国家标准《信息安全技术 数据安全风险评估方法》（征求意见稿）编制说明

一、工作简况

1.1 任务来源

根据国家标准化管理委员会2023年下达的国家标准制修订计划，《信息安全技术 数据安全风险评估方法》由中国电子技术标准化研究院负责承办，并联合国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心等单位编制，计划号：20230257-T-469。本标准由全国信息安全标准化技术委员会归口管理。

1.2 制定背景

2022年3月6日，全国信息安全标准化技术委员会发布《关于发布2022年度网络安全国家标准需求的通知》（信安秘字〔2022〕47号)，在附件《2022年网络安全国家标准需求清单》中明确了有关需求“支撑《数据安全法》第十八条、 第三十条对数据安全风险评估相关规定的落地实施。 ”

我国高度重视数据安全工作，先后出台《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》等法律法规。与此同时，数据安全风险和违法违规问题依然严峻，国家数据安全、企业商业秘密和公民个人信息安全防护需求迫切。为了规范数据处理活动，保障数据安全，《数据安全法》明确提出建立数据安全风险评估机制要求。数据安全风险评估，主要针对数据处理者的数据和数据处理活动进行风险评估，旨在掌握数据安全总体状况，发现存在的数据处理不合理、缺少有效的数据安全措施等风险隐患，为进一步健全数据安全管理制度和技术措施，提高数据安全治理能力奠定基础。

本标准给出了数据安全风险评估的基本概念、要素关系、分析原理、实施流程、评估内容、分析与评价方法等，明确了数据安全风险评估各阶段的实施要点和工作方法。适用于指导数据处理者、第三方评估机构开展数据安全风险评估，也可供有关主管监管部门实施数据安全检查评估时参考。

1.3 起草过程

2022年3月，成立编制工作组，启动标准编制工作，形成标准草案，同步编制研究报告、实施应用方案。

2022年4月，在信安标委标准会议周的WG7工作组内进行立项汇报，通过工作组立项投票。

2022年5-10月。组织多次研讨会，起草组先后完成3次标准草案的修改，形成《数据安全风险评估研究报告》、《<信息安全技术 数据安全风险评估方法>实施应用方案》。

2022年6月，在信安标委标准会议周的WG7工作组内进行立项汇报，通过立项专家评审。

2022年11月2日，信安标委发布标准立项通知，标准获得信安标委立项。

2022年11月16日至11月30日，标准公开征集参编单位。

2022年11月-12月，召开编制组会议，对标准草案进行完善。

2022年11月25日，参与国标委标准项目立项答辩，回应了专家质询。

2022年12月6日，在信安标委会议周的WG7工作组对标准工作进展进行了汇报，通过工作组投票，建议将本标准推进至征求意见稿。

2022 年 12 月至 2023 年 2 月，针对会议周专家意见，完善标准内容。

2023 年 3 月 27 日，参加秘书处组织的征求意见稿专家审查会，评审专家对标准提出 38 条意见。

2023 年 4 月-5 月，处理专家意见，完善标准内容。

2023 年 6 月 1 日，在信安标委会议周的 WG7 工作组对标准工作进展进行了汇报，收集 42 条意见。

2023 年 6 月-8 月，处理专家意见，完善标准内容。

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

本标准在编制过程中遵循了问题导向原则、协调性原则。

2.2 主要内容及其确定依据

本标准为支撑《数据安全法》第十八条、第三十条对数据安全风险评估相关规定落实，贯彻《个人信息保护法》《网络数据安全管理条例（征求意见稿）》有关要求，建设数据安全风险评估的协作和统一管理机制，发现国家、重点行业领

域和地方区域的数据安全风险，理清数据安全建设方向，针对性提升我国数据安全能力水平。

本文件提出了数据安全风险评估的基本概念、要素关系、分析原理、实施流程、评估内容，明确了数据安全风险评估各阶段的实施要点和工作方法，包括：

1）评估要素间关系；

2）风险分析原理；

3）评估适用情形；

4）评估实施流程；

5）评估内容框架；

6）评估方法；

7）数据安全风险评估准备；

8）数据和数据处理活动识别；

9）数据安全风险识别；

10）数据安全风险分析与评价；

11）评估总结；

12）数据安全风险评估报告模板。

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

将根据下一步标准试点工作开展情况而定。

3.2 技术经济论证

将根据下一步标准试点工作开展情况而定。

3.3 预期的经济效益、社会效益和生态效益

通过研究提出统一的数据安全风险评估方法，明确数据安全风险评估的实施流程、内容、风险分析原理，给出数据安全风险评价方法和风险处置方法。支撑国家数据安全相关制度、工作，以及数据安全风险评估要求更好地在各行业领域落地，指导数据处理者开展数据安全风险评估工作，提高我国数据安全保护水平。

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

当前，国外数据安全和个人信息保护方面的评估认证，主要有数据保护影响

评估（DPIA）、受控非密信息安全评估、ISO/IEC 27000 系列管理体系认证、信息技术产品安全评估（CC）等。20 世纪 80 年代，美国、加拿大等发达国家就已经开始建立以信息安全风险评估为基础的信息安全风险管理体系，制定了相关标准、评估方法和相关技术。当前尚缺少数据安全风险评估相关的国际标准。，主要在信息安全、产品安全等标准中引入隐私保护要求。

ISO/IEC 27000 信息安全管理体系认证，扩展到隐私信息管理体系认证。目前，信息安全管理体系认证已形成比较成熟的一套体系认证机制，同时随着 ISO/IEC 27000 系列信息安全管理标准不断完善，已经出台针对个人信息保护的管理体系标准，例如提出隐私信息管理体系的 ISO/IEC 27701《扩展的 ISO/IEC 27001 和 ISO/IEC 27002 隐私信息管理要求和指南》、提出个人信息保护控制措施集合的 ISO/IEC 29151《个人可识别信息保护实践指南》、适用于公有云个人信息保护的 ISO/IEC 27018《公有云作为个人信息处理者保护可识别个人信息的实践指南》，这些标准也常被用于进行管理体系认证。

此外，信息技术产品安全评估正在增加产品的隐私保护功能评估。信息技术产品安全评估（简称 CC）按照 ISO/IEC 15408《信息技术安全评估通用准则》对信息技术产品，尤其是信息安全产品的安全保障级别进行评估。目前 CC 作为国际常用的产品安全测评方式，已形成一套完整的测评方法论。同时，ISO/IEC 15408 系列标准也正在修订，增加了隐私保护等产品安全功能组件，例如 CC 中涉及数据安全的安全功能组件，主要包括用户数据保护、隐私两大功能组件，其中用户数据保护涉及访问控制、数据鉴别、数据完整性、数据输入、数据机密性、内部传输、信息流控制、数据输出、残余信息保护等，隐私组件，包括匿名化、假名化、不可链接性、不可观测性等。

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

无。

六、与有关法律、行政法规及相关标准的关系

本标准与现行法律、法规以及国家标准不存在冲突与矛盾，与其他标准属于配套衔接关系。

法律方面，《中华人民共和国数据安全法》中提出“国家支持有关部门、行

业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。”“国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。”“重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。”的要求。

国家标准方面，GB/T 20984-2022《信息安全技术 信息安全风险评估方法》给出了信息安全风险评估的框架、流程和实施方法，本标准充分借鉴信息安全风险评估的评估模型、工作流程、评估模式，结合数据和数据处理活动的特点，从管理、数据处理活动、技术等方面，结合核心数据、重要数据、个人信息、一般数据安全特点及保护要求，从监管要求、安全需求等方面识别数据安全风险。GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》提供了多维度的数据安全能力评估模型和安全要求，GB/T 35273—2020《信息安全技术 个人信息安全规范》提出了个人信息安全保护要求。行业标准方面，JR/T 0223-2021 《金融数据安全 数据生命周期安全规范》给出了金融行业数据安全保护要求。本标准充分借鉴和参考上述标准，且与相关国家标准协调配套。

七、重大分歧意见的处理经过和依据

无。

八、涉及专利的有关说明

本文件不涉及专利等知识产权。

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

无。

十、其他应当说明的事项

无。

《信息安全技术 数据安全风险评估方法》编制工作组

2023 年 8 月 20 日