ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25067—2020/ISO/IEC 27006:2015
代替 GB/T 25067—2016

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 27006:2015,IDT）

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
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 给出的规则起草。

本标准代替 GB/T 25067—2016《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 GB/T 25067—2016 相比，主要技术变化如下：

——在规范性引用文件中，删除了 ISO 19011，新增了 ISO/IEC 27000(见第 2 章)；

——删除了术语“证书”“认证机构”“标志”和“组织”(见 2016 年版的第 3 章)；

——基于 GB/T 27021.1—2017 的附录 A，细化了参与信息安全管理体系认证的各类人员的能力要求(见 7.1.2)；

——遵从 GB/T 27021.1—2017 的标准结构，调整了第 9 章过程要求的内容(见第 9 章，2016 年版的第 9 章)；

——审核时间计算由资料性附录调整为规范性附录(见附录 B)，并新增了审核时间计算示例(见附录 C)。

本标准使用翻译法等同采用 ISO/IEC 27006:2015《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 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2016，IDT)

本标准做了以下编辑性修改：

——因 ISO 9000:2005 已经废止，所以引言中管理体系的定义调整为参见 GB/T 19000—2016；

——增加了资料性附录 NA；

——词汇“procedure”，在针对认证机构运作管理时翻译为“程序”[见 7.1.2.4.1 b)、9.1.3.2、9.1.5.1.2 等]，在针对客户信息安全控制管理时翻译为“规程”[见 7.1.2.1.4 a)、9.2.2.2 a)、9.3.1.2.1 a)等]，两者意思并无差异；

——由于附录 A 只在 7.1.1 中被引用，根据国家标准起草规定，将 7.1.1 的注调整为标准条文；

——对表 D.1 中控制“A.13.1.3 网络中的隔离”的“审核的评审指南”，更正了网段和网络隔离的示例。

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：中国合格评定国家认可中心、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、广州赛宝认证中心服务有限公司、华夏认证中心有限公司、国家认证认可监督管理委员会、山东省标准化研究院。

本标准主要起草人：付志高、张强、黄俊梅、魏军、田刚、夏芳、张志国、尤其、方洁、王曙光、刘鑫。

本标准所代替标准的历次版本发布情况为：

——GB/T 25067—2010、GB/T 25067—2016。

引　言

GB/T 27021.1—2017 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—2016 开展以信息安全管理体系(以下简称“ISMS”)审核和认证为目的活动,并准备依据 GB/T 27021.1—2017 获得认可,对 GB/T 27021.1—2017 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 GB/T 27021.1—2017 的结构,针对 ISMS 审核和认证所增加的特定要求和指南,用字母“IS”加以标识。

本标准的主要目的是使得认可机构在应用其评审认证机构所依据的标准时能更有效地协调一致。

本标准中术语“管理体系”和“体系”可以互换使用。管理体系的定义见 GB/T 19000—2016。请不要将本标准中使用的管理体系与其他类型的系统混淆,例如,信息技术(以下简称“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

本标准在GB/T 27021.1—2017和GB/T 22080—2016的基础上，对实施ISMS审核和认证的机构规定了要求并提供了指南。本标准的主要目的是为ISMS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中的要求。本标准中的指南提供了对这些要求的进一步解释。

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—2016　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2013，IDT)

GB/T 27021.1—2017　合格评定　管理体系审核认证机构要求　第1部分：要求(ISO/IEC 17021-1:2015，IDT)

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)

3　术语和定义

GB/T 27021.1—2017和ISO/IEC 27000界定的以及下列术语和定义适用于本文件。

3.1

认证文件　certification document

表明客户的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。

4　原则

GB/T 27021.1—2017中第4章的原则适用。

5　通用要求

5.1　法律与合同事宜

GB/T 27021.1—2017中5.1的要求适用。

5.2　公正性的管理

GB/T 27021.1—2017中5.2的要求适用。并且，以下要求和指南适用。