ICS 35.240
L 60

团　　体　　标　　准

T/ISC XXXX—XXXX

数据安全管理能力评估规范

Certification Criteria for Data Security Management Capability

（征求意见稿）

2023－XX－XX 发布　　2023－XX－XX 实施

中　国　互　联　网　协　会　　发 布

目　　次

前　言

本标准按照GB/T 1.1-2020给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国互联网协会归口。

本标准主要起草单位：中国信息通信研究院、中互网来信息技术有限公司、中互智安(北京)科技有限公司。

本标准主要起草人：王景尧、吴荻、宛严、李玮、王亚宁、曹海啸。

数据安全管理能力评估规范

1 范围

本文件规定了组织数据安全管理能力评估规范和评估方法。

本文件适用于涉及数据安全的组织、组织及第三方专业机构开展数据安全管理能力评估工作，为提升组织数据安全管理能力、健全管理手段提供指引和依据。

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，标注日期的引用文件，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 25069—2010 信息安全技术 术语

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 37973—2019 信息安全技术 大数据安全管理指南

GB/T 35273—2020 信息安全技术 个人信息安全规范

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

GB/T 29246—2017 信息技术 安全技术信息安全管理体系

GB/T 39335—2020 信息技术 个人信息安全评估指南

GB/T 19000—2016 质量管理体系 基础和术语

3 术语和定义

GB/T 41479-2022、GB/T 37988-2019、GB/T 36073-2018、GB/T 25069—2010、GB/T 35273—2020、GB/T 39335—2020、GB/T19000—2016等国家标准界定的以及下列术语和定义适用于本文件。

3.1

数据 Data

任何以电子或者其他方式对信息的记录。

3.2

数据处理 Data Processing

数据的收集、存储、使用、加工、传输、提供、公开等。

3.3

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。

3.4

个人信息 Personal Information

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

注 1:个人信息包括姓名、出生日期、公民身份证号、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：不包括匿名化处理后的信息。

3.5

敏感个人信息 Personal Sensitive Information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

3.6

个人信息处理者 Processor Of Personal Information

在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

3.7

去标识化 De-Identification

个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

3.8

匿名化 Anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

注：匿名化处理后的信息不属于个人信息。

3.9

网络数据 Network Data

通过网络收集、存储、使用、加工、传输、提供、公开的各种数据。

示例：个人信息、重要数据等。

3.10

重要数据 Important Data

一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据。

注：重要数据包括未公开的政府信息，数量达到一定规模的基因、地理、矿产信息等，原则上不包括个人信息、组织内部经营管理信息等。

3.11

私人信息 Private Information

个人发送给特定对下不可转发给其他人的信息。

3.12

数据接收方 Data Receiver

数据处理中接收数据的组织或者个人。

3.13

数据脱敏 Data Masking

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

3.14

数据安全管理能力 Data Security Management Capability

组织和机构对数据进行管理和应用的能力。

4 目标策划及风险机遇

4.1 数据安全方针目标及其实现的策划

数据安全第一责任人应制定、实施和保持数据安全管理方针。方针应满足国家法律法规、政策的要求。方针应保持成文信息，并在组织内得到沟通、理解和应用。组织应针对相关职能、层次和数据安全管理能力所需的过程，建立数据安全目标。

数据安全目标应：

1. 与数据安全方针保持一致；
2. 可测量；
3. 考虑适用的法律法规及相关方的要求；
4. 予以监视及沟通；
5. 适时更新。

组织应保持有关数据安全目标的成文信息。策划如何实现数据安全目标时，组织应确定：

1. 要做什么；
2. 需要什么资源；
3. 由谁负责；
4. 何时完成；
5. 如何评价结果。

4.2 应对风险和机遇的措施

1. 组织在策划数据安全管理能力时，应考虑4.1提及的要求，并确定需要应对的数据安全风险和机遇。
2. 组织应策划：应对这些风险和机遇的措施；如何在数据安全管理能力过程中整合并实施这些措施；如何评价这些措施的有效性。

5 内外部环境及制度保障

5.1 内外部环境识别与资源支持

1. 组织应确定与其宗旨和战略方向相关并影响其实现数据安全管理能力的各种外部和内部因素。
2. 组织应确定、提供并维护所需的基础设施，以实现数据安全管理能力。
3. 组织应确定、提供并维护所需的环境，以实现数据安全管理能力。

5.2 相关方的需求与期望

组织应确定：

1. 与数据安全管理能力有关的相关方；

2. 与数据安全管理能力有关的相关方的要求。

组织应监视和评审这些相关方的信息及其相关要求。

5.3 数据安全管理制度保障体系

1. 组织应按照本技术规范的要求，建立、实施、保持和持续改进数据安全管理能力，包括所需的过程及其相互作用。
2. 在必要的范围和程度上，组织应保持成文信息以支持过程运行；保留成文信息以确信其过程按策划进行。
3. 组织应保持数据安全策略相关的成文信息。

5.4 数据安全管理能力涉及范围

组织应确定数据安全管理能力的边界和适用性，以确定其范围。在确定范围时，组织应考虑：

1. 各种外部和内部因素；
2. 相关方的要求；
3. 组织的产品和服务。

该范围应描述所覆盖的产品和服务类型。

6 组织架构及人员保障

6.1 组织建设以及领导作用承诺

1. 数据安全第一责任人应确保组织与数据安全管理相关的职责、权限得到分配、沟通和理解。

   数据安全第一责任人应分配职责和权限，以：

   1) 确保数据安全管理能力符合本技术规范的要求；
   2) 确保各过程获得其预期输出；
   3) 报告数据安全管理能力的绩效以及改进机会，特别是向最高管理者报告；
   4) 确保在整个组织中推动数据安全管理；
   5) 确保在策划和实施数据安全管理能力变更时保持其完整性。

   组织应明确数据安全岗位人员、职责划分，落实数据安全管理工作。

2. 数据安全第一责任人应通过以下方面，证实其对数据安全管理能力的领导作用和承诺：

   1) 对数据安全管理能力的有效性负责；
   2) 确保数据安全管理要求融入组织的业务过程；
   3) 促进使用过程方法和基于风险的思维；

4) 确保数据安全管理所需的资源是可获得的；

5) 确保数据安全管理能力实现其预期结果；

6) 促使人员积极参与数据安全管理；

7) 推动改进数据安全管理能力；

8) 支持其他相关管理者在其职责范围内发挥领导作用。

6.2 组织的岗位、权责和权限

1. 应明确数据安全岗位人员、职责划分，落实数据安全管理工作。

注：相关职责划分至少应包括数据安全第一责任人、监督层、分类分级及敏感数据保护、权限管理、内审应急、教育培训、投诉举报、合作方管理等。

2. 组织应依据国家相关要求，建立数据安全管理机构，明确数据安全负责人。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督促落实；

2) 组织开展数据安全风险评估；

3) 督促整改安全隐患；

4) 按要求向有关部门报告数据安全保护和事件处置情况；

5) 受理并处理用户投诉和举报。

7 数据安全管理运行

7.1 策划

为满足数据安全管理能力的要求，实施所确定的措施，实现数据安全目标，组织应至少建立健全以下数据安全管理体系，对所需的数据安全管理过程进行实施和控制：

1. 数据分类分级及分级管控；
2. 数据安全教育培训管理；
3. 数据安全举报投诉管理；
4. 数据安全内审及整改；
5. 数据安全应急响应；
6. 数据安全合作方管理。
7. 数据安全人员权限管理及数据操作规范。

7.2 数据分类分级与分级管控

1. 组织应建立数据分类分级管理过程，并保持成文信息。覆盖的范围应包括数据处理活动涉及的所有平台系统。
2. 数据分类分级应满足国家法律法规及相关标准的要求，综合考虑数据的类别属性、使用目的等，明确数据分类策略。
3. 在数据分类的基础上，对每一类数据类型制定数据分级标准。分级标准应考虑以下因素：
   1) 数据重要及敏感程度；
   2) 数据的安全保护需求；
   3) 数据泄露、丢失或破坏可能造成的危害程度。
4. 在数据分类分级的基础上规定不同级别数据的管控规则，包括但不限于：数据使用审批、数据权限管理、数据脱敏、数据加密等。

7.3 教育培训与考核

1. 组织应针对数据安全管理相关岗位的人员制定培训计划，定期组织数据安全培训工作。
2. 确定参与数据安全培训的人员角色范围；制定数据安全培训考核体系。
3. 数据安全培训内容包括但不限于：数据安全法律法规、数据安全管理方法、数据安全技能能力等。
4. 组织应保留培训、考核的成文信息。

注：培训课时不低于20课时/每人/每年。

7.4 举报投诉与处理

应建立数据安全用户举报与受理的成文信息，明确用户数据安全举报投诉渠道；明确举报投诉处理流程；明确举报投诉处理完成时限（不得超过15日）。

注：适宜的举报投诉渠道，如电子邮件、电话、传真、网站等。

7.5 权限管理与操作规范

1. 组织应明确关键系统的用户账号分配、开通、使用、变更、注销等安全保障要求，明确账号权限最小化可用原则，明确操作审批要求和操作流程，形成并定期更新系统权限分配表。
2. 组织应关注离职人员账号回收、账号权限变更、沉默账号安全等问题。
3. 明确敏感系统操作安全基线定义，涉及数据重大操作的（如数据批量复制、传输、处理、开放共享和销毁等），组织应采取多人审批授权或操作监督，并实施日志审计。需以操作审计技术能力对应。

7.6 合作方管理

1. 应加强第三方数据合作的管理，与合作方签订服务合同和安全保密协议。
2. 应明确对外合作中数据安全保护方式和合作方责任落实要求，合作结束后数据删除要求，合作方违约责任和处罚等。
3. 应建立合作方台账管理机制，形成并定期更新合作方清单。清单的内容应包含合作方名称、相关资质、合作业务或系统、合作形式、合作期限、合作方联系人等。
4. 根据合作方共享数据的不同级别来制定不同的资质以及数据保护能力要求；对于接收的数据，则需对数据来源进行判定。最终由内部评审后通过。

7.7 管理内审及整改

1. 组织应配备数据安全内审委员，对数据分类分级与管控、数据安全教育培训、举报投诉处理、权限管理与操作规范、合作方管理、技术能力实现效果等数据安全工作进行安全审计管理。
2. 内审依据主要依照数据安全系列管理制度，对其工作过程、结果、及相关留档文件进行审查。如发现缺失与问题，需令其负责人进行整改完善。
3. 最终需留存内审记录与整改记录证明。

7.8 数据安全应急响应

1. 应根据不同的数据安全事件，制定完善的数据安全应急预案，明确应急响应及应急处置方案，从数据安全进行应急处理与处置。
2. 应根据数据安全事件类型，明确事件原由、事件带来的危害、整改补救措施、应急审计、结案留档。

8 数据安全技术运行

8.1 策划

为满足数据安全管理能力的要求，实施所确定的措施，实现数据安全目标，组织应至少建立健全以下数据安全技术能力，对所需的数据安全技术实现过程进行实施和控制：

1. 数据资产识别；
2. 数据防泄漏与溯源；
3. 敏感数据保护；
4. 接口安全管理；
5. 风险操作审计发现。

8.2 数据资产识别

组织应：

1. 确定数据安全相关的资产；
2. 梳理数据资源，明确数据资源内容、数据量、存放位置、保存期限、数据关联系统、数据共享情况等；
3. 按照分类分级法，确定组织的数据资源安全等级；
4. 根据安全等级，制定适宜的数据资产与资源的控制措施；
5. 定期验证控制措施的有效性。

在数据资源识别时，应配备技术能力，定期对相关平台系统数据库数据资产、文件服务器以及终端数据资产、API数据资产进行扫描，发现识别敏感数据信息。

8.3 数据防泄漏与溯源

1. 涉及存储、处理、展示敏感数据的平台系统，应配备数据防泄露能力，优先从网络侧和终端侧等进行部署，逐步扩大能力覆盖范围。
2. 组织应具备对网络、邮件、FTP、USB、多种数据导入导出渠道进行实时监控的能力，可及时对异常数据操作行为进行预警拦截，以防范数据泄露风险。对于已经发生的数据泄露事件，应采取日志审计、水印溯源等方式追溯。

8.4 敏感数据保护

1. 对授权收集到的敏感数据信息，应采取去标识化、关键字段加密安全存储措施。根据相关方要求，删除、销毁的个人信息可进行匿名化处理。
2. 在跨安全域或通过互联网传输敏感数据信息时，采用加密传输措施。

   注:适宜的加密传输措施，例如可确保安全的加密算法或传输通道。
3. 在用户端显示敏感数据信息时，应采取措施防止未授权人员获取敏感数据信息。（动态脱敏：注意脱敏失效）
4. 对于权限较高人员，应采用可逆脱敏，支持查看脱敏数据的明文。

8.5 接口安全管理

1. 具备针对内外部访问流量分析能力，对使用接口的风险行为进行记录并告警；
2. 具备对接口自身的安全性，防外部攻击的发现能力。

8.6 风险操作审计

组织应规划建设具有自动化操作审计能力的平台系统，具备数据操作权限配置、异常操作告警与处置等核心功能，分批次将数据处理活动平台系统接入安全系统。应与组织内部数据分级管控措施规则为基础，进行安全策略配置。

9 绩效评价与改进

9.1 管理审核与纠正改进

1. 最高管理层应按计划的时间间隔评审组织的数据安全管理能力，以确保其持续的适宜性、充分性和有效性。管理评审应考虑：

   1) 以往管理评审提出的措施的状态；

   2) 与数据安全管理能力相关的外部和内部事项的变化；

   3) 有关数据安全绩效的反馈，包括以下方面的趋势：

      a) 不符合和纠正措施；

      b) 监视和测量结果；

      c) 审核结果

      d) 数据安全目标完成情况。

   4) 相关方反馈；

   5) 数据安全风险评估结果及应对措施的状态；

   6) 持续改进的机会。

2. 管理评审的输出，应包括与持续改进机会相关的决定，以及变更数据安全管理能力的任何需求。管理评审结果，应保留成文信息。

3. 当发生不符合时，组织应：

   1) 对不符合作出反应，适用时：

      a) 采取措施，以控制并予以纠正；

      b) 处理后果。

   2) 通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再发生，或在其他地方发生：

      a) 评审不符合；

      b) 确定不符合的原因；

      c) 确定类似的不符合是否存在，或可能发生。

   3) 实施任何需要的措施；

   4) 评审任何所采取的的纠正措施的有效性；

   5) 必要时，对数据安全管理能力进行变更；

4. 纠正措施应与不符合的影响相适合。

5. 不符合的纠正过程，应保留成文信息。

6. 组织应持续改进数据安全管理体系的适宜性、充分性、有效性。

附 录 A
（规范性附录/资料性附录）
XXX

该规范评估方式主要包括人员访谈、资料查阅、系统核验等，目的为明确组织内相关制度要求、工作流程、制度落实情况、数据安全相关技术能力建设等是否符合评估要求。相关评估要点和方法汇总附录A如下。

类别	指标	指标细项	评估方法
组织框架要求	组织环境	组织及其环境的识别	核查组织是否识别/确定了相关的内外部环境或问题，包括：外部环境如物理环境、网络环境、政策法规要求、客户以及供方的数据安全要求等；内部环境如技术资源、设备资源、网络资源、人力资源等。 组织应提供《风险及机遇评估分析表》或相关文件。
		相关方及其需求的识别	核查组织是否识别/确定了体系的相关方，可包含国家、上级主管部门、客户、供方以及和受审核方有关的各方； 组织应提供主要客户清单，客户需求分析、涉及数据的监管单位、涉及敏感数据的需求识别等文件。
		确定数据安全管理能力的范围	核查组织覆盖的产品和服务类型，和数据安全管理相关的数据/业务活动。
	领导作用	领导和承诺	核查组织是否在制度内如数据安全方针策略制度、管理手册等，体现领导和承诺要求内容。
		方针	最高管理者应制定、实施和保持数据安全管理方针。方针应满足国家法律法规、政策的要求。 核查方针是否保持成文信息，并在相关制度内如数据安全方针策略制度、管理手册等，体现方针成文内容。
	策划	应对风险和机遇的措施	核查组织是否对风险和机遇有应对措施；如何在数据安全管理能力过程中整合并实施这些措施；如何评价这些措施的有效性；应对措施应与数据安全风险的潜在影响相适应。 组织应提供应对风险和机遇的措施的分析文件。
		数据安全目标及其实现策划	核查组织是否针对相关职能、层次和数据安全管理能力所需的过程，建立数据安全目标，并形成有关数据安全目标的成文信息。
	支持	资源	核查组织是否对人员、基础设施、环境等明确相关资源投入，可体现在数据安全管理手册或相关文件内。

	绩效评价	监视、测量、分析和评价	核查组织是否定期进行数据安全绩效以及数据安全管理能力的有效性评价，并保留适当的文件化信息，作为监视和测量的证据。
		管审	核查组织是否按时间计划进行内部审核，确定数据安全管理能力是否正常稳定持续运行，应保留内部审核过程文件材料。
	改进	不符合纠正	核查组织对发生不符合时，是否对不符合项目采取措施加以消除和纠正，并保留有成文信息。
		持续改进	核查组织对数据安全管理能力相关维度的有效性、适用性等进行持续改进措施，并保留有成文信息。
数据安全管理能力要求	机构人员	数据安全组织机构	设立数据安全委员会；设立的目的及委员会责任范围，核查组织文件以及在管理系统内或在制度内可见其组织结构，并提供组织机构交流平台。
		数据安全组织架构层级	核查委员会层级构成及责任范围。如：领导层、监督层、管理层、执行层等。
		相关人员岗位任命及任命书	核查组织应对委员会成员下发任命书，任命书内容包含但不限于任命原则，权责描述等，并形成模板付在制度内。
		明确岗位权责	核查不同层级相关人员的任命原则及责任范围。管理层分别涉及哪些部门人员或角色担任，具体工作职责进行描述。
	制度保障	数据安全管理制度	列举提供组织内部数据安全管理制度：数据安全方针策略、数据安全组织建设及人员管理办法、数据资产安全及分类分级管理办法、数据权限审批管理办法、数据安全管理审计规范、合作方数据安全管理、数据安全人员培训管理制度、数据安全投诉举报管理规范、数据安全应急预案、数据安全合规性自评估管理办法。以及体系文件内要求的：数据安全管理手册、管理评审控制程序、内部审核控制程序、监视测量分析评价控制程序、数据安全风险评估控制程序；提供相关制度文件。

	分类分级	数据资产范围	提供组织数据资产范围，列明数据类型、数据级别以及掌控数据量。
		数据分类分级模板	根据组织业务情况，形成分类分级模板。
		数据分类分级操作规范	明确数据分类分级具体操作流程，例如三权分立、内部调研等步骤的确立。
	权限管理	数据使用审批维度	明确组织内部数据使用维度，并列举各个维度数据审批流程，需与分类分级定义结果相关联。
		权限管理	明确关键系统的用户账号分配、开通、使用、变更、注销等安全保障要求，及账号操作审批要求和操作流程，形成并定期更新系统权限分配表，重点关注离职人员账号回收、账号权限变更、沉默账号安全等问题。
	合作方管理	合作方主体	对合作方主体数据安全相关资质及内部管理制度流程的审核机制。
		合作项目	对合作项目针对涉及的数据采集、数据存储、数据传输、数据共享、数据使用、数据销毁的维度，进行相关能力验证机制。
		合同协议	对与涉及数据合作的合同协议内相关必要条款是否满足
		合作方管理台账	是否建立合作方台账，从合作方主体、合作项目、合同协议等要点进行记录。
	投诉处理	举报投诉通道	列举数据安全类型举报投诉通道，如邮箱、电话、在线表单等。

		举报投诉台账	是否建立举报投诉台账，从举报投诉来源、事件描述、处理过程、处理结果、处理周期等方面进行留档。
		举报投诉时间处理	对举报投诉是否在 15 日内处理完成
	教育培训	教育培训内容体系	建立培训体系，包含但不限于法律法规制度、数据安全管理工作流程、数据安全技术要点等维度。
		教育培训落地实操	核查教育培训记录，线上、线下均可。
		教育培训考核体系	核查教育培训考核记录、试卷、考试结果等。
	管理审计	审计维度及流程	核查合作方管理审计、数据使用审批审计、数据资产审计、举报投诉审计、教育培训审计、账号权限审计、日志审计方式概述、步骤。
	应急响应	应急响应维度	核查事前、事中、事后应急相应维度是否全面，事前应急相应是否与审计项目一一对应。
		应急响应处理流程规范	对每一项应急响应处置流程、步骤规范是否合理。
	数据安全自评估体系	自评估体系的能力机制验证	核查组织自评估相关制度、方法方式、或者已完成的自评估报告。报告内容应包含数据安全管理纬度、技术纬度、及管理体系下的“绩效评价”、“改进”等内容。

数据安全技术能力要求	数据识别	数据资产扫描	核查组织是否配备技术能力，定期对相关平台系统数据资产进行扫描，能够发现识别个人敏感信息。核验敏感信息识别的能力。
		验证脱敏效果	核查组织是否定期对数据脱敏效果进行验证，确保各类数据处理场景中数据脱敏的有效性和合规性。核验数据脱敏是否存在伪脱敏和弱脱敏等脱敏失效等情况。
	操作审计	审计能力平台和系统	核查规划建设具有自动化操作审计能力的平台系统，具备数据操作权限配置、异常操作告警与处置等核心功能，分批次将数据处理活动平台系统接入安全系统，数据操作审计内容和组织平台系统权限分配表作为系统策略进行配置。具备告警机制与处置功能。
	数据防泄露	数据防泄漏能力	核查组织涉及存储、处理个人敏感信息和重要数据平台系统配备数据防泄露能力，优先从网络侧和终端侧等进行部署，逐步扩大能力覆盖范围。具备对网络、邮件、FTP、USB 等多种数据导入导出渠道进行实时监控的能力，及时对异常数据操作行为进行预警拦截，防范数据泄露风险。验证数据防泄露的风险效果，重点验证异常操作行为组织的预警和拦截防护情况。
	接口安全管理	接口鉴权能力	面向互联网合作方及内部开放的数据接口具备接口认证鉴权与安全监控能力，能够限制违规设备接入，对接口调用进行必要的自动监控和处理。验证进行接口认证鉴权（身份认证）效果和违规接入（访问控制）及自动监控等安全防护效果。
		日志审计	对涉及敏感数据的传输接口实施调用审批，定期开展接口日志审计。验证接口清单是否存在报备机制，是否存在遗漏和瞒报等情况，以及接口调用记录。
	敏感数据保护	安全存储	对授权收集到的敏感信息，采取去标识化、关键字段加密安全存储措施；
		加密传输	在跨安全域或通过互联网传输敏感信息时，采用加密传输措施（如可确保安全的加密算法或传输通道）。
		个人敏感信息显示	在用户端显示个人敏感信息时，采取措施防止未授权人员获取个人敏感信息。