資訊稽核和保證標準
1207 違規和非法行為

資訊系統 (IS) 稽核和保證的專業性，以及完成此類工作所需的技術，需要專門適用於「資訊稽核和保證」的標準。資訊稽核和保證標準的發展和傳播是 ISACA® 對稽核業界作出專業貢獻的基石。

資訊稽核和保證標準定義資訊稽核和報告的強制性要求，並告知：

- 依據 ISACA 職業道德規範，對於職業責任的規定，資訊稽核和保證專業人員執行績效所應達到的最低標準。
- 管理階層和其他利害關係人對執業者在專業工作上的期待。
- 資訊系統稽核師 (CISA®) 認證持有人的特定要求。如果 CISA 認證持有人未能遵守這些標準，則可能會招致 ISACA 董事會或相關的委員會對其行為進行調查，進而採取相應的紀律措施。

資訊稽核和保證專業人員應當視情況在作業中聲明，已根據 ISACA 資訊稽核和保證標準或其他適用的專業標準完成本項委任作業。

適用於資訊稽核和保證專業人員的 *ITAF™* 框架提供了多層次的指引：

- **標準，**分為三類：
  - 通用標準（1000 系列）—— 是資訊稽核和保證專業人員的工作指導原則。這些標準適用於所有任務的執行，並且涉及到資訊稽核和保證專業人員的道德、獨立性、客觀性和應有的審慎性，以及知識、職業能力和技能。標準聲明（粗體）是強制性的。
  - 績效標準（1200 系列）—— 涉及到任務執行，例如，規劃與監督、任務範圍、風險與重要性、資源調動、監督與任務管理、稽核與保證證據，以及專業判斷和應有的審慎性。
  - 報告標準（1400 系列）—— 涉及到報告類型、溝通方式以及傳達的資訊
- **準則**，支援標準部分，同樣分為三類：
  - 通用準則（2000 系列）
  - 績效準則（2200 系列）
  - 報告準則（2400 系列）
- **工具和技術**，為資訊稽核和保證專業人員提供附加指引，如白皮書、IS 稽核/保證計畫和 COBIT® 5 產品系列

ITAF 中所使用的線上術語表請參見 *www.isaca.org/glossary*。

免責聲明：ISACA 設計此指南是根據 ISACA 職業道德規範中，關於職業責任規定所應達到的最低績效水準。ISACA 承諾使用此產品將保證帶來成功的結果。該出版物不應被視為包含任何適當的程序或測試，或排除在獲得相當結果的其他程序或測試。在確定任何具體程序或測試是否適當時，控制或專業人員應當對特定系統或資訊環境呈現的具體控制情況作出其自己的專業判斷。

ISACA 專業標準和職業管理委員會 (PSCMC) 為準備標準和指南，致力於進行廣泛的意見徵詢。在發佈任何版本之前，將在國際上發佈一份公開的草稿，以徵求公眾意見。您可透過電子郵件 (*standards@isaca.org*)、傳真 (+1.847. 253.1443) 或郵件 (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA) 等方式向專業標準開發總監提出您的寶貴意見。

ISACA 2012-2013 專業標準和職業管理委員會

Steven E. Sizemore, CISA, CIA, CGAP，主席	**Texas Health and Human Services Commission，美國**
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	**HP Enterprises Security Services，英國**
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	**Myers and Stauffer LC，美國**
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	**British American Tobacco IT Services，馬來西亞**
Alisdair McKenzie, CISA, CISSP, ITCP	**IS Assurance Services，紐西蘭**
Katsumi Sakagawa, CISA, CRISC, PMP	**JIEC Co. Ltd. ，日本**
Ian Sanderson, CISA, CRISC, FCA	**NATO，比利時**
Timothy Smith, CISA, CISSP, CPA	**LPL Financial，美國**
Rodolfo Szuster, CISA, CA, CBA, CIA	**Tarshop S.A，阿根廷**

資訊稽核和保證標準 1207 違規和非法行為

聲明

1207.1 資訊稽核和保證專業人員應當在作業期間考慮違規和非法行為的風險。

1207.2 資訊稽核和保證專業人員應當在稽核作業期間保持專業懷疑的態度。

1207.3 資訊稽核和保證專業人員應當即時記錄並向有關單位通報任何重大違規或非法行為。

關鍵要項

資訊稽核和保證專業人員應當：

- 在規劃和執行稽核作業時透過以下方式將稽核風險降低至可接受的水準：
  - 不論法律遵循的風險評估結果為何，仍要意識到有可能因為重大錯誤、控制缺陷、不實陳述等原因，導致有違法情事的存在
  - 獲得並瞭解企業及其環境，包括在預防和偵測稽核作業主題、範圍和目標相關違規和非法行為的內部控制
  - 獲取足夠和適當的證據，以確定企業內部的管理階層或其他人員是否知悉任何實際、懷疑或宣稱的違規和非法行為
- 執行稽核程序時，考慮可能表明違規和非法行為帶來的重大錯誤、控制缺陷或誤報風險的異常或意外關係，
- 設計和執行相關程序，以測試內部控制的適宜性以及管理人員凌駕于預防或偵測違規和非法行為的控制上的風險，
- 評估識別出的錯誤、控制缺陷或誤報是否預示著違規或非法行為。如果具備有此種跡象，考慮這對稽核作業的其他相關面向的影響，尤其是對管理階層陳述的影響。
- 至少每年一次獲取管理階層的書面陳述，或根據稽核作業情況更頻繁地獲取，以便：
  - 承認管理階層有責任設計和執行內部控制以防止和檢測違規和非法行為。
  - 披露表明由於違規或非法行為，可能存在錯誤、控制缺陷或誤報的任何風險評估的中肯結果。
  - 披露管理階層承認，影響企業的違規和非法行為與擔任內部控制重要角色的管理階層和員工有關。
  - 揭露管理階層對於任何宣稱或疑似違規和非法行為之理解，無論是員工、前員工、主管機關、或是其他人員所通報之資訊。
- 即時：
  - 向適當的管理階層通報已識別或獲取的、有關涉及存在重大違規或非法行為的任何資訊。
  - 向治理負責人通報涉及擔任內部控制重要角色的管理階層或員工的任何重大違規或非法行為。
- 向治理負責人報告內部控制設計和執行中的任何重大漏洞，這些內部控制在預防和偵測稽核作業期間已被識別的、即便在範圍之外的任何違規和非法行為。
- 考慮適用於該情形的法律及專業報告要求。
- 如果重大錯誤、控制缺陷、誤報或非法行為影響稽核作業的繼續執行，考慮退出稽核作業。
- 記錄已上報管理層、治理負責人、監管機構及其他人員與重大違規或非法行為相關的所有通訊、規劃、結果、評估及結論。

©2013 ISACA 保留所有權利。

資訊稽核和保證標準 1207 違規和非法行為

術語

術語	定義
違規	違反既定的管理政策或法規要求。它可包括有意誤報或遺漏有關被稽核領域或企業整體的資訊；重大過失或無意的非法行為。
重大誤報	在可衡量的程度上影響稽核結果的、意外或故意的失實陳述
專業懷疑態度	包括質疑心態和批判性評估稽核證據在內的一種態度。來源：美國註冊會計師協會 (AICPA) AU 230.07

關聯標準和準則

類型	標題
標準	1008 衡量標準
標準	1202 規劃中的風險評估
標準	1205 證據
準則	2206 使用其他專家的成果
準則	2207 違規和非法行為

生效日期　本 ISACA 標準自 2013 年 11 月 1 日起對所有資訊稽核和保證作業生效。