IS 审计和鉴证标准
1202 规划中的风险评估

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 1202 规划中的风险评估

声明

1202.1 IS 审计和鉴证职能部门应当运用适当的风险评估方法和佐证方法来制定总体的 IS 审计计划，并确定有效分配 IS 审计资源的优先顺序。

1202.2 IS 审计和鉴证专业人员应当在规划单个项目时，识别和评估与被审领域相关的风险。

1202.3 IS 审计和鉴证专业人员应当考虑主题事项风险、审计风险以及企业所面临的相关风险暴露。

重要方面

规划现行的活动时，IS 审计和鉴证职能部门应当：

- 至少每年进行风险评估一次并书面记录，以便制订 IS 审计计划。
- 包含组织的战略计划和目标及企业风险管理框架和举措作为风险评估工作组成的一部分来考虑。
- 针对每个 IS 审计和鉴证项目，量化并证明满足项目要求所需要的 IS 审计资源数量。
- 在选择审计感兴趣的领域和项目，以及作出关于设计和进行特定 IS 审计和鉴证项目的决定时使用风险评估。
- 向审计利益相关方及其他适当的当事人寻求风险评估的批准。
- 以风险评估为依据考虑和安排 IS 审计和鉴证工作的优先性。
- 以风险评估为依据制订以下性质的计划：
  - 用作 IS 审计和鉴证活动的框架
  - 考虑非 IS 审计和鉴证的要求和活动
  - 每年至少更新一次，并由治理负责人审批
  - 阐述审计章程规定的职责

规划各个项目时，IS 审计和鉴证专业人员应当：

- 识别和评估与被审计单位相关的风险。
- 针对每一个项目初步评估与被审计单位相关的风险。每一项具体项目的目标应当反映初步风险评估的结果。
- 在考虑风险领域和规划具体项目时，要考虑之前的审计、审核和发现，包括任何补救措施。还要考虑董事会的总体风险评估流程。
- 在规划和执行 IS 审计的同时，试图通过适当评估项目的IS 主题事项及与其相关的控制，将审计风险降低到可接受的水平并符合审计目标。
- 规划具体的 IS 审计程序时，要认识到，重要性阈值越低，审计预期越准确，则审计风险越高。
- 若要降低风险、实现较高的重要性，可以通过扩大控制测试的范围（降低控制风险）和/或扩大实质性测试程序的范围（降低检测风险）等补偿措施来获得额外保证。

术语

术语	定义
审计章程	经治理层批准的一种文件，用于定义内部审计活动的目的、职权和责任。 该章程应当：

©2013 ISACA 保留所有权利。

	• 明确内部审计职能部门在企业内部的定位 • 为履行 IS 审计和鉴证业务，授予对相关记录、人员和有形财产的访问权限 • 定义审计职能部门的工作范围
审计风险	根据审计结果得出错误结论的风险。审计风险的三个组件如下： • 控制风险 • 检测风险 • 固有风险
审计主题风险	与被审领域相关的风险： • 业务风险（客户的支付能力、信誉和市场因素等） • 合同风险（债务、价格、类型和处罚等） • 国家风险（政治、环境和安全等） • 项目风险（资源、技能组合、方法和产品稳定性等） • 技术风险（解决办法、架构、硬件和软件基础设施网络、交付渠道等） 参见固有风险。
控制风险	该风险是指存在无法通过内部控制系统及时防止或检测的重大错误。 （参见固有风险。）
检测风险	该风险是指 IS 审计或鉴证专业人员无法通过其实质性程序检测到重大、单个或与其他错误相结合的错误。参见审计风险。
固有风险	不考虑管理层已经或可能采取的措施（即实施控制）的风险水平或风险暴露。参见控制风险。
重要性	关于某个信息项目在其对被审计实体履行职能的影响或作用方面的重要性的审计概念。它表示特定事项在企业作为一个整体的背景下的相对意义或重要性。
风险评估	用于识别和评估风险及其潜在影响的一种流程。 风险评估用于识别会给企业带来最高风险、漏洞或暴露的项目或领域，以便列入 IS 年度审计计划。 风险评估还用于管理项目交付和项目效益风险。
实质性测试	在审计期间获取有关活动或交易的完整性、准确性或存在性的审计证据

关联准则

类型	标题
准则	2202 规划中的风险评估

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。

© ISACA 2013　保留所有权利。