ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25067—2016/ISO/IEC 27006:2011
代替 GB/T 25067—2010

信息技术　安全技术　信息安全管理体系审核和认证机构要求

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

(ISO/IEC 27006:2011,IDT)

2016-10-13 发布　　2017-05-01 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

本标准按照 GB/T 1.1—2009 和 GB/T 20000.2—2009 给出的规则起草。

本标准代替 GB/T 25067—2010《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》。

本标准与 GB/T 25067—2010 相比，主要技术变化如下：

——新增 IS 7.1.2 能力准则的确定；

——监督方案明确为三年内的周期[见 9.1.4.2e)]；

——GB/T 25067—2010 多处“宜”的描述在本标准中改为“应”(见附录 NA)。

本标准使用翻译法等同采用 ISO/IEC 27006:2011《信息技术　安全技术　信息安全管理体系审核和认证机构要求》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 19011—2013 管理体系审核指南(ISO 19011:2011，IDT)

本标准做了下列编辑性修改：

——纠正了原文注日期引用文件不一致的问题；

——增加了资料性附录 NA。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国电子技术标准化研究院、中国合格评定国家认可中心、广州赛宝认证中心服务有限公司、上海质量审核中心、中国质量认证中心、中国信息安全认证中心、中国船级社质量认证公司、华夏认证中心有限公司、黑龙江电子信息产品监督检验院。

本标准主要起草人：黄俊梅、韩硕祥、刘宇、倪文静、蔡北方、费杨、付志高、刘健、赵国祥、田刚、王军、尹冰、刘钢、杨勇、刘佳、魏军、尤其、程瑜琦、朱博、周召、夏芳、刘建毅、王希忠、马遥、黄俊强。

本标准所代替标准的历次版本发布情况为：

——GB/T 25067—2010。

引　言

ISO/IEC 17021 为机构对组织的管理体系实施审核和认证建立了准则。如果这类机构按照 GB/T 22080—2008《信息技术　安全技术　信息安全管理体系　要求》开展以信息安全管理体系(ISMS)审核和认证为目的的活动,并准备依据 ISO/IEC 17021 获得认可,对 ISO/IEC 17021 补充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 ISO/IEC 17021 的结构,针对 ISMS 认证所增加的特定要求和指南,以字母“IS”进行识别。

贯穿本标准全文,使用“应”这一术语,以表示本标准中与 ISO/IEC 17021 和 GB/T 22080—2008 的要求相对应的条款是要求性的;使用“宜”这一术语表示建议。

本标准的目的之一是使得认可机构能更有效地、协调一致地应用本标准,依据此标准评审认证机构。

注:本标准中“管理体系”和“体系”可以互换使用。管理体系的定义见 GB/T 19000—2008。本标准中使用的管理体系请勿与其他类型的系统混淆,例如,信息技术系统(IT 系统)。

信息技术　安全技术　信息安全管理体系
审核和认证机构要求

1　范围

本标准对信息安全管理体系(以下简称 ISMS)审核和认证的机构规定了要求并提供了指南,以作为对 ISO/IEC 17021:2011 和 GB/T 22080—2008 中相关要求的补充。本标准的主要目的是为提供 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。本标准的指南为这些要求提供了进一步的解释。

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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

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)

ISO/IEC 17021:2011　合格评定　管理体系审核认证机构的要求(Conformity assessment—Requirements for bodies providing audit and certification of management systems)

ISO 19011　管理体系审核指南(Guidelines for auditing management systems)

3　术语和定义

GB/T 22080—2008 和 ISO/IEC 17021:2011 界定的以及下列术语和定义适用于本文件。

3.1

证书　certificate

由认证机构根据认可条件颁发的,并带有认可标识或声明的一种证书。

3.2

认证机构　certificate body

按照正式发布的 ISMS 标准和该体系所要求的任何补充性文档,对客户组织的 ISMS 进行评估和认证的第三方机构。

3.3

认证文件　certificate 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档的一类文件。

3.4

标志　mark

在认可机构或认证机构的规则下颁发的依法注册的商标或其他受到保护的标识,表明对机构运行的体系具有足够信心,或者表明相关的产品或人员符合指定的标准的要求。