数据安全风险评估要求

编制说明

标准起草工作组

2024 年 12 月

目 录

1 必要性

近年来，国家陆续出台《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》等法律法规，旨在加强数据安全风险防范。当前已有20230257-T-469 数据安全技术 数据安全风险评估方法（正在征求意见）、YD/T 3801-2020 电信网和互联网数据安全风险评估实施方法、DB3212/T 1117—2022 政务数据安全风险评估规范等数据安全风险评估相关标准，但仍需在已有标准的基础上，持续细化评估流程、评估内容、人员要求、风险分析方法等相应要求，为数据安全风险评估工作开展提供指引，更好地指导评估工作落地，及时找出企业安全措施防护死角，满足国家法律法规安全要求，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

2 工作简述

2.1 任务来源

本标准根据四川省网络空间安全协会数据安全团体标准制修订计划立项，由四川省网络空间安全协会归口，由杭州迪普科技股份有限公司牵头组织编制。

2.2 起草单位

本标准牵头起草单位：杭州迪普科技股份有限公司；

本标准参加起草单位：成都市信息系统与软件评测中心、北京云集至科技有限公司、成都安美勤信息技术股份有限公司、

北京启明星辰信息安全技术有限公司、永信至诚科技集团股份有限公司、豪符密码检测技术（成都）有限责任公司、成都久信信息技术股份有限公司、成都创信华通信息技术有限公司、成都卓越华安信息技术服务有限公司、中铁成都科学技术研究院有限公司、四川智仁信息技术有限公司。

2.3 起草过程

2024 年 7 月，杭州迪普科技股份有限公司向四川省网络空间安全协会提交《数据安全风险评估要求》团体标准项目建议书；

2024 年 8 月，由四川省网络空间安全协会邀请专家对《数据安全风险评估要求》立项评审，标准立项，成立标准起草工作组。

2024 年 9 月，召开《数据安全风险评估要求》团体标准启动会议，会议讨论了标准制定的流程、时间节点，确定了标准起草的总体框架、主要内容、人员分工；

2024 年 11 月，完成了数据安全团体标准《数据安全风险评估要求》草案稿编写；

2024 年 12 月，专家对标准征求意见稿进行了评审，《数据安全风险评估要求》标准质量达到征求意见稿发布要求。

3 标准编制原则和主要内容

3.1 编制原则

本标准的制定工作遵循标准统一、人员可控、信息可控、过程可控、工具可控、业务影响可控的原则。

1．标准统一原则：开展评估前，针对被评估组织所遵行的评估标准是一致的，不因被评估组织的评估对象变化而发生变更；

2．人员可控原则。所有参与评估人员应签署保密协议，以保证与评估相关的所有信息安全；

3．信息可控原则。评估方应对评估过程数据和结果数据进行严格管理，未经授权不得泄露给任何单位和个人；

4．过程可控原则。按照安全管理要求，成立风险评估实施团队，并实行评估组长负责制，达到评估过程的可控；

5．工具可控原则。评估人员所使用的评估工具应保证安全性并事先告知用户，并在评估实施前获得被评估组织的许可；

6．业务影响可控原则。从管理层面和工具技术层面，将评估工作对网络及相关系统正常运行的可能影响降低到最低限度。对需要进行攻击性测试的内容应与被评估组织沟通，对涉及内容进行应急备份，同时避开业务的高峰时段。

3.2 主要内容

本标准共分为十一章，包括评估范围、规范性应用文件、术语和定义、评估原则、概述、总体要求、评估准备、信息调

研、风险识别、综合风险分析、风险评估报告。

1．范围

本文件规定了数据安全风险评估的基本原则、基本概念、数据安全风险评估总体要求、数据安全管理评估要求、数据处理活动评估要求、数据安全技术评估要求等，明确了开展数据安全风险评估在不同场景下的评估要求。

本文件适用于指导数据处理者、第三方评估机构落实数据安全风险评估工作，也可供相关行业主管监管部门作为实施数据安全检查的参考。

2．规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

《信息安全技术 数据安全风险评估方法》（征求意见稿）

TC260-PG-20231A 网络安全标准实践指南—网络数据安全风险评估实施指引

YD/T 3801-2020　电信网和互联网数据安全风险评估实施方法

DB3212/T 1117-2022 政务数据安全风险评估规范

3．术语和定义

数据 data

任何以电子或者其他方式对信息的记录。

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

数据处理活动 data processing activities

数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

数据处理者 data processor

在数据处理活动中自主决定处理目的、处理方式的组织、个人。

风险评估 risk assessment

对数据和数据全生命周期处理活动安全进行风险识别、风险分析和风险评价的整个过程。

数据安全风险评估 data security risk assessment

对数据和数据处理活动安全进行信息调研、风险识别、风险分析和风险评价的整个过程

4．评估原则

标准统一原则：开展评估前，针对被评估组织所遵行的评估标准是一致的，不因被评估组织的评估对象变化而发生变更；

人员可控原则。所有参与评估人员应签署保密协议，以保证与评估相关的所有信息安全；

信息可控原则。评估方应对评估过程数据和结果数据进行

严格管理，未经授权不得泄露给任何单位和个人；

过程可控原则。按照安全管理要求，成立风险评估实施团队，并实行评估组长负责制，达到评估过程的可控；

工具可控原则。评估人员所使用的评估工具应保证安全性并事先告知用户，并在评估实施前获得被评估组织的许可；

业务影响可控原则。从管理层面和工具技术层面，将评估工作对网络及相关系统正常运行的可能影响降低到最低限度。对需要进行攻击性测试的内容应与被评估组织沟通，对涉及内容进行应急备份，同时避开业务的高峰时段。

5．概述

数据安全风险评估是一项主要围绕数据及数据处理活动所开展的一项工作。评估主要通过信息调研识别数据处理者、业务和信息系统、数据资产、数据处理活动、安全措施等相关要素，从数据安全管理、数据处理活动、数据安全技术等方面识别风险隐患，梳理问题清单，分析数据安全风险、视情评价风险，并给出整改建议，用以提升数据安全防攻击、防破坏、防窃取、防泄露、防滥用能力。

6．总体要求

包括评估流程要求、评估手段要求、评估内容要求、人员要求。

7．评估准备

包括评估目标、评估范围、评估团队、前期准备、评估方

案。

8．信息调研

包括信息调研内容包括数据处理者调研、业务和信息系统调研、数据资产调研、数据处理活动调研、安全措施调研。

9．风险识别

风险识别，即针对不同的评估对象，从数据安全管理、数据处理活动、数据安全技术等方面，通过多种识别手段识别可能存在的数据安全风险。已实施并编制的检测评估工作报告，可在分析评估结果真实性、有效性的基础上视情采纳。

10．综合风险分析

综合风险分析要求在风险识别基础上形成问题列表，从而开展风险分析，并视情对风险进行评价，形成风险清单，最后提出整改建议。综合风险分析包括梳理问题清单、风险分析与评价、风险整改建议。

11．风险评估总结

风险评估总结包括编写风险评估报告、风险处置两部分内容。

4 技术论证与效果

本标准中总体要求、评估准备、信息调研、风险识别、综合风险分析、风险评估总结等技术要求，来源于法律法规和相关标准，同时结合了数据安全风险评估工作实践中的经验，不涉及专利授权。

本标准发布后，可适用于指导数据处理者、第三方评估机构落实数据安全风险评估工作，也可供相关行业主管监管部门作为实施数据安全检查的参考，能帮助规范数据安全风险流程，更好地在管理和技术上发现数据处理者在数据安全工作推进方面存在的不足，及时整改并修复缺陷，实现安全管理闭环，从而防范数据安全风险。

5 对标情况

本标准在制定过程中，与现行法律法规以及相关标准中的有关定义协调一致。其中，评估流程、评估前期准备工作、评估内容、信息调研、风险识别、综合风险分析等充分参考了《信息安全技术 数据安全风险评估方法》（征求意见稿）TC260-PG-20231A 网络安全标准实践指南—网络数据安全风险评估实施指引、YD/T 3801-2020 电信网和互联网数据安全风险评估实施方法、DB3212/T 1117—2022 政务数据安全风险评估规范等数据安全风险评估相关标准，并在此基础上，细化人员要求、评估准备工作、风险识别、综合风险分析等内容，有益于后续数据安全风险评估相关标准的持续更新和完善。

6 标准实施建议

本标准是在法律法规和国内相关标准的基础上，从落地的视角对整个数据安全风险评估流程进行了归类和细化，更有利于实施数据安全风险评估时系统化地开展工作，建议作为推荐性团体标准。

7 需要说明的主要问题

本标准在编制过程中未出现需要说明的主要问题。

8 其他说明事项

本标准在编制过程中未出现其他说明事项。