团　　体　　标　　准

能源企业数据安全风险评估方法

（征求意见稿）

编制说明

2025-02-08

《能源企业数据安全风险评估方法》
（征求意见稿）编制说明

1 任务来源、协作单位

1.1 任务来源

根据《关于 2024 年第一批中国能源研究会标准立项的通知》（中能研标[2024]3号）要求，按照《中国能源研究会标准管理办法》，经中国能源研究会标准工作委员会审议，决定对《能源企业数据安全风险评估方法》标准予以立项。

项目名称：能源企业数据安全风险评估方法

负责起草单位：广东电网有限责任公司信息中心

所属委员会：信息通信专业委员会

1.2 协作单位

牵头单位：本标准编写由广东电网有限责任公司信息中心牵头起草，负责标准制定的总体协调和组织编写工作。

参编单位：广东电网有限责任公司、南方电网科学研究院有限责任公司、南方电网超高压输电公司、云南电网有限责任公司信息中心、中国能源建设集团广东省电力设计研究院、广东电网有限责任公司河源供电局、广东电网有限责任公司湛江供电局、上海观安信息技术股份体系公司和南瑞集团有限公司共同参与编制。各参编单位在能源领域和数据安全方面具有不同的优势和专业特长，为标准的制定提供了多方面的支持。

2 编制工作组简况

2.1 编制工作组及其成员情况

编制工作组及其成员情况：

建设单位：广东电网有限责任公司信息中心，沈伍强、王业超、钱正浩、何明东、崔磊，张小陆、刘晔、杨朝谊

建设单位：广东电网有限责任公司，骆书剑

科研院所：南方电网科学研究院有限责任公司，赖博宇

生产单位：南方电网超高压输电公司，钱方、冷宇琦

建设单位：云南电网有限责任公司信息中心，李园、

设计单位：中国能源建设集团广东省电力设计研究院，冯国平

生产单位：广东电网有限责任公司河源供电局，陈兆鹏

生产单位：广东电网有限责任公司湛江供电局，郑韶光、王奕

生产单位：南瑞集团有限公司，许明杰

生产单位：上海观安信息技术股份有限公司，周绪

2.2 标准主要起草人及其所做的工作

（明确起草人及工作任务，建议分工明确到章节。）

[沈伍强]担任标准起草工作组组长，全面统筹协调标准起草工作，并负责起草小组工作会议，调研工作的组织与筹备。

[王业超]担任标准起草工作组副组长，协助组长进行工作统筹与协调，负责标准大纲编写，对标准起草过程中的整体内容的科学性、合理性进行审核与把关。

[钱正浩]、[刘晔]、[赖博宇]：负责标准的第 1-3 章，包括引言、范围、术语和定义、缩略语等章节。

[钱方]、[何明东]、[冷宇琦]：主要负责标准第 4-5 章，包括数据安全风险评估概述和数据安全风险评估准备章节。

[张小陆]、[李园]、[杨朝谊]：主要负责标准第 6 章，包括数据安全风险评估准备相关内容编写。

[骆书剑]、[冯国平]：主要负责标准第 7 章，包括数据安全风险评估调研相关内容编写。

[陈兆鹏]、[许明杰]：主要负责标准第 8 章，包括数据安全风险识别相关内容编写。

[崔磊]、[周绪]、[郑韶光]、[王奕]：主要负责标准第 9 章、第 10 章及附录内容，主要包括数据安全风险分析与评价、数据安全风险评估总结及附录 A 能源大数据分类和分级结果示例、附录 B 典型数据安全风险类别、附录 C 数据安全风险量化分析与评估方法、附录 D 能源企业数据安全风险评估调研表示例和附录 E 能源企业数据安全风险评估报告示例。

3 起草阶段的主要工作内容

（1）编制过程信息：本标制定工作启动后，编制工作组进行了调研讨论，了解国内外能源企业数据安全风险评估的现状和发展趋势。在此基础上，确定了标准的框架和主要内容，组织专家进行研讨和论证，对能源企业数据安全风险评估工作中相关评估内容、评估实施流程和评估方法进行深入分析和优化，经过多轮修改和完善，形成了标准的征求意见稿。

（2）各阶段主要争议问题、征求意见的处理情况：在标准制定过程中，邀请行专家对标准初稿进行了充分的讨论，收集了相关意见和建议，编制组对这些意见进行了认真梳理和分析，对于专家提出的能源的定义、适用性及相关问题进行回复和处理，同时根据收集到的意见进行了逐一讨论和分析，对标准初稿完成了修改。

4 标准编制原则及与国家法律法规和强制性标准及有关标准的关系

4.1 编制原则

统一性：与现行有效的国家数据安全法律、法规、标准，以及对能源企业数据安全风险评估的具体要求保持一致。标准在制定过程中，遵循统一的技术规范和要求，以便于不同能源企业在进行数据安全风险评估时能够采用一致的方法和标准。

协调性：标准与国家法律法规和强制性标准以及其他相关标准相协调，避免出现冲突和矛盾，在数据安全风险评估方面，遵循国家网络数据安全等法律法规的要求，

同时与相关的信息技术标准相衔接，确保能源企业的数据安全管理工作符合国家整体的安全战略和标准体系。

适用性：标准充分考虑能源企业数据安全风险评估需求，具有较强的适用性，在评估方法、评估实施流程方面具备通用性，使标准能够切实指导相关能源企业的数据安全风险评估工作。

一致性：标准在技术内容和语言表述上保持一致，避免出现歧义。例如，在术语和定义的使用上，遵循统一的规范，确保各方对标准的理解一致。

规范性：标准的编写符合国家标准化工作的规范和要求，具有较高的规范性，在标准的结构和格式上，遵循国家标准的编写规范，使标准易于阅读和使用。

目标性：标准的制定以提高能源企业数据安全管理水平为目标，具有明确的目标导向，通过数据安全风险评估，帮助能源企业识别和评估数据安全风险，制定有效的风险控制措施，实现数据安全管理的目标。

4.2 写出本标准与标准编制和实施过程涉及到的法律法规、强制性标准的关系。

本标准与国家网络安全法、数据安全法、个人信息保护法等法律法规密切相关，法律法规为能源企业的数据安全管理提供了法律依据和指导原则，本标准在制定过程中充分遵循国家网络数据安全相关法律法规的要求，确保能源企业的数据安全风险评估工作合法合规，为能源企业落实法律法规提供了具体的技术方法和标准。

与强制性标准的关系方面，本标准在技术要求上与相关的强制性信息技术标准相协调，保障能源企业的数据安全符合国家整体的安全标准体系。

4.3 写出本标准与上位标准或其他相关标准相比较，主要技术指标的不同点，如：填补空白、在某标准的基础上细化、提升等。）

与上位标准相比，本标准更加具体和细化，上位标准只是对数据安全风险评估提出了一般性的要求，而本标准则针对能源企业的特点，建立了专门的风险评估方法和评估模版参考，为能源企业的数据安全风险评估提供了具体的操作指南。

与其他相关标准相比，本标准针具有更强的针对性和适用性，本标准专注于能源企业的数据安全风险评估。

5 标准主要技术内容的论据或依据；修订标准时，应增加新、旧标准水平的对比情况

5.1 标准主要技术内容的论据或依据

（1）理论依据：本规范为能源企业提供数据安全风险评估执行指南，有助于帮助能源企业系统地识别和评估在数据处理过程中可能面临的安全风险，制定相应的预防和应对措施，有利于能源企业保护积累的大量敏感数据，防止数据泄露、篡改或非法获取，保障数据的完整性和可用性，提高能源企业对数据安全事件的应急响应能力，通过数据安全风险评估和规范管理，减少企业数据安全事件导致的直接和间接经济损失，保护涉及公共利益和国家安全的数据，维护社会稳定。通过这一规范的实施，能源企业不仅能够实现经济效益的提升，还能够为社会带来积极的效益。本标准基于风

险管理理论和数据安全管理理论，建立了能源企业数据安全风险评估的实施流程和评估方法，从数据的保密性、完整性、可用性等多个维度对数据安全风险进行评估。

（2）实践依据：结合本规范相关内容，通过在相关能源企业在实际应用中采用了本标准中提出的风险评估方法和技术要求，取得了良好的效果，通过实施本标准中的数据安全管理措施，成功降低了数据泄露风险，提高了数据管理效率，这些实践经验证明了本标准的可行性和有效性。

5.2 修订标准时，应增加新、旧标准水平的对比

目前暂无能源企业相关数据安全风险评估相关旧标准。

6 主要试验（验证）的分析、综述报告，技术经济论证，预期的经济效果

6.1 主要试验（验证）的分析

我们选取了相关能源企业作为试验对象，对企业的数据安全现状进行了全面的调查和分析，包括数据存储、传输、处理等环节的安全措施，以及员工的数据安全意识等方面，然后按照本标准的评估方法对这些企业进行数据安全风险评估，并与企业现有的评估结果进行对比。通过试验验证，我们发现本标准的评估方法能够更准确地识别出能源企业数据安全风险，尤其是在新技术应用和复杂业务场景下，评估结果更加详细和具体，为企业制定针对性的数据安全策略提供了有力的支持。

6.2 综述报告

本标准的制定是为了解决能源企业数据安全风险评估中存在的问题，提高能源企业的数据安全管理水平。通过对国内外相关标准和研究成果的调研，结合能源企业的实际情况，我们制定了本标准。本标准涵盖了能源企业数据安全风险评估的各个方面，同时，本标准还注重与其他相关标准的协调和衔接，确保标准的科学性和实用性。

6.3 技术经济论证

新标准采用了先进的风险评估手段，能够更准确地识别和评估能源企业的数据安全风险，将有助于企业及时采取有效的措施防范风险，减少数据泄露和损失的发生。通过实施本标准，能源企业可以更好地保护企业数据资产，提高数据的安全性和可靠性，为能源企业数字化转型发展筑牢安全基础。

6.4 预期的经济效果

标准实施后预期的经济效益包括：

一是降低数据泄露风险，减少因数据泄露导致的经济损失，包括客户流失、声誉受损等方面的损失。

二是提高数据管理效率，优化数据安全管理流程，提高数据的可用性和可靠性，为企业的生产经营提供更好的支持。

三是增强企业竞争力：提升企业的数据安全保障能力，为能源企业数字化转型筑牢安全基础。

7 采用国际标准的程度及水平的简要说明

本标准在制定过程中，并未采用国际标准，主要原因是能源企业的数据安全具有一定的特殊性，需要结合我国能源行业的实际情况进行制定，同时为了避免版权问题，我们在制定标准时主要采用自主创新的方法和技术。

8　重大分歧意见的处理经过和依据

在标准制定过程中，邀请行专家对标准初稿进行了充分的讨论，收集了相关意见和建议，编制组对这些意见进行了认真梳理和分析，对于专家提出的能源的定义、适用性及相关问题进行回复和处理。

回复如下：这个标准能源的定义是从事电力、石油石化、煤炭、燃气、新能源、核能等主营业务的企业，或支撑以上主营业务开展的咨询、相关设备制造等服务的企业。整体而言能源企业所涉及的数据，在数据各生命周期面临的安全风险具有一定的共性，因此这个标准适用于各能源企业开展数据安全风险评估工作。

9　贯彻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）

（1）组织措施：成立标准贯彻领导小组，负责标准的宣传、培训和实施工作，加强对能源企业的数据安全管理工作的监督和检查，确保标准的有效执行。

（2）技术措施：开发数据安全风险评估工具，为企业提供便捷的评估服务，建立数据安全管控平台，实现对企业数据安全风险的实时监测和预警。

（3）过渡办法：在标准实施初期，预留一定的过渡期，让企业有足够的时间熟悉和适应标准。

10　其他应予说明的事项，如涉及专利的处理等

本标准在制定过程中，未涉及专利问题。如果在未来的应用过程中，发现需要采用专利技术，我们将按照相关规定，在自愿的基础上与专利持有人进行沟通协商，确保标准的顺利实施。