

信息系统 (IS) 审计和鉴证的专业性以及完成此类工作所需的技术需要专门适用于 IS 审计和鉴证的标准。IS 审计和鉴证标准的发展和传播是 ISACA® 对审计业界作出专业贡献的基础。

IS 审计和鉴证标准定义 IS 审计和报告的强制性要求，并告知：

- 根据 ISACA 职业道德规范中关于职业责任的规定，IS 审计和鉴证专业人员的执行绩效所应达到的最低标准
- 管理层和其他利益方对执业者在专业工作上的期望
- 注册信息系统审计师 (CISA®) 认证持有人的特定要求。如果 CISA 认证持有人未能遵守这些标准，则可能会导致 ISACA 董事会或适当的委员会对其行为进行调查，进而采取相应的纪律措施。

IS 审计和鉴证专业人员应当根据情况在其工作底稿中包括一项声明，说明已根据 ISACA IS 审计和鉴证标准或其他适用的专业标准完成该项业务。

适用于 IS 审计和鉴证专业人员的 ITAF™ 框架提供了多层次的指引：

- **标准**，分为三类：
 - 通用标准（1000 系列）——是 IS 审计和鉴证专业人员的工作指导原则。这些标准适用于所有任务的执行，而且还涉及到 IS 审计和鉴证专业人员的道德、独立性、客观性和应有的审慎性，以及知识、职业能力和技能。标准声明（其中**粗体**部分）是强制性的。
 - 履行标准（1200 系列）——涉及到任务执行，例如，规划与监督、任务范围、风险与重要性、资源调动、监督与任务管理、审计与鉴证证据，以及专业判断和应有的审慎性。
 - 报告标准（1400 系列）——涉及到报告类型、沟通方式以及传达的信息
- **准则**，支持标准，并且同样分为三类：
 - 通用准则（2000 系列）
 - 履行准则（2200 系列）
 - 报告准则（2400 系列）
- **工具和技术**，为 IS 审计和鉴证专业人员提供附加指导，如白皮书、IS 审计/鉴证计划和 COBIT® 5 产品系列

ITAF 中所使用的在线术语表请参见 www.isaca.org/glossary。

免责声明：ISACA 设计的此指南是根据 ISACA 职业道德规范中关于职业责任的规定所应达到的最低绩效水平。ISACA 不断言使用此产品将保证带来成功的结果。该出版物不应当被视为包含所有合适的程序或测试，或排除通过合理引导获得相同结果的其他程序或测试。在确定任何具体程序或测试是否适当时，控制或专业人员应当对特定系统或 IS 环境呈现的具体控制情况作出其独立的专业判断。

ISACA 专业标准和职业管理委员会 (PSCMC) 为准备标准和指南，致力于进行广泛的磋商。在发布任何文件之前，会在全球领域公布一份征求意见稿，以征求公众的意见。反馈意见也可以通过电子邮件 (standards@isaca.org)、传真 (+1.847. 253.1443) 或邮件 (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA) 等方式向专业标准开发总监提交。

ISACA 2012-2013 专业标准和职业管理委员会

Steven E. Sizemore, CISA, CIA, CGAP, 主席	Texas Health and Human Services Commission, 美国
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, 英国
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, 美国
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, 马来西亚
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, 新西兰
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., 日本
Ian Sanderson, CISA, CRISC, FCA	NATO, 比利时
Timothy Smith, CISA, CISSP, CPA	LPL Financial, 美国
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., 阿根廷

IS 审计和鉴证标准 1205 证据

声明

1205.1 IS 审计和鉴证专业人员应当获取充分和适当的证据，为项目结果提供合理的结论依据。

1205.2 IS 审计和鉴证专业人员应当评估所获证据是否足以支持结论并实现项目目标。

重要方面

执行某个项目时，IS 审计和鉴证专业人员应当：

- 获得充分和适当的证据，其中包括：
 - 执行的程序
 - 执行程序的结果
 - 原始文件（电子或纸质格式）、记录和用于支持项目的佐证信息
 - 项目的发现和结果
 - 有关已完成工作并遵守适用的法律、法规 and 政策的记录
- 准备文献记录，这些应当：
 - 在一段时间内保留和保持可用，并采用符合审计和鉴证组织的政策以及相关专业标准、法律和法规的格式
 - 在其整个准备和保留期间得到保护，防止未经授权的披露或修改
 - 在保留期结束时得到妥善处理
- 从控制测试中获取证据时，考虑证据是否足以证明评估出来的控制风险水平。
- 适当地对证据进行识别、交叉引用和登记分类。
- 评估证据的可靠性时，考虑其来源、性质（如书面、口头、视像、电子）和真实性（如数字和手工签名、盖章）。
- 考虑收集必要证据、满足项目目标和风险要求的最有效和最及时手段。然而，困难或成本不能成为省略必要程序的有效理由。
- 根据被审计的主题（即其性质、审计时间安排、专业人员的判断）选择最合适的程序收集证据。用于获取证据的程序包括：
 - 问询和确认
 - 重新执行
 - 重新计算
 - 计算
 - 分析程序
 - 检查
 - 观察
 - 其它普遍接受的方法
- 考虑所获任何信息的来源和性质，以评估其可靠性以及是否需要进一步核查。一般而言，下列证据的可靠性较高：
 - 采用书面形式，而不是口头表达
 - 获取自独立的来源
 - 由专业人员而不是被审计的实体获取
 - 经过独立方鉴定
 - 由独立方保管
 - 检查结果
 - 观察结果

IS 审计和鉴证标准 1205 证据

- 重要方面
- 续
- 足以让合格的独立方能够重新执行测试并获得相同结果和结论的证据。
 - 获得与项目的重要性及相关风险相称的证据。
 - 当 IS 审计或鉴证专业人员利用获取自企业的信息执行审计程序时，要适当强调信息的准确性和完整性。
 - 当足够的证据不能以与沟通 IS 审计或鉴证项目结果一致的方式获取时，这种情况应当被披露。
 - 确保证据安全，防止未经授权的访问和修改。
 - 在完成 IS 审计或鉴证工作后保留证据一段时间，而时间的长度需符合所有适用的法律、法规和政策。
-

术语

术语	定义
适当的证据	证据质量的衡量指标
足够的证据	证据数量的衡量指标；支持审计目标和范围方面的所有重大问题。参见证据。

关联准则

类型	标题
准则	2205 证据

生效日期

本 ISACA 标准自 2013 年 11 月 1 日起对所有 IS 审计和鉴证业务生效。