国家标准《网络安全技术 信息安全管理体系审核和认证机构要求》编制说明

**一、工作简况**

**1.1 任务来源**

全国网络安全标准化技术委员会2024年11月下达标准立项通知，《网络安全技术 信息安全管理体系审核和认证机构要求》由中国合格评定国家认可中心负责承办。本标准由全国网络安全标准化技术委员会提出并归口。

**1.2 修订背景**

 《网络安全技术 信息安全管理体系审核和认证机构要求》规定了信息安全管理体系（ISMS）认证机构的通用要求。

本次是通过等同采用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：通用》，对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》进行修订。

本次修订将解决ISMS认证审核中远程审核技术的应用、虚拟组织的认证、审核时间计算、ISMS认证证书中引用其他标准等问题。此外，本次修订还将解决与正在制定的GB/T 22080—202X《网络安全技术 信息安全管理体系 要求》和GB/T 22081—2024《网络安全技术 信息安全控制》之间协调一致的问题，以及与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》之间内容重复的问题。

**1.3 起草过程**

中国合格评定国家认可中心负责组织起草，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等单位共同参与本标准的起草工作。具体起草过程如下：

1. 2024年5月，项目牵头单位联合ISMS认证机构和科研单位，组建标准编制工作组，共同研讨新版标准与旧版标准的差异性，并确定任务分工，形成标准草案初稿。
2. 2024年6月，本项目在南昌标准周期间通过了WG7的立项审议。
3. 2024年7月，本项目通过了全国网安标委秘书处组织的标准立项专家评审；此外，项目牵头单位组织来自ISMS认证机构的专家对标准草案进行了审议，并对标准文本进行了完善。
4. 2024年9月，标准牵头单位面向ISMS认可评审员和ISMS认证机构开展了标准草案培训，介绍了标准的修订内容。
5. 2024年11月，全国网安标委下达立项通知，项目牵头单位在全国网安标委网站和微信公众号面向社会公开征集标准参编单位，完成标准编制组的组建。
6. 2024年12月，标准编制组召开启动会，研讨确定标准文本、下一步编制思路、任务分工等，并征集了编制组成员对标准文本的修订意见。标准编制组邀请来自来自网络安全领域和合格评定领域的专家对标准草案进行审查，根据审查意见再次完善标准文本。WG7工作组在海口“标准周”对本项目进行了审议，同意转征求意见阶段；标准编制组根据WG7专家意见修订完善了标准文本，形成征求意见稿。
7. 2025年2月，全国网安标委秘书处组织召开征求意见稿专家审查会，本项目通过评审可以发起公开征求意见。同时，标准编制组根据专家审查意见完善了标准文本。

**二、标准编制原则、主要内容及其确定依据**

**2.1 标准编制原则**

本标准的研制工作遵循以下原则：

（1）一致性原则

本标准等同采用对应国际标准，与对应国际标准在语境语义等方面连贯一致，在充分理解国际标准原文的基础上进行翻译，做到准确表达原意。

（2）易读性原则

统筹兼顾ISO/IEC 27000系列标准和ISO/IEC 17000系列标准在我国的转标实践经验，确保标准内容翻译符合中文语境，表述通畅，具有可读性并使标准读者能够容易理解。

（3）通用性原则

本标准规定了ISMS认证机构的通用要求，转标过程中充分考虑不同类型的ISMS认证机构的运作特点，维护标准内容的普适性。

**2.2 主要内容及其确定依据**

《网络安全技术 信息安全管理体系审核和认证机构要求》在GB/T 27021.1的基础上，对ISMS审核和认证机构规定了要求并提供了指南。本次是等同采用ISO/IEC 27006-1:2024对GB/T 25067-2020进行修订。

本标准包括十章和五个附录。前三章是标准的通用要素，分别为：范围、规范性引用文件、术语和定义。第4章到第10章是标准的主要技术内容，分别为：通用要求、结构要求、资源要求、信息要求、过程要求、管理体系要求。附录A和C是规范性附录，分别规定了认证人员能力和审核时间的要求，附录B、D和E是资料性附录，分别阐述了能力的其他考虑因素、审核时间计算方法和信息安全控制的审核指南。

**2.3 修订前后技术内容的对比**

与GB/T 25067—2020相比，除编辑性改动外，本次修订的主要技术变化如下：

1. 规范性引用文件中删除ISO/IEC 27000（见第2章）；
2. 增加“控制”、“外部环境”、“信息安全”等术语（见第3章）；
3. 调整审核员的工作经历、培训经历和审核经历要求（见7.2.2.2）
4. 调整技术专家的工作经历要求（见7.2.2.3）
5. 修改远程审核的相关要求（见8.2.2、9.1.3.3、9.4.3.2、C.3.2）；
6. 新增认证文件中引用其他标准的要求（见8.2.3）；
7. 修改审核时间计算的相关要求（见C.2.1、C.3.4、C.6、C.7）；
8. 新增附录A，描述了认证职能与知识域的对应关系；
9. 依据GB/T 22080—202X附录A中的信息安全控制，更新附录E（2020版为附录D）；
10. 删除与GB/T 27021.1—2017重复的内容（见5.2、7.1.3、9.3.2.2、9.4等）。

**三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益**

**3.1 试验验证的分析、综述报告**

本标准计划在2025年2月-6月期间，选择ISMS认证机构管理体系建设、ISMS认证机构的内部审核、认可机构认可评审等典型应用场景开展试点验证工作，验证标准的适用性和可行性，并形成试点应用报告。

**3.2 技术经济论证**

暂无。

**3.3 预期的经济效益、社会效益和生态效益**

我国自2006年正式引用ISMS标准并组织开展认证认可工作。截止到2024年11月，有224家认证机构获得国家认证认可监督管理委员会批准，可从事ISMS认证业务，其中获得中国合格评定国家认可委员会（CNAS）认可的51家认证机构；有43544家组织获得了ISMS认证证书。ISMS认证机构通过应用本标准，可进一步提升了自身的管理水平，保障ISMS审核和认证工作的质量，帮助获证企业改善自身的网络安全管理水平。

此外，ISMS认证机构通过寻求认可机构的认可，可增强我国ISMS认证机构认可证书和ISMS认证证书在全球市场的认可度，有助于推动贸易便利化。

**四、与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况**

ISO/IEC JTC1/SC27于2024年3月发布了新版国际标准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：通用》。国内相关组织长期积极关注ISMS系列标准的变化，将ISO/IEC 27006-1、ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005等国际标准最新版本及时转化为国家标准，保障我国国家标准与国际标准的一致性。

**五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因**

本标准等同采用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：通用》。

**六、与有关法律、行政法规及相关标准的关系**

本标准符合现有法律法规的要求，并与现有GB/T 27021.1、GB/T 22080和GB/T 22081等相关标准协调一致。

**七、重大分歧意见的处理经过和依据**

本标准编制过程中未出现重大分歧。

**八、涉及专利的有关说明**

本标准不涉及专利。

**九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议**

建议本标准作为推荐性国家标准发布，从发布到实施的过渡期设置为6个月。

标准发布后，将在标准起草单位内率先开展应用，并通过标准宣贯、标准应用指南等方式，推进标准落地应用。

**十、其他应当说明的事项**

本标准代替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》。

《网络安全技术 信息安全管理体系

审核和认证机构要求》标准编制组

2025年2月