ICS 35.030;03.120.20
CCS L 70;A 00

中华人民共和国国家标准

GB/T 25067—2026/ISO/IEC 27006-1:2024
代替 GB/T 25067—2020

网络安全技术　信息安全管理体系审核和认证机构要求

Cybersecurity technology—Requirements for bodies providing audit and certification of information security management systems

（ISO/IEC 27006-1:2024，Information security，cybersecurity and privacy protection—Requirements for bodies providing audit and certification of information security management systems—Part 1：General，IDT）

2026-05-25 发布　　2026-12-01 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 25067—2020《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—2020相比,除结构调整和编辑性改动外,主要技术变化如下:

a) 增加了“控制”“外部环境”“信息安全”等术语和定义(见第3章);

b) 更改了管理利益冲突的要求(见5.2.2,2020年版的5.2.1);

c) 更改了审核员的工作经历、培训经历和审核经历要求(见7.2.2.2,2020年版的7.2.1.1);

d) 更改了技术专家的工作经历要求[见7.2.2.3b),2020年版的7.2.1.1];

e) 增加了远程审核的相关要求(见8.2.2、9.1.3.3、9.4.3.2);

f) 增加了认证文件中引用其他标准的要求(见8.2.3);

g) 增加了审核与认证职能所需知识和技能(见附录A);

h) 更改了审核时间计算的相关要求(见C.2.1、C.3.2、C.3.3、C.3.4、C.6、C.7,2020年版的B.2.1、B.3.2、B.3.3、B.6)。

本文件等同采用ISO/IEC 27006-1:2024《信息安全、网络安全和隐私保护　信息安全管理体系审核和认证机构要求　第1部分:通则》。

本文件做了下列最小限度的编辑性改动:

——为与我国网络安全国家标准协调一致,标准名称改为《网络安全技术　信息安全管理体系审核和认证机构要求》。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中国合格评定国家认可中心、中国电子技术标准化研究院、中国网络安全审查认证和市场监管大数据中心、北京赛西认证有限责任公司、广州赛宝认证中心服务有限公司、江苏保旺达软件技术有限公司、杭州趣链科技有限公司、浙江省电子信息产品检验研究院、北京时代新威信息技术有限公司、杭州高新区(滨江)区块链与数据安全研究院、南方电网数字电网集团信息通信科技有限公司、深圳大学。

本文件主要起草人:付志高、张强、许玉娜、翟亚红、黄俊梅、陈艳、方洁、魏立茹、王秉政、王连强、刘险峰、张晴、尹肖栋、魏遵博、陈鹏、刘伟丽、潘文博。

本文件及其所代替文件的历次版本发布情况为:

——2010年首次发布为GB/T 25067—2010,2016年第一次修订,2020年第二次修订;

——本次为第三次修订。

引　言

GB/T 27021.1—2017 对实施管理体系审核和认证的机构规定了要求并提供了指南。符合 GB/T 27021.1—2017 的机构在依据 GB/T 22080—2025 对组织的信息安全管理体系(ISMS)实施审核和认证活动时,有必要对 GB/T 27021.1—2017 补充一些要求和指南。本文件提供了这些要求和指南。

本文件对提供 ISMS 审核和认证的机构规定了要求,这类机构被称为认证机构。本文件规定了 ISMS 认证机构的通用要求。认证机构遵守这些要求,确保其以有能力、一致和公正的方式实施 ISMS 认证,这将促进国内外对这些机构及其认证结果的承认与接受。

本文件正文与 GB/T 27021.1—2017 的结构保持一致。

网络安全技术　信息安全管理体系审核和认证机构要求

1　范围

本文件在GB/T 27021.1—2017的基础上，对ISMS审核和认证机构规定了要求并提供了指南。

提供ISMS认证的机构从能力和可靠性方面证实其符合本文件中的要求。本文件中的指南提供了对这些要求的进一步解释。

注：本文件能作为认可、同行评审或其他审核过程的准则。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2025　网络安全技术　信息安全管理体系　要求(ISO/IEC 27001:2022，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)

3　术语和定义

GB/T 27021.1—2017界定的以及下列术语和定义适用于本文件。

ISO和IEC维护的用于标准化的术语数据库网址如下：

——ISO在线浏览平台：https://www.iso.org/obp；

——IEC电工百科：https://www.electropedia.org/。

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。

注：本定义并没有限制统称为认证文件的文件数量。

3.2

控制　control

保持和/或改变风险(3.10)的措施。

注1：控制包括但不限于保持和/或改变风险(3.10)的任何过程、方针、设备、实践或其他条件和/或行动。

注2：控制并非总能取得预期的改变效果。

[来源：GB/T 22081—2024，3.1.8]

3.3

外部环境　external context

组织(3.9)寻求实现其目标时所处的外部状况。

注：外部环境可能包括如下方面：

——文化、社会、政治、法律、监管、金融、技术、经济、自然和竞争环境，无论是国际的、国家的、地区的还是地方的；