

《数据安全技术能力评估要求》 标准编制说明

中国信息通信研究院标准起草组

2023年11月7日

1、 标准范围。

本文件规定了应具备数据安全能力的企事业单位、政府部门等组织的数据安全技术能力要求。

本文件不仅适用于第三方机构展开数据安全技术能力评估，而且适用于为企业数据安全技术能力自评估提供参考和指导。

2、 工作简况。

本项目计划名称为“数据安全技术能力评估要求”。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、挚理科技(北京)有限公司、北京福田戴姆勒汽车有限公司、北京金山云网络技术有限公司、上海合合信息科技股份有限公司、北京水滴科技集团有限公司、财信证券股份有限公司、辽宁振兴银行股份有限公司、平安健康互联网股份有限公司、青岛海尔科技有限公司、上海蔚来汽车有限公司、深圳乐信控股有限公司、深圳依时货拉拉科技有限公司、小米汽车科技有限公司、智马达汽车有限公司、中国国际金融股份有限公司、中原消费金融股份有限公司、中证数据有限责任公司、爱康健康科技集团有限公司。

本文件主要起草人：王景尧、吴荻、李玮、王亚宁、曹海啸、张灵通、徐治国、宋宏宇、廖超豪、李晓川、邢悬月、杨志学、夏禹、杨曦、肖红亮、何艺、杨毅、张天力、章文婷、杨湘安、李子超、陈飞彦、章锦成、李斌、袁斯山、白雷、乔智明、单渤凯、郭登海、王丹维、李冬、魏涛亮、杨显哲、李刚、苗夏箐、孙乾。

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，最终形成符合组装式应用开发平台行业要求的标准文件。

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 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 39335-2020 信息技术 个人信息安全评估指南

4、 主要试验（或验证）的分析、综述报告。

数据安全技术能力指企业或机构在处理数据过程中所具备的保护数据安全的能力，包括保证数据的机密性、完整性、可用性和可靠性等方面。数据安全能

力对于企业或机构来说非常重要，因为数据是企业 and 机构的核心资产之一，涉及到企业的商业秘密、客户信息、财务信息、内部决策等重要信息。因此，对数据安全能力的评估尤为重要。为了有效预防和应对这类问题，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，协调产业共识，形成数据安全能力统一要求和考量，从而为相关组织的数据安全能力的未来发展奠定技术保障。

本标准的技术内容是从企业角度出发，经过对大量企业数据安全技术能力的调研与分析，通过与各个厂商间对各自数据安全技术与需求方面的讨论，得到了符合行业要求的通用技术要求，最终形成的标准文件得到了相关厂商的认可和验证。

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国内企业数据安全技术能力的建设,形成完善、标准化的数据安全技术能力体系,从而为企业数据安全保障工作奠定技术基础。

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。

