資訊稽核和保證標準
1204 重要性

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 1204 重要性

聲明

1204.1 **資訊稽核和保證專業人員在規劃某個稽核作業時，應當考慮潛在的控制漏洞或缺失，以及此類控制漏洞或缺失是否會導致嚴重缺陷或重大缺失。**

1204.2 **資訊稽核和保證專業人員在確定稽核程序的性質、時間安排和範圍時，應當考慮重要性及其與稽核風險之間的關係。**

1204.3 **資訊稽核和保證專業人員應當考慮細微的控制缺陷或漏洞的累積效應，以及控制缺失是否會導致重要缺陷或重大漏洞。**

1204.4 **資訊稽核和保證專業人員應當在報告中揭露以下事項：**

- **控制缺失或無效控制**
- **控制缺陷的嚴重性**
- **這些漏洞導致重要缺陷或重大缺失的可能性**

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：

- 將重要性的概念套用到：
  - 稽核作業的規劃和執行之中
  - 具體項目、流程、控制或錯誤的影響評估之中

  應當在特定的作業情形下判斷相關策略、程序和控制的任何缺陷、漏洞或缺失。
- 立法或監管機構若有規定，考慮重要性的定義。
- 需注意，於具體情形和不斷變化的環境，不同時間對重要性和稽核風險的評估也不盡相同。
- 在規劃和執行作業的同時，嘗試將稽核風險降低到可接受的水準並且符合目標。
- 在確定稽核程序的性質、時間安排和範圍時，考慮重要性。
- 透過擴大控制測試的範圍（減少控制風險）/擴大實質性測試程序的範圍（減少檢測風險）減少重要性較高的主題領域的稽核風險。
- 評估補償性控制的效果，以及此類補償性控制能否有效用於確定控制缺陷或控制缺陷組合是否屬於重大缺失。
- 在確定重要性時，考慮多個錯誤或控制故障的累積效應。
- 在評估控制缺陷對稽核意見或結論的總體影響時，不僅要考慮其規模，還要考慮其性質及其發生的具體情形。

標準 1204 重要性

術語

術語	定義
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
重大缺失	內部控制中的缺陷或缺陷組合，它會帶來無法即時防止或偵測重大錯誤的情形。 如果控制缺失導致無法提供實際控制目標的合理保證，則控制漏洞應被視為重大。某個漏洞若被歸類為重大，則意味著： • 控制無效/控制未在執行/控制不足 • 需進行提報 重要性與資訊稽核或保證專業人員可以接受的稽核風險水準間存在反比關係，即重要性程度越高，稽核風險的可接受程度越低，*反之亦然*。
重要性	關於某個資訊項目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。

關聯標準和準則

類型	標題
標準	1201 稽核作業規劃
標準	1202 規劃中的風險評估
標準	1207 違規和非法行為
標準	1401 報告
準則	2202 規劃中的風險評估
準則	2204 重要性

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。