ICS 35.240.01
CCS L 67

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T 439—2024

公共数据安全评估方法

Assessment methods of common data security

2024-04-22 发布　　2024-05-01 实施

深圳市市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由深圳市政务服务和数据管理局提出并归口。

本文件起草单位：深圳市信息安全管理中心、全知科技（杭州）有限责任公司、鹏城实验室、中国电子标准化研究院、金砖国家未来网络研究院中国分院、深圳市智慧城市科技发展集团有限公司、深圳国家金融科技测评中心有限公司、深圳赛西信息技术有限公司、蚂蚁科技集团股份有限公司、华为技术有限公司。

本文件主要起草人：董安波、李苏、罗菁春、林宇群、穆端端、赵剑、轩豪男、潘志斌、方兴、周顿科、魏凤玲、李佳雯、包亚鹏、陈崇滨、林生锐、束建钢、何延哲、林桢、刘慧洋、王志、罗丰、吴祖顺、白晓媛、常新苗。

公共数据安全评估方法

1 范围

本文件规定了公共数据安全的通则、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。

本文件适用于各级公共数据主管部门、公共管理和服务机构开展公共数据安全评估，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。

本文件不适用于涉及国家秘密的公共数据安全评估。

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。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求

DB4403/T 271—2022 公共数据安全要求

3 术语和定义

GB/T 35273—2020、GB/T 37988—2019、DB4403/T 271—2022界定的以及下列术语和定义适用于本文件。

3.1

公共数据 common data

公共管理和服务机构及处理大量个人信息的服务平台在依法履行公共管理职责或者提供公共服务过程中产生、处理的数据。

注：本文件提及的数据均指公共数据。

3.2

数据场景 data scenario

为了达到特定业务目的而对数据进行处理和使用的场景，对场景下数据流向进行全链路分析。

注：单个数据场景可能涉及多个机构及其业务系统。

3.3

主责机构 main responsible organization

评估对象为数据场景时，场景涉及主要系统的责任部门。

3.4

关联机构 related responsible organization

评估对象为数据场景时，涉及场景相关处理活动的其他机构。

注：如数据场景处理活动仅在主责机构内部，则不涉及关联机构。

4 缩略语

下列缩略语适用于本文件。

SDK：软件开发工具包（Software Development Kit）

API：应用程序接口（Application Programming Interface）

5 通则

5.1 评估原则

为规范公共数据安全评估工作，全面有效发现公共数据可能面临的各类安全风险，评估机构在评估过程中，遵循下列原则：

a) 公正客观原则：评估机构对评估对象数据安全保障措施进行公平客观的判定，不受机构性质、评估对象、评估时间、评估人员、利益关系等任何因素影响而损害评估的公正及客观性；

b) 最小影响原则：评估机构对评估对象的网络、业务、数据流转等正常运行造成的影响降低到最低，不因评估工作而导致业务连续性的中断；

c) 可控性原则：评估机构确保评估过程可管可控，使用的评估工具或技术手段，已经过实践验证，不存在安全隐患；

d) 全面性原则：评估机构全面覆盖评估要点，基于评估要点对评估对象涉及的资产（如制度类文档、数据资产、软硬件资产、人力资源等）、数据处理活动各环节进行评估；

e) 书面授权原则：评估机构开展评估工作得到被评估机构的正式书面授权；

f) 保密性原则：评估机构及评估人员与被评估机构签订数据安全相关保密协议，明确保密责任、义务及争议条款，除法律要求或获得被评估机构同意外，评估人员获取的评估对象相关信息、过程文档等严格保密，不对外透露。

5.2 评估体系

公共数据安全评估框架见图1，公共数据安全评估体系包含安全要求、安全能力、安全等级三个维度，三个维度具体内容如下：

a) 内容涵盖通用管理安全、通用技术安全及数据处理活动安全三方面安全要求；

b) 针对组织、制度、人员、技术四方面安全能力进行评估；

c) 对于不同的安全等级选取相对应的安全要求进行评估，评估对象涉及不同安全等级的数据类型且无法拆分评估时，依据评定的最高数据安全等级的安全要求开展评估，按照DB4403/T 271—2022中6.7规定的安全等级与安全要求的关系确定安全等级与对应安全要求。

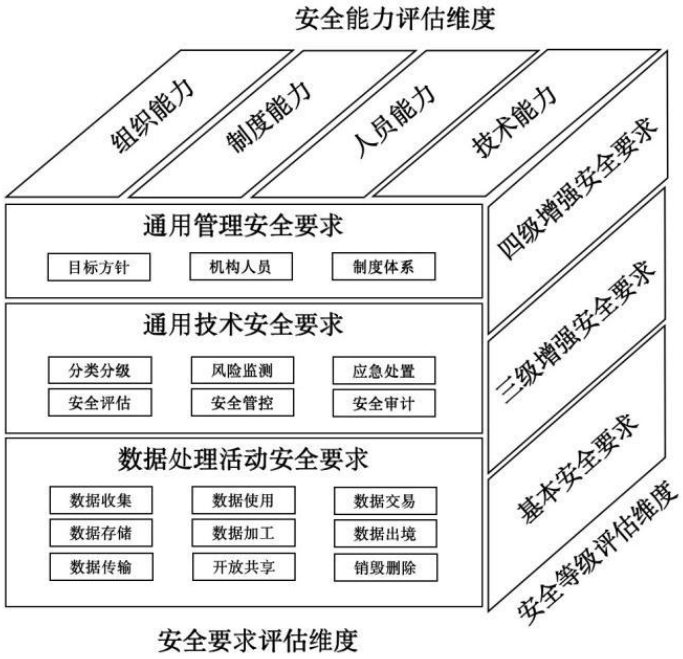

图1　公共数据安全评估框架

5.3　安全能力

评估机构对评估对象的数据安全能力进行评估，安全能力应分为以下四个维度：

a)　组织能力：主要考察数据安全组织架构及人员的设立、职责分工及沟通协作；

b)　制度能力：主要考察数据安全制度及流程建设完备性、可执行性、动态更新性；

c)　人员能力：主要考察人员数据安全建设专业能力、工作执行落地情况；

d)　技术能力：主要考察采取技术手段或自动化技术工具落实数据安全要求的能力。

5.4　评估手段

公共数据安全评估宜采取如下评估手段开展评估工作：

a)　文档查阅：评估人员通过查看数据安全评估相关材料，如数据安全管理制度、业务安全保障措施技术材料、制度落地执行记录表单等，辅助验证是否符合相关安全要求；被评估机构提前准备相关文档以供评估人员查阅；

b)　人员访谈：评估人员与被评估机构相关人员进行交流、讨论、询问等，以初步验证数据安全要求的符合性，可结合其他评估手段，充分验证数据安全保障措施的有效性；访谈人员范围包含数据安全管理机构人员以及承载业务系统运行的应用、系统、网络相关人员等；

c)　技术检测：评估人员对业务系统不同应用形态（如网页应用程序、移动应用程序、小程序、公众号等）、系统、网络等进行技术测试，以验证是否符合数据处理活动技术安全要求；通过评估人员事先准备测试工具（如流量监测工具、扫描工具、渗透测试工具等）、业务注册或使用被评估机构准备的测试账号等以完成技术测试；

d)　系统核验：被评估机构人员根据评估人员的要求，上机核验被评估机构相关安全能力平台或业务数据处理活动各环节、数据操作日志记录等界面；此评估手段可直观验证数据安全保障措施

是否有效，被评估机构人员安排相关人员进行现场演示，评估人员根据演示结果判断安全要求的符合性。

5.5 评估适用情形

满足如下情形之一，应及时启动评估工作：

a) 涉及公共数据的政务信息化建设项目合同终验前；
b) 承载公共数据的信息系统运营阶段，数据承载环境发生重大变更时，如数据处理技术模式变更、数据采集渠道变更、数据种类发生重大变化、批量数据共享对象变更、业务重大版本迭代、网络环境重大变更、数据存储系统升级改造、数据出境等；
c) 行业主管部门要求或法律法规规定的其他情形。

5.6 评估指标和评估对象说明

5.6.1 评估指标

对第 6 章至第 8 章的评估指标进行编码，M 指代通用管理安全，T 指代通用技术安全，P 指代数据处理活动安全，BR 指代基本安全要求，TR 指代三级增强要求，FR 指代四级增强要求，DT 指代数据子类或字段，各评估指标按照附录 A 进行评分。

5.6.2 评估对象

业务系统、数据场景均可作为评估对象。评估机构针对选取的评估对象，确定评估指标，开展评估工作，并编制形成评估报告。不同的评估对象适用于不同的评估指标：

a) 评估对象为业务系统，根据其安全等级选取第6章至第8章相对应安全要求的评估指标进行评估，判别依据为被评估机构数据安全组织架构、人员配备、制度流程、技术能力及与该业务系统相关的资产、已有安全保护措施等；
b) 评估对象为数据场景，应划分主责机构和关联机构，涉及的多个机构及其业务系统均纳入评估范围，评估指标选取原则如下：
   1) 针对主责机构，参照第 6 章至第 8 章的评估指标对其开展评估；
   2) 针对关联机构，一个关联机构可能涉及该场景下单个或多个数据处理活动环节，参照第 8 章中与该关联机构涉及数据处理活动环节所对应的评估指标开展评估。

注：主责机构指数据场景主要系统的管理者，对该场景下处理的数据负主要责任。关联机构指与数据场景有关联关系，涉及该场景下数据处理活动中单个或多个环节的机构，对其涉及的环节负关联责任。

5.7 评估流程

公共数据安全的评估流程按照以下步骤进行：

a) 组建评估团队：数据安全评估前，组建数据安全评估团队，评估团队宜包含评估机构评估人员、被评估机构数据安全管理机构人员，评估过程中涉及的人员包含评估对象相关的业务运营运维部门、业务开发测试部门、数据合作方等人员，评估机构的评估人员应具备数据安全评估能力，确保评估结果的有效性；
b) 确定评估对象：按照5.6.2明确数据安全评估对象，针对选定的评估对象，根据评估对象的安全等级，确定评估指标；
c) 评估对象调研：数据安全评估团队对评估对象相关数据安全工作进行充分调研，包括业务简介、网络拓扑情况、数据安全岗位人员、数据安全管理相关制度流程表单、数据安全设备部署情况、已有安全保护措施等；在组织评估实施之前，提供评估方案，并与被评估机构协商一致；

d) 组织评估实施：数据安全评估团队组织远程及现场评估，采用文档查阅、人员访谈、技术检测、系统核验等评估手段，开展评估指标的评分工作，并进行安全风险分析，附录B给出了高风险项示例，附录C给出了常见的数据安全威胁，可参考进行风险分析；

e) 评估报告编制：数据安全评估团队对评估过程进行记录，保存对应的评估佐证材料，并编制形成数据安全评估报告（评估报告模板见附录D），组织与被评估机构共同确认数据安全评估结果，完成公共数据安全的评估，评估工作案例见附录E。

6 通用管理安全评估

6.1 总体数据安全策略

总体数据安全策略评估内容描述见表1。

表1 总体数据安全策略评估内容

评估项	级别要求	评估子项	评估手段	评估内容
总体数据安全策略（MO1）	基本安全要求	应明确数据安全管理的策略，包括管理目标、原则、要求等内容，制定或修订完善总体安全管理框架，公共数据安全管理应作为重点内容，纳入总体安全管理范畴。（MO1-BRO1）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈，询问被评估机构是否组织专门部门明确总体数据安全策略。 **制度能力：** 2.通过文档查阅，确认总体数据安全策略是否包括管理目标、原则、要求等内容；或相关信息安全总体纲领文档是否体现数据安全方面的总体方针政策。 **人员能力：** 3.通过人员访谈，询问被评估机构是否了解机构制定的总体数据安全策略。
总体数据安全策略（MO1）	三级增强要求	应定期对数据安全策略的合理性及适用性进行论证和审定，动态调整。（MO1-TRO1）	文档查阅	**组织能力：** 1.被评估机构是否组织定期对数据安全策略的合理性及适用性进行论证和审定，查阅相关评审记录。 **制度能力：** 2.是否根据定期审定结果，动态调整数据安全策略，查阅动态调整内容。

6.2 数据安全管理机构与人员

数据安全管理机构与人员评估内容描述见表2。

表2 数据安全管理机构与人员评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管理机构与人员（MO2）	基本安全要求	机构管理：应设立数据安全管理机构，明确数据安全责任人，落实数据安全保护责任。数据安全责任人履行职责包括但不限于： 1)组织制定数据保护计划并落实； 2)组织开展数据安全影响分析和风险评估，督促整改安全隐患； 3)组织按要求向有关部门报告数据安全保护和事件处置情况； 4)组织受理并处理数据安全投诉和举报事项。（MO2-BRO1）	人员访谈 文档查阅	**组织能力：** 1．通过人员访谈，询问被评估机构是否明确数据安全管理机构及数据安全负责人，明确数据安全责任人的工作职责，查阅正式发文文档。 **制度能力：** 2．查阅数据安全负责人的职责内容是否包括但不限于： 1）组织制定数据保护计划并落实； 2）组织开展数据安全影响分析和风险评估，督促整改安全隐患； 3）组织按要求向有关部门报告数据安全保护和事件处置情况； 4）组织受理并处理数据安全投诉和举报事项。
	基本安全要求	机构管理：应按照相关法律法规的要求编制公共数据资源目录，加强数据安全保护。（MO2-BRO2）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否按照相关法律法规的要求编制公共数据资源目录。

表 2　数据安全管理机构与人员评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管理机构与人员（MO2）	基本安全要求	机构管理：数据安全管理机构应明确数据管理员、数据安全管理员、数据安全审计员等岗位职责，落实岗位人员，保障数据安全管理与审计工作开展。相关岗位职责应包括： 1)数据管理员负责数据存储、数据权限分配、数据资产梳理等； 2)数据安全管理员负责数据权限审批、数据分类分级、数据安全风险检测与评估、数据安全事件应急响应处置、教育培训等，可由安全管理员兼任； 3)数据安全审计员负责数据安全审计等。 （MO2-BR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈，询问被评估机构的数据安全管理机构是否设立数据安全相关岗位人员，包括数据管理员、数据安全管理员、数据安全审计员等岗位，其中数据管理员和数据安全审计员不能由同一人兼任，数据安全管理员和数据安全审计员不应由同一人兼任。 **制度能力：** 2.通过文档查阅方式，查看被评估机构是否明确不同数据安全相关岗位的职责明细，查看岗位职责内容是否全面、明确，是否包含如下职责内容： 1）数据管理员负责数据存储安全、数据权限分配、数据资产梳理等； 2）数据安全管理员负责数据权限审批、数据分类分级、数据安全风险检测与评估、数据安全事件应急响应处置、教育培训等，可由安全管理员兼任； 3）数据安全审计员负责数据安全审计等。
	基本安全要求	机构管理：处理个人信息达到国家网信部门规定数量的，应指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督，并公开个人信息保护负责人联系方式，将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责部门。 （MO2-BR04）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈，询问被评估机构是否属于处理个人信息达到国家网信部门规定数量的公共管理和服务机构，如是则是否明确指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。 **制度能力：** 2.查验被评估机构是否公开个人信息保护负责人的姓名、联系方式等，并已报送履行个人信息保护职责的部门。

表 2　数据安全管理机构与人员评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管理机构与人员（MO2）	基本安全要求	机构管理：应针对数据类别级别变更、数据权限变更、重大数据操作及外部系统接入等事项建立审批程序，按照审批程序执行审批过程。（MO2-BR05）	文档查阅	**制度能力：** 1.通过文档查阅方式，查看被评估机构是否已建立针对数据类别级别变更、数据权限变更、重大数据操作及外部系统接入等事项的审批程序。 2.通过文档查阅方式，查看事项审批程序执行记录文件。
	基本安全要求	机构管理：涉及数据合作方的机构，应与数据合作方签订合作协议及数据安全保密协议，明确双方数据安全保密责任与义务，宜定期审核数据合作方资质背景、数据安全保障能力等，并组织动态合规评估。（MO2-BR06）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，查验被评估机构是否定期组织审核数据合作方资质背景、数据安全保障能力等，并组织合规评估，出具评估报告；通过文档查阅方式，查看数据合作方合规评估报告的完整性。 **制度能力：** 2.查验被评估机构是否明确与数据合作方签订合作协议及数据安全保密协议，通过文档查阅方式，查看协议是否明确双方数据安全保密责任与义务。
	三级增强要求	机构管理：应针对重大数据处理活动建立逐级审批机制。（MO2-TR01）	人员访谈 文档查阅	**制度能力：** 1.查验被评估机构是否建立重大数据处理活动逐级审批机制，通过文档查阅方式，查看审批机制的合理性、有效性及可执行性。
	三级增强要求	机构管理：应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。（MO2-TR02）	人员访谈 文档查阅	**组织能力：** 1.查验被评估机构是否组织定期审查审批事项。 **制度能力：** 2.查验被评估机构是否在审查后，动态更新授权和审批的项目、审批部门和审批人等信息，保持审批机制的合理性；通过文档查阅方式，查验是否具有对相关审批事项的定期审查记录和授权更新记录。
	基本安全要求	人员管理：应加强人员管理，明确规定人员录用、人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面管理要求并严格落实。（MO2-BR07）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，明确被评估机构是否制定人员管理相关制度；查阅制度是否包含人员录用、人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面的管理要求，查阅制度执行记录。

表 2　数据安全管理机构与人员评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管理机构与人员（MO2）	基本安全要求	人员管理：应与内部数据岗位人员、数据合作方人员签订保密协议，明确数据访问范围、操作权限、人员调离岗保密要求、保密期限、违约责任等，有效约束操作行为。（MO2-BR08）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否与内部数据岗位人员及数据合作方人员签订保密协议。 2.通过文档查阅方式，查验保密协议内容是否包括数据访问范围、操作权限、人员调离岗保密要求、保密期限、违约责任等。
	基本安全要求	人员管理：应制定数据安全培训计划，定期组织数据安全培训工作，每年至少一次。针对机构全员，培训内容包括但不限于数据安全意识、法律法规。针对数据岗位人员，培训内容包括但不限于标准规范、技能培训、应急响应、应急演练，留存培训记录（MO2-BR09）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定了数据安全培训计划，每年至少组织开展一次数据安全培训工作。 **制度能力：** 2.通过人员访谈、文档查阅方式，查验被评估机构是否针对机构全员开展数据安全培训，针对机构全员的培训内容应包括但不限于数据安全意识、法律法规。 3.通过人员访谈、文档查阅方式，查验被评估机构是否针对相关数据岗位人员开展数据安全培训，针对数据岗位人员的培训课件应包括但不限于标准规范、技能培训、应急响应、应急演练。 4.通过文档查阅方式，查验以往数据安全培训记录，是否包括培训通知、培训照片、培训签到表、培训课件、培训评价表、培训考核记录等。
	基本安全要求	人员管理：宜组织数据岗位人员考取相关资质证书，持证上岗。（MO2-BR10）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构数据岗位人员是否均考取相关资质证书，持证上岗，证书类型包括但不限于：CISP、CISSP、CDPSE、数据库工程师、数据治理工程师。
	三级增强要求	人员管理：应配备专职安全管理员承担数据安全管理员工作。（MO2-TR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否设立专职数据安全管理员或者配备专职安全管理员，其职责范围涉及数据安全管理员工作。

表 2　数据安全管理机构与人员评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管理机构与人员（MO2）	三级增强要求	人员管理：应针对不同数据岗位制定不同的培训计划，对数据安全基础知识、岗位操作规程等进行培训。（MO2-TR04）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否组织针对不同数据岗位制定不同的培训计划，对数据安全基础知识、岗位操作规程等进行培训。
	三级增强要求	人员管理：应定期对不同数据岗位人员进行技能考核。（MO2-TR05）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否定期组织对不同数据岗位人员进行技能考核，查阅技能考核记录文件。 **人员能力：** 2.通过人员访谈方式，了解不同数据岗位人员技能掌握程度，不同数据岗位人员应熟练掌握对应岗位技能。
	四级增强要求	人员管理：关键事务岗位应配备多人共同管理。（MO2-FR01）	人员访谈	**组织能力：** 1.通过人员访谈方式，查验被评估机构是否针对关键事务岗位设立多人共同管理。
	四级增强要求	人员管理：应从内部人员中选拔从事关键数据岗位的人员。（MO2-FR02）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构的关键事务岗位是否从内部人员中选拔产生，查阅选拔执行记录文档。

6.3 数据安全管理制度体系

数据安全管理制度体系评估内容描述见表3。

表3 数据安全管理制度体系评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管理制度体系（M03）	基本安全要求	应指定专门的部门或授权数据安全管理机构负责数据安全管理制度的制定。（M03-BR01）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否指定专门的部门或授权数据安全管理机构负责数据安全管理制度的制定工作，查阅相关指定或授权文件。
	基本安全要求	应建立健全数据安全保护制度体系，制度体系内容包括但不限于数据安全政策、组织机构与人员管理、数据分类分级、数据安全评估、数据安全风险监测、数据访问权限管控、数据安全应急与处置、数据安全审计、数据活动安全管理要求（包括数据收集、存储、传输、使用、加工、共享、交易、出境、销毁）、数据安全教育培训、数据合作方管理、个人信息安全保护。（M03-BR02）	文档查阅	**制度能力：** 1.通过文档查阅方式，查验被评估机构是否已建立数据安全保护制度体系。 2.通过文档查阅方式，查验被评估机构制定的数据安全保护制度体系是否包括但不限于数据安全政策、组织机构与人员管理、数据分类分级、数据安全评估、数据安全风险监测、数据访问权限管控、数据安全应急与处置、数据安全审计、数据活动安全管理要求（包括数据收集、存储、传输、使用、加工、共享、交易、出境、销毁）、数据安全教育培训、数据合作方管理、个人信息安全保护。
	基本安全要求	提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督。（M03-BR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否属于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，若是则是否组建由外部成员组成的独立机构对个人信息保护情况进行监督，查阅相关执行记录文档。 **制度能力：** 2.通过文档查阅方式，查验被评估机构是否建立个人信息保护合规制度体系，查阅个人信息保护合规制度体系文档。

表 3　数据安全管理制度体系评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管理制度体系（MO3）	基本安全要求	应建立投诉、举报受理处置制度，收到通过其平台编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报，自接受投诉举报起，受理时间不超过三天，受理后进行调查取证，一经查实，应依法采取停止传输、消除等处置措施。（MO3-BRO4）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈方式，查验被评估机构是否制定个人信息与数据安全投诉、举报受理处置制度。 2.如属于提供网络信息内容传播服务的网络信息服务提供者，通过文档查阅方式，查验是否明确网络平台运营中，当收到通过其平台编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报时，自接受投诉举报起，受理时间不超过三天，受理后进行调查取证，一经查实，应依法采取停止传输、消除等处置措施。
	基本安全要求	应建立个人信息主体保护权利的渠道和机制，及时响应个人信息主体查阅、复制、更正、删除其个人信息及注销账号的请求，按照 GB/T 35273—2020 中 8.7 规定的要求响应个人信息主体的请求，不应对请求设置不合理条件。（MO3-BRO5）	人员访谈 文档查阅 系统核验	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否建立个人信息主体保护权利的渠道和机制。 **技术能力：** 2.通过系统核验方式，查验被评估机构业务系统是否能及时响应个人信息主体查阅、复制、更正、删除其个人信息及注销账号的请求，按照 GB/T 35273—2020 中 8.7 的要求响应个人信息主体的请求，不对请求设置不合理条件。
	基本安全要求	应通过正式、有效的方式发布数据安全管理制度，并进行版本控制。（MO3-BRO6）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否已通过正式、有效的方式发布数据安全管理制度，查阅制度发布执行记录，查阅制度是否已进行版本控制。
	基本安全要求	应定期对数据安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。（MO3-BRO7）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否定期对数据安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的制度进行修订，查阅修订执行记录文档。

表 3　数据安全管理制度体系评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管理制度体系（M03）	三级增强要求	应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的数据安全管理制度体系。（M03-TR01）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否建立全面的数据安全管理制度体系，体系结构是否由安全策略、管理制度、操作规程、记录表单等构成，查阅制度体系文档。

7　通用技术安全评估

7.1　数据分类分级保护

数据分类分级保护评估内容描述见表4。

表 4　数据分类分级保护评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据分类分级保护（T01）	基本安全要求	应结合数据资产识别技术手段，梳理数据资产，并明确数据资产类型、数据量、存储位置、数据关联系统、数据共享情况、数据出境情况等。（T01-BR01）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈方式，查验被评估机构是否具备数据资产识别相关技术平台。 2.通过系统核验方式，查验平台是否可自动化梳理数据资产，明确数据资产类型、数据量、存放位置、数据关联系统、数据共享情况、数据出境情况等。
	基本安全要求	应明确数据分类标准，依据数据资源属性特征，将数据合理划分类别，形成数据资源分类目录。（T01-BR02）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否依据 DB4403/T 271—2022 中附录 A 建立数据分类标准，被评估机构业务系统是否依据数据资源属性特征，将数据合理划分类别。 **人员能力：** 2.通过人员访谈方式，查验被评估机构业务系统数据分类分级相关岗位人员是否具备数据分类识别能力，能独立开展数据分类工作；如由数据合作方协助开展数据分类工作，则被评估机构业务系统数据分类分级相关岗位人员是否能对数据合作方的数据分类工作进行管理。

表4 数据分类分级保护评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据分类分级保护（T01）	基本安全要求	应明确数据对象安全等级，依据数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用时，对国家安全、社会秩序和公共利益或者个人信息主体、公共管理和服务机构合法权益造成的侵害程度确定安全等级。（T01-BR03）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否依据 DB4403/T 271—2022 第 6 章确定的数据分级方法，建立数据分级标准，被评估机构业务系统是否依据分级标准，明确业务数据安全等级。 **人员能力：** 2.通过人员访谈方式，查验被评估机构业务系统数据分类分级相关岗位人员是否具备数据分级能力，能独立开展数据分级工作；如由数据合作方协助开展数据分级工作，则被评估机构业务系统数据分类分级相关岗位人员是否能对数据合作方的数据分级工作进行管理。
	基本安全要求	应在数据分类分级基础上，形成数据资产清单，落实不同数据安全等级差异化防护措施要求。（T01-BR04）	人员访谈 文档查阅	**制度能力：** 1.通过文档查阅方式，查验被评估机构业务系统是否明确不同数据安全等级差异化防护措施要求。 **人员能力：** 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统数据分类分级相关岗位人员是否已依据制定的数据分类分级标准，形成数据资产清单，对照落实不同数据安全等级差异化防护措施要求。
	基本安全要求	应定期评审数据对象的类别和级别，如需变更数据所属类型或级别，应依据变更审批流程执行变更。（T01-BR05）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否组织定期评审数据对象所属类型及级别，确保数据对象类别及级别的合理性，查阅记录文档。 **制度能力：** 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否建立数据对象类别或级别变更流程，查阅变更审批记录。
	三级增强要求	应采取数据安全防护措施，对重要数据和敏感个人信息进行重点保护。（T01-TR01）	人员访谈 技术检测 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否对重要数据及敏感个人信息进行重点保护，重点安全保护具体技术措施应涉及数据处理活动全过程。 2.通过技术检测方式，查验重点安全保护技术措施是否有效。

表4　数据分类分级保护评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据分类分级保护（T01）	四级增强要求	应建立数据资产识别技术能力，对数据对象进行标记与跟踪，构建数据血缘关系。（T01-FR01）	系统核验	**技术能力：** 1.通过系统核验方式，查验被评估机构业务系统是否已建立数据资产识别技术能力，并能对数据对象进行标记与跟踪，构建数据血缘关系。

7.2　数据安全评估

数据安全评估评估内容描述见表5。

表5　数据安全评估评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据安全评估（T02）	基本安全要求	应结合自身数据安全要求，制定数据安全风险评估方法，明确风险评估目的、范围、依据、评估流程、评估频率、实施评估、综合评估分析等内容。（T02-BR01）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定数据安全风险评估制度；查阅制度是否包括风险评估目的、范围、依据、评估流程、评估频率、实施评估、综合评估分析等内容。
	基本安全要求	在出现法律法规重大更改或增删、业务活动发生重大变化、数据资产发生重大变化、发生重大数据安全事件、数据安全管理方针发生变化等重大情况变化时应进行局部或全面数据安全风险评估，形成数据安全风险评估报告。（T02-BR02）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否建立数据安全风险评估启动机制，是否明确在出现法律法规重大更改或增删、业务活动发生重大变化、数据资产发生重大变化、发生重大数据安全事件、数据安全管理方针发生变化等重大情况变化时应进行局部或全面数据安全风险评估。 2.通过文档查阅方式，查验在重大情况变化发生时是否启动数据安全风险评估，查阅数据安全风险评估报告。

表5 数据安全评估评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全评估（T02）	基本安全要求	涉及国家、行业存在数据安全合规监管要求的机构，应定期开展数据安全合规性评估，并向有关主管部门报送合规性评估报告。（T02-BR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否存在行业或国家相关部门（如工业和信息化部、中共中央网络安全和信息化委员会办公室等）数据安全合规性评估监管要求，查阅相关文件通知。 2.如存在相关监管要求，通过人员访谈、文档查阅方式，查验被评估机构业务系统是否定期开展数据安全合规性评估，并向有关主管部门报送合规性评估报告，查阅数据安全合规性评估报告及报送记录。
	基本安全要求	涉及敏感个人信息处理、个人信息自动化决策、委托处理、他人提供（含境外）、公开、其他对个人权益有重大影响的个人信息处理活动等，应事先开展个人信息保护影响评估，评估记录至少保存三年。（T02-BR04）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定相关制度，明确当涉及敏感个人信息处理、个人信息自动化决策、委托处理、他人提供（含境外）、公开、其他对个人权益有重大影响的个人信息处理活动等时，应事先开展个人信息保护影响评估，评估记录至少保存三年，查阅相关制度内容。 2.如业务系统存在相关活动，通过人员访谈、文档查阅方式，查验被评估机构是否事前开展个人信息保护影响评估，查阅个人信息保护影响评估记录。 3.通过人员访谈、文档查阅方式，查验个人信息保护影响评估记录是否至少保存三年。
	基本安全要求	应按 GB/T 22239—2019 描述的基本要求，同步规划、建设、运营信息系统，并对信息系统组织开展定级备案、等级测评、安全整改工作。（T02-BR05）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否落实网络安全等级保护工作，按 GB/T 22239—2019 描述的基本要求，同步规划、建设、运营信息系统，并对信息系统组织开展定级备案、等级测评、安全整改工作；查阅网络安全等级保护定级备案证明及测评报告。

表5 数据安全评估评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全评估（T02）	基本安全要求	涉及关键信息基础设施信息系统安全要求应遵照相关法律法规执行。（T02-BR06）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否遵照关键信息基础设施相关法律法规执行安全保护，查阅关键信息基础设施系统安全测评报告。
	三级增强要求	应定期开展数据安全自评估工作，涉及处理敏感个人信息及国家规定的重要数据的机构，应按照有关规定定期开展风险评估，并向有关主管部门报送风险评估报告，风险评估报告应包括处理的重要数据种类、数量，开展数据处理活动的情况，面临的数据安全风险以及应对措施等。（T02-TR01）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定相关要求，明确应定期开展数据安全自评估工作。 **组织能力：** 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否定期组织开展数据安全自评估工作，涉及处理敏感个人信息及国家规定的重要数据时，是否按照有关规定定期开展风险评估，主动向有关主管部门报送风险评估报告，查阅报送记录。 3.通过文档查阅方式，查阅风险评估报告是否包括处理的重要数据种类、数量，开展数据处理活动的情况，面临的数据安全风险以及应对措施等。

7.3 数据安全风险监测

数据安全风险监测评估内容描述见表6。

表6 数据安全风险监测评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据安全风险监测（T03）	基本安全要求	应具备常态化数据安全风险监测能力，持续监测数据安全风险，风险类型包括但不限于账号风险、权限风险、异常操作行为、数据出境风险、数据暴露面风险。（T03-BR01）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构是否建立数据安全风险监测相关技术能力；演示是否可持续监测数据安全风险，风险类型是否包括账号风险、权限风险、异常操作行为、数据出境风险、数据暴露面风险等。

表6 数据安全风险监测评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全风险监测（T03）	基本安全要求	应加强数据安全风险闭环管理，持续提升数据安全风险处置能力。（T03-BR02）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否具备数据安全风险闭环管理能力，查阅是否具备完备的数据安全风险台账、整改跟踪记录、残余风险处置计划等文档。
	三级增强要求	应建立数据安全风险监测预警机制，制定合理有效的风险监测指标。（T03-TR01）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构数据安全风险监测技术能力是否已内置合理有效的风险监测指标，如监测预警阈值、敏感数据类型占比、风险类型占比、应用资产监测范围等。
	三级增强要求	应对数据安全事件和可能引发数据安全事件的风险隐患进行收集、分析判断和持续监控预警，建立数据安全监测预警流程，有效保障业务系统所承载数据资产的机密性、完整性、可用性。（T03-TR02）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否建立数据安全监测预警流程，对数据安全事件和可能引发数据安全事件的风险隐患进行收集、分析判断和持续监控预警。 2.通过人员访谈、文档查阅方式，查验被评估机构数据安全管理员是否依据数据安全监测预警流程，开展监测预警工作，查阅相关执行记录文档。
	三级增强要求	应配备专人负责数据安全风险监测工作，定期出具风险监测报告。（T03-TR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否设立专人负责数据安全风险监测工作，定期出具风险监测报告。
	三级增强要求	应定期对数据安全风险监测工作的有效性、全面性进行审核验证。（T03-TR04）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否定期组织对数据安全风险监测工作的有效性、全面性进行审核、验证，查阅评审验证记录。

7.4 数据安全管控

数据安全管控评估内容描述见表7。

表7 数据安全管控评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管控（T04）	基本安全要求	数据访问权限管控：应根据不同数据级别，明确数据管理、审计类账号权限开通、分配、使用、变更、注销等安全管理要求，账号关联对象包括机构内部及数据合作方人员。（T04-BR01）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否建立账号安全管理制度，明确数据管理、审计类账号权限开通、分配、使用、变更、注销等要求，查阅相关制度文档。
	基本安全要求	数据访问权限管控：应对账号及对应权限进行记录，并在账号或权限发生变更时及时更新，重点关注离职人员账号回收、管理权限变更、沉默账号、复活账号。（T04-BR02）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统涉及的各类系统（如业务管理后台、数据库管理系统、操作系统、业务管理相关平台等）账号管理功能，是否能对账号及权限状态及时更新设置，是否可检测沉默账号。 2.通过人员访谈、系统核验方式，抽查检验账号是否不存在离职或调岗人员账号未回收的情况。
	基本安全要求	数据访问权限管控：应严格控制账号访问、操作权限，明确账号权限审批流程。（T04-BR03）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否建立账号申请审批流程，并保留账号审批记录，包括账号开通、变更、注销等，查阅账号审批记录文档。
	基本安全要求	数据访问权限管控：应对账号进行统一身份认证、操作行为记录。（T04-BR04）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否建立账号统一身份认证平台，对业务系统涉及各类系统（如业务管理后台、数据库管理系统、操作系统、业务管理相关平台等）进行统一认证，统一身份认证平台如4A平台、堡垒机、集中账号审计平台等。 2.通过系统核验方式，查验统一身份认证平台是否可记录数据账号操作行为。

表 7　数据安全管控评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管控（T04）	基本安全要求	数据访问权限管控：应对业务系统之间的数据访问采取身份鉴别、访问控制、安全审计、资源控制等技术措施。（T04-BR05）	人员访谈 技术检测	**技术能力：** 1.通过人员访谈、技术检测方式，查验被评估机构业务系统之间是否存在数据交互的场景，并检测各场景是否采取身份鉴别、访问控制等技术措施。 2.通过技术检测方式，查验被评估机构业务系统之间是否能对各数据交互场景进行安全审计，及时发现异常数据操作行为，查阅审计记录。 3.通过技术检测方式，查验被评估机构业务系统之间是否存在资源控制措施，限制资源访问并发数。
	基本安全要求	数据访问权限管控：应对数据批量下载、上传、删除、共享和销毁等重大操作行为设置内部审批流程，并记录操作行为。（T04-BR06）	人员访谈 文档查阅 系统核验	**制度能力：** 1.通过人员访谈、文档查阅方式，查阅被评估机构业务系统是否建立数据重大操作行为（如重要数据或个人信息批量下载、上传、删除、共享和销毁等）内部审批流程，查阅相关制度及执行记录文档。 **技术能力：** 2.通过人员访谈方式，查验被评估机构业务系统存在数据重大操作行为时，是否对操作行为进行日志记录。 3.通过系统核验方式，查验数据重大操作行为日志记录的完整性，是否包括操作账号、时间、操作对象、操作行为、操作结果等。
	三级增强要求	数据访问权限管控：应对数据跨网络区域传输采取安全管控措施，包括但不限于网络及应用层的访问控制策略，控制粒度为端口级。（T04-TR01）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否存在数据跨网络区域传输的场景，演示业务系统在网络设备（如防火墙、交换机等）设置的 ACL 策略，控制粒度是否为应用层协议及端口级别。
	四级增强要求	数据访问权限管控：应基于数据分类分级结果配置主体对客体的访问控制策略，访问控制粒度应达到主体为用户级或进程级，客体为接口、应用功能、文件、数据库表级等。（T04-FR01）	系统核验 技术检测	**技术能力：** 1.通过系统核验方式，查验被评估机构业务系统是否基于数据分类分级结果配置主体对客体的访问控制策略，演示访问控制策略。 2.通过系统核验、技术检测方式，查验被评估机构业务系统的访问控制粒度是否达到主体为用户级或进程级，客体为接口、应用功能、文件、数据库表级等。

表 7　数据安全管控评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管控（T04）	基本安全要求	数据防泄露管控：应在网络层面对数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警。（T04-BR07）	系统核验	**技术能力：** 1.通过系统核验方式，查验被评估机构业务系统网络侧数据防泄露能力，是否能对数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警。
	三级增强要求	数据防泄露管控：应在终端层面对数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警，并在网络层面实现对异常数据操作行为及时定位和阻断。（T04-TR02）	系统核验	**技术能力：** 1.通过系统核验方式，查验被评估机构业务系统终端侧数据防泄露能力，是否能对终端设备（如运维终端）的数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警。 2.通过系统核验方式，查验被评估机构业务系统网络侧数据防泄露能力，是否能对异常数据操作行为及时定位和阻断。
	四级增强要求	数据防泄露管控：应在终端层面对异常数据操作行为及时定位和阻断。（T04-FR02）	系统核验	**技术能力：** 1.通过系统核验方式，查验被评估机构业务系统终端侧数据防泄露能力，是否能对终端设备（如运维终端）的异常数据操作行为及时定位和阻断。
	基本安全要求	数据接口管控：应在数据接口调用前进行身份鉴别，通过技术手段限制非白名单接口接入。（T04-BR08）	技术检测 系统核验	**技术能力：** 1.通过系统核验、技术检测方式，查验被评估机构业务系统存在的数据接口是否具备鉴权能力，如 Cookie 及 Session、Token、Oauth 等。 2.通过系统核验、技术检测方式，查验被评估机构业务系统是否从技术手段上限制非白名单的接口接入。
	基本安全要求	数据接口管控：应对数据接口定期开展安全检测，及时发现并处置数据安全风险隐患。（T04-BR09）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否定期组织针对数据接口的安全风险检测，查阅数据接口安全风险检测报告。 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否及时整改安全风险隐患，查阅安全风险整改记录。

表 7　数据安全管控评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全管控（T04）	基本安全要求	数据接口管控：应对数据接口实施调用审批流程，对接口调用行为进行日志记录。（T04-BR10）	人员访谈 文档查阅 系统核验	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否建立数据接口调用审批流程，查验审批执行记录文档。 **技术能力：** 2.通过系统核验方式，查验被评估机构业务系统是否对接口调用行为进行日志记录，日志记录内容包括接口地址、调用时间、调用对象、数据类型、调用频次、调用结果等。
	基本安全要求	数据接口管控：应定期梳理数据接口，形成接口清单。（T04-BR11）	人员访谈 文档查阅 系统核验	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否定期人工梳理数据接口，形成数据接口清单，查阅数据接口清单。 **技术能力：** 2.通过系统核验方式，查验被评估机构业务系统是否采取自动化技术能力梳理数据接口，形成数据接口清单，演示相关功能。
	三级增强要求	数据接口管控：应对异常数据接口调用行为实现自动预警、拦截功能。（T04-TR03）	系统核验	**技术能力：** 1.通过系统核验方式，查验被评估机构业务系统是否具备对异常数据接口调用行为实现自动预警、拦截的功能；演示相关功能效果。
	三级增强要求	数据接口管控：应对开放数据接口的平台相关接口数据交互行为进行监测，对接口数据交互行为进行日志记录。（T04-TR04）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否属于对外开放数据接口的平台或系统，包括但不限于数据开放平台、数据共享交换平台、数据交易平台、大数据平台、能力开放平台，如是则演示业务系统是否能对接口数据交互行为进行监测，监测内容包括但不限于接口调用情况（如时间、频次等）、传输数据类型或字段、传输数据量大小，并对接口数据交互行为进行日志记录。
	三级增强要求	数据接口管控：应建立数据接口全生命周期管理机制，形成接口清单，动态更新接口活动状态，如新增、活跃、失活、复活、下线等接口状态，并采取安全管控措施。（T04-TR05）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否建立数据接口全生命周期管理机制，是否对接口状态进行管理，具备识别新增接口、启用接口、禁用接口、沉默接口、复活接口及下线接口等的技术能力，并进行安全管控，演示相关功能效果。

7.5 数据安全应急处置

数据安全应急处置评估内容描述见表8。

表8 数据安全应急处置评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据安全应急处置（T05）	基本安全要求	应建立数据安全应急处置机制，依据区级、市级、行业网络安全事件应急相关文件开展应急处置工作。（T05-BR01）	文档查阅	**制度能力：** 1.通过文档查阅方式，查验被评估机构是否制定数据安全事件应急处置预案。 2.通过文档查阅方式，查验数据安全事件应急处置预案是否依据区级、市级、行业网络安全事件应急相关文件的要求开展应急处置工作，查阅相关预案内容。
	基本安全要求	发生数据泄露、毁损、丢失、篡改等数据安全事件时应立即启动应急预案，采取相应的应急处置措施，及时告知相关权利人，并按照有关规定向网信部门、公安机关和有关行业主管部门报告。（T05-BR02）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构数据安全事件应急队伍在发生数据泄露、毁损、丢失、篡改等数据安全事件时，是否及时记录数据安全事件应急处置过程，是否依据应急预案采取应急处置措施。 **组织能力：** 2.通过人员访谈、文档查阅方式，查验被评估机构是否依据有关规定向网信部门、公安机关和有关行业主管部门报告数据安全事件，查阅事件报告记录，涉及智慧城市和数字政府建设相关的数据安全事件，应同时向公共数据主管部门报告。
	基本安全要求	数据安全应急处置后应分析事件发生原因，总结应急处置经验，调整数据安全策略，形成事件调查记录和总结报告，避免再次发生类似情况。（T05-BR03）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构在发生数据安全事件后，是否及时开展事件调查及经验总结，查阅事件调查记录及总结报告。 2.通过人员访谈、文档查阅方式，查验被评估机构是否及时依据事件调查记录及总结报告，调整数据安全事件应急处置策略，查阅策略更新记录文档。

表8 数据安全应急处置评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全应急处置（T05）	基本安全要求	发生个人信息泄露、毁损、丢失等数据安全事件，或发生数据安全事件风险明显加大时，应立即采取补救措施，及时以电话、短信、邮件或信函等方式告知个人信息主体，并主动报告有关主管部门，必要时应向网信部门报告。（T05-BR04）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构在发生个人信息泄露、毁损、丢失等数据安全事件时，或数据安全事件风险明显加大时，是否通过电话、短信、邮件或信函等方式告知个人信息主体，查阅相关执行记录文档。 2.通过人员访谈、文档查阅方式，查验被评估机构是否主动报告有关主管部门（如政务服务和数据管理局、通信管理局等），必要时是否向网信部门报告，查阅相关执行及报告记录。
	基本安全要求	应采取技术手段对数据安全事件的日志或流量关联分析进行溯源，造成严重事件的应依法追究事件主体责任。（T05-BR05）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构在发生数据安全事件后，数据安全审计员是否进行事件溯源（如通过日志或流量溯源、数字水印溯源等），查阅事件溯源执行记录文档。 **组织能力：** 2.通过人员访谈、文档查阅方式，查验被评估机构在发生严重数据安全事件后，是否依法报公安机关追究事件主体责任，查阅报送记录文档。
	基本安全要求	应根据应急预案明确的数据安全事件场景定期开展应急演练，检验和完善应急处置机制，每年至少一次，事件场景包括但不限于数据泄露、丢失、滥用、篡改、毁损、违规使用。（T05-BR06）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈，询问被评估机构业务系统是否每年组织至少一次数据安全事件典型场景的应急演练。 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统数据安全事件应急演练是否包括数据泄露、丢失、滥用、篡改、毁损、违规使用等典型场景，查阅应急演练方案、演练脚本、演练报告等记录文档。
	三级增强要求	应跟踪和记录数据收集、分析、加工、挖掘等过程，保证在发生事件时溯源数据能重现相应过程。（T05-TR01）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否具备数据收集、分析、加工、挖掘等数据处理活动跟踪和记录能力，在发生数据安全事件后，能保证溯源数据重现相应过程，演示相关功能效果。

表8 数据安全应急处置评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全应急处置（T05）	三级增强要求	关键信息基础设施系统数据在发生重要数据泄露、较大规模个人信息泄露时，应及时上报关键信息基础设施安全保护工作部门。（T05-TR02）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否属于关键信息基础设施系统，若属于，在发生重要数据泄露、较大规模个人信息泄露时，被评估机构是否及时上报关键信息基础设施安全保护工作部门，例如重要行业和领域的主管部门、监督管理部门，包括公安机关、省级人民政府有关部门、电信主管部门及其他有关部门，查阅上报记录。
	四级增强要求	应采取技术手段保证数据处理活动的溯源数据真实性和保密性。（T05-FR01）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否采用数字证书、数字水印等技术手段，能确保安全事件溯源数据的真实性和保密性，演示相关功能效果。

7.6 数据安全审计

数据安全审计评估内容描述见表9。

表9 数据安全审计评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据安全审计（T06）	基本安全要求	应制定数据安全审计制度，审计覆盖面包括数据收集、数据存储、数据传输、数据使用、数据加工、数据共享、数据销毁与删除等数据处理活动各环节，明确审计策略、审计对象、审计内容、审计周期、审计结果、审计问题跟踪等要求。（T06-BR01）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定数据安全审计制度。 2.通过文档查阅方式，查阅数据安全审计覆盖面是否包括数据收集、数据存储、数据传输、数据使用、数据加工、数据共享、数据销毁与删除等数据处理活动各环节，是否明确审计策略、审计对象、审计内容、审计周期、审计结果、审计问题跟踪等要求。

表9　数据安全审计评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据安全审计（T06）	基本安全要求	应对数据处理活动环节实施日志留存管理，日志记录至少包括时间、IP 地址、操作账号、操作内容、操作结果等，在发生安全事件时可提供溯源取证能力，日志保存时间不少于 180 天。（T06-BR02）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否针对数据处理活动各环节进行日志记录，日志记录内容包括但不限于时间、IP 地址、操作账号、操作内容、操作结果，演示相关功能效果。 2.通过人员访谈，询问被评估机构业务系统日志记录保存时间是否不少于 180 天，演示 180 天前的日志记录。
	基本安全要求	应定期对数据处理活动各环节日志进行数据安全审计，每年至少一次，形成数据安全审计报告。（T06-BR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否每年至少一次对数据处理活动各环节日志进行数据安全审计，查阅数据安全审计报告。
	三级增强要求	应定期对数据账号操作及接口调用情况进行安全审计。（T06-TR01）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统数据安全审计员是否定期对业务系统管理类账户（如数据库管理员、业务管理员、系统管理员、数据分析员等）的数据操作行为及接口调用情况进行安全审计，查阅审计记录。

8 数据处理活动安全评估

8.1 数据收集

数据收集评估内容描述见表10。

表10 数据收集评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据收集（P01）	基本安全要求	应对数据收集来源进行鉴别和记录，确保数据收集来源的合法性、正当性，明确数据类型及收集渠道、目的、用途、范围、频度、方式等。（P01-BR01）	人员访谈 文档查阅 技术检测	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否对数据收集来源进行鉴别和记录。 2.通过人员访谈、文档查阅方式，查验业务系统是否制定数据采集原则，明确采集数据类型及收集渠道、目的、用途、范围、频度、方式等，确保数据采集的合法性和正当性。 3.通过人员访谈、文档查阅方式，查验业务系统是否对数据收集行为开展数据源合规性审查，确保数据源的合法性、正当性，查阅数据源合规性审查报告。 4.通过技术检测、系统核验方式，核实是否一致。
	基本安全要求	收集外部机构数据前，应对外部机构数据源的合法性、合规性进行鉴别。（P01-BR02）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，查验被评估机构业务系统是否收集外部机构数据，如有收集外部机构数据，查验被评估机构业务系统是否对外部机构数据源的合法性、合规性进行鉴别，查阅数据源鉴别记录。
	基本安全要求	个人信息收集应遵循合法、正当、必要和诚信原则，并获得个人信息主体的明示同意，不应通过误导、欺诈、胁迫或者其他违背个人信息主体真实意愿的方式获取其同意。（P01-BR03）	人员访谈 系统核验	**组织能力：** 1.通过人工访谈、系统核验方式，查验被评估机构业务系统在收集个人信息前是否获得个人信息主体的明示同意，如主动点击隐私政策协议授权方式。 2.通过系统核验，查验业务系统不存在误导、欺诈、胁迫或者其他违背个人信息主体真实意愿的方式获取其同意的情况。

表 10　数据收集评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据收集（P01）	基本安全要求	应按照 GB/T 35273—2020 中 5.1 至 5.6 规定的要求开展个人信息收集工作。（P01-BR04）	人员访谈 系统核验 技术检测	**组织能力：** 1.通过人员访谈、系统核验、技术检测方式，查验被评估机构业务系统是否按照 GB/T 35273—2020 中 5.1 至 5.6 规定的要求开展个人信息收集工作。
	基本安全要求	提供公共服务的移动互联网应用程序或第三方应用，应遵循最小化收集原则，不应因个人信息主体不同意收集非必要个人信息，而拒绝个人信息主体使用移动互联网应用程序或第三方应用。（P01-BR05）	人员访谈 技术检测	**组织能力：** 1.通过人员访谈方式，询问被评估机构业务系统是否有提供公共服务的移动互联网应用程序或第三方应用，若有，通过技术检测查验是否最小化收集个人信息，是否不因个人信息主体不同意收集非必要个人信息，而拒绝使用。
	三级增强要求	收集外部机构数据前，应对数据收集过程中的网络环境、系统进行安全评估，确保收集数据的机密性、完整性和可用性。（P01-TR01）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，查验被评估机构业务系统是否收集外部机构数据，如有收集，通过人员访谈、文档查阅方式，查验被评估机构业务系统是否对数据收集过程中的网络环境、系统进行安全评估，确保收集数据的机密性、完整性和可用性，查阅安全评估记录。
	1 级～4 级	新建系统宜具备数据字段级别的分类分级功能模块，实现对收集的数据字段自动进行分类分级标识。（P01-DT01）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过系统核验方式，查验被评估机构新建的业务系统本身是否具备数据字段级别分类分级的功能模块，能够实现收集的数据字段自动进行分类分级标识。

表 10　数据收集评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据收集（P01）	2 级～4 级	通过 API 或 SDK 方式收集数据字段前，应进行身份鉴别，并存储数据收集日志记录。（P01-DT02）	人员访谈 文档查阅 技术检测 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过技术检测方式，查验被评估机构业务系统使用的 API 接口或 SDK 是否在数据收集前进行身份鉴别。 3.通过系统核验方式，查验被评估机构业务系统是否已存储 API 接口或 SDK 数据收集的日志记录。
注：第 8 章涉及的 1 级～4 级级别要求主要针对数据子类或数据字段的评估，数据子类或数据字段的级别要求见 DB4403/T 271—2022 附录 B。				

8.2　数据存储

数据存储评估内容描述见表11。

表 11　数据存储评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据存储（P02）	基本安全要求	应明确数据存储相关安全管控措施，如加密、访问控制、数字水印、完整性校验等。（P02-BR01）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定数据存储安全管理制度；查验被评估机构业务系统是否明确数据存储安全管控措施。 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否具备加密、访问控制、数字水印、完整性校验等数据存储安全管控措施内容。
	基本安全要求	应明确数据备份与恢复安全策略，建立数据备份恢复操作规程，说明数据备份周期、备份方式、备份地点。建立数据恢复性验证机制，保障数据的可用性与完整性。（P02-BR02）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定数据备份与恢复安全管理制度；查验被评估机构业务系统是否明确数据备份与恢复安全策略。 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否建立数据备份恢复操作规程，说明数据备份周期、备份方式、备份地点。 **组织能力：** 3.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否建立数据恢复性验证机制，保障数据的可用性与完整性，查阅数据恢复性测试报告。

表 11　数据存储评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据存储（P02）	基本安全要求	应提供异地数据备份功能，利用通信网络将数据定时批量传送至备用场地。（P02-BR03）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否具备异地数据备份功能，能利用通信网络将数据定时批量传送至备用场地，查验异地数据备份配置策略，包括备份工具、时间、频次、方式、地点等。
	基本安全要求	个人生物识别信息应与个人身份信息分开存储，原则上不应存储原始个人生物识别信息（如样本、图像等），仅存储个人生物识别信息的摘要信息。（P02-BR04）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈方式、系统核验方式，查验被评估机构业务系统个人生物识别信息是否与个人身份信息分开存储。 2.若业务系统存储了个人生物识别信息，则通过人员访谈、系统核验方式，查验是否仅存储个人生物识别信息的摘要信息。
	基本安全要求	个人信息存储期限应为实现个人信息主体授权使用目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外，超出个人信息存储期限后，应对个人信息进行删除或匿名化处理。（P02-BR05）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，查验被评估机构业务系统是否明确存储的个人信息存储期限应为实现个人信息主体授权使用目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外。 **技术能力：** 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统中存储的个人信息超出个人信息存储期限后，是否进行删除或匿名化处理。
	三级增强要求	应提供异地实时备份功能，利用通信网络将数据实时备份至备份场地。（P02-TR01）	人员访谈 文档查阅	**技术能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否具备异地实时备份功能，可利用通信网络将数据实时备份至备份场地。
	三级增强要求	应具备勒索病毒事前预警、事中阻断及事后恢复的保障能力。（P02-TR02）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否具备勒索病毒事前预警、事中阻断及事后恢复的保障能力，演示相关功能效果。

表 11　数据存储评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据存储（P02）	三级增强要求	应提供数据处理环节关联信息系统的热冗余，保证数据的高可用性。（P02-TR03）	人员访谈 文档查阅	**技术能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否提供数据处理环节关联信息系统（如数据库、应用程序、服务器、网络设备等）的热冗余，例如虚拟化部署、双机热备、负载均衡等，查阅系统网络拓扑图。
	四级增强要求	应建立异地灾难备份中心，提供数据的实时切换。（P02-FR01）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统是否建立异地灾难备份中心，可提供业务系统数据的实时切换，系统核验异地灾难备份平台功能。
	2 级～4 级	宜采用 DBMS 工具字段权限管理模块，合理化配置数据字段访问和使用权限，确保数据字段在合理范围内被查询和使用。（P02-DT01）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过系统核验方式，查验被评估机构业务系统是否具备数据字段权限管理模块，能根据不同数据字段配置访问和使用权限，确保数据字段合理访问及使用。
	3 级～4 级	应采用密码算法或哈希算法对数据字段进行加密或哈希存储，其中口令应采用加盐哈希存储。（P02-DT02）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作，其中口令定为 3 级及以上安全级别。 **技术能力：** 2.通过系统核验方式，查验被评估机构业务系统在数据库管理系统中存储的数据字段是否采用加密或哈希算法存储。 3.通过系统核验方式，查验被评估机构业务系统在数据库管理系统中存储的口令字段是否采用加盐哈希存储。

表 11　数据存储评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据存储（P02）	4 级	应仅存储个人生物识别信息的摘要信息。（P02-DT03）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作，其中个人生物识别信息定为 4 级安全级别。 **技术能力：** 2.通过系统核验方式，查验被评估机构业务系统在数据库管理系统中是否仅存储个人生物识别信息的摘要信息，不存储原始生物识别信息。

8.3　数据传输

数据传输评估内容描述见表12。

表 12　数据传输评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据传输（P03）	基本安全要求	应明确数据传输相关安全管控措施，如传输通道加密、数据内容加密、数据接口传输安全等。（P03-BR01）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定数据传输安全管理制度；查验被评估机构业务系统是否明确数据传输安全管控措施。 2.通过人员访谈、文档查阅方式，查验业务系统数据传输安全管控措施内容是否包括传输通道加密、数据内容加密、数据接口传输安全等。
	基本安全要求	应对数据传输两端进行身份鉴别，确保数据传输双方可信任。（P03-BR02）	系统核验 技术检测	**技术能力：** 1.通过系统核验方式，查验被评估机构业务系统是否启用身份鉴别功能（如账号口令、短信验证码、生物信息鉴别等）。 2.通过技术检测方式，查验身份鉴别功能安全性，核实被评估机构业务系统是否采用数字证书确保数据传输双方可信任。
	基本安全要求	应采用校验技术保证数据在传输过程中的完整性。（P03-BR03）	文档查阅 技术检测	**技术能力：** 1.通过文档查阅方式，查阅并确认业务系统设计文档中具备数据传输完整性保障措施设计。 2.通过技术检测方式，查验并确认被评估机构业务系统已采用校验技术（使用消息摘要算法、CRC 校验码、消息认证码（MAC）、数字签名等）保证数据传输完整性。

表 12　数据传输评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据传输（P03）	三级增强要求	应对关键网络传输线路及核心设备实施冗余建设，确保数据传输的网络可用性。（P03-TR01）	人员访谈 文档查阅 技术测试	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统网络架构中，关键网络传输线路及核心设备冗余建设策略；查阅系统网络拓扑图，确保数据传输的网络可用性。 **技术能力：** 2.通过技术测试方式，查验关键网络传输线路及核心设备实施冗余建设策略，确认与实施方案一致。
	三级增强要求	重要数据不应通过离线或即时通信方式传输。（P03-TR02）	人员访谈 系统核验	**技术能力：** 1.通过人员访谈、系统核验方式，查验被评估机构业务系统涉及的重要数据是否不存在离线（如移动存储介质、光盘、磁盘等）或即时通信方式传输的场景。 2.通过人员访谈、系统核验方式，查验被评估机构业务系统数据管控平台是否能识别重要数据，演示平台具备阻断重要数据下载或阻断重要数据传输能力。
	四级增强要求	在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。（P03-FR01）	人员访谈 文档查阅 技术测试	**技术能力：** 1.通过人员访谈、文档查阅方式，查验业务系统设计文档中是否具备数据传输抗抵赖性及密码算法设计。 2.通过技术测试方式，查验并确认数据传输时业务系统已采用数字签名和时间戳等密码学技术实现原发行为的抗抵赖和数据接收行为的抗抵赖。
	2 级～4 级	对离线或即时通信方式传输的数据字段采取加密、脱敏等安全措施，确保传输安全性。（P03-DT01）	人员访谈 文档查阅 技术检测	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、技术检测方式，查验被评估机构业务系统在通过离线或即时通信方式传输 2 级～4 级数据时是否采取加密、脱敏等安全措施，确保传输安全性。

表 12　数据传输评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据传输（P03）	3 级～4 级	应采用通道加密方式对数据字段进行传输。（P03-DT02）	人员访谈 文档查阅 技术检测	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过技术检测方式，查验被评估机构业务系统是否采用通道加密方式对 3 级～4 级数据字段进行传输。
	4 级	宜在通道加密基础上，采用内容加密方式，对数据字段进行传输。（P03-DT03）	人员访谈 文档查阅 技术检测	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、技术检测方式，查验被评估机构业务系统是否在通道加密基础上，采用内容加密方式，对 4 级数据字段进行传输。

8.4　数据使用

数据使用评估内容描述见表13。

表 13　数据使用评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据使用（P04）	基本安全要求	应明确数据使用业务场景的目的、范围、审批流程（含权限授予、变更、撤销等）、人员岗位职责等，鼓励在保障安全的情况下，开展数据利用。（P04-BR01）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定数据使用安全管理制度；查验被评估机构业务系统是否明确数据使用安全管控措施。 2.通过人员访谈、文档查阅方式，查验数据使用安全管理措施内容是否包含数据使用业务场景的目的、范围、审批流程（含权限授予、变更、撤销等）、人员岗位职责等内容。
	基本安全要求	应明确数据统计分析、展示、发布、公开披露等不同数据使用场景的安全管理要求。（P04-BR02）	人员访谈 文档查阅	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统数据使用管理措施，查看是否明确不同数据使用业务场景（如数据挖掘、数据建模、数据统计分析、数据开发测试、数据展示、数据发布、数据公开披露等）的安全管理要求。

表 13　数据使用评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据使用（P04）	基本安全要求	应根据不同数据使用场景采用安全处理措施（如去标识化、匿名化等），降低数据敏感度及暴露风险。（P04-BR03）	文档查阅 技术检测 系统核验	**制度能力：** 1.通过文档查阅方式，查验被评估机构业务系统数据使用相关管理措施，查看相关措施是否包含数据使用脱敏要求。 **技术能力：** 2.通过技术检测、系统核验方式，查验被评估机构业务系统是否对不同数据使用场景采用技术手段（如去标识化、匿名化等）降低数据使用过程的敏感度及暴露风险。
	基本安全要求	存在利用算法推荐技术进行自动化决策分析的情形，应保证决策的透明度和结果公平合理。（P04-BR04）	人员访谈 文档查阅 技术检测	**技术能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统自动化决策功能设计文档，确认使用的算法推荐技术。 2.通过技术检测方式，核实决策的透明度和结果是否公平合理。
	基本安全要求	数据公开前应开展数据安全风险评估，明确公开数据的内容与种类、公开方式、公开范围、安全保障措施、可能的风险与影响范围等。涉及敏感个人信息、商业秘密信息的，以及可能对公共利益或者国家安全产生重大影响的，不应公开，法律法规另有规定的除外。（P04-BR05）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统在数据公开之前，是否开展数据安全风险评估，查阅数据安全风险评估报告内容是否包含公开数据的内容与种类、公开方式、公开范围、安全保障措施、可能的风险与影响范围等。 2.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否不公开敏感个人信息、商业秘密信息，以及不公开可能对公共利益或者国家安全产生重大影响的数据，法律法规另有规定的除外。
	基本安全要求	利用所掌握的数据资源，公开市场预测、统计等信息时，不应危害国家安全、公共安全、经济安全和社会稳定。（P04-BR06）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统在利用所掌握的数据资源进行公开市场预测、统计等信息前，是否开展安全影响评估，确保不会危害国家安全、公共安全、经济安全和社会稳定。

表 13　数据使用评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据使用（P04）	三级增强要求	应采取技术措施保证汇聚大量数据时不暴露敏感信息。（P04-TR01）	人员访谈 文档查阅 技术检测	**技术能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统设计文档和安全文档，确认已采取相应技术措施保证汇聚大量数据时不暴露敏感信息。 2.通过技术检测方式，查验被评估机构业务系统在汇聚大量数据时安全保障措施的有效性，例如采用数据加密、数据脱敏、接口与数据访问权限管控、个人信息隐私保护（差分隐私保护、K 匿名、假名化等）、数据防泄露监控与审计等技术措施。
	三级增强要求	宜对不同数据使用场景采取数字水印等技术，实现数据防泄密及溯源能力。（P04-TR02）	人员访谈 文档查阅 系统核验	**技术能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统设计文档，是否针对数据使用场景明确数字水印技术使用。 2.通过系统核验方式，演示不同数据使用场景采取数字水印等技术能力。
	三级增强要求	宜对接入或嵌入的第三方应用加强数据安全管理，宜对接入或嵌入的第三方应用开展技术检测，确保其数据处理行为符合双方约定要求，对审计发现超出双方约定的行为及时停止接入。（P04-TR03）	人员访谈 文档查阅 系统核验	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否在接入或嵌入第三方应用前开展技术检测，确认接入的应用已采取的风险控制措施能够有效防范接入风险。 2.通过文档查阅、系统核验方式，查验被评估机构业务系统是否能对第三方接入应用的数据处理活动进行必要的监视；查阅第三方接入应用的数据处理活动日志记录、审计或检查报告，确认安全管理主体是否落实安全管理要求和责任，并对审计发现超出双方约定的行为及时停止接入。
	2 级～4 级	在各类数据使用场景（如生产数据应用为测试数据、数据统计分析、数据对外展示、提供作为参赛数据等）中，采用动态或静态脱敏技术，对非必要使用的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。（P04-DT01）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、系统核验方式，查验被评估机构业务系统是否在各类数据使用场景（如生产数据应用为测试数据、数据统计分析、数据对外展示、提供作为参赛数据等）中，采用动态或静态脱敏技术，对非必要使用的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。

表 13　数据使用评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据使用（P04）	3 级～4 级	数据使用场景（如提供作为参赛数据）中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。（P04-DT02）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、系统核验方式，查验被评估机构业务系统在数据使用场景中，为实现数据可用不可见，是否采用隐私计算技术，例如多方计算、联邦学习等。

8.5　数据加工

数据加工评估内容描述见表14。

表 14　数据加工评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据加工（P05）	基本安全要求	应对参与数据加工活动的主体进行合法性、正当性的评估，确保参与数据加工活动的主体为合法合规的组织机构或个人。（P05-BR01）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统在开展数据加工活动前是否对数据加工各类活动场景的主体进行合法性、正当性的评估，确保参与数据加工活动的主体为合法合规的组织机构或个人，查阅评估报告。
	基本安全要求	应在数据加工前，书面明确数据加工目的、范围、期限、规则及数据加工主体的责任与义务。（P05-BR02）	人员访谈 文档查阅	**制度文档：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否在数据加工前，在数据加工相关协议里书面明确数据加工目的、范围、期限、规则及责任与义务。
	基本安全要求	开展数据加工活动过程中，出现可能危害国家安全、公共安全、经济安全和社会稳定的情形时，应立即停止加工活动。（P05-BR03）	人员访谈 文档查阅	**技术能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否对数据加工过程进行监督和检查或具备行为审计记录，确认符合要求；在出现可能危害国家安全、公共安全、经济安全和社会稳定的情形时，立即停止加工活动。

表 14　数据加工评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据加工（P05）	基本安全要求	委托他人加工处理数据的，应与其订立数据安全保护合同，明确双方安全保护责任。委托加工处理个人信息的，应约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督，不应超出已征得个人信息主体授权同意的范围。（P05-BR04）	人员访谈 文档查阅	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否在委托他人加工处理数据前，与数据加工处理受托方签订数据安全保护合同，查阅合同内容是否明确双方安全保护责任。 2.通过文档查阅方式，查验被评估机构业务系统如果是委托他人加工处理个人信息前，数据安全保护合同内容是否包括约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。 3.通过文档查阅方式，查验被评估机构业务系统对受托方涉及个人信息处理的加工活动的监督审查记录，抽样查验数据加工操作记录，确保未超过已征得个人信息主体授权同意的范围。
	三级增强要求	应对数据加工的过程进行评估与监控，对数据加工过程的数据操作行为进行记录、审计，对异常数据操作行为及时预警、处置。（P05-TR01）	人员访谈 文档查阅 系统核验	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否通过日志或流量方式对数据加工过程进行监督和检查或具备行为审计记录，确认符合数据加工安全要求。 **技术能力：** 2.通过系统核验方式，查验被评估机构业务系统数据加工相关监控平台或技术管控措施，是否能对数据加工过程异常数据操作行为进行预警、处置，演示相关功能效果。
	三级增强要求	应对数据加工结果进行评估，如产生新数据，应对新数据进行安全审核，确保新数据不存在数据泄露风险。（P05-TR02）	人员访谈 文档查阅 技术检测	**人员能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统数据加工安全文档，查看内容是否包含对数据加工产生的新数据进行评估，明确新数据的安全技术措施，如采用数据加密、数据脱敏、接口与数据访问权限管控、个人信息隐私保护（差分隐私保护、K 匿名、假名化等）、数据防泄露监控与审计等技术措施。 **技术能力：** 2.通过技术检测方式，查验采用的安全措施是否具备有效性，确保新数据没有数据泄露风险。

表 14　数据加工评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据加工（P05）	三级增强要求	应提供安全的数据加工环境，包括网络环境、终端环境等，避免加工过程导致数据泄露、数据破坏等安全风险。（P05-TR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统在开展数据加工过程中，是否对数据加工环境（如网络系统、业务系统、主机系统、终端系统等）定期开展安全评估，确保数据加工环境安全，查阅安全评估报告。 **技术能力：** 2.通过系统核验方式，查验被评估机构业务系统是否对数据加工环境（如网络系统、业务系统、主机系统、终端系统等）进行安全管控，如实施网络访问控制和监控措施，以防止未经授权的访问和攻击等。
	三级增强要求	加工重要数据的，应加强访问控制，建立登记、审批机制并留存记录。（P05-TR04）	人员访谈 文档查阅 技术检测	**制度能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统数据加工安全管理措施，查看重要数据加工安全管控要求，包括数据加工登记、审批机制等。 2.通过文档查阅方式，查验被评估机构系统重要数据加工审核落实情况，查阅是否具备登记、审批记录。 **技术检测：** 3.通过人员访谈、技术检测方式，查验被评估机构在加工重要数据过程中，采用的访问控制措施，验证访问控制措施的有效性。
	2 级～4 级	在数据加工场景中，采用动态或静态脱敏技术，对非必要加工的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。（P05-DT01）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、系统核验方式，查验被评估机构业务系统在数据加工场景中，是否采用动态或静态脱敏技术，对非必要加工的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。

表 14　数据加工评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据加工（P05）	3 级～4 级	数据加工场景中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。（P05-DT02）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、系统核验方式，查验被评估机构业务系统在数据加工场景中，为实现数据可用不可见，是否采用隐私计算技术，例如多方计算、联邦学习等。

8.6　数据开放共享

数据开放共享评估内容描述见表15。

表 15　数据开放共享评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据开放共享（P06）	基本安全要求	公共数据提供部门应与公共数据使用部门签署相关协议，明确数据使用目的、供应方式、保密约定、数据共享范围、数据安全保护要求等内容。（P06-BR01）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，询问被评估机构业务系统是否存在公共数据共享的业务场景，如是则访谈被评估机构业务系统作为公共数据提供部门，是否与公共数据使用部门签署相关协议。 **制度能力：** 2.通过文档查阅方式，确认协议内容是否明确数据使用目的、供应方式、保密约定、数据共享范围、数据安全保护要求等内容。
	基本安全要求	公共数据提供部门应采用国家相关标准规定的密码技术，保障数据共享过程的保密性和完整性。（P06-BR02）	人员访谈 技术检测	**技术能力：** 1.通过人员访谈、技术检测方式，询问被评估机构业务系统是否存在公共数据共享的场景，如是则访谈被评估机构业务系统作为公共数据提供部门是否采用密码及校验技术，保障数据共享过程的保密性和完整性。
	基本安全要求	政务信息资源交换平台的政务信息共享应履行 GB/T 39477—2020 第 6 章确定的共享数据安全要求。（P06-BR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，询问被评估机构业务系统是否属于政务信息资源交换平台，如是则逐一核验被评估机构是否履行 GB/T 39477—2020 第 6 章确定的共享数据安全要求。

表 15　数据开放共享评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据开放共享（P06）	三级增强要求	公共数据提供部门应建立内部审批机制，明确数据对外共享目的、范围、期限、频次等内容。（P06-TR01）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，询问被评估机构业务系统是否存在公共数据共享的场景，如是则访谈被评估机构业务系统作为公共数据提供部门，是否建立内部审批机制。 **制度能力：** 2.通过文档查阅方式，查阅内部审批机制是否明确数据对外共享目的、范围、期限、频次等内容。
	三级增强要求	公共数据提供部门宜对共享的数据采取数字水印等技术，确保共享数据可溯源。（P06-TR02）	人员访谈 文档查阅	**技术能力：** 1.通过人员访谈、系统核验方式，询问被评估机构业务系统是否存在公共数据共享的场景，如是则访谈被评估机构业务系统作为公共数据提供部门，是否对共享的数据采取数字水印等技术，确保共享数据可溯源，演示相关功能效果。
	三级增强要求	宜采用多方安全计算、同态加密等数据隐私计算技术实现数据共享的安全性。（P06-TR03）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈方式，询问被评估机构业务系统是否采用多方安全计算、联邦学习等数据隐私计算技术实现数据共享的安全性。 **技术能力：** 2.通过文档查阅、系统核验方式，查阅相关技术方案、评估报告或其他佐证材料，演示相关功能效果。
	2 级～4 级	在数据共享场景中，采用动态或静态脱敏技术，对非必要共享的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。（P06-DT01）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、系统核验方式，查验被评估机构业务系统在数据共享场景中，是否采用动态或静态脱敏技术，对非必要共享的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。

表 15　数据开放共享评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据开放共享（P06）	3 级～4 级	在数据共享场景中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。（P06-DT02）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、系统核验方式，查验被评估机构业务系统在数据共享场景中，为实现数据可用不可见，是否采用隐私计算技术，例如多方计算、联邦学习等。

8.7　数据交易

数据交易评估内容描述见表16。

表 16　数据交易评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据交易（P07）	基本安全要求	应按照相关法律法规的要求开展数据交易，加强交易过程的数据安全保护。（P07-BR01）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，询问被评估机构是否开展数据交易活动，被评估机构业务系统是否涉及数据交易，如是则访谈被评估机构业务系统，是否遵循相关法律法规的要求开展数据交易活动，并加强交易过程的数据安全保护。 **制度能力：** 2.通过文档查阅方式，查阅被评估机构及业务系统开展数据交易活动中留存的监管、审核、交易记录等文件是否合规和完备。

8.8　数据出境

数据出境评估内容描述见表17。

表 17　数据出境评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据出境（P08）	基本安全要求	应明确数据出境业务场景，严格遵守国家法律、行政法规、数据出境安全监管要求，符合国家法律、行政法规规定情形的，应提前开展数据出境安全评估及网络安全审查工作，不应有未授权数据出境行为。（P08-BR01）	人员访谈 文档查阅 技术检测	**组织能力：** 1.通过人员访谈、技术检测方式，询问被评估机构业务系统是否存在数据出境业务场景，如是则访谈被评估机构在数据出境前是否严格遵守国家法律、行政法规、数据出境安全监管要求，如申报数据出境安全评估、通过相关保护认证、订立标准合同等，不存在未授权数据出境行为。 2.通过人员访谈、文档查阅方式，询问被评估机构业务系统是否向境外提供国家规定的重要数据，或属于其他需要申报数据出境安全评估的情形，如是则访谈被评估机构是否向国家网信部门申报数据出境安全评估并通过评估，查阅数据出境安全评估申报材料。 3.通过人员访谈、文档查阅方式，询问被评估机构是否为掌握超过国家相关规定用户个人信息数量的机构赴国外上市的情形，如是则访谈被评估机构是否向网络安全审查办公室申报网络安全审查，查阅网络安全审查材料，是否不存在重要数据或者大量个人信息被非法利用、非法出境的风险。
	基本安全要求	境内用户在境内访问境内网络的，其流量不应路由至境外。（P08-BR02）	人员访谈 技术检测	**技术能力：** 1.通过人员访谈方式，询问被评估机构业务系统境内用户在境内访问境内网络时，是否不存在其流量路由至境外的情形。 2.通过技术检测方式，检测是否不存在其流量路由至境外的情形。
	基本安全要求	应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。（P08-BR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，询问被评估机构业务系统是否内部建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程，查阅相关流程文档。

8.9 数据销毁与删除

数据销毁与删除评估内容描述见表18。

表 18 数据销毁与删除评估内容

评估项	级别要求	评估子项	评估手段	评估内容
数据销毁与删除（P09）	基本安全要求	应建立数据销毁与删除规程，明确数据销毁与删除场景、方式及审批机制，设置相关监督角色，记录数据销毁与删除操作过程。（P09-BR01）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构是否制定数据销毁与删除制度，查验被评估机构业务系统是否明确数据销毁与删除规程。 2.通过文档查阅方式，查阅规程内容是否明确数据销毁与删除场景、方式及审批机制，设置相关监督角色，记录数据销毁与删除操作过程。
	基本安全要求	如因业务终止或组织解散，无数据承接方的，应及时有效销毁其控制的数据，法律法规另有规定的除外。（P09-BR02）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，询问被评估机构业务系统是否具备如因业务终止或组织解散且无数据承接方时，能有效销毁其控制数据的机制，法律法规另有规定的除外。
	基本安全要求	委托数据合作方完成数据处理后，应要求数据合作方及时销毁委托的相关数据，法律法规另有规定或者双方另有约定的除外。（P09-BR03）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，询问被评估机构业务系统是否存在委托数据合作方完成数据处理工作的场景，是否协商确定数据处理完成后的销毁时间。 **技术能力：** 2.通过文档查阅方式，查阅数据合作方是否在完成数据处理后提供委托处理数据销毁证明，销毁证明应当包括销毁的时间、销毁的方式和销毁的范围等信息，并应当由数据合作方的负责人签字确认，明确被评估机构业务系统与数据合作方结束委托行为后，及时销毁委托处理的数据，法律法规另有规定或者双方另有约定的除外。

表 18　数据销毁与删除评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据销毁与删除（P09）	基本安全要求	根据要求、约定删除数据或完成数据处理后无需保留源数据的，应及时删除相关数据。（P09-BR04）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈方式，询问被评估机构业务系统是否根据要求、约定及时删除相关数据；完成数据处理后无需保留源数据的，应及时删除相关数据。 **技术能力：** 2.通过文档查阅方式，查阅数据删除证明，是否根据要求、约定删除数据或完成数据处理后无需保留源数据的，及时删除相关数据。
	基本安全要求	应按照 GB/T 35273—2020 中 8.3 规定的要求执行个人信息删除操作。（P09-BR05）	人员访谈 文档查阅 技术检测	**组织能力：** 1.通过人员访谈方式，询问被评估机构业务系统是否按照 GB/T 35273—2020 中 8.3 规定的要求执行个人信息删除操作。 **技术能力：** 2.通过文档查阅、技术检测方式，查阅个人信息删除证明，核实个人信息删除有效性。
	三级增强要求	应在中国境内对介质存储的数据进行销毁或删除。（P09-TR01）	人员访谈 文档查阅	**组织能力：** 1.通过人员访谈、文档查阅方式，询问被评估机构业务系统是否在中国境内对介质存储的数据进行删除或销毁，查阅境内数据销毁或删除证明。
	三级增强要求	应对存储数据的介质或物理设备采取无法恢复的方式进行数据销毁与删除，如物理粉碎、消磁、多次擦写等。（P09-TR02）	人员访谈 文档查阅	**技术能力：** 1.通过人员访谈、文档查阅方式，查验被评估机构业务系统是否采取无法恢复的数据销毁或删除技术手段，如物理粉碎、消磁、多次擦写等，对存储介质或物理设备中的数据进行销毁或删除。

表 18　数据销毁与删除评估内容（续）

评估项	级别要求	评估子项	评估手段	评估内容
数据销毁与删除（P09）	2 级～3 级	采用多次重写、覆盖、删除等方式对销毁数据字段进行擦除，确保数据不能被恢复。（P09-DT01）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、系统核验方式，查验被评估机构业务系统在数据销毁或删除场景中，是否采用多次重写、覆盖、删除等方式对销毁数据字段进行擦除，确保数据不能被恢复。
	4 级	应采用物理破坏的方式，对存储的数据字段进行数据销毁处理，确保数据不能被恢复。（P09-DT02）	人员访谈 文档查阅 系统核验	**组织能力：** 1.通过人员访谈、文档查阅方式，查验业务系统是否依据 DB4403/T 271—2022 附录 B，对数据子类或字段开展数据分类分级工作。 **技术能力：** 2.通过人员访谈、系统核验方式，查验被评估机构业务系统在数据销毁或删除场景中，是否对 4 级数据采用物理破坏的方式，对存储的数据字段进行数据销毁处理，确保数据不能被恢复。

9　整体评估

9.1　整体评估要求

评估对象整体评估应从以下两方面进行评估：

a)　评估子项间评估：对不同评估子项的安全要求进行关联评估分析，确定这些关联对评估对象整体安全保护能力的影响；

b)　例外情况评估：对数据安全评估子项之外的例外情况进行评估分析，确定是否有其他因素影响评估对象整体安全保护能力。

9.2　评估子项间评估

9.2.1　在单个评估子项完成评估后，应进行评估子项间评估，含评估类内及类间的评估子项，分析是否存在其他评估子项对该评估子项具有安全功能上的增强、补充或削弱等关联作用。

注 1：安全功能上的增强和补充可以使两个评估子项发挥更强的综合效能，可以使单个评估子项的状态在该情况下达到更高的安全状态。

注 2：安全功能上的削弱会使一个评估子项的状态影响另一个评估子项的状态或者给其带来新的脆弱性。

9.2.2　经过评估子项间评估，确实存在安全功能上的增强、补充或削弱等关联作用的，则对受影响评估子项的评估结果予以调整，如不符合调整为部分符合或符合。

9.3 例外情况评估

9.3.1 在评估子项间完成评估后，应结合评估对象关联的例外情况进行整体评估，如从数据安全评估子项之外的物理环境、计算环境、通信网络、安全区域等因素出发，分析评估对象是否存在其他安全措施或技术与数据安全各评估子项具有安全功能上的增强、补充或削弱等关联作用。

9.3.2 经过例外情况评估，确实存在安全功能上的增强、补充或削弱等关联作用的，则对受影响评估子项的评估结果予以调整，如不符合调整为部分符合或符合。

10 评估结论

10.1 安全风险分析和评价

对整体评估后单个评估子项评估结果中存在的不符合或部分符合项进行安全风险分析，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，威胁类型宜按照附录C进行识别，风险分析过程如下：

a) 针对整体评估后的单个评估子项评估结果中部分符合或不符合所产生的安全问题，结合关联资产和威胁，分析可能对评估对象、被评估机构、个人信息主体、社会秩序和公共利益及国家安全造成的危害；
b) 结合安全问题所影响业务及数据的重要程度、相关数据处理活动的重要程度、安全问题严重程度以及安全事件影响范围等，综合分析可能造成的安全危害中的最大安全危害结果；
c) 根据最大安全危害严重程度进一步确定单个评估子项面临的风险等级，结果为“高”“中”或“低”。

10.2 评估结论判定

应结合整体评估及安全风险分析和评价情况，计算评估对象总分值，给出评估对象的数据安全评估结论，确认评估对象是否通过相应等级数据安全保护要求评估，评估结论判别依据见表19。

表19 评估结论判别表

评估结论	判别依据
优	被评估对象总分值大于等于90分，且不存在高风险项。
良	被评估对象总分值大于等于80分，且不存在高风险项。
中	被评估对象总分值大于等于70分，且不存在高风险项。
差	被评估对象总分值小于70分，或总分值虽然大于等于70分但存在高风险项。
注：高风险项判定示例见附录B。	

附 录 A
（规范性）
公共数据安全评估评分细则

A.1 公共数据安全评估评分表

公共数据安全评估按照以下方式进行评估，各评估子项结果判定细则和分值见表A.1：

a) 公共数据安全评估评分表由评估类、评估项、评估子项、结果判定及各级别安全要求下该评估子项分值组成；
b) 公共数据安全评估评分表中的结果判定依据第6章至第8章评估内容执行；
c) 根据重要性设置各评估子项的分值，一般为1～10的整数，针对不同安全等级对象，因该等级下的安全要求存在差异，故同一评估子项分值存在不同；
d) 数据处理活动安全评估中级别要求涉及1级～4级的评估子项，针对数据子类或数据字段进行评估，对照各级别数据子类或数据字段的安全保护情况进行结果判定，若未进行数据子类或数据字段的分类分级，则判定为不符合；
e) 公共数据安全评估以单个业务系统作为评估对象时，评估子项的结果判定根据被评估机构的安全情况进行评分；以数据场景作为评估对象时，可能涉及多个机构的系统，按照5.6的说明，通用管理安全评估类和通用技术安全评估类的评估子项依据主责机构的安全情况进行评分，数据处理活动安全评估类的评估子项应同时考虑主责机构和关联机构，部分评估子项应对主责机构和涉及的关联机构分别进行评分，当单个评估子项有多个评分时，取最低值作为该评估子项的最终得分；
f) 以数据场景作为评估对象时，如关联机构或系统数量较多时，按照重要程度进行抽样评估，抽样比例不低于50%。

表A.1 公共数据安全评估评分表

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
制度文档	通用管理安全（M）	总体数据安全策略（M01）	M01-BR01	符合：满足第1～3项，得满分。 部分符合：满足第1项，部分满足第2～3项，得1/2分值。 不符合：其他情况，得0分。	8	6	4
制度文档			M01-TR01	符合：满足第1～2项，得满分。 部分符合：满足第1或者2项，得1/2分值。 不符合：其他情况，得0分。	—	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
组织人员	通用管理安全（M）	数据安全管理机构与人员（M02）	M02-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	10	10	10
制度文档			M02-BR02	符合：满足第1项，得满分。 不符合：其他情况，得0分。	4	4	4
组织人员			M02-BR03	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	6	4	4
组织人员			M02-BR04	符合：满足第1～2项，得满分。 部分符合：满足第1项，得1/2分值。 不符合：其他情况，得0分。 不适用：处理个人信息未达到国家网信部门规定数量，得满分。	6	6	6
审批机制			M02-BR05	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	5	5	5
数据合作方			M02-BR06	符合：满足第1～2项，得满分。 部分符合：满足第1或者2项，得1/2分值。 不符合：其他情况，得0分。	8	8	8
审批机制			M02-TR01	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
审批机制	通用管理安全（M）	数据安全管理机构与人员（M02）	M02-TR02	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	—	1	1
制度文档			M02-BR07	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	4	3	3
制度文档			M02-BR08	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	5	5	5
组织人员			M02-BR09	符合：满足第1～4项，得满分。 部分符合：满足第1项，部分满足第2～4项，得1/2分值。 不符合：其他情况，得0分。	6	6	6
组织人员			M02-BR10	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	3	1	1
组织人员			M02-TR03	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	2	2
组织人员			M02-TR04	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	1	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
组织人员	通用管理安全（M）	数据安全管理机构与人员（M02）	M02-TR05	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	—	1	1
组织人员			M02-FR01	符合：满足第1项，得满分。 不符合：其他情况，得0分。	—	—	1
组织人员			M02-FR02	符合：满足第1项，得满分。 不符合：其他情况，得0分。	—	—	1
组织人员		数据安全管理制度体系（M03）	M03-BR01	符合：满足第1项，得满分。 不符合：其他情况，得0分。	5	3	3
制度文档			M03-BR02	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	8	8	8
制度文档			M03-BR03	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。 不适用：被评估机构不属于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，得满分。	6	6	6
制度文档			M03-BR04	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	3	3	3
制度文档			M03-BR05	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	7	7	7

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
制度文档	通用管理安全（M）	数据安全管理制度体系（M03）	M03-BR06	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	2	2	2
制度文档			M03-BR07	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	4	2	2
制度文档			M03-TR01	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	2	2
技术工具/平台	通用技术安全（T）	数据分类分级保护（T01）	T01-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	3	3	3
制度文档组织人员			T01-BR02	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	2	2	2
制度文档组织人员			T01-BR03	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	2	2	2
制度文档组织人员			T01-BR04	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	3	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
制度文档 组织人员	通用技术安全（T）	数据分类分级保护（T01）	T01-BR05	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	2	1	1
技术工具 /平台			T01-TR01	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	—	1	1
技术工具 /平台			T01-FR01	符合：满足第1项，得满分。 不符合：其他情况，得0分。	—	—	1
制度文档		数据安全评估（T02）	T02-BR01	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	4	2	2
组织人员			T02-BR02	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	2	2	2
组织人员			T02-BR03	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不存在国家或行业数据安全合规监管情形，得满分。	2	2	2
制度文档			T02-BR04	符合：满足第1～3项，得满分。 部分符合：满足第1项，部分满足第2～3项，得1/2分值。 不符合：其他情况，得0分。	2	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
制度文档	通用技术安全（T）	数据安全评估（T02）	T02-BR05	符合：满足第 1 项，得满分。 不符合：其他情况，得 0 分。	2	2	2
制度文档			T02-BR06	符合：满足第 1 项，得满分。 不符合：其他情况，得 0 分。 不适用：业务系统不属于关键信息基础设施信息系统，得满分。	2	2	2
组织人员制度文档			T02-TR01	符合：满足第 1～3 项，得满分。 部分符合：满足第 1 项，部分满足第 2～3 项，得 1/2 分值。 不符合：其他情况，得 0 分。	—	2	2
技术工具/平台		数据安全风险监测（T03）	T03-BR01	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。	3	3	3
技术工具/平台			T03-BR02	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。	3	2	2
技术工具/平台			T03-TR01	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。	—	1	1
组织人员			T03-TR02	符合：满足第 1～2 项，得满分。 部分符合：部分满足第 1～2 项，得 1/2 分值。 不符合：其他情况，得 0 分。	—	1	1
组织人员			T03-TR03	符合：满足第 1 项，得满分。 不符合：其他情况，得 0 分。	—	1	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
组织人员	通用技术安全（T）	数据安全风险监测（T03）	T03-TR04	符合：满足第 1 项，得满分。 不符合：其他情况，得 0 分。	—	1	1
制度文档		数据安全管控（T04）	T04-BR01	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。	4	3	3
技术工具/平台			T04-BR02	符合：满足第 1～2 项，得满分。 部分符合：部分满足第 1～2 项，得 1/2 分值。 不符合：其他情况，得 0 分。	3	2	2
审批机制			T04-BR03	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。	3	3	3
技术工具/平台			T04-BR04	符合：满足第 1～2 项，得满分。 部分符合：部分满足第 1～2 项，得 1/2 分值。 不符合：其他情况，得 0 分。	3	2	1
技术工具/平台			T04-BR05	符合：满足第 1～3 项，得满分。 部分符合：部分满足第 1～3 项，得 1/2 分值。 不符合：其他情况，得 0 分。 不适用：业务系统不存在与其他系统数据交互场景，得满分。	2	1	1
制度文档 技术工具/平台			T04-BR06	符合：满足第 1～3 项，得满分。 部分符合：满足第 1 项，部分满足第 2～3 项，得 1/2 分值。 不符合：其他情况，得 0 分。 不适用：业务系统不存在数据重大操作行为，得满分。	3	3	3

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
技术工具/平台	通用技术安全（T）	数据安全管控（T04）	T04-TR01	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。 不适用：业务系统不存在数据跨网络区域传输场景，得满分。	—	2	2
技术工具/平台			T04-FR01	符合：满足第 1～2 项，得满分。 部分符合：满足第 1 项，部分满足第 2 项，得 1/2 分值。 不符合：其他情况，得 0 分。	—	—	2
技术工具/平台			T04-BR07	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。	4	3	3
技术工具/平台			T04-TR02	符合：满足第 1～2 项，得满分。 部分符合：部分满足第 1～2 项，得 1/2 分值。 不符合：其他情况，得 0 分。	—	2	2
技术工具/平台			T04-FR02	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。	—	—	2
技术工具/平台			T04-BR08	符合：满足第 1～2 项，得满分。 部分符合：部分满足第 1～2 项，得 1/2 分值。 不符合：其他情况，得 0 分。 不适用：业务系统不存在 API 接口，得满分。	4	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
组织人员	通用技术安全（T）	数据安全管控（T04）	T04-BR09	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不存在API接口，得满分。	4	2	2
制度文档技术工具/平台			T04-BR10	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不存在API接口，得满分。	4	3	2
组织人员技术工具/平台			T04-BR11	符合：满足第1或2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不存在API接口，得满分。	3	2	1
技术工具/平台			T04-TR03	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不存在API接口，得满分。	—	2	1
技术工具/平台			T04-TR04	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不属于对外开放数据接口的平台或系统，得满分。	—	1	1
技术工具/平台			T04-TR05	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不存在API接口，得满分。	—	2	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
制度文档	通用技术安全（T）	数据安全应急处置（T05）	T05-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	5	5	5
组织人员			T05-BR02	符合：满足第1～2项或被评估机构未发生过数据安全事件，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	3	3	3
组织人员			T05-BR03	符合：满足第1～2项或被评估机构未发生过数据安全事件，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	2	1	1
组织人员			T05-BR04	符合：满足第1～2项或被评估机构未发生过个人信息安全事件，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	3	3	3
组织人员			T05-BR05	符合：满足第1～2项，或被评估机构未发生过数据安全事件，得满分。 部分符合：满足第1项，不满足第2项，得1/2分值。 不符合：其他情况，得0分。	2	1	1
组织人员			T05-BR06	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	3	3	3

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
技术工具/平台	通用技术安全（T）	数据安全应急处置（T05）	T05-TR01	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	1	1
组织人员			T05-TR02	符合：满足第1项，或关键信息基础设施系统未发生过重要数据泄露、较大规模个人信息泄露事件，得满分。 不符合：其他情况，得0分。 不适用：业务系统不属于关键信息基础设施系统，得满分。	—	2	2
技术工具/平台			T05-FR01	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	—	1
制度文档		数据安全审计（T06）	T06-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	4	3	2
技术工具/平台			T06-BR02	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	5	5	5
组织人员			T06-BR03	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	4	2	2
组织人员			T06-TR01	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
组织人员	数据处理活动安全要求（P）	数据收集（P01）	P01-BR01	符合：满足第1～4项，得满分。 部分符合：满足第1项，部分满足第2～4项，得1/2分值。 不符合：其他情况，得0分。	4	3	3
组织人员			P01-BR02	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统未收集外部机构数据，得满分。	3	2	2
组织人员			P01-BR03	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。	4	3	2
组织人员			P01-BR04	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	4	3	2
组织人员			P01-BR05	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不存在提供公共服务的移动互联网应用程序或第三方应用，得满分。	3	2	2
组织人员			P01-TR01	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统未收集外部机构数据，得满分。	—	1	1
数据子类或字段			P01-DT01	符合：满足第1或2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不属于新建系统，得满分。	1	1	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
数据子类或字段	数据处理活动安全要求（P）	数据收集（P01）	P01-DT02	符合：满足第1～3项，得满分。 部分符合：满足第1项，部分满足第2～3项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不存在以API接口或SDK方式收集数据字段或无对应级别数据，得满分。	1	1	1
制度文档		数据存储（P02）	P02-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	3	2	2
组织人员制度文档			P02-BR02	符合：满足第1～3项，得满分。 部分符合：满足第1项，部分满足第2～3项，得1/2分值。 不符合：其他情况，得0分。	3	3	2
技术工具/平台			P02-BR03	符合：满足第1项，得满分。 不符合：其他情况，得0分。	3	2	2
技术工具/平台			P02-BR04	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统未存储个人身份识别信息，得满分。	3	2	2
组织人员技术工具/平台			P02-BR05	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	3	2	1
技术工具/平台			P02-TR01	符合：满足第1项，得满分。 不符合：其他情况，得0分。	—	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
技术工具/平台	数据处理活动安全要求（P）	数据存储（P02）	P02-TR02	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	1	1
技术工具/平台			P02-TR03	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	—	2	2
技术工具/平台			P02-FR01	符合：满足第1项，得满分。 不符合：其他情况，得0分。	—	—	2
数据子类或字段			P02-DT01	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无对应级别数据，得满分。	1	1	1
数据子类或字段			P02-DT02	符合：满足第1～3项，得满分。 部分符合：满足第1项，部分满足第2～3项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统无对应级别数据，得满分。	2	2	2
数据子类或字段			P02-DT03	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统未存储个人生物识别信息，得满分。	1	1	1
制度文档		数据传输（P03）	P03-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	2	1	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
技术工具/平台	数据处理活动安全要求（P）	数据传输（P03）	P03-BR02	符合：满足第1～2项，得满分。 部分符合:满足第1项或第2项，得1/2分值。 不符合：其他情况，得0分。	3	2	2
技术工具/平台			P03-BR03	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。	3	2	2
制度文档 技术工具/平台			P03-TR01	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。	—	2	2
技术工具/平台			P03-TR02	符合：满足第1项或第2项，得满分。 不符合：其他情况，得0分。	—	2	2
技术工具/平台			P03-FR01	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。	—	—	2
数据子类或字段			P03-DT01	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统未通过离线或即时通信方式传输2～4级数据或无对应级别数据，得满分。	1	1	1
数据子类或字段			P03-DT02	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无对应级别数据，得满分。	1	1	1
数据子类或字段			P03-DT03	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无对应级别数据，得满分。	1	1	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
制度文档	数据处理活动安全要求（P）	数据使用（P04）	P04-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	2	1	1
制度文档			P04-BR02	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。	2	1	1
制度文档 技术工具/平台			P04-BR03	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。	2	2	2
技术工具/平台			P04-BR04	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无自动化决策分析场景，得满分。	2	1	1
组织人员			P04-BR05	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据公开场景，得满分。	2	1	1
组织人员			P04-BR06	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无公开市场预测、统计等数据使用场景，得满分。	2	1	1
技术工具/平台			P04-TR01	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无大量数据汇聚场景，得满分。	—	1	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
技术工具/平台	数据处理活动安全要求（P）	数据使用（P04）	P04-TR02	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据使用场景，得满分。	—	1	1
组织人员			P04-TR03	符合：满足第1～2项，得满分。 部分符合：满足第1项或第2项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不存在接入或嵌入第三方应用的场景，得满分。	—	2	2
数据子类或字段			P04-DT01	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据使用场景或无对应级别数据，得满分。	1	1	1
数据子类或字段			P04-DT02	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据使用场景或无对应级别数据，得满分。	1	1	1
组织人员		数据加工（P05）	P05-BR01	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据加工业务场景，得满分。	1	1	1
制度文档			P05-BR02	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据加工业务场景，得满分。	1	1	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
制度文档	数据处理活动安全要求（P）	数据加工（P05）	P05-BR03	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据加工业务场景，得满分。	1	1	1
组织人员			P05-BR04	符合：满足第1～3项，得满分。 部分符合：满足第1项，部分满足第2～3项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统无数据加工业务场景，得满分。	1	1	1
技术工具/平台			P05-TR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统无数据加工业务场景，得满分。	—	1	1
组织人员技术工具/平台			P05-TR02	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据加工业务场景，得满分。	—	1	1
组织人员			P05-TR03	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统无数据加工场景，得满分。	—	1	1
制度文档技术工具/平台			P05-TR04	符合：满足第1～3项，得满分。 部分符合：满足第1项，部分满足第2～3项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统无重要数据加工场景，得满分。	—	1	1

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
数据子类或字段	数据处理活动安全要求（P）	数据加工（P05）	P05-DT01	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据加工场景或无对应级别数据，得满分。	1	1	1
数据子类或字段			P05-DT02	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据加工场景或无对应级别数据，得满分。	1	1	1
制度文档		数据开放共享（P06）	P06-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不存在公共数据共享业务场景，得满分。	2	1	1
制度文档技术工具/平台			P06-BR02	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不存在公共数据共享业务场景，得满分。	2	1	1
制度文档			P06-BR03	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不属于政务信息资源交换平台，得满分。	2	1	1
制度文档			P06-TR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不存在公共数据共享业务场景，得满分。	—	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
制度文档	数据处理活动安全要求（P）	数据开放共享（P06）	P06-TR02	符合：满足第 1 项，得满分。 部分符合：部分满足第 1 项，得 1/2 分值。 不符合：其他情况，得 0 分。 不适用：业务系统不存在公共数据共享业务场景，得满分。	—	1	1
技术工具/平台			P06-TR03	符合：满足第 1～2 项，得满分。 不符合：其他情况，得 0 分。 不适用：业务系统不存在公共数据共享业务场景，得满分。	—	1	1
数据子类或字段			P06-DT01	符合：满足第 1～2 项，得满分。 不符合：其他情况，得 0 分。 不适用：业务系统无数据共享场景或无对应级别数据，得满分。	1	1	1
数据子类或字段			P06-DT02	符合：满足第 1～2 项，得满分。 不符合：其他情况，得 0 分。 不适用：业务系统无数据共享场景或无对应级别数据，得满分。	1	1	1
制度文档		数据交易（P07）	P07-BR01	符合：满足第 1～2 项，得满分。 部分符合：满足第 1 项，部分满足第 2 项，得 1/2 分值。 不符合：其他情况，得 0 分。 不适用：业务系统不涉及数据交易，得满分。	2	2	2
制度文档		数据出境（P08）	P08-BR01	符合：满足第 1～3 项，得满分。 不符合：不满足任意一项，得 0 分。 不适用：业务系统不存在数据出境的场景，得满分。	3	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
技术工具/平台	数据处理活动安全要求（P）	数据出境（P08）	P08-BR02	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不存在数据出境的场景，得满分。	2	1	1
制度文档			P08-BR03	符合：满足第1项，得满分。 部分符合：部分满足第1项，得1/2分值。 不符合：其他情况，得0分。 不适用：业务系统不存在数据出境的场景，得满分。	2	1	1
制度文档		数据销毁与删除（P09）	P09-BR01	符合：满足第1～2项，得满分。 部分符合：满足第1项，部分满足第2项，得1/2分值。 不符合：其他情况，得0分。	2	2	2
组织人员			P09-BR02	符合：满足第1项，得满分。 不符合：其他情况，得0分。	2	2	2
制度文档			P09-BR03	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不存在委托数据合作方进行数据处理的场景，得满分。	2	2	2
制度文档			P09-BR04	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。	2	1	1
制度文档 技术工具/平台			P09-BR05	符合：满足第1～2项，得满分。 部分符合：部分满足第1～2项，得1/2分值。 不符合：其他情况，得0分。	3	2	2
技术工具/平台			P09-TR01	符合：满足第1项，得满分。 不符合：其他情况，得0分。	—	2	2

表A.1　公共数据安全评估评分表（续）

关联资产	评估类	评估项	评估子项	结果判定	一、二级分值	三级分值	四级分值
技术工具/平台	数据处理活动安全要求（P）	数据销毁与删除（P09）	P09-TR02	符合：满足第1项，得满分。 不符合：其他情况，得0分。 不适用：业务系统不涉及存储介质或物理设备销毁情况，得满分。	—	1	1
数据子类或字段			P09-DT01	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据销毁或删除场景或无对应级别数据，得满分。	1	1	1
数据子类或字段			P09-DT02	符合：满足第1～2项，得满分。 不符合：其他情况，得0分。 不适用：业务系统无数据销毁或删除场景或无对应级别数据，得满分。	1	1	1

A.2　公共数据安全评估评分方法

公共数据安全评估总分值计算方式如下：

a) 公共数据安全评估对评估对象进行评分，评分团队根据公共数据安全评估表计算评估项的分值，各评估项分值由对应安全要求分值之和，评估项分值计算公式分为以下三种：

1) 通用管理安全评估项分值按照公式（A.1）进行计算；

$$M_n = \sum_1^n X_n + \sum_1^n Y_n * 0.8 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots（A.1）$$

式中：

M_n ——通用管理安全评估项分值；

X_n ——适用项评估子项得分；

Y_n ——不适用项评估子项得分；

n ——第n个评估子项。

2) 通用技术安全评估项分值按照公式（A.2）进行计算；

$$T_n = \sum_1^n X_n + \sum_1^n Y_n * 0.8 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots（A.2）$$

式中：

T_n ——通用技术安全评估项分值；

X_n ——适用项评估子项得分；

Y_n ——不适用项评估子项得分；

n ——第n个评估子项。

3） 数据处理活动安全评估项分值按照公式（A.3）进行计算。

$$P_n = \sum_1^n X_n + \sum_1^n Y_n * 0.8 \cdots\cdots (A.3)$$

式中：

P_n——数据处理活动安全评估项分值；

X_n——适用项评估子项得分；

Y_n——不适用项评估子项得分；

n ——第n个评估子项。

b） 根据计算的各评估项分值，计算各评估类的分值，评估类分值计算公式分为以下三种：

1） 通用管理安全评估类分值按照公式（A.4）进行计算；

$$M = \sum_1^3 M_n \cdots\cdots (A.4)$$

式中：

M ——通用管理安全评估类分值；

M_n——通用管理安全评估项分值；

n ——第n个评估子项。

2） 通用技术安全评估类分值按照公式（A.5）进行计算；

$$T = \sum_1^6 T_n \cdots\cdots (A.5)$$

式中：

T ——通用技术安全评估类分值；

T_n——通用技术安全评估项分值；

n ——第n个评估子项。

3） 数据处理活动安全评估类分值按照公式（A.6）进行计算；

$$P = \sum_1^9 P_n \cdots\cdots (A.6)$$

式中：

P ——数据处理活动安全评估类分值；

P_n——数据处理活动安全评估项分值；

n ——第n个评估子项。

c） 根据计算的各评估类分值，计算评估对象的总分值，其中M评估类分值权重占比20%，T评估类分值权重占比30%，P评估类分值权重占比50%，总分值按照公式（A.7）进行计算。

$$SUM = M * 0.2 + T * 0.3 + P * 0.5 \cdots\cdots (A.7)$$

式中：

M ——通用管理安全评估类分值；

T ——通用技术安全评估类分值；

P ——数据处理活动安全评估类分值；

SUM——评估对象总分值。

附 录 B
（资料性）
高风险项判例

表B.1给出了高风险判例与DB4403/T 271—2022安全要求的对应关系，高风险项宜依据国家、行业公共数据安全政策变化及10.1的安全风险分析评价结果进行动态调整。

表B.1 高风险项判例与DB4403/T 271—2022安全要求对应关系

序号	评估类	评估项	评估子项	DB4403/T 271—2022的对应条款编号	判例场景	适用范围
1	通用管理安全（M）	数据安全管理机构与人员（M02）	M02-BR01	7.2.1.1	被评估机构未按照《数据安全法》《深圳经济特区数据条例》等要求设立数据安全管理机构，未明确机构数据安全负责人及相应的职责内容。	二级及以上
2			M02-BR04	7.2.1.1	处理个人信息达到国家网信部门规定数量的机构，未按照《个人信息保护法》等要求指定个人信息保护负责人并公开个人信息保护负责人联系方式，未将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责部门。	二级及以上
3			M02-BR06	7.2.1.1	被评估机构未与数据合作方签订合作协议及数据安全保密协议，未明确双方数据安全保密责任与义务，可能导致数据合作方对数据安全保护不当，存在引发数据安全事件的风险。	二级及以上
4		数据安全管理制度体系（M03）	M03-BR02	7.3.1	被评估机构未建立任何与数据安全保护相关的管理制度或相关管理制度无法适用于当前对象。	二级及以上

表B.1　高风险项判例与DB4403/T 271—2022安全要求对应关系（续）

序号	评估类	评估项	评估子项	DB4403/T 271—2022的对应条款编号	判例场景	适用范围
5	通用技术安全（T）	数据分类分级保护（T01）	T01-BR02	8.1.1	未按照《数据安全法》《深圳经济特区数据条例》等要求明确业务系统数据分类标准，未依据数据资源属性特征，将业务系统数据合理划分类别，对数据实行分类分级保护。	二级及以上
6			T01-BR03	8.1.1	未按照《数据安全法》《深圳经济特区数据条例》等要求明确业务系统数据对象安全等级，对业务系统数据实行分类分级保护。	二级及以上
7		数据安全评估（T02）	T02-TR01	8.2.2	对涉及处理敏感个人信息及国家规定的重要数据的机构，未按照《数据安全法》《深圳经济特区数据条例》等有关规定定期开展风险评估，并向有关主管部门报送风险评估报告。	三级及以上
8		数据安全风险监测（T03）	T03-BR01	8.3.1	未按照《数据安全法》《深圳经济特区数据条例》等有关规定加强风险监测，不具备常态化数据安全风险监测能力，造成无法识别数据泄露、数据篡改、数据滥用、违规传输、非法访问、流量异常等数据安全风险。	二级及以上
9		数据安全管控（T04）	T04-BR09	8.4.2.3	经过技术检测，发现系统存在接口未鉴权，敏感数据未脱敏、伪脱敏传输等情况，尤其是面向互联网开放的数据接口，导致存在数据泄露高危风险或已经发生数据泄露事件。	二级及以上
10		数据安全应急处置（T05）	T05-BR01	8.5.1	被评估机构未按照《数据安全法》《深圳经济特区数据条例》等有关规定建立数据安全应急处置机制，未依据区级、市级、行业网络安全事件应急相关文件开展应急处置工作。	二级及以上

表B.1　高风险项判例与DB4403/T 271—2022安全要求对应关系（续）

序号	评估类	评估项	评估子项	DB4403/T 271—2022的对应条款编号	判例场景	适用范围
11	通用技术安全（T）	数据安全审计（T06）	T06-BR02	8.6.1	未对业务系统数据处理活动环节实施日志留存管理，或日志记录不全面，日志保存时间少于180天，可能导致在发生安全事件时不能提供溯源取证能力。	二级及以上
12	数据处理活动安全（P）	数据收集（P01）	P01-BR01	9.1.1	未按照《个人信息保护法》《深圳经济特区数据条例》有关规定对业务系统数据收集来源进行鉴别和记录以确保数据收集来源的合法性、正当性，未明确数据类型及收集渠道、目的、用途、范围、频度、方式等。	二级及以上
13		数据存储（P02）	P02-BR02	9.2.1	业务系统未进行数据备份、未定期进行数据恢复性测试，不能确保备份数据的有效性、完整性及其可用性。	二级及以上
14		数据存储（P02）	P02-DT02	附录B	系统未采用密码算法或哈希算法对3～4级数据子类或字段进行加密或哈希存储。	二级及以上
15		数据传输（P03）	P03-DT02	附录B	系统即未采用通道加密，也未采取内容加密的方式对3～4级数据子类或字段进行传输，不能保障数据传输的完整性和保密性。	二级及以上
16		数据出境（P08）	P08-BR01	9.8.1	未按照《数据安全法》《深圳经济特区数据条例》有关规定明确数据出境业务场景，或未严格遵守数据出境安全监管要求提前开展数据出境安全评估及网络安全审查工作，存在未授权数据出境行为。	二级及以上

附 录 C
（资料性）
常见威胁列表

表C.1给出了常见数据安全威胁，如恶意代码注入、数据无效写入、数据污染等，安全风险分析和评价可参考进行。

表C.1 常见数据安全威胁

威胁分类	威胁子类	描述
数据采集	恶意代码注入	数据入库时，恶意代码随数据注入数据库或业务系统，危害数据机密性、完整性、可用性。
	数据无效写入	数据入库时，数据不符合规范或无效，或者数据不合法、正当。
	数据污染	数据入库时，攻击者接入采集系统污染待写入的原始数据，破坏数据完整性。
数据传输	数据窃取（传输）	攻击者伪装成外部通信代理、通信对端、通信链路网关通过伪造虚假请求或重定向窃取数据。
	网络监听	有权限的员工、第三方运维与服务人员接入，或攻击者越权接入内部通信链路与网关、通信代理监听数据；攻击者接入外部通信链路与网关、通信代理、通信对端监听数据等。
	数据泄露（传输）	传输过程中的数据未采用加密、安全配置或安全防护技术手段等，可能导致敏感数据泄露。
	数据篡改（传输）	攻击者伪装成通信代理或通信对端篡改数据。
数据存储	数据破坏	由于业务系统自身故障、物理环境变化、自然灾害、政策形势变化等因素导致的数据破坏，影响数据安全性、完整性和可用性。
	数据篡改（存储）	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等，破坏数据完整性和可用性。
	数据丢失	由于业务系统自身故障、物理环境破坏、网络攻击、恶意代码执行等原因，可能导致业务系统数据丢失，影响业务系统数据可用性。
	数据分类分级或标记错误	数据分类分级判断错误或打标记错误，导致数据受保护级别降低。
	数据窃取（存储）	在业务数据存储管理系统、文件存储系统、办公终端等存储系统安装恶意工具窃取数据；业务系统数据存储系统存在安全漏洞、权限设置不合理等因素，可能导致数据被窃取。
	数据泄露（存储）	数据存储管理系统由于未采取安全防护措施，如未进行加密或哈希存储敏感数据、权限未合理设置等，可能导致数据一旦泄露，攻击者获取明文敏感数据，造成明文数据泄露安全事件。
	恶意代码执行	故意在数据库服务器、文件服务器、员工终端等存储系统上执行后门、病毒、木马、蠕虫、窃听软件、间谍软件等恶意程序或代码，窃取、篡改或破坏数据。

表C.1　常见数据安全威胁（续）

威胁分类	威胁子类	描述
数据存储	非授权访问	由于业务逻辑存在漏洞、安全配置参数不合理或账号权限管理不严谨等因素，可能导致敏感数据非授权访问。
	数据不可控（存储）	依托第三方云平台、数据中心等存储数据，没有有效的约束与控制手段在使用云计算或者其他技术时，数据存放位置不可控，导致数据存在境外数据中心，数据和业务的司法管辖关系发生改变。
数据共享	共享数据未脱敏	与第三方机构共享数据时，第三方机构及其人员可以直接获取敏感元数据的调取、查看权限。
	共享权限混乱	与第三方机构共享数据时，接口权限混乱，导致第三方能访问其他未开放的数据。
	数据过度获取	由于业务对数据需求不明确，或未实现基于业务人员与所需数据关系的访问控制，业务人员获取超过业务所需的数据，容易造成数据泄露。
	数据泄露（共享）	共享数据未采取安全防护技术，如加密共享、权限设置不合理等，可能导致数据有意或无意的泄露事件。
	数据不可控（共享）	数据可被内部员工获取，组织对内部员工对所获数据的保存、处理、再转移等活动不可控；数据可被第三方服务商、合作商获取，组织对第三方机构及其员工对所获数据的使用、留存、再转移等活动未约束或不掌握；数据共享给恶意的第三方机构。
数据使用和加工	注入攻击	数据处理系统可能遭到恶意代码（如勒索病毒）注入、SQL 注入等攻击，可能造成数据泄露，危害数据机密性、完整性、可用性。
	数据抵赖	不承认收到的信息，或人员访问数据后，不承认在某时某刻用某账号访问或操作过数据。
	使用权限混乱	处理系统调用数据接口权限混乱，导致能访问其他未开放的数据。
	数据过度获取	由于相关业务对数据需求不明确，或未实现业务人员、系统运维人员与所需要数据的关系的访问控制，导致业务人员或系统运维人员获取超过业务所需数据，容易造成数据泄露。
	数据不可控（使用和加工）	依托第三方机构或外部处理系统处理数据，没有有效的约束与控制手段；未有效使用数据安全技术防护手段，可能导致数据保密性、完整性及可用性受到影响。
	越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出破坏业务系统的行为。
	敏感元数据未脱敏使用	处理系统可直接调取敏感元数据，容易导致信息泄露。
数据销毁	数据到期未销毁	数据失效或业务关闭后，遗留了敏感数据仍然可以被访问，破坏了数据的机密性。
	数据未正确销毁	被销毁数据通过技术手段可恢复，破坏数据的机密性；待销毁数据未按照规定正确销毁，导致数据可被恢复或未完全销毁，造成数据泄露事件。
其他	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题。
	物理环境影响	对系统正常运行造成影响的物理环境问题和自然灾害。
	无作为或操作失误	应执行而没有执行相应的操作，或无意执行了错误的操作。
	管理不到位	安全管理制度无法落实或不到位，从而破坏业务数据正常有序运行或数据的完整性、保密性及可用性；无法满足国家或行业监管要求，导致数据安全不合规等。

表C.1　常见数据安全威胁（续）

威胁分类	威胁子类	描述
其他	恶意代码	故意在计算机系统上执行恶意任务的程序代码。
	网络攻击	利用工具和技术通过网络对系统或数据接口进行攻击和入侵。
	物理攻击	通过物理的接触造成对软件、硬件、数据的破坏。
	性能过载	由于不断对主机、数据库及业务系统进行系统资源请求，可能导致系统拒绝服务，数据可用性受到影响。
	网页篡改	连接互联网的网站面临被篡改的可能性较大。
	单点故障	由于主要设备为单机运行，可能导致单机故障发生影响业务运行，从而破坏数据的可用性。
	供应链失效	业务或系统所依赖的数据合作方、接口等不可用；委托数据处理的数据合作方数据安全防护能力不足，导致委托处理的数据存在安全风险；数据合作方数据安全责任义务不明确，导致数据未授权处理等。

附 录 D
（资料性）
公共数据安全评估报告模板

D.1 公共数据安全评估报告封面

公共数据安全评估报告封面见图D.1。

（被评估对象名称）
公共数据安全评估报告

委托单位：_____

测评单位：_____

报告时间：_____

图D.1 公共数据安全评估报告封面

D.2　公共数据安全评估基本信息表

公共数据安全评估基本信息表见图D.2。

公共数据安全评估基本信息表

评估对象与范围					
评估对象					
涉及业务系统					
被评估机构					
单位名称					
单位地址				邮政编码	
联系人	姓名		职务/职称		
	所属部门		办公电话		
	移动电话		电子邮件		
评估机构					
单位名称					
单位地址				邮政编码	
联系人	姓名		职务/职称		
	所属部门		办公电话		
	移动电话		电子邮件		

图D.2　公共数据安全评估基本信息表

D.3　公共数据安全评估报告大纲

公共数据安全评估报告大纲见图D.3。

1 项目概述
1.1 评估背景
……
1.2 评估目标
……
1.3 评估依据
……
1.4 评估过程
……
1.5 报告分发范围
……
2 评估对象描述
……
3 评估指标
3.1 基本评估指标
……
3.2 不适用的评估指标
……
3.3 技术检测工具
……
4. 单项评估
4.1 通用管理安全
……
4.2 通用技术安全
……
4.3 数据处理活动安全
……
5 整体评估
……
6 安全问题风险分析
……
7 公共数据安全评估结论
……
8 安全问题整改建议
……

图D.3　公共数据安全评估报告大纲

附 录 E
（资料性）
公共数据安全评估案例

E.1 组建评估团队

由评估机构牵头，对某公共数据管理机构X系统进行公共数据安全评估。评估团队包括评估机构评估实施人员、被评估机构数据安全管理机构人员，评估过程中涉及的人员包含X系统的业务运营运维部门、业务开发测试部门及数据合作方等人员。

E.2 确定评估对象及评估范围

本次公共数据安全评估的评估对象为某公共数据管理机构的X系统，评估范围包括该公共数据管理机构数据安全相关组织架构、人员及制度，X系统数据处理活动涉及资产（如应用、系统、平台等）、X系统已有安全保护措施等。

E.3 评估对象调研

评估实施人员对被评估机构及评估对象的数据安全整体情况进行调研，包括被评估机构整体情况、评估对象系统情况、网络拓扑情况、数据安全管理相关制度流程、数据安全设备部署情况、数据安全岗位人员等。按照DB4403/T 271—2022描述的安全等级与安全要求关系，结合调研得到的X系统具体情况，选取基本安全要求、三级增强安全要求及针对所有级别数据子类/字段的评估子项进行评估。评估团队确定了评估时间和技术检测方案，最终形成书面评估方案，与被评估机构协商一致。

E.4 组织评估实施

评估实施过程包含以下工作内容。

a) 组织现场评估：数据安全评估团队组织了现场评估，采用文档查阅、人员访谈、技术检测、系统核验等评估手段，对评估对象的管理及技术安全保障能力进行评估。评估团队依据第6章至第8章的安全评估内容针对选取的评估指标对评估对象开展公共数据安全评估，评估过程中对于部分指标符合情况的判断使用相关数据安全技术测试工具作为风险辅助验证。评估团队对评估过程进行记录，保存对应的评估佐证材料，形成现场原始评估记录。

b) 评估子项结果及分值判定：根据现场原始评估记录表，结合A.1的公共数据安全评估评分表写明的结果判定方法，对评估子项作出符合/部分符合/不符合的判定，并给出每一评估子项的得分。鉴于系统的特殊性，以及数据处理活动场景的复杂性，基本评估指标的某些评估子项可能不适用该评估对象。且因X系统未进行数据子类/字段的分类分级，针对所有级别数据子类/字段的评估子项对于该系统本次评估均评为不符合。各评估子项得分如表E.1所示。

表E.1　评估子项得分

评估类	评估项	级别要求	评估子项	结果判定	权重	得分
通用管理安全（M）	总体数据安全策略（M01）	基本安全要求	M01-BR01	符合	6	6
		三级增强要求	M01-TR01	符合	2	2
	数据安全管理机构与人员（M02）	基本安全要求	M02-BR01	部分符合	10	5
		基本安全要求	M02-BR02	符合	4	4
		基本安全要求	M02-BR03	部分符合	4	2
		基本安全要求	M02-BR04	不符合	6	0
		基本安全要求	M02-BR05	部分符合	5	2.5
		基本安全要求	M02-BR06	部分符合	8	4
		三级增强要求	M02-TR01	符合	2	2
		三级增强要求	M02-TR02	符合	1	1
		基本安全要求	M02-BR07	符合	3	3
		基本安全要求	M02-BR08	符合	5	5
		基本安全要求	M02-BR09	部分符合	6	3
		基本安全要求	M02-BR10	部分符合	1	0.5
		三级增强要求	M02-TR03	部分符合	2	1
		三级增强要求	M02-TR04	不符合	1	0
		三级增强要求	M02-TR05	不符合	1	0
	数据安全管理制度体系（M03）	基本安全要求	M03-BR01	符合	3	3
		基本安全要求	M03-BR02	部分符合	8	4
		基本安全要求	M03-BR03	不适用	6	6
		基本安全要求	M03-BR04	部分符合	3	1.5
		基本安全要求	M03-BR05	符合	7	7
		基本安全要求	M03-BR06	符合	2	2
		基本安全要求	M03-BR07	符合	2	2
		三级增强要求	M03-TR01	符合	2	2
通用技术安全（T）	数据分类分级保护（T01）	基本安全要求	T01-BR01	不符合	3	0
		基本安全要求	T01-BR02	不符合	2	0
		基本安全要求	T01-BR03	不符合	2	0
		基本安全要求	T01-BR04	不符合	2	0
		基本安全要求	T01-BR05	不符合	1	0
		三级增强要求	T01-TR01	符合	1	1
	数据安全评估（T02）	基本安全要求	T02-BR01	不符合	2	0
		基本安全要求	T02-BR02	不符合	2	0
		基本安全要求	T02-BR03	不适用	2	2
		基本安全要求	T02-BR04	不符合	2	0
		基本安全要求	T02-BR05	不符合	2	0
		基本安全要求	T02-BR06	不适用	2	2
		三级增强要求	T02-TR01	部分符合	2	1

表E.1　评估子项得分（续）

评估类	评估项	级别要求	评估子项	结果判定	权重	得分
通用技术安全（T）	数据安全风险监测（T03）	基本安全要求	T03-BR01	不符合	3	0
		基本安全要求	T03-BR02	不符合	2	0
		三级增强要求	T03-TR01	不符合	1	0
		三级增强要求	T03-TR02	不符合	1	0
		三级增强要求	T03-TR03	不符合	1	0
		三级增强要求	T03-TR04	不符合	1	0
	数据安全管控（T04）	基本安全要求	T04-BR01	符合	3	3
		基本安全要求	T04-BR02	符合	2	2
		基本安全要求	T04-BR03	符合	3	3
		基本安全要求	T04-BR04	符合	2	2
		基本安全要求	T04-BR05	符合	1	1
		基本安全要求	T04-BR06	部分符合	3	1.5
		三级增强要求	T04-TR01	符合	2	2
		基本安全要求	T04-BR07	不符合	3	0
		三级增强要求	T04-TR02	不符合	2	0
		基本安全要求	T04-BR08	符合	2	2
		基本安全要求	T04-BR09	部分符合	2	1
		基本安全要求	T04-BR10	符合	3	3
		基本安全要求	T04-BR11	部分符合	2	1
		三级增强要求	T04-TR03	不符合	2	0
		三级增强要求	T04-TR04	不适用	1	1
		三级增强要求	T04-TR05	不符合	2	0
	数据安全应急处置（T05）	基本安全要求	T05-BR01	不符合	5	0
		基本安全要求	T05-BR02	符合	3	3
		基本安全要求	T05-BR03	符合	1	1
		基本安全要求	T05-BR04	符合	3	3
		基本安全要求	T05-BR05	符合	1	1
		基本安全要求	T05-BR06	不符合	3	0
		三级增强要求	T05-TR01	符合	1	1
		三级增强要求	T05-TR02	不适用	2	2
	数据安全审计（T06）	基本安全要求	T06-BR01	不符合	3	0
		基本安全要求	T06-BR02	符合	5	5
		基本安全要求	T06-BR03	部分符合	2	1
		三级增强要求	T06-TR01	符合	2	2
数据处理活动安全要求（P）	数据收集（P01）	基本安全要求	P01-BR01	部分符合	3	1.5
		基本安全要求	P01-BR02	不适用	2	2
		基本安全要求	P01-BR03	符合	3	3
		基本安全要求	P01-BR04	符合	3	3
		基本安全要求	P01-BR05	符合	2	2

表E.1　评估子项得分（续）

评估类	评估项	级别要求	评估子项	结果判定	权重	得分
数据处理活动安全要求（P）	数据收集（P01）	三级增强要求	P01-TR01	不适用	1	1
		1～4 级数据子类或字段	P01-DT01	不符合	1	0
		2～4 级数据子类或字段	P01-DT02	不符合	1	0
	数据存储（P02）	基本安全要求	P02-BR01	部分符合	2	1
		基本安全要求	P02-BR02	部分符合	3	1.5
		基本安全要求	P02-BR03	不符合	2	0
		基本安全要求	P02-BR04	符合	2	2
		基本安全要求	P02-BR05	符合	2	2
		三级增强要求	P02-TR01	不符合	2	0
		三级增强要求	P02-TR02	部分符合	1	0.5
		三级增强要求	P02-TR03	符合	2	2
		2～4 级数据子类或字段	P02-DT01	不符合	1	0
		3～4 级数据子类或字段	P02-DT02	不符合	2	0
		4 级数据子类或字段	P02-DT03	不符合	1	0
	数据传输（P03）	基本安全要求	P03-BR01	部分符合	1	0.5
		基本安全要求	P03-BR02	符合	2	2
		基本安全要求	P03-BR03	符合	2	2
		三级增强要求	P03-TR01	符合	2	2
		三级增强要求	P03-TR02	符合	2	2
		2～4 级数据子类或字段	P03-DT01	不符合	1	0
		3～4 级数据子类或字段	P03-DT02	不符合	1	0
		4 级数据子类或字段	P03-DT03	不符合	1	0
	数据使用（P04）	基本安全要求	P04-BR01	部分符合	1	0.5
		基本安全要求	P04-BR02	不符合	1	0
		基本安全要求	P04-BR03	符合	2	2
		基本安全要求	P04-BR04	不适用	1	1
		基本安全要求	P04-BR05	不适用	1	1
		基本安全要求	P04-BR06	不适用	1	1
		三级增强要求	P04-TR01	不适用	1	1
		三级增强要求	P04-TR02	不符合	1	0
		三级增强要求	P04-TR03	不适用	2	2
		2～4 级数据子类或字段	P04-DT01	不符合	1	0
		3～4 级数据子类或字段	P04-DT02	不符合	1	0
	数据加工（P05）	基本安全要求	P05-BR01	不适用	1	1
		基本安全要求	P05-BR02	不适用	1	1
		基本安全要求	P05-BR03	不适用	1	1
		基本安全要求	P05-BR04	不适用	1	1
		三级增强要求	P05-TR01	不适用	1	1
		三级增强要求	P05-TR02	不适用	1	1

表E.1　评估子项得分（续）

评估类	评估项	级别要求	评估子项	结果判定	权重	得分
数据处理活动安全要求（P）	数据加工（P05）	三级增强要求	P05-TR03	不适用	1	1
		三级增强要求	P05-TR04	不适用	1	1
		2～4 级数据子类或字段	P05-DT01	不符合	1	0
		3～4 级数据子类或字段	P05-DT02	不符合	1	0
	数据开放共享（P06）	基本安全要求	P06-BR01	不适用	1	1
		基本安全要求	P06-BR02	不适用	1	1
		基本安全要求	P06-BR03	不适用	1	1
		三级增强要求	P06-TR01	不适用	2	2
		三级增强要求	P06-TR02	不适用	1	1
		三级增强要求	P06-TR03	不适用	1	1
		2～4 级数据子类或字段	P06-DT01	不符合	1	0
		3～4 级数据子类或字段	P06-DT02	不符合	1	0
	数据交易（P07）	基本安全要求	P07-BR01	不适用	2	2
	数据出境（P08）	基本安全要求	P08-BR01	不适用	2	2
		基本安全要求	P08-BR02	不适用	1	1
		基本安全要求	P08-BR03	不适用	1	1
	数据销毁与删除（P09）	基本安全要求	P09-BR01	部分符合	2	1
		基本安全要求	P09-BR02	符合	2	2
		基本安全要求	P09-BR03	不符合	2	0
		基本安全要求	P09-BR04	不适用	1	1
		基本安全要求	P09-BR05	符合	2	2
		三级增强要求	P09-TR01	不适用	2	2
		三级增强要求	P09-TR02	不适用	1	1
		2～3 级数据子类或字段	P09-DT01	不符合	1	0
		4 级数据子类或字段	P09-DT02	不符合	1	0

c）　整体评估：在单个评估子项完成评估后，进行整体评估，根据整体评估结果，修改了评估子项符合情况及得分，整体评估情况如表E.2所示。

表E.2　整体评估情况汇总

评估子项编号	修正前符合情况	修正前得分	修正内容	修正后符合情况	修正后得分
P02-TR02	部分符合	0.5	X系统没有制定数据备份恢复操作规程文件，未定期进行数据恢复测试并出具报告验证审核，结合P02-BR03项X系统也未进行异地备份，可能造成在遇到勒索病毒时难以做到事后恢复，削弱其应对勒索病毒的能力，对P02-TR02评估项产生削弱作用。	不符合	0

d) 安全风险分析和评价：整体评估后，对单个评估子项评估结果中的不符合或部分符合项进行安全风险分析和评价，高风险项判定对照附录B进行。

e) 计算综合得分：根据A.2的评分方法，先计算各评估项分值，再依次计算各评估类的分值，最后得出综合得分，步骤如下：

1) 计算得M（通用管理安全评估类分值）为67.3；

2) 计算得T（通用技术安全评估类分值）为46.1；

3) 计算得P（数据处理活动安全评估类分值）为61.2；

4) 最后计算评估对象的综合得分，计算得出最终分值为57.89分。

f) 评估结论判定：根据安全问题风险分析结果统计高、中、低风险安全问题的数量，根据10.2列明的评估结论判别依据，X系统综合得分小于70分，且存在高风险项，最终评估结论为差，评估结果如表E.3所示。

表E.3 评估结果

评估对象名称	安全问题数量			综合得分	评估结论
	高风险	中风险	低风险		
X系统	6个	30个	31个	57.89	差

E.5 评估报告编制

评估团队在完成公共数据安全评估工作后，与被评估机构共同确认公共数据安全评估结果，并编制形成公共数据安全评估报告，如实反映评估情况，针对评估过程中发现的问题和风险，提出合理化建议。

参 考 文 献

[1] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[2] GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南
[3] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
[4] YD/T 3956—2021 电信网和互联网数据安全评估规范
[5] DB33/T 2488—2022 公共数据安全体系评估规范
[6] 深圳市第七届人民代表大会常务委员会.深圳经济特区数据条例.2021-07-06