《公共数据安全评估规范》（送审稿）

编制说明

一、项目背景

2021年6月10日，全国人大常委会第二十九次会议通过了我国首部数据保护领域专项法律《中华人民共和国数据安全法》，以国家法律的形式对我国数据安全保护工作提出要求，并明确说明我国促进并支持数据安全检测评估、认证等服务发展和活动开展。2021年10月，中共中央、国务院印发《国家标准化发展纲要》，也明确提出要强化数据安全领域标准的制定与实施。

公共数据构成复杂、涉及范围广、处理环节多样、数据流动频繁，过程中潜藏了诸多安全风险问题，公共数据安全防护面临巨大挑战。当前各公共管理和服务机构数据安全能力尚处于参差不齐的状态，整体数据安全保护仍有待进一步统筹协调，逐步实现规范化和标准化。

为加强公共数据安全风险防控，统一指导并有序推进公共管理和服务机构数据安全管理工作，有必要对深圳市公共数据安全评估工作进行规范化和标准化要求。因此，基于我国现有法律法规、《深圳经济特区数据条例》、目前已发布的DB4403/T 271—2022《公共数据安全要求》等所明确的数据安全要求，结合实际情况，组织开展本文件的研制工作。

本文件的制定和实施，一方面能够推动公共管理和服务机构落实公共数据安全要求，提升数据安全保护工作的规范化和标准化程度，另一方面有助于公共管理和服务机构及时全面掌握本机构数据安全管理水平，有效防控数据安全事件风险和危害，为数据的应用和流动提供有力保障。

二、工作简况

1、任务来源

2021年我国相继发布《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》，其中数据安全法第十八条、二十二条、三十条均提及数据安全风险评估法规要求。我市《深圳经济特区数据条例》第八十七条、八十九条明确

需建立健全数据安全监督机制，组织数据安全监督检查，以及需对数据处理者开展数据安全管理认证以及数据安全评估工作，并对其进行安全等级评定。

地市层面，为提升深圳市公共数据安全建设能力，维护数据安全，切实保护公共数据的敏感信息，保护社会公众的合法权益，推动我市《深圳经济特区数据条例》贯彻实施，落实公共数据保护责任与义务，指导公共管理和服务机构的公共数据安全管理与建设工作，2021年由深圳市信息安全管理中心牵头编制了《公共数据安全要求》地方标准，于2022年11月已正式发布。但《公共数据安全要求》仅对我市公共管理和服务机构提出数据安全建设要求，未有公共数据安全评估细则。因此亟需制定《公共数据安全评估规范》，用于指导公共管理和服务机构开展安全自评估工作。《公共数据安全评估规范》属于公共数据安全建设相关系列标准之一，是《公共数据安全要求》的配套标准，依托于《公共数据安全要求》中具体安全要求条款，提出可操作的评估操作方法。

2、主要起草过程

1）2022 年 3 月，深圳市信息安全管理中心提交《深圳市地方标准制修订计划项目建议书》，2022 年 4 月 28 日深圳市市场监督管理局批准立项。

2）2022 年 5 月至 2022 年 10 月，深圳市信息安全管理中心组织内部专家及其它参与起草单位，对相关技术要求、政策标准及行业实践等情况进行多轮次的研讨和交流，形成了标准草案。

3）2022 年 11 月，深圳市信息安全管理中心组织外部专家针对标准草案召开专家研讨会。

4）2022 年 12 月至 2023 年 2 月，深圳市信息安全管理中心及其他参与起草单位对标准草案进行了进一步修改，形成征求意见稿。

5）2023 年 2 月 27 日至 3 月 3 日，深圳市政务服务数据管理局发函征求 79 个单位意见，共收到反馈意见 85 条，其中采纳 10 条，部分采纳 4 条，不采纳 1 条，无意见 70 条。

6）2023 年 3 月至 8 月，根据收到的反馈意见进行修改，形成送审稿。

三、标准主要内容依据

1、同类标准编制情况

国家标准层面目前暂无数据安全评估相关，全国信息安全标准化技术委员会

2023 年 5 月发布了技术文件《网络安全标准实践指南—网络数据安全风险评估实施指引》。

行业标准层面，涉及数据安全评估相关的包括金融行业的《金融数据安全 数据安全评估规范》（征求意见稿）、通信行业的《电信领域数据安全评估规范》（报批稿）、YD/T 3801—2020《电信网和互联网数据安全风险评估实施方法》等。

地方标准层面，2022 年 4 月 26 日，浙江省市场监督管理局批准发布了 DB33/T 2488—2022《公共数据安全体系评估规范》。

目前国家及行业层面暂无公共数据安全领域的评估标准，我市亦无数据安全评估相关地方标准。

2、标准主要依据

本文件制定的主要依据为：

1)第 1 至 4 章节主要依据《深圳经济特区数据条例》第 1 章节，结合 DB4403/T 271—2022《公共数据安全要求》编写；

2）第 5 章节主要依据 GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》第 5 章节、YD/T 3956—2021《电信网和互联网数据安全评估规范》第 4 章节编写；

3）第 6 至 8 章节主要依据 GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》第 6 至 9 章节、GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》的第 6 至 12 章节、YD/T 3956—2021《电信网和互联网数据安全评估规范》的第 5 至 6 章节，并结合 DB4403/T 271—2022《公共数据安全要求》的第 7 至 9 章节内容编写；

4）第 9 章节主要依据 GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》第 11 章节编写；

5）第 10 章节主要依据 GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》第 12 章节，并结合 GB/T 20984—2022《信息安全技术 信息安全风险评估规范》第 5 章节编写。

四、主要条款说明、技术指标参数及试验验证

1、编制原则

由于公共数据复杂多样、影响面广，在标准编制过程中，标准编制组以“兼顾管理”为基本编制思路，充分考虑当前公共数据数据安全管理现状，同时兼顾国家相关政策和行业发展趋势，遵循以下几个原则：

1）行业适用性——本文件在编制过程中始终坚持公共数据安全评估内容体系在公共数据管理领域的普遍适用性，同时重点关注数据安全评估策略及方法在各公共管理和服务机构的可落地性；

2）安全合规性——本文件在编制过程中始终遵循与我国现有的法律法规、标准规范等规定相一致的原则，同时也兼顾行业主管及监管部门对公共数据进行安全管理的实际监管要求。

2、主要条款说明、技术指标参数

《公共数据安全评估规范》属于公共数据安全建设相关系列标准之一，是《公共数据安全要求》的配套标准，依托于《公共数据安全要求》中具体安全要求条款，提出可操作的评估操作方法。本文件主要内容包括：

1）范围；

本文件规定了公共数据安全的评估规范，主要包括总体概述、通用管理安全评估要求、通用技术安全评估要求、数据处理活动安全评估要求、整体评估与评估结论。

本文件适用于公共管理和服务机构数据安全能力的评估，也适用于处理大量个人信息的服务平台数据安全能力的评估，各级公共数据主管部门、公共管理和服务机构可参照执行。

2）规范性引用文件；

对本文件规范引用进行说明。

3）术语和定义；

对评估机构、被评估机构、数据场景、主责机构及关联机构进行了界定和说明。

4）缩略语；

对缩略语进行界定。

5）概述；

本文件明确了评估机构在评估过程中应遵循的原则，包括公正客观、最小影响、可控性、全面性、书面授权、保密性等原则；本文件明确了评估过程中评估机构和被评估机构应承担的责任和义务；本文件提出评论能力维度可划分为组织能力、制度能力、人员能力、技术能力四个方面。本文件提出的评估方法包括文档查阅、人员访谈、技术检测、系统核验；本文件提出了评估适用情形和评估流程；并对评估对象进行了说明。

本文件提出了如下图所示的评估框架：

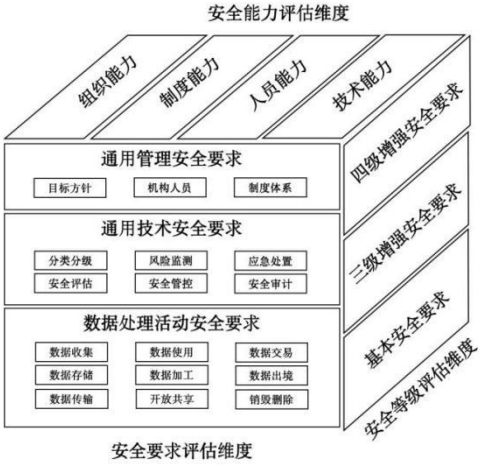

图1　公共数据安全评估框架

6）通用管理安全评估；

给出包含总体数据安全策略、数据安全管理机构和人员、数据安全管理制度体系三个评估项的具体评估细则，包括级别要求、评估子项、评估方法、评估内容。

7）通用技术安全评估；

给出包含数据分类分级保护、数据安全评估、数据安全风险监测、数据安全管控、数据安全应急处置、数据安全审计六个评估项的具体评估细则，包括级别要求、评估子项、评估方法、评估内容。

8）数据处理活动安全评估；

给出包含数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据交易、数据出境、数据销毁与删除九个评估项的具体评估细则，包括

级别要求、评估子项、评估方法、评估内容。

9）整体评估；

给出评估子项间评估、例外情况评估的定义。

10）评估结论；

提出采用风险分析的方法对单个评估子项评估结果中存在的不符合或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对公共数据安全造成影响的程度，综合评价这些不符合项或部分符合项对评估对象造成的安全风险，公共数据安全评估报告应给出评估对象的评估结论，确认评估对象达到相应数据安全等级保护要求的程度。评估结论分为优、良、中、差。

11）附录。

给出了公共数据安全评估评分细则、高风险项判例、常见威胁列表、公共数据安全评估报告模版、公共数据安全评估案例等资料性附录。

3、主要试验情况分析

1）标准编制组成员对数据安全领域相关法律法规、上位标准的内容和框架进行充分研究，并广泛查阅相关文献完善技术细节。

2）自 2020 年起，为摸清深圳市党政机关数据安全管理工作现状，识别数据安全短板，评估其与数据安全相关政策法规、标准规范差距点，深圳市信息安全管理中心已连续三年对重点单位开展数据安全风险评估。《公共数据安全评估规范》的编制也充分吸纳了评估工作的实践经验，未来也会结合每年度的数据安全风险评估活动进行该标准的推广和贯标。

3）本文件在编制过程中已选取某单位系统作为试点，对评估细则的合理性和可操作性进行论证，并提供评估案例作为资料性附录。

五、知识产权情况说明

本文件不涉及专利及知识产权问题。

六、重大意见分歧的处理依据和结果

无。

七、实施标准的措施建议

本文件拟通过标准宣贯、标准实施监督检查、配套机制完善等方式推动实施。

八、其它应予说明的事项

无。