《数据安全管理能力评估规范》
标准编制说明

中国信息通信研究院标准起草组

2024 年 04 月 16 日

1、 标准范围。

本文件规定了组织数据安全管理能力评估规范和评估方法。

本文件适用于涉及数据安全的组织、组织及第三方专业机构开展数据安全管理能力评估工作，为提升组织数据安全管理能力、健全管理手段提供指引和依据。

2、 工作简况。

本项目计划名称为“数据安全管理能力评估规范”。由中国互联网协会归口。由中国信息通信研究院牵头研制。

本文件起草单位包括中国信息通信研究院、中互网来信息技术有限公司、中互智安(北京)科技有限公司。

本文件主要起草人：王景尧、吴荻、宛严、李玮、王亚宁、曹海啸。

本文件于2023年7月在中国互联网协会通过立项申请。

起草组于2023年11月召开线上讨论会，汇报讨论标准的研制情况。会上各企业根据产品的共同需求及差异性进行讨论，对标准中的相关内容提出合理建议，最终形成符合数据安全管理能力评估规范要求的标准文件。

3、 标准编制原则和确定标准主要内容的依据：

编制原则：

- 标准性要求，充分借鉴国内相关标准规范，并结合我国实际情况，力求该标准的可执行性和规范性更强；
- 实用性要求，建立在对企业数据安全技术能力充分调研及相关国际规范深度研究的基础之上，具有充分的技术先进性和实用性；
- 可行性要求，充分结合目前国家数据安全法及企业数据安全技术能力现状需求而制定；

- 有效性要求，考虑到技术的发展与扩充需求，故全面考虑标准架构和兼容性，满足未来标准发展与扩充需求。

标准内容依据：

GB/T 25069—2010 信息安全技术 术语

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 37973—2019 信息安全技术 大数据安全管理指南

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求

GB/T 29246—2017 信息技术 安全技术信息安全管理体系

GB/T 39335—2020 信息技术 个人信息安全评估指南

GB/T 19000—2016 质量管理体系 基础和术语

4、 主要试验（或验证）的分析、综述报告。

数据安全管理能力是指组织在数据处理过程中，采取一系列技术和管理措施，以保障数据的保密性、完整性、可用性和可靠性等安全属性的能力。这种能力是组织综合运用数据安全技术、管理流程、人员培训、制度规范、应急响应等方面的综合体现。数据安全管理能力对于组织来说至关重要，因为数据是组织的核心资产之一，涉及到商业秘密、客户信息、财务信息、内部决策等关键信息。对数据安全管理的评估和提升可以帮助组织识别数据安全风险，采取有效的防护措施，确保数据安全。

为了提升我国数据安全的保障能力，需要制定相应的标准和规范，形成产业共识，统一要求和考量数据安全能力。这有助于相关组织在数据安全方面的发展，为组织提供技术支持和指导。

5、 标准在起草过程中遇到的问题及解决办法：重大分歧意见的处理经过和依据：有无重要技术问题需要说明。

在标准起草过程中遇到的问题通过项目组内部协调和讨论已经解决。无重大分歧意见。没有重要技术问题需要说明。

6、 与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异（可引用标准前言的内容）：

国内外对该技术研究情况简要说明：国内已制定了针对数据安全能力评估相关的部分国家标准，如GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》、GB/T 41479-2022《信息安全技术 网络数据处理安全要求》等，本标准制定过程中可参考。

7、 修订标准时，说明与标准前一版本的重大技术变化，并列出所涉及的新、旧版本的有关章条（可引用标准前言的内容）：废止/代替现行有关标准的建议：

本标准为第一版制定标准。

8、 说明标准与其他标准或文件的关系(可引用标准前言的内容)，特别是与有关的现行法律、法规和强制性国家标准的关系：

与国内相关标准间的关系：GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》主要对组织数据安全能力建设进行评估，侧重于规定组织数据安全能力的成熟度划分；GB/T 41479-2022《信息安全技术 网络数据处理安全要求》侧重于规范对网络运营者的网络数据处理的安全度进行要求和规范，而本技术规

范侧重于规范企业开展业务运营活动中应具备的数据安全技术能力或手段的评估，其中涉及数据安全管控要求与GB/T 37988-2019中数据安全全生命周期管理要求保持一致，数据资产识别、数据传输、数据防泄漏等技术要求将参考GB/T 41479-2022相关要求。这三个标准都是为了提升数据安全能力和保障数据安全而制定的，可以相互参考和补充，帮助组织建立健全的数据安全管理体系和技术能力。

9、 标准作为强制性标准或推荐性标准的建议：

建议本文件作为推荐性团体标准发布实施。

10、 贯彻国家标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）：标准发布后，对国内外业界可能产生的影响。

本标准的发布与实施可促进涉及数据安全的组织、组织及第三方专业机构开展数据安全管理能力评估工作，为提升组织数据安全管理能力、健全管理手段提供指引和依据。

11、 标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程。

本文件不涉及知识产权的问题。

12、 其他应予说明的事项。

无。