ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25067—2010/ISO/IEC 27006:2007

信息技术　安全技术
信息安全管理体系审核认证机构的要求

Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems

(ISO/IEC 27006:2007,IDT)

2010-09-02 发布　　2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准等同采用 ISO/IEC 27006:2007《信息技术　安全技术　信息安全管理体系审核认证机构的要求》。

本标准是信息安全管理体系标准族的标准之一。

为了便于理解，并与 GB/T 27021—2007 和 GB/T 22080—2008 协调，本标准针对 ISO/IEC 27006:2007 做以下编辑性处理：

——针对认证机构的管理时，用词汇“程序”表示“procedure”；针对客户组织的管理时，用词汇“规程”表示“procedure”；

——针对认证机构的管理时，用词汇“政策”表示“policies”；针对客户组织的管理时，用词汇“策略”表示“policies”；

——用词汇“客户组织”表示“client”或“client organization”；

——用词汇“审核时间”表示“audit time”或“ autitor time”。

本标准的附录 A、附录 B、附录 C 和附录 D 是资料性附录。

本标准由全国认证认可标准化技术委员会(SAC/TC 261)和全国信息安全标准化技术委员会(SAC/TC 260)提出。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)归口。

本标准起草单位：中国合格评定国家认可中心、中国电子技术标准化研究所、北京知识安全工程中心、广东赛宝认证中心服务有限公司、中国信息安全认证中心、华夏认证中心有限公司、北京同方信息安全技术股份有限公司、北京北大青鸟商用信息系统有限公司、中讯软件集团股份有限公司。

本标准主要起草人：刘晓红、胡啸、汪修慈、王新杰、宋红茹、闵京华、王梅、王连强、费杨、韩硕祥、赵战生、娄天峰、娄丹、布宁、刘宇。

引　言

GB/T 27021—2007 是针对实施组织管理体系审核和认证的机构提出运作准则的国家标准，它等同采用 ISO/IEC 17021:2006。如果这类机构按照 GB/T 22080—2008 开展以信息安全管理体系(ISMS)审核和认证为目的的活动，并打算依据 GB/T 27021—2007 获得认可，对 GB/T 27021—2007 增加一些要求和指南是必要的。本标准提供了这样的内容。

本标准正文遵循 GB/T 27021—2007 的结构，针对 ISMS 审核和认证所增加的特定要求和指南，用“IS”加以标识。

贯穿本标准全文，使用“应”(shall)这一术语，以表示本标准中与 GB/T 27021—2007 和 GB/T 22080—2008 的要求相对应的条款是要求性的，认证机构必须遵循；使用“宜”(should)这一术语，以表示尽管本标准中与 GB/T 27021—2007 和 GB/T 22080—2008 的要求相对应的条款是指南性的，构成了对这些标准中要求的应用指南，但仍然期望认证机构采纳。

本标准的目的之一是使得那些认可机构能够更加协调一致地应用评审认证机构所依据的标准。认证机构在贯彻本标准的指南性条款时所形成的任何不同，可视为一个例外。针对这种不同，只有当认证机构向认可机构证实那些例外以等效的方式满足 GB/T 27021—2007 和 GB/T 22080—2008 的相关条款要求以及本标准的意图时，并仅在具体问题具体分析的基础上才被允许。

信息技术　安全技术
信息安全管理体系审核认证机构的要求

1　范围

本标准对实施信息安全管理体系(以下简称“ISMS”)审核和认证的机构提出要求并提供指南,以作为对 GB/T 27021—2007 和 GB/T 22080—2008 要求的补充。制定本标准的主要意图是对实施 ISMS 认证的认证机构的认可提供支持。

任何提供 ISMS 认证的机构需要在能力和可靠性方面证实其满足本标准的要求。本标准的指南性条款为这些要求提供了进一步的说明。

注:本标准可以作为认可、同行评审或其他审核过程的准则性文件。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 19011　质量和(或)环境管理体系审核指南(GB/T 19011—2003,ISO/IEC 19011:2002,IDT)

GB/T 22080—2008　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2005,IDT)

GB/T 27021—2007　合格评定　管理体系审核认证机构的要求(ISO/IEC 17021:2006,IDT)

3　术语和定义

GB/T 27021—2007 和 GB/T 22080—2008 中确立的以及下列术语和定义适用于本标准。

3.1

认证证书　certificate

由认证机构依照认可条件颁发的,并带有认可标识或声明的一种文件。

3.2

认证机构　certification body

按照正式发布的 ISMS 标准及 ISMS 所要求的任何补充性文件,对客户组织的 ISMS 进行评定和认证的第三方机构。

3.3

认证文件　certification document

表明客户组织的 ISMS 符合指定的 ISMS 标准及 ISMS 所要求的任何补充性文件的一类文件。

3.4

标志　mark

依法注册的商标或在认可机构或认证机构的规则下颁发的受到保护的标识,以表明对组织所运行的管理体系建立足够信心,或者表明相关的产品或人员符合指定标准的要求。

3.5

组织　organization

公司、集团、事务所、工厂、政府机构、科研机构、学校等,或者其部分或组合,无论其是否是法人,还是公有或私有的,均具有其自身的职能和管理并能够确保实施其信息安全。