



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	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 原则	4
5 通用要求	4
5.1 法律与合同事宜	4
5.2 公正性的管理	4
5.3 责任和财力	4
6 结构要求	4
7 资源要求	4
7.1 人员能力	4
7.2 参与认证活动的人员	7
7.3 外部审核员和外部技术专家的使用	8
7.4 人员记录	8
7.5 外包	8
8 信息要求	8
8.1 公开信息	8
8.2 认证文件	8
8.3 认证的引用和标志的使用	8
8.4 保密	8
8.5 认证机构与其客户间的信息交换	9
9 过程要求	9
9.1 认证前的活动	9
9.2 策划审核	12
9.3 初次认证	12
9.4 实施审核	13
9.5 认证决定	14
9.6 保持认证	14
9.7 申诉	15
9.8 投诉	15
9.9 客户的记录	15

10 认证机构的管理体系要求	16
10.1 可选方式	16
10.2 方式 A:通用的管理体系要求	16
10.3 方式 B:与 ISO 9001 一致的管理体系要求	16
附录 A (规范性) ISMS 审核与认证所需的知识和技能	17
附录 B (资料性) 能力的其他考虑因素	18
B.1 通用能力	18
B.2 特定知识和经验	18
附录 C (规范性) 审核时间	19
C.1 通则	19
C.2 概念	19
C.3 确定初次认证审核时间的程序	20
C.4 监督审核的审核时间	23
C.5 再认证审核的审核时间	23
C.6 多场所的审核时间	23
C.7 扩大认证范围的审核时间	23
附录 D (资料性) 审核时间计算方法	24
D.1 概述	24
D.2 审核时间计算因素的分级	24
D.3 审核时间计算的示例	25
附录 E (资料性) 对已实现的 GB/T 22080—2025 附录 A 中控制的审核指南	28
E.1 目的	28
E.2 如何使用表 E.1	28
参考文献	39

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;