

## S16 電子商務

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。ISACA<sup>®</sup>的目標之一就是制定全球適用的標準以實現其願景。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<sup>™</sup>(CISA<sup>®</sup>)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 委員會對資訊系統稽核師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。

**資訊和相關技術的監控目標 (CobiT<sup>®</sup>)**是一種資訊技術(IT)管理框架和支援工具集合，管理人員可以利用它來溝通與銜接控制規定、技術問題和業務風險之間的差距。CobiT 有助於為公司上下的資訊技術控制制定明確的政策並提供良好的實務。它強調法規遵循性，有助於企業提高 IT 價值，並能調整與簡化 CobiT 架構概念的實施過程。

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、溝通良好實施作為及建議的達成共識並形成廣受尊重的架構。請登入 ISACA 網站 [www.isaca.org/cobit](http://www.isaca.org/cobit) 下載 CobiT。依照 CobiT 架構的定義，下列各項相關產品及/或要素按 IT 管理程序進行組織：

- **監控目標**—概括說明與 IT 流程有關的最低限度的良好控制
- **管理指導方針**—有關如何運用成熟度模型、負責、承擔、諮詢及/或知會(RACI)表、目標和指標來評估和提高 IT 流程執行績效的指導方針。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：
  - 績效的評量
  - 資訊技術控制剖面圖
  - 意識性
  - 標竿管理
- **CobiT 監控實務**—風險和價值陳述以及「如何實現」監控目標的指導方針南
- **IT 保證指南**—對於不同監控領域中的瞭解協調、監控評估、考核符合性和證實不合標準之監控風險的指導方針。

**辭彙表**可在 ISACA 的網站：[www.isaca.org/glossary](http://www.isaca.org/glossary) 上查閱。在資訊系統稽核標準、指導方針和程序中，稽核和審核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。任何關於標準的建議，請傳送電子郵件至 ([standards@isaca.org](mailto:standards@isaca.org))，傳真至(+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 2007 年 12 月 1 日發佈。

## S16 電子商務

### 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（黑體字）標示。  
02 本 ISACA 標準旨在制定有關審核電子商務環境的標準並提供相關的指導方針。

### 標準

- 03 資訊系統稽核師在審核電子商務環境時，應評估其適用的控制和風險以確保電子商務交易得到適當的控制。**

### 註解

- 04 電子商務的定義為企業使用網際網路作為實現技術而與其客戶、供應商和其他外部業務合作夥伴以電子方式進行業務的過程。因此，它包括企業對企業(B2B)以及企業對客戶(B2C)這兩種電子商務模式。  
05 在發展整體資訊系統稽核計劃時，資訊系統稽核師應運用適當的風險評估技巧或方法，其中應包括電子商務環境所涉及的範圍。  
06 資訊系統稽核師應考慮使用資料分析技術，包括使用持續保證，這樣資訊系統稽核師便可在審核電子商務活動時，透過電腦持續監控系統的可靠性並且收集選擇性的稽核證據。  
07 瞭解電子商務的控制和風險管理涉及問題所需的技術和知識水準，因企業電子商務活動的複雜性而有所不同。  
08 資訊系統稽核師在開始稽核工作之前，應先瞭解電子商務應用程式所支援的業務流程的性質和關鍵程度，以便在適當的相關背景下評估結果。  
09 請參考下列的指導方針，以便瞭解有關電子商務的詳細資訊：
  - 指導方針 G21 企業資源規劃(ERP)系統審核
  - 指導方針 G22 企業對客戶(B2C)的電子商務審核
  - 指導方針 G24 網上銀行
  - 指導方針 G25 虛擬專用網(VPN)的審核
  - 指導方針 G33 有關網際網路使用的一般考慮
  - 程序 P6 防火牆
  - COBIT 架構和監控目標

### 實施日期

- 10 本 ISACA 標準於 2008 年 2 月 1 日起實施。

#### 2007~2008 年度 ISACA 基準委員會

議長、ラビ・ムサクリシュナン(Ravi Muthukrishnan)、 CISA、CISM、FCA、ISCA	インド、キャブコ IT サービスーズ・インド・プライベート (Capco IT Services India Private Limited)
ブラッド・デビッド・チ(Brad David Chin)、CISA、CPA	米国、グーグル(Google Inc.)
セルジオ・フレジンスキー(Sergio Fleginsky)、CISA	ウルグアイ、ICI ペイント(ICI Paints)
マリア・ゴンザレス(Maria Gonzalez)、CISA	スペイン、ホームランドオフィス(HomeLand Office)
ジョン・ホー・チ(John Ho Chi)、CISA、CISM、CBCP、CFE	シンガポール、アーンスト&ヤング(Ernst & Young)
アンドリュー J. マクリオード(Andrew J. MacLeod)、 CISA、CIA、FCPA、MACS、PCP	オーストラリア、ブリスベン市評議会(Brisbane City Council)
ジョン G. オット(John G. Ott)、CISA、CPA	アメリカ、アメリソースバージェン(AmerisourceBergen)
ジェイソン・トンブソン(Jason Thompson)、CISA、CIA	米国、(KPMG LLP)
ミーラ・ベンカテッシュ(Meera Venkatesh)、 CISA、CISM、ACS、CISSP、CWA	米国、マイクロソフト(Microsoft Corp., USA)

© 2007 年 ISACA 版權所有。保留所有權利。

ISACA  
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  
網址：www.isaca.org