ICS 35. xxx
CCS Lxx

团　　体　　标　　准

T/ISC XXX—XXXX

数据合规能力成熟度评估模型

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中 国 互 联 网 协 会　　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。

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专利的责任。

本文件由中国互联网协会提出并归口。

本文件起草单位：

本文件主要起草人：

本文件及其所代替文件的历次版本发布情况为：

引　言

随着数字经济的快速发展，数据已成为新型生产要素和战略性资源。数据的合规处理不仅关系到个人信息权益保护、数据安全和国家数据主权，也是数据要素市场化配置、数据流通交易的前提和基础。

当前，我国已形成以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及《网络数据安全管理条例》为核心的“三法一条例”数据合规法律框架，各行业领域也陆续出台专项监管要求。但各类组织在数据合规能力建设方面仍存在水平参差不齐、体系建设缺乏统一指引、合规管理难以量化评估等问题。

本文件旨在建立一套科学、系统、可评估的数据合规能力等级模型，为组织数据合规能力建设提供指引，为第三方评估提供依据，推动数据合规管理从被动应对向主动防控、从分散管理向体系化管理转型，促进数据要素安全有序流通与价值释放。

本文件在能力等级设计中，充分考虑了不同数据处理角色和不同流通地位的合规义务差异，采用“通用基线+角色差异标注”的方式，在统一的能力框架内体现角色的合规要求差异。同时设置特殊制度补充模块作为附加层，覆盖关键信息基础设施保护、个人信息处理、重要数据处理、数据跨境传输、公共数据授权运营、生成式人工智能数据合规、人类遗传资源与生物安全数据管理、地理信息数据管理等特殊合规场景，并为行业特别要求预留接口条款，确保标准的通用性和适用性。

数据合规能力成熟度评估模型

1 范围

本文件确立了数据合规能力成熟度等级模型的总体框架，规定了能力域、能力项的构成，以及各能力项在不同能力等级下的要求。

本文件适用于组织数据合规能力成熟度的自我评估和第三方评估，也可为数据合规管理体系建设与优化提供指引。

本文件不替代法律法规对数据处理的强制性要求。未满足法定要求的组织不具备等级评估条件。

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 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

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 25069-2022 信息安全技术 术语

GB/T 43697—2024 数据安全技术 数据分类分级规则

GB/T 45577—2025 数据安全技术 数据安全风险评估方法

GB/T 46903—2025 个人信息保护合规审计要求

GB/T 45574—2025 敏感个人信息处理安全要求

注：《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《网络数据安全管理条例》等法律法规为强制适用的上位法，在本文件相关条款中直接引用，不作为规范性引用文件列出。

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据处理

数据的收集、存储、使用、加工、传输、提供、公开、删除等活动的总称。

[来源：《中华人民共和国个人信息保护法》第四条第二款]

3.2

数据合规

在数据全生命周期中，确保数据资源、数据产品和服务的来源、内容、可交易性等符合法律法规的相关规定。

3.3

数据合规能力

组织为保障数据处理活动符合数据合规要求所具备的组织、制度、流程、技术和管理等方面的综合能力。

3.4

能力域

数据合规能力在某一管理维度的集合，由一组相关的能力项组成。

3.5

能力项

能力域内可独立评估的数据合规能力单元。

3.6

能力等级

组织在特定能力项上数据合规能力达到的水平，从低到高依次分为一级至三级。

3.7

合规场景

一组目的相近、处理方式相似、涉及数据类型相同的数据处理活动的集合，是合规义务映射和等级评估的基本单元。

3.8

自主处理者

自行决定数据处理目的和方式的组织。

注：本标准将《中华人民共和国个人信息保护法》中的“个人信息处理者”按处理决定权的不同，区分为自主处理者、受托处理者和共同处理者三类，以实现合规义务的差异化映射。

[来源：《中华人民共和国个人信息保护法》第四条，有修改]

3.9

受托处理者

接受自主处理者委托，按照委托方的指示处理数据的组织。

[来源：《中华人民共和国个人信息保护法》第二十一条]

3.10

共同处理者

与一个或多个组织共同决定数据处理目的和方式的组织。

[来源：《中华人民共和国个人信息保护法》第二十条]

3.11

数据提供方

产生、持有或控制数据，并在流通中出售、提供数据的组织。

3.12

数据需求方

在数据流通中采集、接收、购买或使用数据的组织。

3.13

数据流通中介方

为数据供需双方提供交易、匹配、撮合或平台服务的组织。

3.14

数据产品经营方

对数据进行加工形成数据产品并向市场提供的组织。

3.15

重要数据

特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

注：仅影响组织自身或公民个体的数据一般不作为重要数据[GB/T 43697—2024，3.2]。

3.16

数据产品

自然人、法人或者非法人组织对其合法获取的数据资源，经过实质性加工和创新性劳动后形成的，可满足特定需求的数据加工品和数据服务。

3.17

数据产权

权利人对特定数据享有的财产性权利，包括数据持有权、数据使用权、数据经营权等。

3.18

数据产权登记

数据产权登记机构对数据的描述、来源、权利内容等进行审查，记载数据权利归属等信息，并出具登记凭证的行为。

3.19

数据产权登记凭证

登记机构依据数据产权登记程序核发的、记载数据产权归属和内容等信息的证明文件。

3.20

特殊制度补充模块

针对特定法律制度领域设定的、在通用基线和角色差异之上叠加的附加合规评估模块。

本标准设八个特殊制度补充模块，采用触发式叠加机制。

3.21

触发条件
导致特定合规评估模块被激活的事实条件。

4 符号和缩略语

下列缩略语适用于本文件。
AI：人工智能（Artificial Intelligence）
CII：关键信息基础设施（Critical Information Infrastructure）
DSMM：数据安全能力成熟度模型（Data Security Capability Maturity Model）

5 总体原则

5.1 底线法定原则

能力等级一级为法定要求底线，采用清单式逐条判定。组织满足全部法定要求的，方可进入等级评估；未满足法定要求的组织不具备等级评估条件。

5.2 角色差异原则

不同数据处理角色承担不同的合规义务。组织应根据自身的数据处理活动和数据流通地位，识别所承担的角色，履行对应角色的合规要求。一个组织同时具备多个角色的，合规义务取并集。

5.3 场景驱动原则

以合规场景作为活动认定和合规义务映射的基本单元，避免逐条活动认定带来的操作负担。组织应先识别合规场景，再确定角色，最后映射合规义务。

5.4 渐进提升原则

能力等级呈渐进关系，高等级要求以低等级要求为基础。组织应逐级提升，不宜跨级。

5.5 持续改进原则

数据合规能力建设是持续的过程。组织应建立持续改进机制，根据法律法规变化、业务发展和技术演进动态优化合规管理体系。

6 模型概述

6.1 模型结构

数据合规能力等级模型由能力域、能力项和能力等级三个层次构成：
a）能力域：数据合规能力在某一管理维度的集合，本文件设置6个能力域；
b）能力项：能力域内可独立评估的能力单元，每个能力域分解为若干能力项；
c）能力等级：每个能力项按3个等级描述能力要求，从低到高依次为一级（基础级）、二级（规范级）、三级（优化级）。

6.2 能力等级描述

6.2.1 一级（基础级）

组织满足数据合规的基本底线要求。一级采用清单式逐条判定，所有要求条目均判定为“满足”方为通过。一级不设评分，通过一级判定后自动进入二级及以上等级评估。未通过一级判定的，不具备等级评估条件，应先行整改。

6.2.2 二级（规范级）

组织建立了系统化的数据合规管理体系，在组织层面统一了合规战略、制度和流程，明确了合规职责分工。数据合规工作与业务流程融合，能够主动识别和管理合规风险，实现常态化管理。

6.2.3 三级（优化级）

组织建立了合规绩效指标体系，能够对合规能力进行量化评估。组织的数据合规管理达到行业领先水平，形成持续改进和创新机制。合规管理应用智能化技术手段，实现部分环节的自动化管控。在行业内外分享最佳实践经验，推动行业合规水平提升。

6.3 能力域与能力项

数据合规能力等级模型包含 6 个能力域和 20 个能力项，见表 1。

表 1 能力域与能力项

能力域	能力项
合规战略与组织	合规战略规划（7.1）
	合规组织架构与岗位设置（7.2）
	合规培训教育（7.3）
合规制度与流程	制度体系建设（8.1）
	合规需求管理（8.2）
	合规流程设计与执行（8.3）
数据全生命周期合规	数据分类分级合规（9.1）
	数据采集合规（9.2）
	数据存储合规（9.3）
	数据使用与加工合规（9.4）
	数据流通合规（9.5）
	数据退役与销毁合规（9.6）
合规风险与事件管理	合规风险识别与评估（10.1）
	合规风险监测与预警（10.2）
	合规事件应急处置（10.3）

能力域	能力项
	合规事件通报与整改（10.4）
合规技术支撑	合规技术体系与工具（11.1）
	合规追溯与存证（11.2）
合规文化与能力	合规文化建设（12.1）
	合规考核与激励（12.2）

6.4 角色识别与合规义务映射

6.4.1 合规场景识别

组织应将数据处理活动归类为合规场景。合规场景是一组目的相近、处理方式相似、涉及数据类型相同的数据处理活动的集合。合规场景的识别应：

a）覆盖组织全部数据处理活动；

b）按处理目的、处理方式和涉及数据类型进行归类；

c）对每个合规场景标注其对应的角色组合。

6.4.2 角色识别

组织应通过识别自身的数据处理活动和数据流通地位，确定在角色矩阵中的角色组合。角色识别采用两个正交维度：

a）处理关系维度：根据组织对数据处理目的和方式的决定权，分为自主处理者、受托处理者、共同处理者三类；

b）流通关系维度：根据组织在数据流通中的位置，分为数据提供方、数据需求方、数据流通中介方、数据产品经营方四类。

一个组织可同时具备多个角色，合规义务取并集。不涉及数据对外流通活动的组织，在流通关系维度不标注角色，仅评估通用基线与处理关系差异。

6.4.3 合规义务映射

组织应将法律法规、监管要求、行业标准中的合规义务，按角色差异映射至各合规场景。合规义务映射应：

a）识别通用合规义务（所有角色均需遵守），其中涉及个人信息、敏感个人信息、重要数据等特定数据类别的要求，仅在组织处理相应类别数据时适用；经合规场景识别确认不涉及相应数据类别的，相关要求不作为评估项；

b）识别角色特定合规义务（特定角色需额外遵守）；

c）识别特殊制度补充模块触发的额外合规义务。

6.4.4 特殊制度补充模块

当组织的数据处理活动触发以下特殊制度条件时，应在满足通用要求和角色差异要求的基础上，叠加对应的特殊制度补充模块合规要求：

S1 关键信息基础设施保护：运营关键信息基础设施的；

S2 个人信息处理：以自然人为产品或者服务的对象，收集、使用其个人信息的（员工、求职者及业务联系人场景除外）；

S3 重要数据处理：处理重要数据的；

S4 数据跨境传输：向中华人民共和国境外提供数据的；

S5 公共数据授权运营：经授权运营公共数据资源的；

S6 生成式AI数据合规：提供生成式人工智能服务涉及数据处理的；

S7 人类遗传资源管理：采集、保藏、利用人类遗传资源或对外提供人类遗传资源材料的；采集、保藏、利用我国生物资源（含动植物遗传资源、病原微生物数据等）或对外提供生物资源材料或数据的；

S8 地理信息数据管理：采集、存储、使用高精度地理信息数据，或向境外提供测绘地理信息成果的。

特殊制度补充模块的合规要求见附录B。

6.4.5 行业特别要求的衔接

对于特定行业（如金融、医疗、电信、能源等）存在专门数据合规监管要求的，通过以下接口规则与本文件衔接：

a）行业特别要求严于本文件通用基线的，从其特别要求；

b）行业特别要求在本文件未覆盖领域设定义务的，作为附加评估项纳入评估；

c）行业特别要求与特殊制度补充模块重叠的，取较严者。

行业法规索引表见附录C，供评估时参照。

7 合规战略与组织

7.1 合规战略规划

7.1.1 一级（基础级）

a）基于合规需求识别结果（见8.2），形成数据合规核心目标和重点方向；

7.1.2 二级（规范级）

a）在组织层面制定数据合规战略，明确合规愿景、目标和实施路径；

b）编制数据合规战略实施计划，明确实施步骤、责任主体和资源保障；

c）将合规战略与业务战略对齐，确保合规要求嵌入业务决策。

7.1.3 三级（优化级）

a）建立合规战略绩效指标体系，量化评估战略执行效果；

b）在行业层面分享合规战略规划最佳实践。

7.2 合规组织架构与岗位设置

7.2.1 一级（基础级）

a）重要数据处理者应指定数据安全负责人和管理机构，明确数据合规职责；

b）对依法应设置或指定的关键合规岗位（数据安全负责人、个人信息保护负责人等），明确任职要求、职责权限和汇报关系；

c）处理重要数据的处理者的网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由管理层成员担任；

d）掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应对网络数据安全负责人和关键岗位人员进行安全背景审查。

7.2.2 二级（规范级）

a）在组织层面建立数据合规管理组织体系，设立专门的数据合规管理部门；
b）明确合规治理架构，包括决策层、管理层和执行层的职责分工；
c）建立跨部门合规协调机制，确保合规工作协同推进；
d）在组织层面建立数据合规岗位体系，覆盖决策、管理、执行各层次；
e）制定合规岗位任职资格要求，包括知识、技能、经验等方面的要求；
f）建立数据合规岗位的绩效考核机制。

【角色差异】

——受托处理者：应协助个人信息处理者履行相关法定义务，通过指定对接委托方的合规联络人等方式，确保及时响应委托方的合规要求。

——数据流通中介方：应设立交易合规审核岗位，负责交易标的合规性审查。

——数据产品经营方：应设立数据产品合规管理岗位，覆盖产品全生命周期合规管控。

7.2.3 三级（优化级）

a）建立合规组织建设评估指标体系，量化评估组织架构运行效果；
b）组建覆盖法务、技术、数据、业务等领域的复合型合规管理团队；
c）建立敏捷的合规组织响应机制，快速适应监管环境变化；
d）建立岗位效能评估指标体系，量化评估岗位设置效果；
e）建立数据合规岗位能力模型，指导人才培养和发展；
f）合规组织架构形成可推广的行业治理模式，引领行业合规组织建设方向。

7.3 合规培训教育

7.3.1 一级（基础级）

a）定期对涉及个人信息保护、数据合规处理业务岗位的人员开展个人信息保护和数据安全培训教育；
b）培训教育内容覆盖核心法律法规、内部管理制度和岗位要求。

7.3.2 二级（规范级）

a）在组织层面建立数据合规培训体系，覆盖各层级人员；
b）制定系统的培训计划，明确培训内容、时间和资源保障；
c）开展合规意识培训，提升全员合规意识；
d）建立培训效果评估机制。

【角色差异】

——受托处理者：应对受托处理人员开展专项培训，重点覆盖委托范围约束和数据处理限制要求。

——数据流通中介方：应对交易审核人员开展数据权属、数据交易法规专项培训。

7.3.3 三级（优化级）

a）建立培训效果量化评估体系，科学评估培训成效；
b）搭建智能化培训平台，实现培训的个性化和精准化；
c）针对不同岗位开展差异化培训；

d）与高校、研究机构合作开展合规人才培养。

8 合规制度与流程

8.1 制度体系建设

8.1.1 一级（基础级）

a）建立覆盖数据处理全流程的数据合规管理制度和操作规程；
b）制度体系内容应严格符合适用法律、行政法规的规定和国家标准的强制性要求；
c）对制度内容进行及时公开发布、宣传和定期培训、维护。

8.1.2 二级（规范级）

a）在组织层面建立分层分类的数据合规制度体系，形成“合规总纲—专项管理办法—操作实施细则”三级架构；
b）制度覆盖数据全生命周期各环节，明确合规标准与操作流程；
c）建立制度全生命周期管理机制，包括立项、起草、评审、发布、宣贯、执行监督、评估和修订；
d）及时响应法律法规更新，定期开展制度评估与修订。
【角色差异】
——受托处理者：应制定受托处理专项管理制度，明确委托合同审查、处理范围限制、安全措施要求、报告机制等。
——共同处理者：应与共同处理方签署合规责任约定，建立合规协调机制，明确各自义务与连带责任范围。
——数据提供方：应制定数据对外提供专项管理制度，覆盖提供行为合法性审查、接收方约束、风险识别与处置措施等。
——数据需求方：应制定外部数据获取专项管理制度，覆盖来源合规审查、授权核实、用途限制等。
——数据流通中介方：应建立交易标的合规性审核制度，对交易数据的来源合法性、权属清晰性、内容合规性进行审查。
——数据产品经营方：应建立数据产品合规管理制度，覆盖产品来源合规性、加工正当性、产品权属清晰性、产品质量责任。

8.1.3 三级（优化级）

a）建立制度执行效果量化评价体系；
b）采用技术手段监控制度执行情况，定期形成量化评估报告；
c）制度体系形成可输出的行业合规制度框架，引领行业制度建设方向。

8.2 合规需求管理

8.2.1 一级（基础级）

a）识别组织面临的主要法律、行政法规、监管要求和强制性国家标准中的合规义务。
【角色差异】
——受托处理者：应识别委托合同约定的合规义务，确保处理活动不超出委托范围。
——共同处理者：应与共同处理方明确各自的数据保护权利、义务与责任划分。

8.2.2 二级（规范级）

a）建立系统的合规需求识别机制，全面识别法律法规、监管规定、行业标准和合同约定的合规要求；

c）建立合规需求分析机制，深入分析合规要求的具体内容、适用范围和执行标准；

d）建立合规需求转化机制，将合规要求转化为内部管理要求和技术要求；

e）建立法律法规动态追踪机制和合规需求跟踪机制，及时更新合规措施。

8.2.3 三级（优化级）

a）建立合规需求满足度量化评估体系；

b）运用合规需求分析工具，提升需求管理效率；

c）建立合规需求智能化管理平台，实现需求的动态管理

d）在行业层面分享需求管理方法论和最佳实践。

8.3 合规流程设计与执行

8.3.1 一级（基础级）

a）在数据收集、存储、使用、加工、传输、提供、公开、删除等关键处理环节建立合规流程，并在各环节落实合法处理依据、处理权限控制、数据安全保护措施、个人信息保护影响评估、风险评估、突发事件处置等核心合规要求；

b）对依法需记录、评估或审计的数据合规流程，形成并保存相应记录。

8.3.2 二级（规范级）

a)在组织层面建立完善的数据合规管理流程体系,覆盖数据全生命周期各环节,并明确各流程步骤、责任主体和工作标准；

b）建立流程执行监督机制，确保流程落地实施；

c）建立流程评估和优化机制。

【角色差异】

——受托处理者：应建立受托处理合规流程，包括委托范围核验、处理活动记录、定期报告等流程环节。

——数据提供方：应建立数据对外提供合规审批流程，包括提供行为合法性评估、接收方合规能力评估、数据出境必要性评估。

——数据需求方：应建立外部数据获取合规审查流程，包括来源合法性核验、授权范围核实、数据质量与合规性评估。

——数据流通中介方：应建立数据交易标的审核流程和交易存证流程。

——数据产品经营方：应建立数据产品上架前的合规审查流程，覆盖来源、加工、权属各环节。

8.3.3 三级（优化级）

a）建立合规流程效能量化评估体系；

b）运用智能化技术工具分析合规流程实际执行路径，识别执行与设计的偏差并持续改进；

c）实现合规流程与业务系统的集成，实现合规控制点随业务流程自动触发和执行留痕；；

d）合规流程体系形成可推广的行业合规流程标准方案。

9 数据全生命周期合规

9.1 数据分类分级合规

9.1.1 一级（基础级）

a）依据数据分类分级保护制度，开展数据分类分级，识别个人信息、敏感个人信息和重要数据等特殊类别数据；

b）形成数据分类分级目录和重要数据识别清单；

c）对个人信息、敏感个人信息和重要数据采取相应的安全防护措施。

9.1.2 二级（规范级）

a）在组织层面建立数据分类分级管理制度，明确分类分级原则、方法和流程；

b）形成完整的数据分类分级目录，覆盖全部业务数据；

c）根据分类分级结果，对不同类别、不同级别的数据采取差异化的管控措施；

d）建立分类分级动态调整机制，及时响应数据属性变化和法规更新。

9.1.3 三级（优化级）

a）采用智能化技术工具实现数据分类分级；

b）建立分类分级效果量化评估体系；

c）实现分类分级结果与数据访问控制、脱敏策略的联动；

d）数据分类分级体系形成行业示范方案，覆盖产业链数据分类分级协同。

9.2 数据采集合规

9.2.1 一级（基础级）

a）数据采集具有合法处理依据和明确、合理的目的，遵循合法、正当、必要和诚信原则；

b）处理个人信息前，应当以显著方式、清晰易懂的语言，真实、准确、完整地告知个人信息处理事项，法律、行政法规规定应当保密或者不需要告知的情形除外；基于个人同意处理个人信息的，应当取得个人在充分知情的前提下自愿、明确作出的同意；

c）采集个人信息应当遵循最小必要原则，限于实现处理目的的最小范围，不得过度采集；

d）采集重要数据的，按照规定识别、申报重要数据并向主管部门报备。

9.2.2 二级（规范级）

a）在组织层面建立数据采集合规管理制度，覆盖采集目的限定、合法性基础认定、同意管理、最小必要评估等环节；

b）建立数据采集合规审查流程，对新增数据采集场景进行合规评审；

c）定期开展数据采集合规自查。

【角色差异】

——数据需求方：应按制度与流程要求开展外部数据来源合法性核验、数据权属、授权范围核实、数据用途限制等审核。

9.2.3 三级（优化级）

a）建立数据采集合规量化评估体系，设置采集合规率等指标；

b）采用技术手段实现采集合规的自动化管控，包括最小必要校验等；

c）建立数据采集合规风险预警机制；

d）数据采集合规体系形成行业最佳实践方案，推动行业采集标准建设；

9.3 数据存储合规

9.3.1 一级（基础级）

a）按照法律法规要求和个人信息处理目的限定存储期限；
b）对存储的个人信息、敏感个人信息和重要数据采取相应的安全防护措施；
【角色差异】
——受托处理者：应在委托合同约定的期限内存储数据，委托关系终止后及时删除或返还数据。

9.3.2 二级（规范级）

a）在组织层面建立数据存储合规管理制度，覆盖存储期限管理、存储安全防护、存储位置管理等；
b）建立存储安全等级与数据分类分级结果的对应关系；
c）建立数据存储合规审查流程。

9.3.3 三级（优化级）

a）建立数据存储合规量化评估体系；
b）采用自动化工具实现存储期限管理和到期数据自动处置；
c）存储安全策略依据数据分类分级结果自动配置并动态调整；。

9.4 数据使用与加工合规

9.4.1 一级（基础级）

a）数据使用和加工不得超出告知事项或约定目的、方式、范围处理个人信息；
b）使用和加工个人信息应具备合法性依据，遵循最小必要原则；
c）处理敏感个人信息应当具有特定的目的和充分的必要性，采取严格保护措施，并向个人告知处理敏感个人信息的必要性以及对个人权益的影响；
d）建立便捷的个人信息权利请求受理与响应机制，依法响应个人查阅、复制、更正、删除其个人信息的请求，拒绝的应当说明理由；
【角色差异】
——受托处理者：使用和加工数据不超出委托范围。
——共同处理者：应在约定范围内使用和加工数据。

9.4.2 二级（规范级）

a）在组织层面建立数据使用与加工合规管理制度，覆盖目的限定管理、必要性评估、加工过程管控等；
b）建立数据使用目的变更审查机制，变更目的需重新获取同意或确认合法性基础；
c）建立数据加工过程合规管控措施，确保加工行为可追溯；
【角色差异】
——数据产品经营方：应按制度与流程要求开展产品来源合规性、加工过程正当性、产品权属清晰性、产品质量责任等审查。

9.4.3 三级（优化级）

a）建立数据使用与加工合规量化评估体系；
b）采用智能化技术手段实现数据使用范围自动校验和目的偏离预警；
c）数据使用与加工合规体系形成行业数据加工合规方法论。

9.5 数据流通合规

9.5.1 一级（基础级）

a）向境外提供个人信息或重要数据应当符合法定条件；

b）传输和提供数据过程中应采取必要的安全技术防护措施；

c）一般数据共享和流通活动具有相应的合法性基础；

d）共享和流通重要数据符合法定要求；

e）数据流通活动应确保数据来源合法，权属关系基本清晰。

【角色差异】

——受托处理者：未经委托方同意不得向第三方提供受托处理的数据。

——共同处理者：应按共同处理约定履行对外提供前的义务要求。

——数据提供方：应核实所提供数据的来源合法性，确认数据采集/获取环节具有合法授权基础。

——数据需求方：应核验数据提供方的合法持有身份和提供授权范围，留存数据来源合法性证明材料；确认获取数据的授权范围和用途限制，变更原先处理目的、处理方式时应当重新取得个人同意。

9.5.2 二级（规范级）

a）在组织层面建立数据流通合规管理制度，覆盖数据对外提供审查、传输安全、接收方约束、共享审批、流通方式合规、合同约束等；

b）建立数据对外提供审批流程，评估提供行为的合法性；

c）与数据流通相关方签署数据保护协议，约束接收方的数据处理行为；

d）建立数据传输安全管控措施，确保传输过程安全；

e）建立数据流通记录管理机制；

f）建立数据产权管理制度，覆盖权属识别、权属配置、权属变更、权属争议处理；建立数据产权登记管理流程，按需按要求开展数据产权登记。

【角色差异】

——数据提供方：应按制度与流程要求开展提供行为合法性评估，接收方合规能力评估等；应在数据提供合同中明确约定数据的权属归属、使用范围、再流转限制等产权条款。

——数据流通中介方：应按制度与流程要求，对平台上流通交易标的合规性、权属状况等进行审查，包括数据来源合法性、权属清晰性等。

——数据需求方：应确保在授权范围内使用数据，不得超出授权范围进行再处理或再流转；对获取的数据进行加工形成数据产品的，应明确数据产品的权属归属。

——数据产品经营方：应确保数据产品的经营权属清晰，建立数据产品权属证明机制，在授权范围内使用数据资源。

9.5.3 三级（优化级）

a）建立数据流通合规量化评估体系；

b）采用技术手段实现数据对外提供的自动化合规审查；

c）建立数据产权数字化管理能力，实现数据产权确权、登记、评估、流转的全链条管理；

d）数据流通合规体系引领行业数据要素流通合规生态建设。

【角色差异】

——数据流通中介方：应引领数据要素流通市场的产权登记规范和交易合规标准建设。

9.6 数据退役与销毁合规

9.6.1 一级（基础级）

a）存储期限届满或处理目的已实现或无法实现等情形的个人信息应及时删除或匿名化处理，难以删除的应停止除存储和必要安全保护外的处理；

b）受托处理关系终止后及时删除或返还受托处理的数据；

c）对数据退役、删除、匿名化、销毁活动进行记录和审计。

9.6.2 二级（规范级）

a）在组织层面建立数据退役与销毁合规管理制度，覆盖退役条件认定、销毁方式选择、销毁验证等；

b）建立数据退役判定机制，明确退役条件和流程；

c）建立数据销毁验证机制，确保数据不可恢复；

d）建立数据退役与销毁的记录管理机制。

【角色差异】

——受托处理者：应建立委托关系终止后的数据删除或返还机制。

——数据产品经营方：应建立数据产品下架后的数据处理机制。

9.6.3 三级（优化级）

a）建立数据退役与销毁合规量化评估体系；

b）采用自动化工具实现到期数据自动识别和销毁；

c）建立数据销毁效果验证机制；

d）数据退役与销毁合规体系形成行业级数据销毁标准方案。

10 合规风险与事件管理

10.1 合规风险识别与评估

10.1.1 一级（基础级）

a）建立数据安全和个人信息保护风险识别、监测和评估机制，形成风险清单；

b）对已识别的合规风险采取相应的控制措施；

c）发生数据安全和个人信息安全事件后能够进行应急处置。

10.1.2 二级（规范级）

a）在组织层面建立系统的合规风险识别机制，全面识别合规风险；

b）建立合规风险评估机制，科学评估风险的可能性和影响程度，确定风险等级；

c）建立合规风险应对策略，制定风险控制措施；

d）定期开展合规风险评估，更新风险清单。

【角色差异】

——数据提供方：应重点评估数据对外提供场景的合规风险，包括提供行为合法性风险、接收方违约风险、数据出境风险等。

——数据需求方：应重点评估外部数据获取场景的合规风险，包括来源合规风险、授权不足风险、数据质量风险等。

——数据流通中介方：应重点评估交易标的合规风险、交易纠纷风险、平台运营风险等。

——数据产品经营方：应重点评估数据产品权属风险、加工正当性风险、产品质量责任风险等。

10.1.3 三级（优化级）

a）建立合规风险量化评估体系；
b）运用智能化技术实现风险的自动识别。

10.2 合规风险监测与预警

10.2.1 一级（基础级）

a）对数据处理活动开展合规风险监测；
b）能够发现明显的合规风险并及时做出预警，采取补救措施。

10.2.2 二级（规范级）

a）在组织层面建立合规风险监测与预警制度，明确监测范围、频次和方法；
b）定期报告合规风险状况。

10.2.3 三级（优化级）

a）建立合规风险监测量化评估体系；
b）运用智能化技术实现风险的自动识别和预警；
c）建立风险态势感知平台，实现风险的实时监测和可视化展示；
d）在行业层面分享并形成可复用、可推广的实践经验。

10.3 合规事件应急处置

10.3.1 一级（基础级）

a）发生数据安全事件后，应立即采取应急处置和补救措施，并按规定告知用户、向有关主管部门报告。

10.3.2 二级（规范级）

a）在组织层面建立数据合规事件应急管理制度，明确应急处置要求；
b）制定系统的应急预案体系，覆盖各类合规事件；
c）建立应急响应机制，实现快速响应；
d）定期开展应急演练。
【角色差异】
——受托处理者：应建立向委托方报告合规事件的机制，确保委托方及时知悉。
——数据流通中介方：应建立交易纠纷应急处理机制。

10.3.3 三级（优化级）

a）建立应急处置效能量化评估体系；
b）运用智能化技术实现应急响应的自动化；
c）在行业层面分享数据合规处置优秀实践经验。

10.4 合规事件通报与整改

10.4.1 一级（基础级）

a）发生数据安全事件后按照法定要求向主管部门报告；

b）对合规事件和检查发现的问题采取整改措施。

10.4.2 二级（规范级）

a）在组织层面建立完善的数据合规事件通报制度，明确通报范围、程序和时效要求；
b）建立内部通报管理机制，确保信息及时传达；
c）建立外部报告管理机制，履行法定报告义务；
d）建立系统的损失评估和原因分析机制；
e）建立整改方案制定和执行机制，确保整改落实；
f）建立整改效果验证机制。

10.4.3 三级（优化级）

a）建立合规事件通报与整改量化评估体系；
b）运用技术手段实现通报流程的自动化；
c）建立整改跟踪系统，实现整改过程可视化管理；
d）在行业层面分享事件管理最佳实践。

11 合规技术支撑

11.1 合规技术体系与工具

11.1.1 一级（基础级）

a）针对个人信息和重要数据采取加密、去标识化等安全技术措施；
b)根据数据处理活动的合规要求部署必要的安全技术措施和工具,并确保相关技术工具有效运行。。

11.1.2 二级（规范级）

a）在组织层面建立完善的数据合规技术体系规划，明确技术架构、部署范围和功能要求；
b）分层分类部署覆盖数据全生命周期的合规技术工具，包括数据分类分级工具、数据加密与脱敏工具、数据访问权限管控系统、个人信息告知－同意管理工具等；
c）以正式文件形式明确各工具的管理规范和操作流程。

11.1.3 三级（优化级）

a）建立合规技术效应用效果评估体系，设置工具覆盖率、管控有效率、合规校验准确率等指标；
b）部署智能化合规技术工具，包括合规风险智能监测引擎、法规动态智能追踪平台、自动化合规审计工具等；
c）实现合规技术工具与业务系统的深度打通，将合规校验节点嵌入核心业务流程；
d）合规技术工具形成行业级解决方案并开源或对外输出。

11.2 合规追溯与存证

11.2.1 一级（基础级）

a）对数据处理活动进行记录，确保相关处理活动具备基本的可追溯性；
b）操作记录能够支持合规审计和核查。

11.2.2 二级（规范级）

a）在组织层面建立完善的数据合规追溯与存证管理制度，明确追溯范围、存证标准、记录要求和留存期限；

b）实现企业数据处理活动全生命周期、全处理环节的全覆盖追溯，记录内容包含操作主体、操作时间、操作对象、操作内容等追溯要素；

c）建立追溯与存证信息的查询、调取和使用管理机制，明确相关权限和操作要求；

d）定期开展追溯体系有效性验证。

11.2.3 三级（优化级）

a）建立合规追溯与存证能力评估体系；

b）采用区块链等技术实现提高存证信息的真实性、完整性和可信性；

c）实现数据处理全流程操作行为的自动化记录和全链路可视化追溯；

d）建立智能化追溯分析能力。

e）合规追溯与存证机制形成行业级可信存证基础设施方案。

12 合规文化与能力

12.1 合规文化建设

12.1.1 一级（基础级）

a）组织开展数据合规教育培训与制度宣传；

b）员工明晰核心合规底线。

12.1.2 二级（规范级）

a）在组织层面确立合规价值观，纳入企业文化建设体系；

b）制定组织级合规文化建设年度规划与实施方案；

c）搭建多渠道合规宣贯矩阵，定期开展合规宣贯、政策解读和案例警示教育；

d）建立员工合规咨询与反馈渠道。

12.1.3 三级（优化级）

a）建立合规文化建设评价体系，设置合规认知度、宣贯覆盖率、员工参与度等指标；

b）搭建智能化合规文化传播平台，实现合规文化精准触达；

c）合规文化体系形成行业级合规文化品牌，引领行业合规价值取向；

12.2 合规考核与激励

12.2.1 一级（基础级）

a）在内部管理制度中明确违反数据合规要求的责任追究和处置措施；

b）建立与岗位职责相匹配的数据合规考核评价机制，对员工合规行为进行定期评价。

12.2.2 二级（规范级）

a）在组织层面建立数据合规考核与激励约束体系；

b）将数据合规工作纳入各部门、各岗位的绩效考核体系；

c）建立明确的奖惩机制，对合规工作成效显著的团队与个人给予正向激励，对违反合规红线的行

为明确惩戒标准。

12.2.3 三级（优化级）

a）建立精细化、可量化的数据合规考核指标体系，针对不同岗位设置差异化考核指标；
b）通过合规管理平台实现考核数据的自动采集和实时统计；
c）将合规考核与员工职业发展深度融合；
d）建立合规容错纠错机制，在严守合规底线的前提下鼓励业务创新；
e）合规考核与激励体系形成行业级合规绩效管理标杆方案。

13 评估方法

13.1 评估流程

13.1.1 评估准备

评估准备阶段的主要活动包括：
a）评估申请与受理：被评估方向评估机构提交评估申请，评估机构对申请进行审核；
b）评估团队组建：评估机构组建由熟悉数据合规管理和能力评估的专业人员组成的评估团队；
c）评估方案制定：评估团队制定评估方案，明确评估目标、评估范围、评估方法和评估进度；
d）评估材料收集：被评估方准备相关评估材料，包括组织基本信息、合规管理制度文件、合规组织架构说明、合规培训记录、合规技术系统说明、合规事件记录和处置报告等。

13.1.2 合规底线判定

在进入正式等级评估前，评估团队应对被评估方进行合规底线判定，内容包括：
a）法律遵守底线：数据处理活动不存在违反法律、行政法规强制性规定的情形；
b）监管合规底线：不存在因数据合规问题受到行政处罚且未完成整改的情形；
c）事件底线：近12个月内未发生因数据合规管理缺失导致的重大数据安全事件。
合规底线判定结果为“通过”或“不通过”。判定为“不通过”的，不进入等级评估，应先行整改。

13.1.3 角色识别与场景确认

评估团队应确认被评估方在角色矩阵中的角色组合，具体包括：
a）识别被评估方的数据处理活动，归类为合规场景；
b）按处理关系维度确认被评估方的角色（自主处理者/受托处理者/共同处理者）；
c）按流通关系维度确认被评估方的角色（数据提供方/数据需求方/数据流通中介方/数据产品经营方），不涉及数据对外流通活动的组织在流通关系维度不标注角色；
d）确认被评估方是否触发特殊制度补充模块；
e）根据角色组合和特殊制度补充模块触发情况，确定被评估方需满足的完整合规义务集。

13.1.4 正式评估

正式评估阶段的主要活动包括：
a）信息收集与分析：通过文件审查、人员访谈、问卷调查、系统演示、现场观察等方式收集与被评估方数据合规能力相关的信息；
b）既有评估结果参考：被评估方在评估之日前一年内已开展个人信息保护合规审计、数据管理能力成熟度评估（DCMM）、数据安全能力成熟度评估（DSMM）等相关审计或评估的，对于与本文件要求相

同或相近的评估项，经核验相关结果有效、适用且与本文件要求一致的，可将其作为相应评估项的评价依据；

c）一级判定：逐条核查一级（基础级）要求是否满足，全部满足即为通过；

d）能力评估：对通过一级判定的组织，根据本文件规定的各能力项二级及以上等级标准，对照被评估方需满足的合规义务集，逐项评估能力等级；

e）证据核实：对被评估方声称满足的能力等级标准，通过文件审查、人员访谈、系统演示等方式进行核实；

f）差距分析：识别被评估方在每个能力项上与更高等级之间的差距。

13.1.5 结果确认

结果确认阶段的主要活动包括：

a）评估结果沟通：评估团队与被评估方进行评估结果沟通，听取反馈；

b）评估报告编制：评估团队编制数据合规能力等级评估报告，包括评估基本情况、合规底线判定结果、各能力项评估结果及详细分析、各能力域评估结果、组织整体能力等级、特殊制度补充模块评估结果、差距分析和改进建议等；

c）评估结果审核与发布：评估报告经评估机构内部审核后，向被评估方出具正式的评估结果。

13.2 等级判定方法

13.2.1 一级判定方法

一级（基础级）采用清单式逐条判定法。评估团队对照各能力项一级要求中标注的条目，逐条判定“满足”或“不满足”。全部条目均判定为“满足”的，一级判定通过；存在“不满足”条目的，一级判定不通过。

13.2.2 能力项等级判定（二级及以上）

通过一级判定后，二级及以上等级的每个能力项评分采用满足程度评分法，见表2。

表 2 满足程度与得分对应表

满足程度	分数	说明
完全满足	3	存在准确良好的直接证据，有间接证据和访谈验证支持，有效实施了标准的要求
大部分满足	2	存在准确的直接证据，有间接证据支持，实施情况存在个别轻微不足
部分满足	1	缺少直接证据或证据不够充分，仅实施了标准要求的某些部分，存在明显不足
不满足	0	缺少必要的管理文件，没有证据表明实施了标准的要求

每个能力项的等级得分按公式（1）计算：

$$P_i = \sum (C_j \times B_j)/n_i \cdots\cdots (1)$$

式中：

P_i——第i个能力项的得分；

C_j——第j条要求的得分；

B_j——第j条要求的权重因子

n_i——第i个能力项包含要求的数量。

注：各要求权重因子默认取 1。权重因子的调整应通过行业指引规定，不应由评估机构自行调整。

13.2.3 能力域等级判定

每个能力域的等级得分按公式（2）计算：

$$P_k = \sum (P_i \times B_i)/m_k \cdots\cdots (2)$$

式中：

P_k——第k个能力域的得分；

P_i——第i个能力项的得分；

B_i——第i个能力项的权重因子；

m_k——第k个能力域包含能力项的数量。

注：各能力项权重因子默认取1。权重因子的调整应通过行业指引规定，不应由评估机构自行调整。

13.2.4 整体等级判定

组织整体的数据合规能力等级得分按公式（3）计算：

$$D = \sum (P_k \times f_k)/m \cdots\cdots (3)$$

式中：

D——整体能力等级得分；

P_k——第k个能力域的得分；

f_k ——第k个能力域的权重因子；

m——能力域的数量。

注：各能力域权重因子默认取1。权重因子的调整应通过行业指引规定，不应由评估机构自行调整。

整体能力等级得分与等级的对应关系见表3。

表 3 等级得分与等级对应表

能力等级	等级得分范围
二级（规范级）	$1 < D \leq 2$
三级（优化级）	$2 < D \leq 3$

注：一级不设评分，通过合规底线判定和一级清单式判定后自动进入二级及以上评分。

13.2.5 取最低等级规则

当同一组织在多个合规场景或角色模式下的等级评估结果不一致时，取最低等级作为该组织的合规能力等级。

13.2.6 特殊制度补充模块评估

特殊制度补充模块的评估结果独立标注，不影响通用基线等级判定。评估报告应同时呈现通用基线等级和各触发模块的评估结果。

13.2.7 评价证据指引

评估时应根据不同要求类型收集相应证据，见表4。

表 4 评价证据指引

证据类型	适用要求	示例
制度文件	制度体系建设、流程设计	合规管理办法、操作规程、审批流程图
培训记录	合规培训教育、文化建设	培训计划、签到表、考核成绩、培训课件
系统截图	合规技术支撑、追溯与存证	系统界面截图、配置记录、日志导出
登记信息	数据流通合规、合规追溯与存证	数据产权登记凭证、登记信息存证记录
第三方报告	风险评估、安全检测	安全评估报告、审计报告、认证证书
事件记录	事件管理	事件报告、处置记录、整改报告
访谈记录	全部能力项	人员访谈笔录、问卷结果

附 录 A
（规范性）
角色矩阵表

A.1 处理关系维度

处理关系维度根据组织对数据处理目的和方式的决定权，分为三类，见表A.1。

表 A.1 处理关系维度分类

角色	定义	核心合规义务特征
自主处理者	自行决定数据处理目的和方式的组织	承担数据处理的全部合规义务，包括告知、同意、影响评估等
受托处理者	接受自主处理者委托，按照委托方的指示处理数据的组织	在委托范围内处理数据，采取安全措施，不得转委托，配合审计，委托终止后删除或返还数据
共同处理者	与一个或多个组织共同决定数据处理目的和方式的组织	约定各自的权利和义务，承担连带责任

A.2 流通关系维度

流通关系维度根据组织在数据流通中的位置，分为四类，见表A.2。

表 A.2 流通关系维度分类

角色	定义	核心合规义务特征
数据提供方	产生、持有或控制数据，并在流通中出售、提供数据的组织	提供行为合法性、接收方约束、数据出境合规
数据需求方	在数据流通中采集、接收、购买或使用数据的组织	获取合法性（来源合规、授权核实）、数据用途限制
数据流通中介方	为数据供需双方提供交易、匹配、撮合或平台服务的组织	交易标的合规性审查义务、信息披露义务、交易存证义务
数据产品经营方	对数据进行加工形成数据产品并向市场提供的组织	产品合规性（来源合法性、加工正当性）、产品权属清晰性、产品质量责任

A.3 角色识别指引

组织进行角色识别时，应：

a）梳理组织全部数据处理活动，归类为合规场景；

b）对每个合规场景，分别判断处理关系维度角色和流通关系维度角色；

c）汇总各合规场景的角色识别结果，形成组织的角色组合；

d）一个组织同时具备多个角色的，合规义务取并集；

e）不涉及数据对外流通活动的组织，在流通关系维度不标注角色，仅评估通用基线与处理关系差异；

f）组织角色随业务变化发生改变的，应及时更新角色识别结果。

附 录 B
（规范性）
特殊制度补充模块合规要求

B.1 概述

本附录规定了8个特殊制度补充模块的触发条件、合规依据和等级增量要求，供组织在合规义务映射和评估时对照执行。

特殊制度补充模块与角色矩阵正交。当组织的数据处理活动触发特殊制度条件时，应在满足通用要求和角色差异要求的基础上，叠加对应的特殊制度补充模块合规要求。特殊制度补充模块的评估结果独立标注，不影响通用基线等级判定。

B.2 S1 关键信息基础设施保护

触发条件：运营关键信息基础设施。

合规依据：

- 《中华人民共和国网络安全法》；
- 《关键信息基础设施安全保护条例》；
- 《中华人民共和国数据安全法》。

等级增量要求：

等级	增量要求
一级	明确专门安全管理机构和安全管理负责人 依法开展网络安全审查 采购网络产品和服务应通过安全审查
二级	建立供应链安全管理制度，对关键产品和服务采购进行安全评估 建立安全信息共享机制，与行业主管部门和保护工作部门保持信息互通
三级	建立 CII 安全保护效能量化评估体系，实现供应链安全风险的动态监测和预警； 形成行业级 CII 数据合规保护方案

B.3 S2 个人信息处理

触发条件：以自然人为产品或者服务的对象，收集、使用其个人信息的（员工、求职者及业务联系人场景除外）

合规依据：

- 《中华人民共和国个人信息保护法》；
- 《网络数据安全管理条例》；

- 《个人信息保护合规审计管理办法》；
- 《小型个人信息处理者个人信息保护简化措施规定》。

等级增量要求：

等级	增量要求
一级	a）处理个人信息前，以显著方式、清晰易懂的语言履行告知义务；基于个人同意处理的，取得有效同意，并提供便捷的撤回同意方式； b）基于个人同意处理敏感个人信息的，取得单独同意； c）处理不满十四周岁未成年人个人信息的，取得其父母或者其他监护人的同意，并制定专门的个人信息处理规则； d）向其他个人信息处理者提供个人信息的，告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，取得单独同意，并事前开展个人信息保护影响评估； e）定期对处理个人信息遵守法律、行政法规的情况开展合规审计。 f）处理敏感个人信息应取得个人单独同意并采取更严格的保护措施
二级	a）建立统一的个人信息处理活动管理机制，形成并动态维护个人信息处理活动清单或者台账，记录处理目的、处理方式、个人信息种类、合法性基础、保存期限等信息； c）针对敏感个人信息、未成年人个人信息、自动化决策、个人信息对外提供等高风险处理活动，建立专项审核和管理流程；
三级	a）运用技术工具对个人信息告知、同意、撤回、权利请求等活动实施自动化管理，并设置告知覆盖率、撤回处理及时率、权利请求按期办结率等指标进行量化评估； b）将个人信息保护要求嵌入产品设计、系统开发和业务运行流程，实现关键合规要求的自动校验和管控； c）持续优化个人信息保护规则和管理措施，在行业层面分享个人信息保护实践经验。

B.4 S3 重要数据处理

触发条件：处理重要数据的。

合规依据：

- 《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》；
- 《网络数据安全管理条例》；
- GB/T 43697—2024。

等级增量要求：

等级	增量要求
一级	a）按照国家有关规定识别、申报重要数据，并对确认为重要数据的数据落实相应安全保护要求； b）明确数据安全负责人和管理机构，落实重要数据安全保护责任； c）每年度对重要数据处理活动开展风险评估，并按照规定向有关主管部门报送风险评估报告； d）提供、委托处理或者共同处理重要数据的，按照规定事前开展风险评估，并采取相应安全保护措施。
二级	a）建立重要数据专项安全管理机制，明确重要数据识别申报、处理使用、权限管理、风险评估、安全事件处置等管理要求； b）建立并动态维护重要数据清单，明确重要数据的种类、规模、处理目的、处理方式、存储位置、责任主体等信息； c）根据重要数据处理活动的风险，对访问权限、存储使用、传输提供等关键环节实施专项安全管控，并对相关操作进行记录和定期检查。
三级	a）建立重要数据安全管理评估机制，并根据评价结果持续优化； b）运用技术工具对重要数据处理活动实施自动化监测，对异常访问、违规操作等风险进行自动识别和预警； c）在行业层面分享重要数据处理合规实践经验。

B.5 S4 数据跨境传输

触发条件：向中华人民共和国境外提供个人信息或重要数据。

合规依据：

- 《中华人民共和国个人信息保护法》；
- 《中华人民共和国数据安全法》；
- 《网络数据安全管理条例》；
- 《数据出境安全评估办法》；
- 《个人信息出境标准合同办法》；
- 《促进和规范数据跨境流动规定》。

等级增量要求：

等级	增量要求
一级	依法识别数据出境活动，判断出境数据类型、规模以及是否适用数据出境安全评估、个人信息出境标准合同、个人信息出境认证或者相关豁免情形，并按照规定选择适用的数据出境合规路径； b）向境外提供个人信息的，应依法履行告知、取得个人单独同意、开展个人信息保护影响评估等义务； c）向境外提供重要数据或者关键信息基础设施运营者向境外提供个人信息、重要数据的，按照规定申报数据出境安全评估； d）依法适用个人信息出境标准合同的，与境外接收方订立标准合同，并按照规定向所在地省级网信部门备案；依法适用个人信息出境认证的，按照规定申请认证； e）按照法律法规要求与境外接收方明确数据安全和个人信息保护责任义务，并采取必要管理和技术措施保障出境数据安全； f）不得采取数量拆分等手段，将依法应当申报数据出境安全评估的数据出境事项拆分处理、规避安全评估。
二级	a）建立数据跨境传输专项合规管理制度，覆盖出境场景识别、合规路径选择、安全评估申报、标准合同备案、认证管理等环节 b）建立数据出境风险自评估机制，按《数据出境安全评估办法》要求开展出境风险自评估，形成自评估报告 c）建立数据出境持续合规监测机制，对出境后数据的安全状况和境外接收方履约情况进行跟踪监督 d）建立境外接收方数据保护能力评估机制，评估境外接收方所在国家或地区的数据安全保护政策法规和网络安全环境
三级	a）建立数据出境合规量化评估体系，采用技术工具实现出境数据自动识别和合规校验 b）建立行业级数据跨境流通合规方案

B.6 S5 公共数据授权运营

触发条件：获得公共收数据授权运营的运营机构。

合规依据：

- 《公共数据资源授权运营实施规范（试行）》；
- 《公共数据资源登记管理暂行办法》；
- 《公共数据资源授权运营监测评估指南》（征求意见）；
- 《公共数据资源登记实施指南（征求意见稿）》。

等级增量要求：

等级	增量要求
一级	a）依法取得公共数据授权运营资格，按照授权运营协议约定的范围、方式和期限开展运营活动 b）按要求进行公共数据资源登记 c）在授权范围内开展数据加工运营，不得直接或间接参与授权范围内已交付的公共数据产品和服务再开发 d）建立公共数据运营安全管理制度，采取数据安全、个人信息保护措施和应急处置措施 e）依法接受对授权运营活动的监督评估，定期向社会披露公共数据资源使用情况
二级	a）建立公共数据授权运营专项合规管理制度，明确授权管理、数据治理、产品和服务开发、安全管理、登记披露、价格管理和监督检查等管理要求； b）建立公共数据运营全流程合规管控机制，覆盖数据采集、加工处理、产品开发、对外提供各环节； c）建立公共数据产品和服务合规审查机制，确保数据产品来源合规、加工正当、权属清晰，并通过公共数据资源登记平台进行登记； d）建立授权运营情况定期报告机制，按规定向实施机构和数据管理部门报告运营情况； e）建立运营风险识别与处置机制，对数据安全、个人信息保护、反垄断等风险进行识别和管控。
三级	a）建立授权运营合规量化评估体系，实现运营活动的实时监测和数据流通全程可追溯； b）运用技术工具对公共数据资源加工、产品开发和对外提供等活动实施自动化监测和合规校验，对超范围使用、异常访问、违规流转等风险进行自动识别和预警； c）形成公共数据授权运营合规行业方案

B.7 S6 生成式AI数据合规

触发条件：提供生成式人工智能服务涉及数据处理的。

合规依据：

- 《生成式人工智能服务管理暂行办法》；
- 《生成式人工智能服务安全基本要求》；
- 《人工智能生成合成内容标识办法》；
- 《中华人民共和国个人信息保护法》。

等级增量要求：

等级	增量要求
一级	a）使用合法数据源训练 AI 模型； b）开展训练数据标注的合规管理； c）采取必要措施防范生成违法违规内容；发现违法内容或者发现使用者利用生成式人工智能服务从事违法活动的，依法采取停止生成、停止传输、消除、限制服务、模型优化整改、记录保存和报告等相应处置措施；； d）按照国家有关规定对人工智能生成合成内容添加显式标识和隐式标识，并在用户服务协议中明确有关标识规则； e）不得采用技术手段删除、篡改、伪造、隐匿生成合成内容标识； g）提供具有舆论属性或者社会动员能力的生成式人工智能服务的，按照国家有关规定履行安全评估、算法备案或者登记等相关程序。
二级	a）建立 AI 训练数据全生命周期合规管理制度，覆盖数据来源审查、标注质量管控、标注安全审查； b）建立用户输入信息保护机制，不得非法留存用户输入的敏感信息； c）建立违法内容处置与整改闭环机制，覆盖监测发现、停止生成与传输、消除处置、模型优化训练整改、主管部门报告、记录保存全流程； f）建立生成合成内容标识管理机制，对标识生成、添加、展示、传递、日志记录和异常处置等活动进行统一管理和定期检查。
三级	a）建立生成式 AI 数据合规量化评估体系，实现训练数据合规性的自动化审查和内容安全智能检测； b）形成行业级生成式 AI 数据合规方案； c）运用智能化技术对生成内容安全风险进行持续监测和分析，实现违法违规内容及其他高风险内容的自动识别、预警和辅助处置； d）应用标识加固与内容溯源技术，提升标识抗删除篡改能力和生成内容全流程可追溯能力。

B.8 S7 人类遗传资源与生物安全数据管理

触发条件：采集、保藏、利用人类遗传资源或对外提供人类遗传资源材料的；采集、保藏、利用我国生物资源（含动植物遗传资源、病原微生物数据等）或对外提供生物资源数据的。

合规依据：

- 《中华人民共和国生物安全法》；
- 《中华人民共和国人类遗传资源管理条例》；
- 《人类遗传资源管理条例实施细则》；
- 《病原微生物实验室生物安全管理条例》。

等级增量要求：

等级	增量要求
一级	a）采集、保藏中国人类遗传资源应获得审批； b）保藏中国人类遗传资源应获得审批； c）利用人类遗传资源开展国际合作科学研究应获得审批或备案； d）将人类遗传资源材料对外提供应获得审批； e）境外组织、个人及其设立或实际控制的机构不得在境内采集、保藏我国人类遗传资源和生物资源； f）将人类遗传资源信息向境外组织、个人及其设立或实际控制的机构提供或开放使用的，应向国务院有关部门事先报告并提交信息备份。
二级	a）建立人类遗传资源与生物资源安全专项管理制度，明确资源识别、采集、保藏、利用、对外提供、退出处置以及安全事件处置等管理要求； b）建立人类遗传资源和生物资源使用情况定期检查机制，对超范围使用、未经授权提供、许可或者备案事项变更等风险进行识别、整改和跟踪。
三级	a）建立人类遗传资源与生物资源数据安全管理评估体系，实现资源使用情况的动态监测和合规预警； b）形成行业级人类遗传资源与生物安全数据合规管理方案。

B.9 S8 地理信息数据管理

触发条件：采集、存储、使用高精度地理信息数据，或向境外提供测绘地理信息成果的。

合规依据：

- 《中华人民共和国测绘法》；
- 《中华人民共和国测绘成果管理条例》；
- 《地图管理条例》；
- 《卫星导航定位基准站管理办法》；
- 《自然资源部非涉密测绘地理信息成果管理办法》；
- 《中华人民共和国个人信息保护法》；
- 《关于加强智能网联汽车有关测绘地理信息安全管理的通知》；
- 《数据出境安全评估办法》。

等级增量要求：

等级	增量要求
一级	a）地理信息数据采集主体应具备相应测绘资质； b）重要地理信息数据应在境内存储； c）向境外提供属于重要数据的地理信息成果应通过数据出境安全评估； d）涉及军事管理区、国防科工单位等敏感区域的地理信息数据禁止对外提供； e）不得擅自公布重要地理信息数据；在依法需要使用重要地理信息数据的活动中，使用依法审核公布的数据；

等级	增量要求
二级	a）建立地理信息数据分类分级管理制度，区分核心数据、重要数据和一般数据实施分级防护； b）建立高精度地理数据加密传输与访问控制机制，采用国家规定的密码保护措施； c）建立地理信息数据对外提供审批流程和数据安全协议签署机制; d）对测绘资质有效性、数据采集范围合规性进行定期审查
三级	a）建立地理信息数据合规评估体系，实现地理信息数据采集、存储、使用、出境的全流程动态监测和合规预警； b）形成行业级地理信息数据合规管理方案。

参 考 文 献

[1] GB/T 36073—2025 数据管理能力成熟度评估模型
[2] 《中华人民共和国网络安全法》（2016 年）
[3] 《中华人民共和国数据安全法》（2021 年）
[4] 《中华人民共和国个人信息保护法》（2021 年）
[5] 《网络数据安全管理条例》（2025 年）
[6] 《关于构建数据基础制度更好发挥数据要素作用的意见》（中共中央、国务院，2022 年）
[7] 《关键信息基础设施安全保护条例》（国务院令第 745 号，2021 年）
[8] 《中华人民共和国人类遗传资源管理条例》（国务院令第 717 号，2019 年）
[9] 《公共数据资源授权运营实施规范（试行）》（发改数据规〔2025〕27 号）
[10] 《数据出境安全评估办法》（国家网信办，2022 年 9 月）
[11] 《个人信息出境标准合同办法》（国家网信办，2023 年 2 月）
[12] 《生成式人工智能服务管理暂行办法》（国家网信办等七部门，2023 年 7 月）
[13] 《中华人民共和国测绘法》（2017 年修订）
[14] 《中华人民共和国测绘成果管理条例》（国务院令第 488 号）
[15] 《地图管理条例》（国务院令第 664 号，2016 年）
[16] 《中华人民共和国生物安全法》（2021 年）
[17] 《病原微生物实验室生物安全管理条例》（国务院令第 424 号）
[18] 《卫星导航定位基准站管理办法》（自然资源部，2026 年）
[19] 《数据产权登记工作指引（试行）》（国家数据局，2026 年 7 月）
[20] 《网络数据安全风险评估办法》（网信办、工信部、公安部三部门令第 24 号，2026 年）
[21] 《促进和规范数据跨境流动规定》（网信办令第 16 号，2024 年 3 月）