IS 审计和鉴证标准
1008 衡量标准

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 1008 衡量标准

声明

1008.1 **IS 审计和鉴证专业人员所选择的用于对照评估主题事项的衡量标准应当客观、完整、相关、可测量、易理解、得到广泛认可、具权威性的，并且所有阅读和使用 IS 审计和鉴证报告的人员均能了解或可以得到。**

1008.2 **IS 审计和鉴证专业人员应当考虑衡量标准的来源，并且在采用知名度较低的标准之前，重点考虑那些由相关权威机构发布的衡量标准。**

重要方面

IS 审计和鉴证专业人员应当：

- 慎重考虑衡量标准的选择，并且能够提出该选择的依据。
- 运用专业判断，以确保一旦应用，衡量标准的使用将有助得出公正和客观、不会误导报告的读者或使用者的意见。要认识到，管理层可能提出不符合所有要求的衡量标准。
- 在确定项目要求时，考虑衡量标准的适用性和可用性。
- 若衡量标准不容易得到、不完整或需要解释时，报告应该包含必要的描述及其他信息，以确保报告公正、客观及可理解，同时确保报告中包含使用该标准之背景。

应当参照以下五条适用性衡量标准，来评价主题事项评估标准的适用性和可用性：

- **客观性**——标准不应具有任何偏颇，否则会对专业人员的结果和结论造成不良影响，并且可能会相应地误导报告的使用者。
- **完整性**——标准应足够完整，才能在执行 IS 审计或鉴证项目时，识别和使用会对专业人员就相应主题事项得出的结论造成影响的所有标准。
- **关联性**——衡量标准应与主题事项相关，并有助于得出满足 IS 审计或鉴证项目目标的结果和结论。
- **可衡量性**——衡量标准应确保对主题事项的衡量方法一致，并保证不同的专业人员在类似情况下得出一致的结论。
- **可理解性**——标准应表达清晰，而不会造成不同使用者的理解明显不同。

衡量标准的可接受性受衡量标准的可用性影响，专业人员报告的使用者只有能够得到衡量标准，才能理解鉴证活动的依据以及结果和结论的相关性。来源应具有以下性质：

- **公认性**——衡量标准应当得到足够广泛的认可，这样才能保证其使用不会受到目标使用者的质疑。
- **权威性**——应当寻求能够反映该领域的权威性公告并切合主题事项的衡量标准。例如，权威性公告可能来自专业机构、行业团体、政府和监管机构。
- **公开提供**——衡量标准应当面向专业人员报告的使用者提供。实例包括 ISACA、国际会计师联合会 (IFAC) 等专业会计与审计机构以及其他公认的政府或专业机构开发的标准。
- **面向所有使用者提供**——衡量标准若不公开提供，则应当通过专业人员报告的认定表述向所有使用者传达。认定由有关主题事项的、符合适用的衡量标准的要求的声明组成，以保证其可以接受审计。

© ISACA 2013 保留所有权利。

重要方面（续）

除适用性和可用性之外，就其使用及潜在受众而言，选择 IS 鉴证标准时还应当考虑其来源。例如，当处理政府法规时，适用于主题事项的相关法律及法规而制定的认定应该是最恰当，基于这些认定的衡量标准可能是最合适的选择。在其他情况下，行业或专业协会的衡量标准可能更适合。衡量标准的来源如下（按考虑因素列举）：

- **ISACA 制定的衡量标准**——这些是可以通过公开渠道获取的准则和标准，并已得到由国际公认的 IT 治理、控制、安全和鉴证领域的专家参与的同业评审和全面的尽职审查。
- **其他专家团体制订的衡量标准**——类似于 ISACA 标准和准则，这些切合主题事项的标准由各领域的专家编制，并接受过同行评审和彻底的尽职调查。
- **法律和法规制定的衡量标准**——尽管法律和法规可以提供衡量标准的依据，但必须慎重使用。通常法律的措词非常复杂，并且具有特定的法律含义。许多情况下，这些法律和法规的要求有必要以认定的形式进行表述。另外，通常仅限由法律界人士表达法律意见。
- **由未遵循审慎程序的机构制定的衡量标准**——这些包括由不遵循审慎程序的其他机构制订，并且未接受过公众谘询和讨论的相关标准。
- **专为 IS 审计或鉴证项目制订的衡量标准**——尽管专为 IS 审计或鉴证项目制定的标准也许是适当的，但需特别慎重，以保证这些标准符合适用性原则，尤其是完整性、可测性和客观性。专为 IS 审计或鉴证项目制定的标准以认定的形式表述。

应当慎重考虑选择的条件。尽管遵循地方法律和法规非常重要，并且必须被视为一项强制性要求，但许多 IS 审计和鉴证项目所涉及的领域往往不受法律或法规所规范，如变更管理、IT 一般控制和访问控制。此外，某些行业，如支付卡行业，却制订了必须遵循的强制性要求。当法律要求仅为原则性的要求时，专业人员应当确保所选择的衡量标准符合项目目标。

随着项目的推进，当有额外的信息指出某衡量标准已经不再适用于实现审计目标。在这些情况下，不需要继续完成与该等衡量标准相关的工作。

术语

术语	定义
衡量标准	用于衡量和表述主题事项、同时供 IS 审计师参照评估主题事项的标准和基准指标。 衡量标准应该： • 客观——不偏不倚 • 完整——包含得出结论所需要的所有相关因素 • 相关——切合主题事项 • 可衡量——提供一致的衡量方法 在鉴证项目中，可参照基准指标评估管理层有关主题事项的书面认定。从业人员通过引述适用的衡量标准

	形成有关主题事项的结论。

关联准则

类型	标题
准则	2008 衡量标准

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。