



資訊稽核和保證標準 1203 執行和監督

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 1203 執行和監督

聲明

- 1203.1** 資訊稽核和保證專業人員應當根據資訊稽核計畫展開工作，以在議定的時間表內涵蓋識別的風險。
- 1203.2** 資訊稽核和保證專業人員應當向對其負有監督責任的資訊稽核工作人員進行監督，以實現稽核目標和達到適用的專業稽核標準。
- 1203.3** 資訊稽核和保證專業人員應當只接受在其知識和技能範圍內的，或能夠合理預期在委任作業過程中獲得相關技能，或者在監督之下能夠完成任務的任務。
- 1203.4** 資訊稽核和保證專業人員應當獲得足夠和適當的證據以達到稽核目標。稽核結果和結論應有對應的證據分析及解釋作支持。
- 1203.5** 資訊稽核和保證專業人員應當記錄稽核過程，在其中描述支援結果和結論的稽核工作和稽核證據。
- 1203.6** 資訊稽核和保證專業人員應當識別結果並對其作出結論。
-

關鍵要項

資訊稽核和保證專業人員應當：

- 分配團隊成員，使其技能和經驗符合作業需求。
- 視情況向資訊稽核團隊增加外部資源，同時確保其工作得到適當的監督。
- 在整個作業過程中管理特定資訊稽核團隊成員的角色和職責，至少確認以下問題：
 - 執行和審核角色
 - 設計方式和方法的職責
 - 建立稽核或保證計畫
 - 展開工作
 - 在出現各種問題、議題時進行處理
 - 記錄和整理結果
 - 撰寫報告
- 安排一名團隊成員執行作業任務，另一名適當的團隊成員進行審核。
- 使用可得到的最佳稽核證據。它應當與稽核目標的重要性以及獲得證據所需的時間和工作量相一致。
- 如果根據專業人員的判斷，所獲證據不符合衡量標準，不足以且不適合形成意見或支援結果和結論，則要獲得更多證據。
- 組織並記錄在作業期間的工作 - 需遵循預先定義、記錄和經過批准的程序。
- 在紀錄中包含：
 - 稽核目標和工作範圍、稽核計畫、執行的稽核步驟、收集的證據、結果、結論和建議
 - 詳情需慎重與詳細，讓人員能夠重新執行在稽核作業期間所執行的任務，並得出相同的結論
 - 執行每一項任務者的身份及其在準備和審核記錄方面的角色
 - 準備和審核紀錄的日期
- 獲得受稽方提供的書面陳述，其中明確詳述作業的關鍵領域、已然出現的問

資訊稽核和保證標準 1203 執行和監督

- 關鍵要項
續
- 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，以表示承認其在作業方面的職責。
 - 在工作底稿中記錄並保留執行作業過程中收到的任何書面或口頭陳述。
-

關聯標準
和準則

類型	標題
標準	1005 專業之謹慎注意責任
標準	1205 證據
標準	1401 報告
準則	2202 規劃中的風險評估

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。