資訊稽核和保證標準
1202 規劃中的風險評估

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 1202 規劃中的風險評估

聲明

1202.1 **資訊稽核和保證職能部門應當使用適當的風險評估方法和配套方法，制定總體 IS 稽核計畫，並確定有效分配資訊稽核資源的優先順序。**

1202.2 **資訊稽核和保證專業人員應當在規劃各個作業時，識別和評估與被審核領域的相關風險。**

1202.3 **資訊稽核和保證專業人員應當考慮企業面臨的主要風險、稽核風險及相關暴露。**

關鍵要項

規劃現行的活動時，資訊稽核和保證職能部門應當：

- 至少每年執行一次風險評估並記錄之，以便制訂資訊稽核計畫。
- 組織的戰略計畫和目標及企業風險管理框架和措施，應作為風險評估的一部分。
- 針對每一項資訊稽核和保證作業，需量化並證明滿足作業要求所需要的資訊稽核資源數量。
- 在選擇領域和感興趣的稽核項目，以及作出關於設計和進行特定資訊稽核和保證作業的決定時，應進行風險評估。
- 向稽核利害關係人及其他適當的當事人核准風險評估。
- 以風險評估為依據優先考慮和安排資訊稽核和保證工作。
- 以風險評估為依據制訂以下性質的計畫：
  - 用作資訊稽核和保證活動的框架
  - 考慮非資訊稽核和保證的要求和活動
  - 每年至少更新一次，並由治理負責人核准
  - 闡述稽核規程規定的職責

規劃各個稽核作業時，資訊稽核和保證專業人員應當：

- 識別和評估與被審核領域相關的風險。
- 針對每一項作業初步評估與被審核領域相關的風險。每一項具體作業的目標應當反映初步風險評估的結果。
- 在考慮風險領域和規劃具體作業時，要考慮之前的稽核、審核和結果，包括任何補救活動。還要考慮董事會的總體風險評估流程。
- 在規劃和執行資訊稽核的同時，試圖透過適當評估資訊主要及相關控制，將稽核風險降低到可接受的水準並符合稽核目標。
- 規劃具體的資訊稽核程序時，當重要性基準越低時，稽核預期將越準確，但稽核風險越高。
- 若要降低風險、實現較高的重要性，可以透過擴大控制測試的範圍（降低控制風險）/擴大實質性測試程序的範圍（降低檢測風險）等補償措施來獲得額外保證。

術語

術語	定義
稽核規程	經治理負責人批准的一種文檔件，用於定義內部稽核活動的目的、職權和職責。 該規程應當： • 在企業內部設立內部稽核職能的職位

	• 為履行資訊稽核和保證作業，授予相關紀錄、人員和有形財產的存取許可權 • 定義稽核職能部門的運作範圍
稽核風險	根據稽核結果得出錯誤結論的風險。稽核風險的三個組件如下： • 控制風險 • 偵測風險 • 固有風險
稽核主要風險	與被審領域相關的風險： • 業務風險（客戶的支付能力、信譽和市場因素等） • 契約風險（債務、價格、類型和處罰等） • 國家風險（政治、環境和安全等） • 專案風險（資源、技能組合、方法和產品穩定性等） • 技術風險（解決辦法、架構、硬體和軟體基礎設施網路、支付管道等） 參見固有風險。
控制風險	該風險是指存在無法透過內部控制系統即時防止或檢測的重大錯誤。（參見固有風險。）
偵測風險	該風險是指資訊稽核或保證專業人員無法透過其實質性程序檢測到重大、單個或與其他錯誤相結合的錯誤。參見稽核風險。
固有風險	不考慮管理層已經或可能採取的措施（即實施控制）的風險水準或風險暴露。參見控制風險。
重要性	關於某個資訊專案在其對被稽核實體履行職能的影響或作用方面的重要性的稽核概念。它表示特定事項在企業作為一個整體的背景下的相對意義或重要性。
風險評估	用於識別、評估風險及其潛在影響的一種流程。 風險評估用於識別會給企業帶來最高風險、漏洞或暴露的專案或領域，以便列入 年度資訊稽核計畫。 風險評估還用於管理專案交付和專案效益風險。
實質性測試	在稽核期間獲取有關活動或交易的完整性、準確性或存在性的稽核證據

關聯準則

類型	標題
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。