化，就像安全文化在高風險產業中一般。幾乎每個石油大廠一開始都需召開會議，針對安全議題逐一簡要探討。管理人也經常提醒員工注意安全相關議題。高階主管們經常討論風險議題，並在員工疏忽時提醒他們。資訊科技領域的高階主管可效法高風險產業主管的做法來提升企業風險意識文化。此項原則也與 ISACA 第三部分 Risk IT 執業者指南及 Risk IT 的風險治理（RG）程序 1 與程序 2（尤其是 RG1.5）相對應。

## 在成熟風險管理下開創新價值

大多數企業在這三大原則上都已有長足的進步，但在運用此三大原則的成熟度上卻不盡相同。對於 ISACA 會員及 CobiT 使用者來說，掌控資訊科技基礎架構的重要性不言而喻。然而，CobiT 較少強調簡化基礎架構、建立風險意識文化及提升風險治理上的成熟度。Risk IT 將 CobiT 做延伸，更加強調風險治理及文化的部分；但無論是 CobiT 或 Risk IT，都沒有專精於基礎架構上的簡化[13]。問卷調查中提供了資訊科技風險管理人一些建議，使他們可以在資訊風險管理上開創更多的商業價值—改善資訊科技管理，而非僅僅確保企業不受資訊科技意外事件的影響。

第一，三大原則間的成熟度需均衡發展。若三大原則中僅一或兩者發展成熟，成效將遠不如三者皆發展成熟。舉例來說，專注於 COBIT 中的交付與支持（DS）過程而忽略 Risk IT 中的風險評估（RE）流程將可能誤導整體程序，或甚至浪費多餘的資金在不同層面的維修上。同樣的，建立起龐大的風險治理制度卻沒有改善資訊科技基礎架構與風險意識文化，就像是人盛裝打扮後卻漫無目的一般。由其是在當今競爭激烈的經濟環境下，風險管理者必須專注以創新且全面性的方式來投資與評估，而非僅修正某些常見的風險。

第二，成熟度需經由三大原則來評估與改進。風險管理者可藉由 Risk IT 或其它框架中的成熟度模型來評估自身組織[14]。接著管理者們必須指出各原則發展上的落差，經調整修正各原則後將整體成熟度帶向適切的發展。舉例來說，若一企業為 COBIT 營運商，該企業或許會擁有一些改善網路或倉儲的機制，但卻不知該如何建立客戶群。在這種狀況下，最明智的方式或許是先提升自身風險治理上的成熟度來改善企業資訊科技校準，使股東支持該企業後續上的投資。資訊科技治理流程在專注於資訊科技法規遵循與稽核的公司中會發展得較成熟，但管理人或許需不斷思考如何突破僅止於「紙上談兵」的運作模式，以突顯真正的營運衝擊。然而，或許亦有其他公司仍固守過度複雜的基礎架構，因而忽略可藉由簡化架構來降低營運風險的機會。

第三，資訊科技風險管理概念需與其他資訊科技及企業管理流程嚴謹整合。管理者們若可將資訊科技風險視為企業目標的一環，那麼便可將資訊科技基礎架構導向正確的方向—讓整體架構更簡化，而非只改善管理的部分。而這些管理者們也藉由讓員工了解操作性資訊科技風險的起因，及在資訊科技相關重大決策中突顯暗藏於其中的風險，來強化組織中的風險意識文化。以風險考量為基準的各項方案皆有助於資訊科技及商業主管們更精確調整其目標。

再者，藉由影響決策，風險治理可讓組織獲得事半功倍的成效，而非一昧固守遭風險蒙蔽的決策結果。它降低意外的發生，同時讓基礎建設更加成熟，企業獲利也因此提高。舉例來說，任職於信用卡公司及加拿大銀行的作業風險管理者表示當檢視企業流程風險時，他們都發現能有效重組企業流程的方法。因藉由提升企業效益與服務品質，他們原先在風險管理上的投資已得到相當大的回報。

最後，資訊科技主管們可與其他擁有共同目標的主管們一起合作，來讓資訊科技相關活動所產出的結果更好。資訊科技治理、企業架構設計、企業持續營運、資訊科技法規、企業安全及專案組合管理等部門管理人都有理由強調風險及其報酬的重要性、更簡化的基礎架構以及更具風險意識的企業文化。潛在的企業夥伴在投資的先後順序及專案執行上通常都較風險管理者有影響力。相對來說，在風險考量上，風險管理者有時也可幫助這些夥伴的新提議在組織內部更加合理化。舉例來說，許多企業架構設計工程師發現遵守沙賓法案中風險相關條例有助於釐清一開始無法合理化的困難點。

**結論**

調查數據指出，上述三大原則：風險治理流程、資訊科技基礎架構、風險意識文化都已發展成熟的公司，很明顯較少發生意外，且資訊科技運作效益、企業調準能力及靈活度都較高。但發展成熟意味著這些公司須著重在比基礎更深一層的地方，而非僅僅只有辨識風險、固守既有資產與提高查覺週遭威脅的能力。擁有成熟風險管理能力的公司懂得以風險治理來降低基礎架構的複雜度。他們不僅只會察覺風險；而是在查覺風險之外，建立起在組織中可以恣意探討風險議題的文化，且一切相關討論都被視為合理。他們不只降低意外發生的機率，同時亦提高了企業整體效益。而這些企業在風險管理的投資上所獲得的報酬，除了造就更有效益的風險管理外，也造就了更有效益的資訊科技管理與企業成果。

## 作者簡介

The authors continue their research into IT and enterprise risk management. If you are interested in being a case study or survey participant, please contact George Westerman at georgew@mit.edu or Brian Barnier at brian@valuebridgeadvisors.com.

### 註

1. Westerman, George; Richard Hunter; *IT Risk: Turning Business Threats Into Competitive Advantage*, Harvard Business School Press, 2007
2. This article is the third paper based on this research. Previous papers are: Westerman, G.; B. Barnier; "How Mature Is Your IT Risk Management?," MIT Sloan CISR Research Briefing, vol. VIII, no. 3C, December 2008. Westerman, G.; B. Barnier; "IT Risk Management: Balanced Maturity Can Yield Big Results," IBM white paper, February 2009.
3. Op cit, Westerman and Hunter
4. CobiT (IT Governance Institute, 1996-2007) is an IT governance framework and supporting tool set that allows managers to bridge the gaps among control requirements, technical issues and business risks. CobiT enables clear policy development and good practice for IT control throughout organizations. More information is available at www.isaca.org/cobit.
5. As defined in Risk IT (ISACA, 2009, www.isaca.org/riskit), "Any metric showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk tolerance is a KRI." KRIs are described in more detail in section 7, "Essentials of Risk Response," of Risk IT.
6. Westerman, G.; R. Walpole; "PFPC: Building an IT Risk Management Competency," MIT Sloan CISR Working Paper #348
7. Op cit, Westerman and Hunter
8. The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM (The Public Risk Management Association), A Risk Management Standard (ARMS), UK, 2002, www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf
9. Standards Australia and Standards New Zealand, AS/NZS 4360:2004, Australian/New Zealand Standard for Risk Management, 2004
10. Committee of Sponsoring Organizations (COSO) of the Treadway Commission, Enterprise Risk Management—Integrated Framework (COSO ERM), 2004. This should not be confused with the COSO Control Framework that is familiar to many CobiT practitioners. A summary of COSO ERM is available at www.coso.org.
11. Office of Government Commerce, IT Infrastructure Library V3, UK, 2008, www.ogc.gov.uk/guidance_itil.asp
12. Val IT (ISACA, 2008, www.isaca.org/valit) is an ISACA framework and supporting publications addressing the governance of IT-enabled business investments.
13. To cover this, ISACA provides a 281-page mapping from CobiT to The Open Group Architecture Framework (TOGAF). See ISACA, CobiT® Mapping: Mapping of TOGAF 8.1 With CobiT® 4.0, 2007, www.isaca.org/cobitmapping.
14. Readers are welcome to contact the authors for the short set of assessment questions used in their research.

Feature

# 財務審計所需評估之基本資訊科技控制(上)
# The Minimum IT Controls to Assess in a Financial Audit (Part I)

作者: **Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA** is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. In 1999, he Alabama Society of CPAs awarded Singleton the 1998-1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the ISACA Journal.

譯者: 孫嘉明, CISA, ISO27001 LA,雲林科技大學會計系 助理教授

資訊科技一般控制(ITGC: IT general control)的某些領域，幾乎對整個財務審計有著重大的影響，其控制失效的潛在風險，因為與財務報導及作業相關，而可能導致重大錯誤報導的風險(RMM: risk of material misstatement)。因此，這些重要的IT控制項目可適用於各個進行財務審計的組織，並且應當依據評估出來的風險，考量其對於財務審計目標的影響。

在風險評估程序中，如何制訂出合適的資訊科技一般控制關鍵議題，並不容易。由於資訊科技所涵蓋的範圍廣泛，使得就算是內控制度良好的組織，仍然可能存在著一些潛在資訊科技風險，導致有太多的風險因素都可能被IT稽核人員判斷為潛在問題。尤其對於偏向IT專長背景和僅有IT查核經驗的稽核人員而言，更將難以判斷何者為與財務審計相關的查核項目。因此，新手的IT稽核人員將傾向將各個IT問題都視為控制上的缺失，但實際上並不是每個IT問題都具有導致財務報導出現重大錯誤的風險。

本系列文章主要分成（上）（下）兩個單元，介紹IT稽核人員如何訂出與財務審計相關的重要稽核範圍，以發展所需IT稽核程序[1]。首先，本文先說明如何依據查核對象的整體IT環境複雜程度，以決定IT稽核的主要範圍。另外，在後續的文章中將說明財務審計相關最基本IT控制的五大類型。

## IT複雜度的判定

在SAS第94號[2]「審計人員於資訊科技對財務報導相關控制之考量」(“The Effect of IT on the Auditor’s Consideration of Internal Control in a Financial Statement Audit”) 中提及資訊科技對財務報導的影響，不必然與組織的規模大小相關，而應當由資訊科技的複雜程度判斷其影響力。例如，有一家中小企業，利用電子資金轉帳(EFT)支付員工薪資與供應商貨款，以及利用即時網路連線的資訊系統管理企業的各式交易活動；那麼即使這家公司，員工數少於50人，企業規模不大，但卻應視為擁有中高度的IT複雜度。相對而言，如果一家擁有數百個員工的公司，但卻是僅使用簡易的小型商業套裝軟體(COTS：commercial off-the-shelf)處理公司的業務，則該公司的資訊複雜度反而較低。

為了方便辨別與討論，資訊科技的複雜度通常被區分為低、中、高度，也有可能採用1級、2級、3級表示。雖然資訊科技的複雜度仍存在部分主觀的認定而沒有絕對客觀的標準，但是區分企業的IT複雜度，將有助於選擇相關的查核議題與查核程序。

一般而言，資訊科技的複雜度與查核項目的數量及所需的查核程序證實效力成正比，例如：若公司的IT複雜度較低[3]，則可能僅採用較簡單的查核程序(如詢問和觀察)，查核程序的步驟較為簡略；相反的，若公司擁有較高的IT複雜度，則其財務審計風險較高，故需要更有證實效力的查核程序，例如：重新計算或是驗證而非僅僅只是詢問和觀察。

為了要幫助IT稽核人員評估查核的範圍，故以下提出可供評估IT複雜程度的模型，此模型還可以用以幫助產業的領域專家(如中小企業)或IT稽核人員(如CISA：國際電腦稽核師)判斷是否需要在財務審計活動中增加特定的IT查核程序，或是由一般的財務審計人員自行執行相關的IT查核程序即可。

**IT複雜度評估模型**

我們將企業的IT複雜度分為三個等級，各個等級的分類特徵及區分標準，如表一所示。但這些分類的評估標準僅限於與財務資訊系統相關的資訊技術及作業流程有關，而那些與財務報導沒有直接相關的資訊科技因素，其風險將予以忽略。

第一級(level 1)指的是擁有較低的IT複雜度，一般來說可能只有一台與財務報導有關的伺服器，數量有限的個人電腦工作站(不多於15台)，沒有財務報導業務相關之遠端連線位置，採用標準的的套裝應用軟體與基本設備環境，未採用或僅少數之新興或先進資訊技術，而且沒有線上交易活動。與財務報表有關的內部控制(ICFR)並未過度依賴資訊科技或套裝軟體的系統控制機制，或是僅有極少數的人工作業與控制。許多的小中型企業都符合這個層級的描述，這個層級所需的IT稽核程序較為簡略，故一般的財務審計人員稍加訓練後即可自行執行查核。

表一、IT 複雜度評估基準

| IT 複雜程度 | 1：低 | 2：中 | 3：高 |
|---|---|---|---|
| 伺服器數量 | 1 | 2-3 | >3 |
| 網路作業系統類型 | 標準套裝系統 | 非標準套裝，或使用一種以上的系統環境 | 使用多種的作業系統環境或廣域網路 |
| 工作站數量 | 1-15 | 15-30 | 30 台以上 |
| 應用程式 | 標準套裝系統 | 部分模組採用客製化 | ERP 或自行客製開發 |
| 遠端連線點數 | 無 | 1-2 | >2 |
| 財報相關控制(ICFR) | 現成或少量 | 中等數量或手動 | 大量 |
| 新興資訊科技 | 無~少 | 少~中等 | 中等~多 |
| 線上交易系統 | 無 | 少 | 多 |

第二級(level 2)的IT複雜度為中級，一般來說可能擁有超過一台與財務報導業務相關的伺服器，採用多種不同的網路作業系統，或是為非標準的網路作業系統環境；個人電腦工作站的台數較第一級更多(level 1)，但仍不到30台；在應用系統上，可能有部分為客製化的系統；與財務報表有關的內部控制(ICFR)對資訊科技控制的需求為中度依賴；且已採用一些新興或先進的資訊技術，和部分的線上交易活動。這個層級已經需要領域專家或電腦稽核師協助設計或執行必要的IT稽核程序。

第三級(level 3)為高度IT複雜度，這個層級通常擁有三台以上與財務報導相關的伺服器；個人電腦工作站一般都已超過30台；可能採用大型ERP

系統或是全部自行客製開發的應用系統；採用了大量的新興先進資訊技術；或是具有大量或頻繁的線上交易活動。此類的企業，通常需要一個或多個領域專家或IT稽核人員來協助執行適當的IT稽核程序。

## 結論

此篇文章為系列文章中的第一部分，其討論的重點為決定企業的IT複雜度，用以判定IT稽核的範圍，進而決定所需的稽核程序。也就是說，資訊科技複雜程度越高的企業就越可能需要較多或較完整的IT稽核程序。而第二部份的文章將在下期發表，其內容主要說明如何針對ITGC的五個領域進行查核，且採用本文中的IT複雜度評估模型決定查核的性質、時間及範圍。

## 註

1. Singleton, Tommie; “What Every IT Auditor Should Know About Scoping an IT Audit,” ISACA Journal, vol. 4, 2009
2. The use of the term “IT sophistication” implies that, as the IT portfolio becomes more sophisticated, there is more likelihood of RMM related to IT. Thus, occasionally, for clarification of reading, the term will be stated as “IT sophistication and relevance.” That relevance is the back end of the IT sophistication process, where eventually the IT auditor in a financial statement audit must eliminate IT-related controls, problems and risks that do not represent RMM and cannot be directly linked to RMM. That is, only those IT issues that could lead to a material misstatement are relevant to the financial audit and are included in the IT audit procedures. But, that level of risk is invariably directly associated with the level of IT sophistication of the entity.
3. The risk-based standards state that inquiry alone is not sufficient to gain adequate assurance over some control in the further audit procedures. Thus, some other type (“nature”) of procedure would be needed to complement inquiry, and the lowest level “nature” procedure other than inquiry is observation. Thus, for a “low” level of risk where some procedure is being designed, something other than simple inquiry would need to be included. Examination and reperformance are considered “stronger” types (“nature”) of procedures in a financial audit.

Feature

# 要綠環保還真不簡單：綠 IT 對於電腦審計人員職業生涯的衝擊

# It's Not Easy Being Green: How the Green IT Movement Is Impacting Careers in IT Audit

作者: **Michael Juergens CISA, CGEIT**

is a principal with Deloitte & Touche LLP, where he specializes in IT auditing. His background includes numerous IT security, audit and control assessments for a variety of companies in a wide range of industries. He is a sought-after thought leader and speaker on IT controls topics, and has served as an expert legal witness in litigation related to IT security and controls. He has also taught graduate-level IT courses at the University of Southern California (USA) and the University of California, Irvine (USA).

譯者: 張騰龍, CPA, CISA, ISO27001 LA 安永聯合會計師事務所風險管理諮詢部執行總監

政治環境和社會風俗在過去幾年來引發無數的企業提倡企業社會責任（CSR）。隨著經濟環境的衰退，企業再度將營運重點從極有善意但昂貴的企業社會責任倡議轉至於營運收益。但還是有一大例外，那就是“綠IT “。 綠IT計劃佔據了獨特的地位，它可以同時實現公司的社會責任及財務目標。因此，雖然有一些企業社會責任案件因經濟環境的衰退而被擱置，綠IT方案卻被積極的爭取及實施。

綠IT方案的實施結果好壞參半。有一些企業通過綠化資訊科技措施而得到優良的成果，而也有其他企業就沒有那麼幸運。一個綠IT計劃的成敗取決於多種因素，而這些因素對於各企業而言並非一致的。本文不會試圖解決這一挑戰。反而，本文將假設綠IT行動，至少在短期內，將繼續發展下去，並將集中於討論綠IT的演變將會如何影響電腦審計人員的職業生涯。

這已經不是第一次電腦審計人員不得不與迅速變化的IT環境抗衡。企業資源規劃（ERP）系統的普及化，Y2K轉換，電子商務的盛行對企業的IT環境都有重大影響。這些變化也都挑戰電腦審計人員不得不提升自己的技能並重新設計審計策略。同時，這些變化賦與電腦審計人員在職業生涯中成長的機會。綠IT運動也沒有什麼不同。能抓住這一次機會而成長的電腦審計人員將比那些沒有把握機會的同行更為成功。

綠IT會如何影響電腦審計人員的職業生涯呢？如同上述的IT環境演變（例如，ERP普及化），這些變化將採取多種方式形成，而每種方式都有不同程度的複雜性。有一些綠IT計劃（如資訊環境虛擬化）對於電腦審計人員而言可能代表多幾天的教育訓練。本文將點出幾個重大的變化以提醒電腦審計人員在這個受綠 IT影響的環境下如何管理自己的職業生涯。

## 變化中的電腦審計領域

綠IT方案改變了固有的IT環境。綠議題，例如雲端計算，資訊環境虛擬化，系統外包和數據中心的重新設計都會對影響到電腦審計人員執行電腦審計的範圍與組件。這就產生了兩個問題：

1. 今年的電腦審計範圍是否應包含綠 IT 來頻估整個公司的環保措施？
2. 環保控制目標是否應該被包含到每項電腦審計？

從表面上看，這似乎是兩個很容易回答的問題，直到電腦審計人員需要做深入及詳細的審計規劃為止。例如，一家企業為了改善空氣流通以及降低能源成本，想要執行一個電腦機房的重新設計。

電腦審計人員的查核範圍是否只包含電腦機房的重新設計的部份，然後下一個月再執行另外一個年度的電腦機房安全和環境控制查核？或者，這兩次的查核應一起執行？其實這個問題沒有正確答案，因為每個環境都是不同的，但它是值得的電腦審計人員思考的議題。

這個問題會因政治，時間與可用的資源等因數，更加棘手。有一些IT部門可能會主動的邀請電腦審計人員參與相關綠議題的規劃。但也有其他IT部門可能希望電腦審計人員將其查核範圍僅限於對財務報告有影響的IT控制，不包括綠IT計劃在其範圍內。電腦審計人員同時也須考量預算和資源的壓力。即使大家同意應把綠IT包含在查核範圍內，電腦審計人員仍需嚴謹評估是否有足夠的資源來完成此查核範圍。

**建議**

電腦審計人員應於案件規劃時先了解企業有哪一些綠IT活動正在策劃中，正在進行中或剛完成。這將協助電腦審計人員判斷審計範圍應如何改變。將這些綠IT活動與IT審計活動互相比較，電腦審計人員應能了解如何應變。首先，電腦審計人員可考慮添加一些綠IT查核程序於其查核策略，或者要求執行更全面性的審核程序或更完整的綠IT審核案件。有可能影響企業關鍵任務系統的重大案件應要求電腦審計人員參與。經思考過綠IT可能對IT審計的影響，電腦審計人員可更有效率的控管IT審計資源。

**審計結果和報告的變化**

綠 IT活動正在改變IT部門的運作模式。有遠見的電腦審計人員了解這些變化並會修改相應的查核程序和發現事項。有一些綠IT的解決方案出現一些與 IT控制目標不一致做法，甚至有可能是相互排斥的。

例如，誰會忘記不久前有多少IT部門追求高可用性 (high-availability) 策略？此策略理論上來講是合理的：於IT環境中建立備援建設以消除單點故障的機率。理論是，如此一來任何一個單一的設備故障就不會中斷資訊服務。 電腦審計人員非常樂見如此的發展因為他們終於可以解決以往對於災難恢復計劃所出具的查核發現。

對現在來講，這些備援建設代表的是浪費與耗電。綠IT方案可能會開始刪除這些備援建設，這將有助於降低成本以及實現綠 IT的目標，但電腦審計人員也將因此陷入困境 – 要認定綠IT方案所帶來的結果為“優良改善“和“成功案例“還是認定為“缺失“和“查核發現。“

**建議**

解決這個問題的最好方法是把重點放在與IT部門的事先溝通。電腦審計人員應於規劃案件時先了解企業的綠IT策略以及案件規劃，並密切關注案件項目，如系統整合，虛擬化，資訊環境控制修改和移除現有的IT系統硬體與軟體。通過了解企業於其綠IT策略下會執行的改變，電腦審計人員可以主動識別這些綠IT計劃可能造成的資訊安全與控制問題，並與IT管理階層事先討論以防患於未然。

在某些情況下，電腦審計功能可能會在變化發生之後才被告知，限制了它對於可能造成控制問題的決策的影響力。如果是這樣，電腦審計人員應當了解查核目標已經改變並考慮新的目標及其優先順序。這需要電腦審計人員於論述查核結果與撰寫查核報告時更加細心。電腦審計人員應設法從IT部門的角度來看待查核結果，同時也需考慮是否延長案件時間表以能完成與IT部門額外的討論。

## 更多的增值機會

電腦審計人員一般都希望由其查核結果能提出對企業有增值機會的建議，或能將 IT 控制和風險的觀點和經驗帶入 IT 案件中。但能辨識出對企業能增值的機會並不多，特別是當電腦審計人員每次都只查核法令遵循所必要的控制及範圍。

綠 IT 是一個機會能夠讓電腦審計人員從新參與關鍵業務策略並帶入能增加股東權益的觀點於 IT 案件中。例如，儘管許多電腦機房於建造時都是經過精心策劃的，但隨著時間的改變，資訊設備的採購決策往往基於電腦機房空間考量，而不是基於如何幫助減少電腦機房的冷卻用電需求。往往一個簡單的電腦機房冷熱主機的交互安排可以大幅提高機房內的空氣流動率，並相應的降低電力成本。這不代表主機的交互安排可很簡單的完成，但一般至少不需要大量的資本開支。

電腦審計人員也可以協助 IT 部門建立新的個人電腦綠政策。例如，屏幕保護程序比睡眠模式需要使用更多的電力。個人電腦、印表機設置和其他設備的節能設置對能源消耗可以有很大的影響，同時也可提高安全性控制。

最後，許多企業正在尋找相關的”綠成就”來當宣傳議題。電腦審計人員可以主動協助企業提倡這樣的議題。這樣，他們不僅能帶給組織實質的價值，也可以增加他們的個人在組織內的知名度。

## 建議

想出新辦法。綠 IT 是一個還在成長的領域，目前並沒有一個清單能告訴你如何做是正確的。能夠達到節源效益的機會將處於每個個別環境的細節中。在許多企業中，電腦審計人員可能比 IT 人員更了解企業的廣大 IT 環境，因此，電腦審計人員可能可以看到被 IT 人員所錯過的機會。

電腦審計人員必須繼續教育自己才能提出展新的思維，並提高自己的知識範圍：硬體，作業單位，空調系統，稅收補貼和獎勵，建築設計軟件等。會花額外的時間來持續教育自己的電腦審計人員才能夠繼續增加股東價值並帶給 IT 功能和企業有價值的觀點。

## 結論

綠 IT 改變了企業如何看待其 IT 環境與規劃。這對電腦審計人員來說代表了挑戰與機會。綠 IT 是一個持續發展的領域，接受它的電腦審計人員將於其職業生涯中得到好處，而那些排斥它的電腦審計人員將面臨客戶 IT 管理階層的挑戰。電腦審計人員應想想客戶的 IT 環境正在如何的變化中，並開始評估如何重新設計一套適用於該環境的審計策略。

## 作者簡介

Feature

# 資訊安全稽核的社會心理學
# 從被稽核者的角度稽核: 避免認知失調

## The Social Psychology of IT Security Auditing From the Auditee's Vantage Point: Avoiding Cognitive Dissonance

作者: **Thomas J. Bell III, Ph.D., CISA,**

is a professor of business administration in the School of Business at Texas Wesleyan University in Forth Worth, Texas, USA, and an IT security auditor for ComputerMinds.com in Euless, Texas, USA. His IT auditing specialty is IT audits for small community banks (IT security audits and external penetration testing) and SAS 70 Type I and II audits. Bell has published quarterly material for the Business/Technology Chapters of Continuing Professional Education (CPE) Direct, which is released in conjunction with the American Institute of Certified Public Accountants (AICPA)'s Journal of Accountancy.

譯者: 洪嫚君, 安永聯合會計師事務所

獨立性、客觀性與公正性皆為重要的稽核指標，但若稽核者希望其專業意見能為企業治理與資源分配評估帶來具建設性的見解，上述指標將更是稽核必要條件。然而，這看似無害的形容詞卻充滿著諷刺與不和諧。或許心理學家 Leon Festinger 的認知失調理論(**Cognitive Dissonance Theory**)能對於了解此議題有所幫助。該理論檢視了一種特殊的心理現象，就是當個人信仰與行為出現差異時所引發的不安。依據該認知失調理論，人的心理總會希望其思考 (如信仰、意見) 與其行為一致。而當態度與行為出現了不一致性 (失調)，人會不自覺的想去除其失調性。將此套用至資訊的環境，當審計人員的思考與其道德準則有邏輯上的矛盾時，則會出現所謂失調的現象。ISACA 對於審計人員的專業道德準則有以下說明:

*履行職責時應保有客觀性，盡其所能與保有專業素養，並遵循專業標準與最佳實踐 (Best Practices)。*[1]

本文探討審計人員的客觀性及其職責，此為兩個不可或缺的軟技巧，並從社會心理學的角度，深論資訊安全稽核的執行與了解被稽核者的思想、感覺、行為及作用[2]。一些人類社會行為學所持有的原則，事實上能夠教導審計人員許多有用的技巧，以利提供於增進稽核服務。

許多資訊科技專家都會同意，資訊安全的重點在於人多過於政策、控制或者是科技。同理而論，人 (員工) 對於資訊安全所帶來的威脅也遠勝於外人。

總結這些觀察結果，改善資訊安全取決於改變被稽核的員工與審計人員的信仰、態度及行為。而社會心理學可以協助審計人員了解人類的嗜好與傾向，以利達到改善資訊安全的最終目標。

當審計人員的獨立性與客觀性被先入為主的觀念或一般概論所損壞時，則會導致社會心裡學裡所說的失調。此論調與之前所敘述 ISACA 專業道德準則與客觀性、盡職與專業素養，形成強烈衝突對比，先入為主的觀念或一般概論無疑會損壞審計人員的客觀性。

資訊稽核的目標是為了在測試某個系統後，能針對其公正的評估提供一個意見。基於時間與資源的短缺，審計人員無法測試整個資訊系統架構，故僅能審視整個系統的一小部分。因此，當審計人員找到不符合標準或資訊安全漏洞，對於被稽核者來說較具爭議性，但審計人員卻認為是公正的。

然而，受查客戶的人類心裡學卻常常被忽略(當在蒐集與評估企業的資訊系統、實踐與行動相關的證據時)，並通常重點會放在流程而非客戶。以許多方面來說，稽核應是人際關係業務。

因此，審計人員應該了解稽核的社會心理學或關於人的那一面，此為超越標準、程序與最佳實作的稽核。當然，取得或評估證據的流程以了解資訊系統是否足夠保護資產與維護資料完整性，並同時能有效率的達成企業目的與目標，是非常重要的。然而，了解資訊安全稽核的社會心理學也是與稽核流程與程序有著相同的重要性。Doug Schweitzer，一位網路安全專家與自由寫作者曾說過：

*安全不僅止於保護你的網路不受外部威脅; 也應同時確保其不受內部威脅。安全的第一步是警戒，故讓您的員工了解不僅止於潛在的風險，更必須能夠判別或避免此類的風險，是非常重要的。教育及警戒會讓每個員工了解，各個角色在保護企業網路所需盡到的職責。*[3]

若要說服受查客戶變的更有安全意識則需有效的溝通並讓他們知道自己的職責，及審計人員會如何提供相關的協助使組織的資訊資產能更受到保護。然而，若組織的員工是非常天真、缺乏訓練或缺乏安全危機意識，則不可能有任何安全控管或科技可以成功的保護一個組織。這讓我們再次了解到，安全取決於人多過科技。因此，改善資訊安全取決於改變受查客戶的信仰、態度與行為。社會心理學使我們能更加了解人類的偏好與傾向，並使審計人員能更容易達成改善資訊安全的目標。

**認知失調理論**

半個世紀前，社會心理學家 Leon Festinger 提出了認知失調理論[4]。認知失調是當同時有兩個相互矛盾的想法時，所產生的一種不舒服感覺。與思想相關的問題包括了態度、信仰與個人行為的認知。認知失調的理論闡述了人們為了想要減低失調時，而改變他們的行為、信仰與行為或合理化辯解他們的態度、信仰與行為。

通常當人們感受到一種思想邏輯上的不協調時則會產生失調。當一個想法隱含著相反的想法時，則會發生這種情況。例如，若審計人員於稽核前有先入為主的想法，則違反了 ISACA 專業道德準則。當意識到了此矛盾感則會引起失調，而這會導致情感上情緒的變動，如壓力、焦慮、羞恥、內疚、憤怒和尷尬。受查客戶可能也會體會到失調當他們笑並需誠心的同意協助審計人員，當事實上受稽核者可能感到審計人員：

- 為了找到問題而忽視正確的做法
- 盲目的遵從一套陳舊的法律與法規，當他/她知道那些已不再符合現況
- 只是為了要做管理階層的骯髒事 (如，解雇員工)
- 沒有正確的評估風險的重要性與為了去除其風險所需付出的代價
- 詢問一些不聰明的問題
- 未能察覺系統如何運作，導致一直詢問相同的問題
- 要求取得沒人會閱讀或根本不存在的文件
- 浪費時間取得文件或執行無意義的測試
- 僅是為了找到錯誤而來訪並將錯誤報告給老闆

因受查客戶的這些感受，導致客戶可能對審計人員隱瞞、漏報、甚至隱藏某些資訊。這些矛盾的情感會使被稽核者感到焦慮並導致合理化。(創造更多理由或原因來支持其行為的傾向)

Festinger 的認知失調的理論是基於以下三項基礎假設：

1. **人類對於行為與信仰的不一致產生的敏感度。**被稽核者在某種程度上都會意識到其信仰、態度及意見的不一致性。事實上，可能有人會爭論說，每個人都有個內建的濾網並

於行為與想法產生不一致時會發出警報。

2. **當意識到這種不一致性時會造成失調並促使其想解決這種失調。**當一個被稽核者意識到她/他已冒犯了個人原則，則會產生某種型態的精神折磨。而失調的程度則會因個人信念的程度與行為及行動的不協調的程度而異。想要解決失調的慾望也會隨著失調的程度按比例增加。

3. **失調會藉由以下三種基本方式被解決：**

- 改變信仰—或許最根本解決行為與信仰的失調方式就是改變信仰。不知道是有幸或不幸的，個人的基本信仰與態度都有一定的穩定度，而並不能被輕易的改變，除非他們能了解或意會要改變的理由。雖然這個選擇看似簡單，卻不能輕易達成。
- 改變行為—第二個選擇則是停止—永遠不要再有相同的行為。然而，負面的情緒 (如:內疚/焦慮) 通常是不易被修改的。這個選擇通常會產生另一個問題，因人通常會合理化負面的情緒以減輕他們需改變行為的程度。
- 改變對於行為的看法—這是第三個也是個較複雜的解決方法，就是改變一個人如何觀看、記得或感受一個行為。這也就是，合理化的發生。例如，被稽核者可將拒絕與審計人員合作合理化，因為認為審計人員只是在浪費時間。或著，他們也可以說，因為大家都拒絕跟審計人員合作，所以有何不可? 藉由參與一些思想練習，被稽核者可以重新將他們的行為套入不同的想法與環境，這是為了調整他們的看法以讓其信仰與行為對齊。這種行為通常對於他人是顯而易見的，但對於本身卻是較難感受到的。

## 資訊安全的警覺性

一個能教導並讓受查客戶同時參與的資安警覺流程才能有效的使組織的資訊資源更加的安全。使大部分的員工能確實的掌握相關訊息是有效降低資訊安全風險最具經濟效益，且能協助審計人員的方式。若要改變受查客戶的負面想法，最需要了解的是受查客戶的行為模式，這通常是造成誤解的核心問題。審計人員應了解受查客戶如何：

- 私下建立制度，給予審計人員表面上看似無止境的控制測試另外的意義
- 因先入為主的觀念，無意中扭曲他們了解與配合稽核流程的能力
- 因為誤會，對審計人員有不良或負面的行為或反應，並更加惡化雙方溝通不良的情形，最後導致合理化與概括理論並造成更多反抗行為

稽核最常被忽略的目標，就是要讓每一個使用者慢慢的建立起資安意識。事實上，許多研究都顯示，當人們了解為什麼該做一件事時，會更加的想要去配合執行。一個研究指出，當動物園將標示從:“請離籠子三尺遠”改至“動物會吐口水，”就大大的轉變了動物園顧客的行為。只是簡單的解釋了安全距離就足以帶來正面的反應[5]。在改變標示前，遊客會坐在或靠在安全護欄上，但在了解需求的理由後，遊客們在看動物時都會自動站在比三尺更遠的地方。改變動物園遊客的想法或信仰，最終改變了他們的行動，而這正證實了認知失調理論。

稽核最初是被設計成一種教導人的專業，並為了能將他人的錯誤及負面行為或做法紀錄成查核發現事項。以往審計人員會在未通知的情況下，突擊客戶，這對客戶隱喻著驚愕或不信任的訊息，並說明著審計人員的目標僅是為了能夠抓到客戶做錯事。或者，更嚴重的，審計人員會在未跟客戶解釋前要求客戶做調整或修改。

為了達到安全意識的目標，審計人員必須放棄使用控制做為量測標準，並使用有效的

溝通減低風險。一但被稽核者了解到他們擁有保護組織資訊資產的資源與權利，將會以實際行動來回覆。為了達到安全意識不可或缺的部分就是讓被稽核者改變原有的主觀意識—就是稽核在無意識下所製造的問題。

## 結論

從被稽核者的角度看資安稽核，這種社會心理學是自相矛盾的，因人類雖是一樣的卻也各自有所不同。人類雖於生理上是相同的(眼睛、耳朵、鼻子、嘴巴、心智等) 並分享著一樣的生理需要 (空氣、水、食物、衣物、住宿)。但反過來說，人類也是獨一無二的，情感上、身體上、心智上，並有著不同程度的意志。這足以說明，平等對待每個人，卻也同時保有能發現各個人差異的敏感度，在這兩者中間維持一種平衡是個很大的挑戰。

人類執行稽核時會帶著自己的看法，並被其偏好與傾向所影響著。被稽核者應該了解在人類行為層面上，行為與安全狀態是穩定的，並兩者會隨著新的與不斷在變化的資安風險所影響著。安全的觀念是組成態度與信仰的前身，並最終會形成安全印象[6]。了解認知失調理論，並運用其基本社會思想結構因子或稽核認知，可協助稽核人員避免稽核失調；這可能會損害 ISACA 專業道德準則所述敘的客觀性、盡職與專業素養或是最佳實作。以下總結是一些社會心理學較有名的理論。這些原則，沒有任何特別的排序，指出稽核者如何可以避免稽核失調:[7]

- 花費心力在參與資安認知上，並涵蓋許多現實上安全需求與違規行為的例子
- 努力提倡安全的承諾，而不是僅僅描述它
- 將重點放在進步而不僅是減低失敗
- 聆聽並了解，員工與管理階層目前的資安信仰
- 不要表揚或以正面形像或言詞讚美電腦罪犯
- 挑戰不在乎資訊疑慮或藐視資訊需求的員工，千萬不要忽略這種態度或信仰
- 辨識在往後會成功立下正面影響的資深管理層
- 鼓勵某個員工去承擔工作團隊裡資訊安全的公共職責
- 與管理階層合作 建立一個能獎勵負責任的態度，如: 舉報資安違規的文化
- 貢獻精力於建立一個受員工尊重的工作環境，解釋為什麼資訊安全是重要的，並說明每個員工對於系統安全所扮演的角色為何，以此作為支持資訊安全理念的行為；這比起在一個會貶低員工的環境推行資安是相對更重要的。
- 若有可能，在一般會議前，與各個參與者討論資安議題
- 保持中立並在資安會議時鼓勵公開辯論
- 適當的帶入外部的專家並響應團體思考，例行的在資安會議扮演挑戰的一方 (持有相反的看法)

## 註


1. ISACA, Code of Professional Ethics, www.isaca.org
2. Lippa, Richard A.; Introduction to Social Psychology, Wadsworth, USA, 1990
3. Schweitzer, Doug; “Security Lessons Learned—Employee Training and Education Can Mitigate Threats,” Processor Magazine, vol. 27, issue 20, 20 May 2005, p. 1
4. Festinger, Leon; A Theory of Cognitive Dissonance, Stanford University Press, USA, 1957
5. Randolph, Alan; Getting the Job Done! Managing Project Teams and Task Forces for Success, Prentice Hall, USA, 1992
6. Op cit, Lippa
7. Ibid.

Feature

# 使用活頁簿和 Benford 法則來測試會計資料
# Using Spreadsheets and Benford's Law to Test Accounting Data

作者: **Mark G. Simkin, Ph.D.,**
is a professor of information systems at the University of Nevada (USA). He can be reached at markgsimkin@yahoo.com.
譯者:謝蕙萱，勤業眾信聯合會計師事務所資料風險管理顧問

會計系統是財務舞弊(Financial frauds)最常見的標的。原因呢，引用銀行搶匪Willie Sutton的名言，"錢都在那邊"。

舞弊者最常使用的犯案手法就是創建一個虛假的交易分錄，例如偽造一筆雇用記錄或供應商付款，然後根據自己的利益操作這筆虛假交易。密謀成功與否，端看是否能夠把這筆交易隱藏於合法交易之中，藉此逃過管理階層和審計人員的法眼。

有趣的是，多數的人並不擅長創造"自然資料"，使得優秀的審計人員可以運用一些簡單的統計工具去發現異常狀況。其中一種測試方法就是去看資料是否符合Benford法則。

Benford法則在探討自然產生數字的第一位數字的分布狀況。所謂自然產生的數字，例如供應商的付款、客戶的發票，和其他企業日常營運中發生的財務交易。舉例來說，供應商付款$123.45的首位數字是1。供應商發票$4,231.55的首位數字是4，以此類推。

與一般人的認知相反，Frank Benford發現首位數字並非呈現一個平均分配的狀況。相反的，數字1是最容易發生的，接著是2和3，以此類推。根據Benford法則，人員可以計算首位數字1、2....發生的次數，然後檢視它們的次數分配。第一位數值越小其出現的頻率就越大，而數值越大者出現的機率就越小，則此分配符合Benford's分配，為"自然"分配。如非，則數值有人工製造的嫌疑。

部分專業會計期刊已刊登了一些介紹Benford法則的文章(如文末建議)。但大部分的文章多偏重理論，或要求使用者去下載其它的軟體去進行統計測試。對EXCEL的使用者來說，這是非必要的額外花費。本文解說如何運用簡易的Excel公式來運用Benford法則進行測試

## 運用 Benford 法則去測試首位數字

舉公司舞弊最容易發生的地方—供應商發票之測試為例。雖然每張發票含有大量的資料量，本例僅針對採購金額做分析。目標是要運用Benford法則去瞭解這些交易是否為"自然"。圖1中列出測試的步驟，將於下列小節逐步說明：

### 步驟 1：選擇樣本

首先取得樣本資料並把他們存放到Excel活頁簿中。觀察的資料越多越好，最好使用一整年的資料。但如果測試項目數字很多，較小的樣本亦可。不過，基於統計推論之需，資料筆數最好超過100。(圖1僅為範例，

只顯示少於100筆之資料)

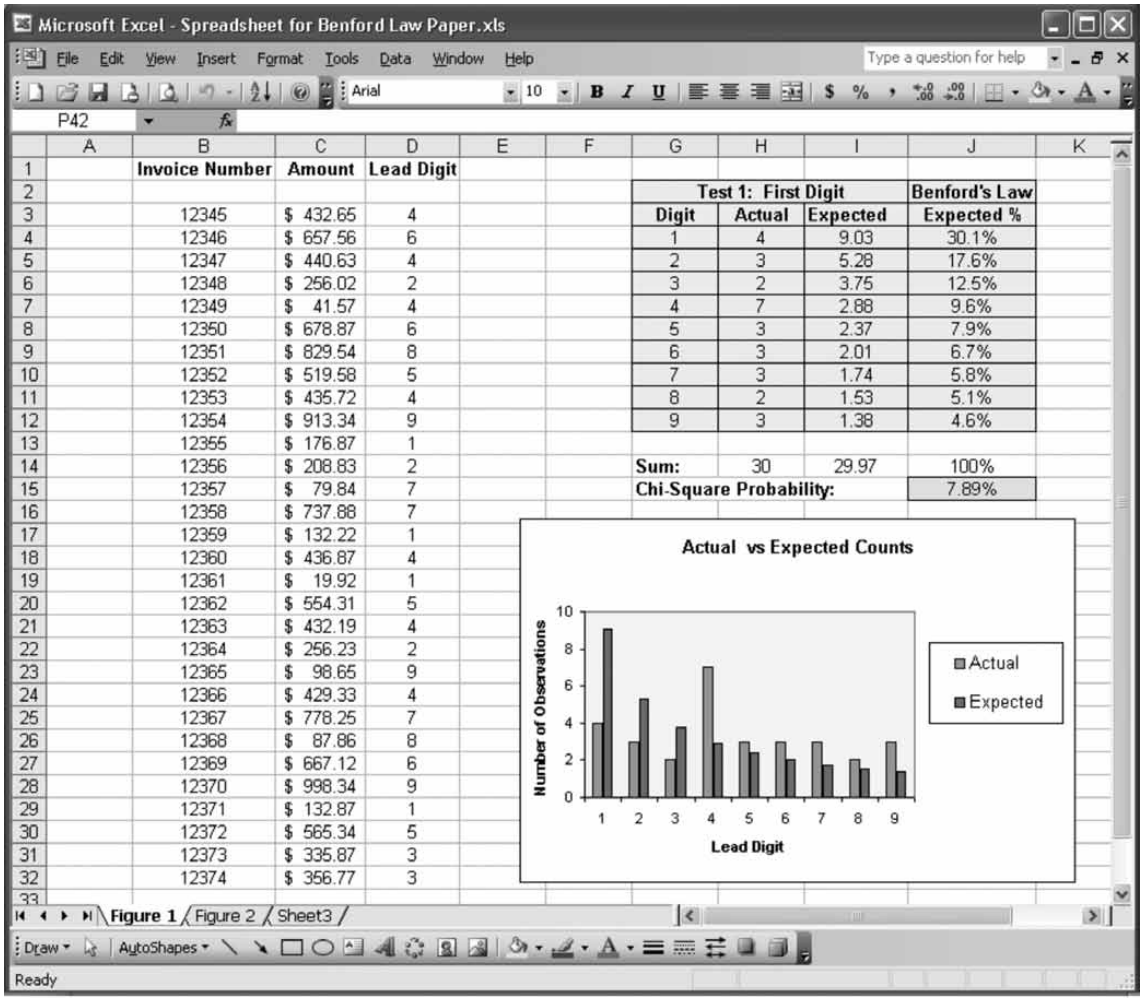
**步驟 2: 取出首位數字**

如前述，Benford 法則是要檢視首位數字的分配。實際資料的位數(如 $10, $100 or $1,000) 並不重要。在活頁簿中，我們可以使用EXCEL 的LEFT 公式來擷取首位數字。公式的格式如下：

=LEFT("資料項目", "字元數")

公式中，"資料項目"指的是資料所在的欄位，而"字元數"指的是要擷取的數目(從文字或數字的最左邊數過來)。舉例來說，如果"字元數"是2，則EXCEL 會把欄位中的資料從左邊數過來的兩個位數擷取出來， 如果"字元數"是3則 會擷取三個位數。在此我們僅需取出一個字元，故欄位C3的公式應該是：

=LEFT(C3, 1)




| | Invoice Number | Amount | Lead Digit |
|---|---|---|---|
| 3 | 12345 | $ 432.65 | 4 |
| 4 | 12346 | $ 657.56 | 6 |
| 5 | 12347 | $ 440.63 | 4 |
| 6 | 12348 | $ 256.02 | 2 |
| 7 | 12349 | $ 41.57 | 4 |
| 8 | 12350 | $ 678.87 | 6 |
| 9 | 12351 | $ 829.54 | 8 |
| 10 | 12352 | $ 519.58 | 5 |
| 11 | 12353 | $ 435.72 | 4 |
| 12 | 12354 | $ 913.34 | 9 |
| 13 | 12355 | $ 176.87 | 1 |
| 14 | 12356 | $ 208.83 | 2 |
| 15 | 12357 | $ 79.84 | 7 |
| 16 | 12358 | $ 737.88 | 7 |
| 17 | 12359 | $ 132.22 | 1 |
| 18 | 12360 | $ 436.87 | 4 |
| 19 | 12361 | $ 19.92 | 1 |
| 20 | 12362 | $ 554.31 | 5 |
| 21 | 12363 | $ 432.19 | 4 |
| 22 | 12364 | $ 256.23 | 2 |
| 23 | 12365 | $ 98.65 | 9 |
| 24 | 12366 | $ 429.33 | 4 |
| 25 | 12367 | $ 778.25 | 7 |
| 26 | 12368 | $ 87.86 | 8 |
| 27 | 12369 | $ 667.12 | 6 |
| 28 | 12370 | $ 998.34 | 9 |
| 29 | 12371 | $ 132.87 | 1 |
| 30 | 12372 | $ 565.34 | 5 |
| 31 | 12373 | $ 335.87 | 3 |
| 32 | 12374 | $ 356.77 | 3 |

| Test 1: First Digit | | | Benford's Law |
|---|---|---|---|
| Digit | Actual | Expected | Expected % |
| 1 | 4 | 9.03 | 30.1% |
| 2 | 3 | 5.28 | 17.6% |
| 3 | 2 | 3.75 | 12.5% |
| 4 | 7 | 2.88 | 9.6% |
| 5 | 3 | 2.37 | 7.9% |
| 6 | 3 | 2.01 | 6.7% |
| 7 | 3 | 1.74 | 5.8% |
| 8 | 2 | 1.53 | 5.1% |
| 9 | 3 | 1.38 | 4.6% |
| Sum: | 30 | 29.97 | 100% |
| Chi-Square Probability: | | | 7.89% |

因為C3的數值是"432.65,"所以跑出來的結果是"4"。錢字符號($)沒有顯示因為它是格式符號，Excel 公式運算時會把它掠過。在Excel 中針對第一個欄位將公式設好，可以複製到其它欄位。圖一顯示了這個結果。

**步驟 3: 建立次數分配**

接下來要建立首列數字的次數分配。首先建立

圖1 右方表格的表頭，而數字“1,” “ 2,” … , “9”要被放在第一欄，就在”Digit”欄名的下方 。

現在我們可以看到，針對這九個數字，有多少發票金額是以此為開頭(0被忽略了，因為以0 開頭的數字可以被縮短再被其它數字取代)。雖然可以用EXCEL 的計數公式來處理，不過使用COUNTIF 公式更簡單。此公式是用來計算某一資料區間內符合特定數值的發生次數。公式的格式如下：

=COUNTIF(資料範圍, 條件)

公式中，“資料範圍”指的是預定衡量的資料集合，而“條件”參數是文字或數值所在的欄位。舉例來說，公式COUNTIF(Z1:Z100, “Smith”) 會把資料範圍Z1:Z100中含有”Smith ”這個名字的欄位數目傳回來；公式COUNTIF(Z1:Z100, X3) 則會將資料範圍Z1:Z100中，數值等於欄位X3內數值的欄位數目傳回來。根據案例，我們想要了解測試數值中，每個九個數字的首位數字出現幾次 因此，在欄位H4—”Actual”欄名底下的第一個欄位，設下列的公式：

=COUNTIF($D$3:$D$32, G4)

一旦建立好COUNTIF公式，可以複製到表單中的其他欄位。圖1說明了這個結果。以本範例，首位字元是數值1 的狀況出現了四次，首位字元是數值2出現了三次，以此類推。

**步驟 4: 計算期望分配**

首位數字可能呈現甚麼樣的分佈? Benford’s 法則預測，約有30.1%的機率首位數字會是1；17.6%的機率首位數字是2，其餘依此類推。圖1 J欄中，列出了所有首位數字的百分比。Nigrini曾撰文詳細解說此統計分配的演算法(詳見建議閱讀Suggested Reading)。

從圖1中J欄列示的百分比，我們可以從樣本數30來進行推估。每個首位數字，期望數字是百分比乘以樣本數。舉例來說，首位數字是1的情形，期望數字應該是30.1% 乘以樣本數30，即9.03。因為H14欄位放的是所有的樣本數，因此I欄的第一個的欄位(I4)的公式就是：

=J4*$H$14

公式中，欄位J4 內容是百分比(如第一個項目的30.1%)而欄位H14 是整個樣本數—本例中的30。如果公式設定為欄位H4的絕對位置(如$H$4)，則公式可以直接複製到I欄到其他欄位。如結果顯示，首位數字為2的期望數字是5.28，首位數字為3的狀況是3.75，其他以此類推。當然，實務上是沒有辦法看到剛剛好有9.03張發票的首位數字是1，或5.28張發票的首位數字是2。此處的計算是用來告訴我們，以一個概略的，平均值的角度，如果使用不同的樣本，重複這樣的實驗可能會得出甚麼樣的結果。

**步驟 5: 繪製結果**

現在有兩列數值—首位數字的實際分配，以及由Benford法則理論推論出來的期望分配。我們想要了解的就是它們是否一致。

一個解決方案是去把兩個資料繪製成圖表來進行觀察。可以使用Excel 的繪圖工具，以直方圖的方式呈現(詳見圖一)。期望數值表達的是根據Benford 法則推出出來的狀態—首位字元為 1 期望值最高，接著首位數字2，以此類推。實際數值則顯示了目前樣本中的首位數字的實際分配。

繪圖工作有兩種作用。首先，針對樣本中發生的實際資料和期望資料是否一致的問題，圖表提供了一目了然的答案。以本例來看，答案是”不大符合”。我們可以看到，首位數字1發生的機率大概只有預測的二分之一，而首位數字4發生的狀況遠高於預測。

其次，圖表可以顯示資料異常狀況—如本例中

的首位數字4。當然資料異常不表示一定是有舞弊問題，但是數字確實是一種警訊。如果本例中的發票是公司採購，則首位數字4 的異常資料可能特別需要高度重視，如果每位採購人員有特定的採購金額上限。曾有審計人員於查核中發現，採購部門主管開了很多張金額剛好稍少於$5,000的支票，原因是為了迴避公司採購金額超過$5,000就要進行招標程序的規定。

**步驟 6: 執行獨立性檢定**

雖然樣本和期望值不一致，另一個尚待釐清的問題是—"有多麼不一致"。審計員可以使用Excel的獨立性檢定(CHTEST)公式—卡方檢定—來獲得協助。獨立性檢定又被稱為"配適度"(goodness-of-fit)檢定。亦即，此統計檢定在測量樣本的實際分配和假定分配狀態的一致程度。以我們的樣本為例，就是要去了解圖一中樣本實際分配狀態的H欄和Benford 法則的I欄的一致程度。Excel 獨立性檢定的公式內容：

=CHITEST(實際值的範圍, 預測值的範圍).

公式中"實際值的範圍"代表的是樣本的數值，"預測值的範圍"代表是理論分配。檢定所需的數值就在H欄和I 欄中。因此，欄位J15中所含的獨立性檢定的公式，就是

=CHITEST(H4:H12,I4:I12)

**步驟 7:形成結論；資料是"自然的"嗎?**

執行完Excel 獨立性檢定，我們可以發現樣本實際數與Benford 法則的符合程度。93%的數值表示實際分配與理論分配之間有很高的一致性，而數值很小，如3%，表示兩個分配非常的不一致。如果把圖1 的資料鍵入另一個活頁簿，且變換發票的數字，則實際數值的直方圖會開始接近預測值，而獨立性檢定傳回的數值也會上升。

如圖一的欄位J15所示，獨立性檢定的結果是7.89%—非常小的數值。這樣的數值表示是公司有舞弊狀況? 不一定。不過，一般而言，低於5%的數值表示表示實際分配符合預測分配(Benford)的機率非常低；而數值10%或以下，表示至少有90%的機率，資料可能是不正常的。

所以結論呢？獨立性檢定結果數值很低，表示樣本資料可能是人工假造的。在作出這樣的結論之前，還有另一個作法：使用新的資料進行重複測試。這是使用Spreadsheet 模型的優點：只要在B欄和C欄重新置換資料，則Excel 會重新計算出圖一中的結果。 那如果再次執行檢定的結果數值依舊是很低？那這樣其中的意義就很值得玩味，因為結果其實要用倍數來檢視。如果兩次樣本測試下，卡方檢定的結果都是10%，則原始資料是"自然"的機率會變成(0.1 * 0.1 =0.01)。這樣結果對審計員來是一個重大的訊號，表示極需要進一步的追蹤和問題成因的調查。

**Benford 法則的適用情境**

首位數字的自然分配狀況是不平均，這個概念似乎違反一般人的直覺。畢竟，如果我們在一個完美的紡紗車上繪上1到9數字，則每個數字出現的機率應該是一樣的。但是自然產生的財務交易資料不能和轉輪的資料相提並論，因為他們資料的長度是不受限的。可以用這個方式來思考，當銀行帳戶增加，從數百美金變成數千美金，哪個首位數字會最先出現在新的餘額？答案是"1" (一千元)會先出現，然後是"2"(二千元)，接著是3(三千元)，以此類推。因此，每一次數值會依序增加，數字1先出現，然後是2和3，Benford 解釋的就是這個狀況，這就是為什麼Benford 分配中首位數字1,2,3 的發生機率合起來就占了整個分配的60%以上，而非一般人想像的30% (詳見圖1的J 欄中的數字)。

上述狀況也說明了使用Benford 法則時的一些限制。首先，本法則只適用於自然發生的資料，採購金額、付款金額、股價、應付資料，存貨價格、客戶退貨都是類似的範例。而足球賽、湖泊分佈、城鎮人口—Benford 在他的研究中使用的

範例，也是一樣的狀況，只是這些資料通常不會是財會專業人員的興趣。人工給定的號碼，如電話號碼、彩券號碼、客戶或支票的編號，原本資料就被定義為單一且不能重複，亦不適用於Benford 法則。

其次，要避免使用非自然狀況產生的財務資料。舉例來說，折扣店的購買金額可能不會符合Benford 分析，因為每一個項目經常只會列有一種價格。同樣的，有上限的數值，像是每班飛機的所載的乘客數，或企業員工每年的工作天數，並無法運用到這種分析方式。

第三，當擷取分析資料時，很重要的是抽樣要平均。舉例來說，如果抽樣的發票金額在美金$100~$999之間，則Benford 法則會失效，因為分析的資料被限縮在一個固定範圍。對於小型公司而言，因為原本的交易量就較少，使用一整個月完整的資料或針對每個月的資料進行抽樣，可能會是較佳的做法。

第四，Frank Benford 的研究不僅限於自然交易發生數字的首位數字，他也提出了第二位位元數字的機率分配。這個法則也可以被運用來作分析，類似本文案例所示，只要把Excel 改成使用Mid 公式功能，把將測試的字元取出來，即可進行類似的分析。

最後，從技術的角度，資料量必須要夠大才能產生有用的統計分析結果。卡方分配的原則是，期望數字的筆數至少要有5筆。因為Benford 分配的最小比例是4.6%，回推以後實際值(樣本數)至少應該有100筆資料。(本文範例使用的筆數較少，只是方便讀者瀏覽所有的測試資料)。

## 結論

Benford 法則是一個強大的工具，可以協助審計人員去檢視，查核的財務資料到底有多"自然"。使用Excel 的公式來做運算，不僅步驟直觀容易執行，且無需額外購置其他的軟體。但審計人員也必須瞭解，並非所有的財務資料都適合做類似的測試。在進行分析時應該要考慮到這些限制。

## 推薦讀物


Benford, Frank; "The Law of Anomalous Numbers," Proceedings of the American Philosophy Society, vol. 78, 1938, p. 551-572

Browne, Malcolm W.; "Following Benford's Law, or Looking Out for No. 1," New York Times, 4 August 1998

Cleary, Richard; Jay C. Thibodeau; "Applying Digital Analysis to Benford's Law to Detect Fraud: The Dangers of Type I Errors," Auditing, vol. 24, no. 1, May 2005, p. 77-81

Hill, T.P.; "The First-Digit Phenomenon," American Scientist, vol. 86, no. 4, July-August 1998, p. 358-364

Johnson, Peter; "Fraud Detection with Benford's Law," Accountancy Ireland, vol. 37, no. 4, August 2005, p. 16-17

Nigrini, Mark; "I've Got Your Number," Journal of Accountancy, vol. 187, no. 5, May 1999, p. 79-83

Rodriguez, Ricardo; "Reducing False Alarms in the Detection of Human Influence on Data," Journal of Accounting, Auditing, and Finance, vol. 19, no. 2, 2004, p. 141-159

Rose, Anna M.; Jacob M. Rose; "Turn Excel Into a Financial Sleuth," Journal of Accountancy, vol. 176, no. 2, August 2003, p. 58-60

Stone, Amey; "Using Software to Sniff Out Fraud," Business Week Online, 30 September 2003, p. N

Williamson, Duncan; "Vital Statistics," Accountancy,vol. 133, no. 1327, March 2004, p. 108-110

# 中華民國電腦稽核協會

# *ISACA Journal*

摘譯文章第 7 期　民國 100 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

ISACA Taiwan Chapter

授 權 者：ISACA

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


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