# 資訊稽核和保證標準
# 1401 稽核報告

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。

# 資訊稽核和保證標準 1401 稽核報告

## 聲明

**1401.1** **資訊稽核和保證專業人員應當提供稽核報告，以溝通作業完成的結果，其中包括：**

- **企業的身份、預期的受理人以及對內容和流通的任何限制**
- **範圍、作業目標、覆蓋期間以及執行工作的性質、時間和程度**
- **結果、結論和建議**
- **資訊稽核和保證專業人員有關稽核作業範圍方面的任何資格或限制**
- **符合稽核規章或稽核作業書條款的簽章、日期和分發**

**1401.2** **資訊稽核和保證專業人員應當保證稽核報告中的結果有足夠與適當的證據支持。**

## 關鍵要項

資訊稽核和保證專業人員應當：

- 獲得受稽方提供的書面陳述，其中明確詳述稽核作業的關鍵領域、已然出現的問題及其解決辦法以及受稽方作出的聲明
- 確定受稽方的陳述已經過受稽方簽署並註明日期，以表示承認受稽方在稽核作業方面的職責
- 在工作底稿中紀錄並保留執行稽核作業過程中收到的任何陳述。對於保證稽核作業，從受稽方獲取的陳述應當採用書面形式，以減少可能產生的誤解。
- 定制報告的形式和內容，以支援被執行稽核作業的類型，如：
  - 稽核（直接或證明）
  - 檢閱（直接或證明）
  - 議定的程序
- 在報告中描述重大或嚴重漏洞及其對實現稽核作業目標的影響。
- 在定稿和發佈之前與管理階層討論主題範圍的報告草案內容，並視情況在最終報告中包含管理階層對結果、結論和建議的答復。
- 向治理負責人，並視情況向主管部門通報控制環境中的重要缺陷和重大漏洞，並在報告中揭露已通報的內容。
- 在最終報告中引用任何獨立的報告。
- 向受稽方管理階層通報不夠嚴重但並非無關緊要的內部控制缺陷。此時，應通知治理負責人或主管部門，已向受稽核方管理階層通報此類控制缺陷。
- 識別執行稽核作業過程中套用的標準，並視情況通報不符合這些標準的任何情形。

## 術語

| 術語 | 定義 |
|---|---|
| 相關資訊 | 與控制有關，向評估員告知有關基礎控制或控制元件運行情況的有用資訊。直接確認控制運行情況的資訊最為相關。間接涉及控制運行情況的資訊也可能相關，但不如直接資訊。參見 COBIT 5 資訊品質目標 |
| 可靠資訊 | 準確、可考證和來自客觀來源的資訊。參見 COBIT 5 資訊品質目標 |
| 足夠資訊 | 當評估員已收集足夠的資訊，可以得出合理的結論時，即為足夠。然而，資訊若要足夠，它首先必須是合適的。參見 COBIT 5 資訊品質目標 |

| | |
|---|---|
| 合適資訊 | 相關（即適合預期目的）、可靠（即準確、可核對和來自客觀來源）和即時（在適當的時限內產生和使用）的資訊。參見 COBIT 5 資訊品質目標 |
| 即時資訊 | 有可能在對企業產生重大影響之前預防或檢測控制缺陷的時限內產生和使用。參見 COBIT 5 資訊品質目標 |

關聯標準和準則

| **類型** | **標題** |
|---|---|
| 準則 | 2401 稽核報告 |

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。