ISCCA

中互协认证技术规范

ISCCA-033：2023

数据安全管理能力
认证技术规范

Certification Criteria for Data Security Management

2023-03-31 发布 **2023-03-31 实施**

中互协（北京）检测认证中心有限公司

目 录

前言 IV
1. 范围 5
2. 规范性引用文件 5
3. 术语及定义 5
3.1 数据 5
3.2 数据处理 5
3.3 数据安全 5
3.4 个人信息 5
3.5 敏感个人信息 5
3.6 个人信息处理者 6
3.7 去标识化 6
3.8 匿名化 6
4 组织环境 6
4.1 理解组织及其环境 6
4.2 理解相关方的需求和期望 6
4.3 确定数据安全管理能力的范围 6
4.4 数据安全管理能力及其过程 6
5 领导作用 6
5.1 领导作用和承诺 6
5.2 方针 7
5.3 组织的岗位、职责和权限 7
6 策划 7
6.1 应对风险和机遇的措施 7
6.2 数据安全目标及其实现的策划 7
7 支持 8
7.1 资源 8
7.2 能力 8
8 运行 8
8.1 运行的策划 8
8.2 数据分类分级 8
8.3 数据访问权限管理 9
8.4 数据安全审计 9
8.5 数据合作方管理 10
8.6 数据安全事件应急管理 10
8.7 数据安全举报投诉管理 10
8.8 数据资产与数据资源管理 10
9 绩效评价 11
9.1 监视、测量、分析和评价 11
9.2 内部审核 11
9.3 管理审核 11

10 改进.....12
10.1 不符合及纠正措施.....12
10.2 持续改进.....12

前言

本技术规范参照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》要求的格式进行编写。

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。

本技术规范由中互协（北京）检测认证中心有限公司归口。

本规范起草单位：中互协（北京）检测认证中心有限公司、中国信息通信研究院。

本规范主要起草人：代小芳、王景尧、吴荻、王亚宁。

数据安全管理能力认证技术规范

1.范围

本文件规定了对组织的数据安全管理能力要求。

本文件仅适用于中互协（北京）检测认证中心有限公司开展数据安全管理能力认证。

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 37973—2019 信息安全技术 大数据安全管理指南

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

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.术语及定义

GB/T 25069—2010、GB/T 37988—2019、GB/T 35273—2020、GB/T 39335—2020、GB/T 19000—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

任何以电子或者其他方式对信息的记录。

3.2 数据处理

数据的收集、存储、使用、加工、传输、提供、公开等。

3.3 数据安全

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

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，不包括匿名化处理后的信息。

3.5 敏感个人信息

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

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

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

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。

4 组织环境

4.1 理解组织及其环境

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。

4.2 理解相关方的需求和期望

组织应确定：

a）与数据安全管理能力有关的相关方；

b）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。

4.3 确定数据安全管理能力的范围

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：

a）4.1中提及的各种外部和内部因素；

b）4.2中提及的相关方的要求；

c）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。

4.4 数据安全管理能力及其过程

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。

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。

组织应保持数据安全策略相关的成文信息。

5 领导作用

5.1 领导作用和承诺

最高管理者应通过以下方面，证实其对数据安全管理能力的领导作用和承诺：

a）对数据安全管理能力的有效性负责；

b）确保数据安全管理要求融入组织的业务过程；

c）促进使用过程方法和基于风险的思维；

d）确保数据安全管理所需的资源是可获得的；

e）确保数据安全管理能力实现其预期结果；

f）促使人员积极参与数据安全管理；

g）推动改进数据安全管理能力；

h）支持其他相关管理者在其职责范围内发挥领导作用。

5.2 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。

方针应保持成文信息，并在组织内得到沟通、理解和应用。

5.3 组织的岗位、职责和权限

最高管理者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。

最高管理者应分配职责和权限，以：

a）确保数据安全管理能力符合本技术规范的要求；

b）确保各过程获得其预期输出；

c）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；

d）确保在整个组织中推动数据安全管理；

e）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。

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资产梳理、分类分级、权限管理、管理审计、应急响应、教育培训、投诉举报、合作方管理等。

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：

a） 组织制定数据保护计划并督促落实；

b） 组织开展数据安全风险评估；

c） 督促整改安全隐患；

d） 按要求向有关部门报告数据安全保护和事件处置情况；

e） 受理并处理用户投诉和举报。

6 策划

6.1 应对风险和机遇的措施

组织在策划数据安全管理能力时，应考虑4.1所提及的因素和4.2所提及的要求，并确定需要应对的数据安全风险和机遇。

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。

应对措施应与数据安全风险的潜在影响相适应。

6.2 数据安全目标及其实现的策划

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：

a）与数据安全方针保持一致；

b）可测量；

c）考虑适用的法律法规及相关方的要求；

d）予以监视及沟通；

e）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：

a）要做什么；

b）需要什么资源；

c）由谁负责；

d）何时完成；

e）如何评价结果。

7 支持

7.1 资源

7.1.1 总则

组织应确定并提供所需的资源，以建立、实施、保持和持续改进数据安全管理能力。

组织应考虑：

a）现有内部资源的能力和局限；

b）需要从外部供方获得的资源。

7.1.2 人员

组织应确定并配备所需的人员，以实现数据安全管理能力。

7.1.3 基础设施

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。

7.1.4 运行环境

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。

7.2 能力

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。

数据安全相关人员，应每年至少参加一次数据安全管理培训。

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。

组织应保留培训、考核的成文信息。

注：培训课时宜不低于20课时/每人/每年。

8 运行

8.1 运行的策划

为满足数据安全管理能力的要求，实施第6章所确定的措施，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制度体系，对所需的数据安全管理过程进行实施和控制：

a）数据分类分级管理；

b）数据访问权限管理；

c）数据安全管理审计；

d）数据合作方管理；

e）数据安全应急响应；

f）数据安全举报投诉制度。

g）数据资产管理

8.2 数据分类分级

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。

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。

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：

a）数据重要及敏感程度；

b）数据的安全保护需求；

c）数据泄露、丢失或破坏可能造成的危害程度。

8.3 数据访问权限管理

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，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。

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。

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。

8.4 数据安全审计

8.4.1 审计委员

组织应配备数据安全管理审计委员，对日志、数据使用、数据资产、合作方、应急响应、举报投诉、教育培训等数据安全工作进行安全审计管理。

8.4.2 日志

组织应对数据授权访问、批量复制、开放共享、销毁、数据接口调用等重点环节实施日志留存管理。

日志记录至少包括执行时间、操作账号、处理方式、授权情况、IP地址、登录信息等，能够对识别和追溯数据操作和访问行为提供支撑。

日志保存时间不少于180天。

8.4.3 数据使用

应定期对内部数据使用等申请流程进行审计。

8.4.4 数据资产

应对组织内部数据资产定期进行审计工作，了解数据资产情况。

8.4.5 合作方

应定期对涉及数据共享所有合作方的相关资质及项目安全性进行审计。

8.4.6 应急响应

应定期对组织内部应急响应事件的处理过程及结果进行审计。

8.4.7 举报投诉

应定期对涉及数据安全类型投诉的处理过程及结果进行审计。

8.4.8 教育培训

应定期对组织内部人员的数据安全培训过程及考核结果进行审计。

8.4.9 账号权限

应定期对涉及敏感数据系统日志及数据库操作日志的内容进行审计，审计范围包括但不限于：账号异常登录、高敏感操作、不合理操作等。

8.4.10 技术及工具

应对数据安全管理技术或工具进行有效性监督。

8.4.11 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。数据操作审计内容和企业平台系统权限分配表作为系统策略进行配置。

8.5 数据合作方管理

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。

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。

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。

应对合作方数据使用情况进行监督管理。

8.6 数据安全事件应急管理

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，从数据安全事前防范和事中处理等维度进行应急处理与处置。

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。

应急预案应至少包含：数据使用审批应急响应、数据资产应急响应、举报投诉应急响应、教育培训应急响应、账号权限应急响应、日志审计应急响应、合作方应急响应。

8.7 数据安全举报投诉管理

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。

注：适宜的举报投诉渠道，如电子邮件、电话、传真、网站等。

8.8 数据资产与数据资源管理

8.8.1 组织应：

a）确定数据安全相关的资产；

b）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；

c）按照8.2条的分类分级法，确定组织的数据资源安全等级；

d）根据安全等级，制定适宜的数据资产与资源的控制措施；

e）定期验证控制措施的有效性。

8.8.2 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、终端数据资产进行扫描，发现识别敏感数据信息。

8.8.3 在验证控制措施的有效性时，应配备技术能力，对数据脱敏、数据分类分级效果进行验证，确保各类数据处理场景中数据脱敏的有效性和合规性。

8.8.4 数据防泄露

涉及存储、处理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。

组织应具备对网络、邮件、FTP、USB等多种数据导入导出渠道进行实时监控的能力，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。

8.8.5 接口安全管理

面向互联网及合作方开放的数据接口，应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。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。

8.8.6 敏感数据保护

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。

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。

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。

9 绩效评价

9.1 监视、测量、分析和评价

组织应评价数据安全绩效以及数据安全管理能力的有效性。

组织应确定：

a）需要被监视和测量的内容，包括数据安全管理过程、控制、目标；

b）适用的监视、测量、分析和评价，以确保得到有效的结果；

按照国家法律法规与标准规范的要求，组织应定期开展自评估活动。自评估的内容应包括：

a）依据国家法律法规、标准规范，制定数据安全管理制度，涵盖数据安全策略、组织建设、制度建设、数据资产管理、权限管理、安全审计、应急响应、合作方管理、教育培训、举报投诉等方面

b） 数据识别、操作审计、数据防泄漏、接口安全管理、敏感数据保护等数据安全技术措施。

组织应保留适当的文件化信息，作为监视和测量的证据。

9.2 内部审核

组织应按计划的时间间隔进行内部审核，确定数据安全管理能力：

a）是否符合

1）组织自身的要求；

2）本技术规范的要求。

b）是否得到有效实现和维护。

9.3 管理审核

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：

a）以往管理评审提出的措施的状态；

b）与数据安全管理能力相关的外部和内部事项的变化；

c）有关数据安全绩效的反馈，包括以下方面的趋势：

1）不符合和纠正措施；

2）监视和测量结果；

3）审核结果

4）数据安全目标完成情况。

d）相关方反馈；

e）数据安全风险评估结果及应对措施的状态；

f）持续改进的机会。

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。

10 改进

10.1 不符合及纠正措施

当发生不符合时，组织应：

a）对不符合作出反应，适用时：

1）采取措施，以控制并予以纠正；

2）处理后果；

b）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：

1）评审不符合；

2）确定不符合的原因；

3）确定类似的不符合是否存在，或可能发生。

c）实施任何需要的措施；

d）评审任何所采取的的纠正措施的有效性；

e）必要时，对数据安全管理能力进行变更；

纠正措施应与不符合的影响相适合。

不符合的纠正过程，应保留成文信息。

10.2 持续改进

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。