IS 审计和鉴证标准
1207 违规和非法行为

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。

IS 审计和鉴证标准 1207 违规和非法行为

声明

1207.1 在完成审计和鉴证项目期间，IS 审计和鉴证专业人员应当考虑违规和非法行为的风险。

1207.2 在完成审计和鉴证项目期间，IS 审计和鉴证专业人员应当保持职业怀疑态度。

1207.3 IS 审计和鉴证专业人员应当将任何重大违规或非法行为记录在案，并及时通报给相应的当事方。

重要方面

IS 审计和鉴证专业人员应当：

- 在规划和执行项目时通过以下手段将审计风险降低到可接受的水平：
  - 意识到由于违规和非法行为造成的重大错误、控制缺陷或误报仍可能存在，无论违规和非法行为的风险评估结果如何
  - 获取并了解企业及其环境，包括旨在预防和检测项目主题、范围和目标相关的违规和非法行为的内部控制
  - 获取充分和适当的证据，以确定企业内部的管理层或其他人员是否知悉任何实际、怀疑或宣称的违规和非法行为
- 执行审计程序时，考虑可能表明违规和非法行为带来的重大错误、控制缺陷或误报风险的异常或意外关系，
- 设计和执行相关程序，以测试内部控制的适宜性以及管理人员凌驾于旨在预防或检测违规和非法行为的控制之上的风险，
- 评估识别出的错误、控制缺陷或误报是否预示着违规或非法行为。 如果确有这种迹象，考虑这对项目的其他相关方面的影响，尤其是对管理层声明的影响。
- 至少每年一次获取管理层的书面声明，或根据项目情况更频繁地获取，以便：
  - 承认管理层有责任设计和执行内部控制以防止和检测违规和非法行为。
  - 披露表明由于违规或非法行为，可能存在错误、控制缺陷或误报的任何风险评估的中肯结果。
  - 披露管理层知晓的，影响企业的违规和非法行为其与担任内部控制重要角色的管理层和员工有关的事件。
  - 披露如员工、前员工、监管机构和其他人员所通报，管理层知晓的影响企业的任何宣称或怀疑的违规或非法行为。
- 及时：
  - 向适当的管理层通报识别或获取的、有关可能存在重大违规或非法行为的任何信息
  - 向治理负责人通报涉及担任内部控制重要角色的管理层或员工的任何重大违规或非法行为
- 向治理负责人报告内部控制设计和执行中的任何重大漏洞，这些内部控制旨在预防和检测项目期间识别的、即便在范围之外的任何违规和非法行为。
- 考虑适用于该情形的法律及专业报告要求。
- 如果重大错误、控制缺陷、误报或非法行为影响项目的继续执行，考虑退出项目。
- 记录已上报管理层、治理负责人、监管机构及其他人员的、与重大违规或非法行为相关的所有通讯、规划、结果、评估及结论。

IS 审计和鉴证标准 1207 违规和非法行为

术语

术语	定义
违规	违反既定的管理政策或法规要求。作为重大过失或无意的非法行为，它可包括有意误报或遗漏有关被审计领域或企业整体的信息。
重大误报	在可衡量的程度上影响审计结果的、意外或故意的失实陈述
职业怀疑态度	包括质疑心态和批判性评估审计证据在内的一种态度。 来源：美国注册会计师协会 (AICPA) AU 230.07

关联标准和准则

类型	标题
标准	1008 衡量标准
标准	1202 规划中的风险评估
标准	1205 证据
准则	2206 使用其他专家的成果
准则	2207 违规和非法行为

生效日期　本 ISACA 标准自 2013 年 11 月 1 日起对所有 IS 审计和鉴证业务项目生效。