

資訊系統 (IS) 稽核的特殊性和進行稽核所需的專門技術，需要制定專門針對資訊系統稽核的相關標準。推動全球適用的標準以實現該目標是資訊系統稽核與監控協會 (ISACA®) 的宗旨之一。資訊系統稽核標準的發展和傳播是ISACA為稽核行業做出專業貢獻的基礎。資訊系統稽核標準的架構提供多層次的指導方針：

- **標準**為資訊系統稽核和報告定義了強制性的規定。它們告知：
  - 資訊系統稽核師根據「ISACA職業道德規範」中對職業責任的規定，其工作績效所應達到的最低標準。
  - 管理階層和有關方面對稽核工作從事者在專業工作上的期待。
  - 認證資訊系統稽核師 (CISA®) 資格持有人特定的相關要求。若未能遵守上述標準，可能導致ISACA董事會或相關ISACA委員會對CISA資格持有人進行調查，甚至最終採取懲戒性的行爲。
- **指導準則**為實施資訊系統稽核標準提供指導方針。資訊系統稽核師應在標準的實行過程中參考準則，同時作出專業性的判斷，並能為任何標準使用的偏差提供合理的解釋。資訊系統稽核指導準則的目標在於，為達到資訊系統稽核標準提供進一步的資訊。
- **程序**為資訊系統稽核師提供在實施稽核專案時可以遵循的步驟範例。程序文件提供進行資訊系統稽核工作時如何達到專業標準的資訊，但並非硬性規定。資訊系統稽核程序目標在於，為達到資訊系統稽核標準提供進一步的資訊。

應以COBIT®資源來做為最佳實施指導方針的來源。COBIT架構強調：「管理階層的責任在於保護企業的所有資產。管理階層必須建立一套充分的內部監控體系，以便履行此一責任並且實現企業的期望。」COBIT為資訊系統管理環境提供一套詳細的監控及監控方法。根據特殊的COBIT資訊技術 (IT) 程序選取和對COBIT資訊標準考慮來選擇於特定稽核範圍最相關的材料。

依照COBIT架構的定義，下列各項按IT管理程序進行組織。COBIT是專為商務和IT管理階層以及資訊系統稽核師而設計；因此它的運用有助於瞭解商業目標、溝通最佳實施作為及建議的達成共識並形成廣受尊重的參考標準。COBIT包括：

- 監控目標—對於所需達到的最低限度的良好監控的高層次和詳細的一般性陳述。
- 監控實施—監控目標的原理和“如何實行” 監控目標的指導準則。
- 稽核指導準則—於不同監控領域中，如何瞭解和評估各種監控、考核符合性和證實失控風險的指導方針。
- 管理指導準則—有關如何運用成熟度模型、指標和關鍵性成功因素等方法來評估和改善IT程序績效的指導方針。它們針對管理階層提供一種應用於持續性和自發性監控自我評估的架構。特別著重於：
  - 績效衡量—IT功能具體支援業務需求果效如何？管理指導準則既可用於支援自我評估的研討，也可做IT管治方案的一部分，用以支援管理階層持續性的監督和改善程序的實行。
  - IT監控剖面圖—有哪些重要的IT程序？監控有哪些關鍵性的成功因素？
  - 意識性—無法達成目標的風險何在？
  - 確立基準—其他人做了些什麼？如何衡量與比較結果？管理指導準則可提供用於評估商務領域中IT績效的範例指標。關鍵的目標指標可以鑒別並衡量IT程序的成果，同時關鍵的績效指標可藉由衡量程序的實現者來評估程序的績效。透過成熟度模型和成熟度屬性提供能力評估和基準，幫助管理階層衡量監控的能力並且鑒別監控漏洞並提出相應的改善策略。

**辭彙表**可在ISACA的網站：[www.isaca.org/glossary](http://www.isaca.org/glossary)上查閱。稽核和審查這兩個詞可以互換使用。

**免責聲明：**根據ISACA職業道德規範中對職業責任的規定，ISACA設計本指導方針做為工作績效所應達到的最低標準。ISACA不聲明或保證使用此產品一定會取得成功的結果。本出版物不得被視作包括所有適當的程序和測試，亦不得被視作排斥通過合理引導獲得同樣結果的其他程序和測試。在決定任何具體的程序或測試的合理性時，監控專業人士應根據其自身的專業判斷來鑒別由特定系統或資訊技術環境產生的特定監控條件。

ISACA標準管理委員會致力於為資訊系統稽核標準、指導準則和程序的制定提供廣泛的諮詢。標準管理委員會將於發佈任何文件之前，向全球提供公開草案以供大眾評論。標準管理委員會也尋求相關論點專家和有關方面對必要之處提出諮詢意見。

標準管理委員會現設有研發部門，歡迎ISACA成員和其他感興趣的人士就有關任何需要制定新標準的新問題提出意見。所有建議請電郵至 ([standards@isaca.org](mailto:standards@isaca.org))。或傳真 (+1.847.253.1443) 或寫信 (地址在文件末尾) 至ISACA國際總部，收件人註明研究標準和學術關係主任。本文於2005年7月1日發佈。

## 違規和非法行為 S9

### 導言

- 01 ISACA 標準以及其他相關指導方針包含強制性的基本原則和重要程序，以粗體標示。
- 02 制定 ISACA 標準的目的是為資訊系統稽核師在稽核期間所應考慮的違規和非法行為確立並提供指導方針。

### 標準

- 03 在規劃與執行稽核以降低稽核的風險程度，資訊系統稽核師應考慮違規和非法行為的風險。
- 04 資訊系統稽核師在稽核期間應保持專業懷疑態度，承認由於違規和非法行為而導致重大錯報的可能性，無論其對違規和非法行為風險的評估結果如何。
- 05 資訊系統稽核師應對被稽核單位及其環境有所瞭解，包括內部監控在內。
- 06 資訊系統稽核師應取得充分且適當的稽核證據，以確定被稽核單位內部的管理階層或其他相關人士是否瞭解任何實際的、被懷疑的或被指稱的違規和非法行為。
- 07 在執行稽核程序以取得對被稽核單位及其環境的瞭解時，資訊系統稽核師應考慮不尋常或意料之外的關係，此類關係可能表明由於違規和非法行為而導致的重大錯報的風險。
- 08 資訊系統稽核師應設計與執行程序以測試內部監控是否適當，以及管理階層凌駕於監控之上的風險。
- 09 當資訊系統稽核師確認錯報時，資訊系統稽核師應評估此類錯報是否表明違規或非法行為。如果表明違規或非法行為，資訊系統稽核師應考慮其對稽核的其他層面，特別是管理階層陳述方面的影響。
- 10 資訊系統稽核師應根據稽核業務情況至少每年一次或者多次取得管理階層的書面陳述。明確管理階層應該：
  - 承認有責任設計和實行內部監控以防止和發現違規或非法行為
  - 向資訊系統稽核師披露由於違規或非法行為所導致的重大錯報的風險評估結果
  - 向資訊系統稽核師披露所知在以下方面對被稽核單位有所影響的違規或非法行為：
    - 管理階層
    - 在內部監控中舉足輕重的員工
  - 向資訊系統稽核師披露所知員工、離職員工、監管當局和其他相關人士所傳達的影響被稽核單位的任何被指稱的違規或非法行為、或者是被懷疑的違規或非法行為
- 11 如果資訊系統稽核師確認了重大的違規或非法行為，或取得重大的違規或非法行為可能存在的資訊，資訊系統稽核師應及時向適當的管理階層傳達這些問題。
- 12 如果資訊系統稽核師確認了涉及管理階層或在內部監控中舉足輕重的員工的重大違規或非法行為，資訊系統稽核師應及時向監督管理人員傳達這些問題。
- 13 資訊系統稽核師應告知適當的管理階層以及監督管理人員在內部監控的設計和實行方面的重大薄弱環節，以防止和發現稽核期間可能引起資訊系統稽核師注意的違規和非法行為。
- 14 如果由於重大的違規或非法行為，致使資訊系統稽核師遇到影響其繼續執行稽核工作的能力的意外情況，資訊系統稽核師應考慮在這種情況下適用的法律責任和專業責任，包括是否需要資訊系統稽核師向該項稽核業務的簽約方進行匯報，或者在某些情況下向監督管理人員或監管當局進行匯報，或者考慮完全退出稽核業務。
- 15 資訊系統稽核師應將已向管理階層、監督管理人員、監管當局和其他相關人士匯報的有關重大違規和非法行為的所有溝通內容、規劃、結果、評估和結論書面記錄下來。

### 註解

- 16 資訊系統稽核師應參考《資訊系統稽核指導準則 G19，違規和非法行為》，以瞭解構成違規和非法行為的定義。
- 17 資訊系統稽核師應取得合理的保證，確保沒有因違規和非法行為所導致的重大錯報。由於運用判斷力、測試範圍以及內部控制的固有侷限性等諸多因素，因此資訊系統稽核師無法取得絕對的保證。資訊系統稽核師在稽核期間取得的稽核證據，應具有實質上的說服力但並非結論性。
- 18 因非法行為造成重大錯報沒有被發現的風險高于因違規或失誤造成的重大錯報沒有被發現的風險，因為非法行為可能涉及隱藏或隱瞞重要事件或故意向信息系統審計師虛假陳述的用心。
- 19 資訊系統稽核師過去對被稽核單位的經歷和瞭解應在稽核期間為其提供協助。在質詢和執行稽核程序期間，不應期望資訊系統稽核師完全忽視過去的經歷，但應期望其保持一定的專業懷疑態度。資訊系統稽核師不應對以相信管理階層和監督管理人員誠信可靠為根據的不具有說服力的稽核證據感到滿意。資訊系統稽核師及稽核業務團隊應在規劃期間以及整個稽核過程中討論對被稽核單位對違規和非法行為的易受害程度。
- 20 若要評估重大違規和非法行為存在的風險，資訊系統稽核師應考慮運用：
  - 其對被稽核單位已有的了解和經驗（包括其對管理階層和監督管理人員在誠信方面的經歷）
  - 向管理階層提出質詢所取得的資訊
  - 管理階層的陳述以及內部監控簽字認可
  - 在稽核期間取得的其他可靠資訊
  - 管理階層對違規和非法行為風險的評估，以及確認和應對這些風險的程序
- 21 有關違規和非法行為的進一步資訊，應參考下列指導準則：
  - 資訊系統稽核指導準則 G5，稽核綱領
  - COBIT 架構，監控目標 DS3、DS5、DS9、DS11 和 PO6
  - 2002 年頒布的《Sarbanes-Oxley 法案》
  - 1977 年頒布的《反海外腐敗法》

### 實施日期

- 22 所有資訊系統稽核業務皆自 2005 年 9 月 1 日起或之後實施本 ISACA 資訊系統稽核標準。

資訊系統稽核與監控協會 2004-2005 年標準管理委員會

主席， Sergio Fleginsky, CISA ICI Paints，烏拉圭

Svein Aldal Aldal Consulting，挪威

John Beveridge, CISA, CISM, CFE, CGFM, CQA Office of the Massachusetts State Auditor，美國

Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP Tangerine Consulting，義大利

Christina Ledesma, CISA, CISM Citibank NA Sucursal，烏拉圭

Andrew MacLeod, CISA, CIA, FCPA, PCP Brisbane City Council，澳洲

V. Meera, CISA, CISM, ACS, CWA Microsoft Corporation，美國

Ravi Muthukrishnan, CISA, CISM, FCA, ISCA Ikanos Communications，印度

Peter Niblett, CISA, CISM, CA, CIA, FCPA WHK Day Neilson，澳洲

John G. Ott, CISA, CPA AmerisourceBergen，美國

Thomas Thompson, CISA Ernst & Young，阿拉伯聯合大公國

© 2005 年版權所有

Information Systems Audit and Control Association

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

電話：+1.847.253.1545

傳真：+1.847.253.1443

電郵：[standards@isaca.org](mailto:standards@isaca.org)

網址：[www.isaca.org](http://www.isaca.org)