資訊稽核和保證標準
1205 證據

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。

聲明

1205.1 **資訊稽核和保證專業人員應當獲得足夠和適當的證據，為稽核作業結果提供合理的結論依據。**

1205.2 **資訊稽核和保證專業人員應當評估所獲證據是否足以支持結論並實現稽核作業目標。**

關鍵要項

執行某個稽核作業時，資訊稽核和保證專業人員應當：

- 獲得足夠與適當的證據，其中包括：
  - 執行的程序
  - 執行程序的結果
  - 用來支援該次稽核作業的原始文件資料（電子或紙本）、紀錄以及確切的資訊
  - 該次稽核作業的發現與結果
  - 有關已完成工作並遵守適用法律、法規和政策的紀錄
- 準備相關文件，這些應當：
  - 保留和提供一段時間，並採用符合稽核和保證組織的政策以及相關專業標準、法律和法規的格式
  - 在整個準備和保留期間適當保護以防止未經授權的揭露或修改
  - 保留期結束時進行妥善處置
- 從控制測試中獲取證據時，考慮證據是否足以證明評估出來的控制風險水準。
- 適當地對證據進行識別、交叉引用和登記分類。
- 評估證據的可靠性時，考慮其來源、性質（如書面、口頭、視覺、電子）和真實性（如數位和親筆簽名、印鑑）。
- 考慮收集必要證據、滿足稽核作業目標和風險要求的最有效和最即時的手段。然而，困難或成本不能成為省略必要程序的有效理由。
- 根據被稽核的主題（即其性質、稽核時程安排、專業人員的判斷）選擇最合適的程序收集證據。用於獲取證據的程序包括：
  - 諮詢和確認
  - 重新執行
  - 重新計算
  - 計算
  - 分析程序
  - 檢查
  - 觀察
  - 其他普遍接受的方法
- 考慮獲得任何資訊的來源和性質，並評估其可靠性以及是否需要進一步核查。一般而言，下列證據的可靠性是較高的：
  - 採書面形式，而非口頭表達
  - 獲取自獨立的來源
  - 來自專業人員而不是受稽核者
  - 經過獨立方鑒定
  - 由獨立方保管
  - 檢查結果
  - 觀察結果

資訊稽核和保證標準 1205 證據

關鍵要項續

- 足以讓合格的獨立方能夠重新執行測試並獲得相同結果和結論的證據。
- 獲得與項目的重要性及相關風險相稱的證據。
- 當資訊稽核或保證專業人員利用獲取自企業的資訊執行稽核程序時，要適當強調資訊的準確性和完整性。
- 披露無法透過與資訊稽核或保證作業獲取足夠證據的任何情形。
- 確保證據安全，防止未經授權的存取和修改。
- 只要有必要遵守所有適用的法律、法規和政策，就必須在完成資訊稽核或保證工作後保留證據。

術語

術語	定義
適當的證據	證據品質的衡量指標
足夠的證據	證據數量的衡量指標；支援稽核目標和範圍方面的所有重大問題。參見證據。

關聯準則

類型	標題
準則	2205 證據

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。