資訊稽核和保證標準
1008 衡量標準

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

1008.1 **資訊稽核和保證專業人員應當於選擇評估主題時，參考對照的衡量標準以客觀、完整、相關、可衡量、可理解、得到廣泛認可、權威性的，以及報告的所有讀者和使用者可以理解或得到的為主。**

1008.2 **資訊稽核和保證專業人員應當考慮衡量標準的來源，並且在接受鮮為人知的標準之前，著重於相關權威機構發佈的標準。**

關鍵要項

資訊稽核和保證專業人員應當：

- 慎重考慮衡量標準的選擇，並且能夠證明該項選擇。
- 運用專業判斷，以確保一旦應用，衡量標準的使用將有助得出公正和客觀、不會誤導讀者或使用者的意見或結論。一般認為管理階層可能頒佈不符合所有要求的衡量標準。
- 在確定作業要求時，考慮衡量標準的適用性和可用性。
- 若衡量標準不容易得到、不完整或需要解釋，包含必要的描述及任何其他資訊，以確保報告公正、客觀和可理解，同時確保報告中包含所使用衡量標準的環境。

應當參照以下五條適用性衡量標準，以評估主題評估標準的適用性和可用性：

- **客觀性** —— 標準不應具有任何偏頗，否則會對專業人員的結果和結論將造成不良影響，並且會相對地誤導報告的使用者。
- **完整性** —— 標準應足夠完整，有效的識別和使用，才能在執行資訊稽核或保證作業時，不致對專業人員就主題得出的結論造成影響。
- **關聯性** —— 衡量標準應與主題相關，並有助於得到滿足資訊稽核或保證作業目標的結果和結論。
- **可衡量性** —— 衡量標準應確保主題的衡量方法的一致性，並保證不同的專業人員在類似情況下得出一致的結論。
- **可理解性** —— 準則應表達清晰，而不會造成不同使用者有不同的詮釋。

對專業報告的使用者而言，衡量標準的可接受性，受衡量標準的可用性影響，因此使用者才能理解保證活動的依據，以及結果和結論的相關性。來源應具有以下性質：

- **公認性** —— 衡量標準應得到足夠廣泛的認可，這樣才能保證其使用，不受到目標使用者的質疑。
- **權威性** —— 應尋求能夠反映該領域的權威公告，並切合主題的衡量標準。例如，權威公告可能來自專業機構、產業團體、政府和監管機構。
- **公開提供** —— 衡量標準應提供給專業人員報告的使用者。例如： ISACA、國際會計師聯合會 (IFAC) 等專業會計與稽核機構以及其他公認的政府或專業機構所開發的標準。
- **提供給所有使用者** —— 衡量標準若不公開提供，應當透過聲明向所有使用者通報，這些聲明構成專業人員報告的一部分。聲明包含主題相關、符合適用的衡量標準的要求聲明，以保證其可以得到稽核。

關鍵要項（續）

除適用性和可用性之外，就其使用與潛在客戶而言，選擇資訊保證準則時還應當考慮其來源。例如，就遵守政府法規而言，基於依據適用主題的法律和法規而制定的聲明準則也許是最適合的。在其他情況下，產業或貿易協會的衡量標準也可能是相關的。相關衡量標準來源如下（按考慮因素列舉）：

- **ISACA 制定的衡量標準 ——** 這些是公開可用的準則和標準，已由資訊治理、控制、安全和保證領域的國際公認專家進行同行審查和徹底的盡職審查流程。
- **其他專家團體制訂的衡量標準 ——** 類似於 ISACA 標準和準則，這些標準切合主題，由各領域的專家開發，並接受過同行審查和徹底的盡職審查流程。
- **法律和法規制定的衡量標準 ——** 儘管法律和法規可以提供衡量標準的依據，但必須慎重使用。措詞通常非常複雜，並且具有特定的法律含義。許多情況下，有必要以聲明的形式復述要求。另外，通常僅限由法律界人士表達法律意見。
- **企業未遵循正當程序制定的衡量標準 ——** 這些包括其他未遵循正當程序的企業所制訂，並且未接受過公眾諮詢和辯論的相關準則。
- **專為 IS 稽核或保證約定發展的衡量標準 ——** 儘管專為 IS 稽核或保證約定制定的標準也許是適當的，但仍需慎重使用，以保證這些標準符合適用性準則，尤其是完整性、可衡量性和客觀性。專為 IS 稽核或保證約定制定的標準以聲明的形式存在。

應當慎重考量衡量標準的選擇。儘管遵守地方法律和法規非常重要，並且必須被視為一項強制性要求，但 一般認為，許多 IS 稽核和保證作業涵蓋法律或法規未涉足的領域，如：變更管理、資訊技術 一般控制和存取控制。此外，信用卡付款業之類的某些產業也制訂了必須遵循的強制性要求。法律要求是原則性的，而專業人員應當確保選擇的衡量標準符合稽核作業的目標。

隨著稽核作業的進展，更多的資訊可能導致某些衡量標準無法達成目標。在這些情況下，沒有必要完成與該標準有關的更多工作。

術語

術語	定義
衡量標準	標準和基準指標，作為衡量和展現稽核主題，同時供 IS 稽核師對稽核主題的參照評估 衡量標準應該： • 客觀 —— 不偏不倚 • 完整 —— 包含得出結論所需要的所有相關因素 • 相關 —— 切合主題 • 可衡量 —— 提供一致性的衡量方法 在簽證業務中，可參照基準指標評估管理階層對於主題事項的書面聲明。從業人員透過引述適用的衡量標準形成對稽核主題的結論。

關聯準則

類型	標題
準則	2008 衡量標準

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。