



資訊系統稽核標準

稽核綱領

文件編號 S1

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為。
- **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。資訊系統稽核程序的目標在於，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 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)。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。本資料於 2004 年 10 月 15 日頒佈。

稽核綱領 S1

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 制定資訊系統稽核標準的目的是就有關稽核程序中引用的稽核綱領制定與提供指導方針。

標準

- 03 稽核綱領或委任書中應於正確地記錄登載有關資訊系統稽核功能或資訊系統稽核任務之目的、責任、授權和義務。
04 稽核綱領或委任書應獲得組織內適當階層的同意和批准。

註解

- 05 應為所有正在進行的內部資訊系統稽核工作準備一份稽核綱領。稽核綱領通常應每年加以審查。如果職業責任有所不同或產生改變，則應更經常審查。內部資訊系統稽核師可用委任書來進一步澄清或確認參與特定的稽核或非稽核任務。通常應為外部資訊系統稽核師參與每項稽核或非稽核任務準備委任書。
06 稽核綱領或委任書應儘可能詳細，以便能傳達稽核功能或稽核任務之目的、責任和限制。
07 稽核綱領或委任書應定期審查，以確保稽核之目的和責任皆已記錄登載。
08 為了獲得準備稽核綱領或委任書的進一步資訊，請參考下列的指導方針：
■ 資訊系統稽核指導準則 G5，稽核綱領
■ COBIT 架構，監控目標 M4

實施日期

- 09 此 ISACA 標準適用於所有資訊系統的稽核，於 2005 年 1 月 1 日起（之後）開始實施。

資訊系統稽核與監控協會 2004-2005 年標準管理委員會

Chair, Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay
Svein Aldal Aldal Consulting, Norway
John Beveridge, CISA, CISM, CFE, CGFM, CQA Office of the Massachusetts State Auditor, USA
Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP Value Partners, Italy
Christina Ledesma, CISA, CISM Citibank NA Sucursal, Uruguay
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Brisbane City Council, Australia
V. Meera, CISA, CISM, ACS, CISSP, CWA Microsoft Corporation, USA
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA NextLinx India Private Ltd., India
Peter Niblett, CISA, CISM, CA, CIA, FCPA WHK Day Neilson, Australia
John G. Ott, CISA, CPA Aetna Inc., USA
Thomas Thompson, CISA Ernst & Young, UAE

© Copyright 2004

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

網站：www.isaca.org