

《数据合规能力成熟度评估模型》 标准编制说明

标准起草小组

1. 标准范围

本标准确立了数据合规能力成熟度评估模型的总体框架，规定了能力域、能力项的构成，以及各能力项在不同能力等级下的要求。

本标准适用于组织数据合规能力的自我评估和第三方评估，也可作为数据合规管理体系建设与优化提供指引。

本标准不替代法律法规对数据处理的强制性要求。未满足法定要求的组织不具备等级评估条件。

2. 工作简况

随着数字经济的快速发展，数据已成为新型生产要素和战略性资源。数据的合规处理不仅关系到个人信息权益保护、数据安全和国家数据主权，也是数据要素市场化配置、数据流通交易的前提和基础。

当前，我国已形成以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及《网络数据安全管理条例》为核心的“三法一条例”数据合规法律框架，各行业领域也陆续出台专项监管要求。但各类组织在数据合规能力建设方面仍存在水平参差不齐、体系建设缺乏统一指引、合规管理难以量化评估等问题。

为引导数据要素市场主体建立健全合规管理能力，推进数据要素合规有效流通利用，标准起草小组开展了广泛调研与技术研讨，吸纳了行业专家的改进建议，最终形成了本征求意见稿。

3. 标准编制原则和确定标准主要内容

本标准依据《标准化工作导则 第1部分：标准化文件的结构和起草规则》（GB/T 1.1-2020）编制。标准编制原则包括，严谨性：本标准以“三法一条例”等数据合规领域法律法规、部门规章等制度文件为核心依据，在制定过程中确保数据合规能力成熟度模型的法律严谨性。系统性：采用“通用基线+角色差异+特殊模块”的架构，建立覆盖战略、制度、全生命周期、风险、技术、文化六大维度的全方位评估体系。可操作性：确立了“合规底线判定+等级量化评分”的评估路径，一级采用清单式逐条判定，二级及以上采用量化评分公式，为组织自我评估和第三方评估提供明确指引

本标准核心内容包括：模型架构设定了合规战略与组织、合规制度与流程、数据全生命周期合规、合规风险与事件管理、合规技术支撑、合规文化与能力6大能力域及20个能力项，划分为基础级、规范级、优化级三个等级。差异化义务映射机制构建了包含处理关系与流通关系两个维度的角色矩阵，明确了不同角色的合规义务并集，并设置了数据产权、重要数据处理、跨境传输等9个特殊制度补充模块以应对特定场景。评估方法规定了从合规底线判定、角色识别、场景确认到最终等级判定的完整流程，明确了满足程度评分法与整体等级计算方法。

4. 主要试验(或验证)的分析、综述报告

起草小组选取了国内5家不同领域代表性组织（涵盖自主处理者、受托处理者等典型角色）进行了模拟试评估。验证结果显示，该模型能有效区分不同角色的合规能力成熟度；“角色矩阵”与“特殊制度补充模块”的设置精准匹配了差异化合规义务，依据标准评定的等级与试点组织实际的合规体系建设水平基本吻合。

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

在本文件的修订过程中，无重大分歧意见和技术问题。

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

该项目没有对应的国际标准或国外先进标准。

7. 修订标准时，说明与标准前一版本的重大技术变化，并列岀所涉及的新、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

不涉及。

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

本标准内容符合数据合规领域现行法律、法规和强制性国家标准相关要求。

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标准。

10. 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)；标准发布后，对国内外业界可能产生的影响

建议本文件发布后，优先在中国互联网协会会员单位及能源、金融、医疗等重点行业领域推广应用。

本标准的实施将有助于解决当前数据合规建设水平参差不齐、缺乏统一指引的问题，为监管部门、评估机构及数据处理者提供科学、量化的评估依据。引导组织从“被动合规”向“主动合规”转型，有效防范数据安全风险，促进数据要素市场化配置与安全有序流通，为数字经济高质量发展提供坚实的合规保障。

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

本文件未涉及。

12. 其他应予说明的事项

.