# 数据治理技术规范

文件编号：DNI-GZ-JS-87

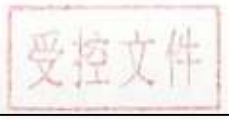
技术规范编号：CTS DNI-DG01

文档版本：A/0

编制：技术部　　日期：2026.01.04

审核：杨舒　　日期：2026.01.04

批准：杨舒　　日期：2026.01.04

受控状态： 


发布日期：2026.01.04　　实施日期：2026.01.04

发布单位：数网信认证服务（北京）有限公司

# 变更履历

| 日期 | 变更描述 | 版本/版次 | 审核 | 批准 |
| --- | --- | --- | --- | --- |
| 2026.01.04 | 初始发布 | A/0 | 杨舒 | 杨舒 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# 目录

1.适用范围 ..... 4
2.规范性引用文件 ..... 4
3.术语与定义 ..... 4
4.数据治理机构和数据治理机制 ..... 6
4.1 数据治理机构的角色、岗位职责 ..... 6
4.2 数据治理机构的角色权限 ..... 8
4.3 数据治理机制 ..... 8
5.数据治理的具体要求 ..... 8
5.1 总则 ..... 8
5.2 评估 ..... 9
5.3 指导 ..... 9
5.4 监控 ..... 10
6.绩效评价 ..... 10
6.1 监视、测量、分析和评价 ..... 10
6.2 内部审核 ..... 11
6.3 管理评审 ..... 12
7.改进 ..... 13
7.1 事件、不符合和纠正措施 ..... 13
7.2 持续改进 ..... 14
附录 A:数据治理过程与数据管理过程的具体要求 ..... 15

## 1.适用范围

本技术规范适用于所有组织的数据治理机构（可由所有者、董事、合伙人、执行经理或类似人员组成），包括公共和私营公司、政府实体和非营利组织，无论其对数据的依赖程度如何。

数据治理不同于数据管理，因此本技术规范仅对评估、指导和监控数据的使用（数据的使用包括但不限于：由 IT 系统创建、收集、存储或控制的数据的当前和未来使用，并影响与数据相关的管理流程和决策）活动提出要求，不对数据管理活动规定要求。

## 2.规范性引用文件

以下文件在本技术规范中的引用方式应使其部分或全部内容构成本文件的要求。凡是注日期的引用文件，仅注日期的版本适用于技术规范。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本技术规范。

ISO 38505-1:2017《信息技术 IT 治理 数据治理 第 1 部分:ISO/IEC 38500 在数据治理中的应用》

ISO/IEC 38500《信息技术 组织的 IT 治理》

ISO/IEC/TS 38501

ISO/IEC/TR 38502

## 3.术语与定义

在本技术规范中，引用 ISO/IEC 38500 给出的术语和定义

**3.1 匿名化** anonymization

个人可识别信息（PII）被不可逆转地改变的过程，使得个人可识别信息的主体不再能够被 PII 控制者单独或与任何其他方合作直接或间接地识别

**3.2 大数据** big data

具有特征的数据集（例如，体积、速度、多样性、可变性、准确性等）在给定时间点的特定问题领域无法使用当前/现有/已建立/传统的工艺和技术进行有效处理，以便提取价值

**3.3 云计算** cloud computing

通过自助资源调配和按需管理，实现对可共享物理或虚拟资源的可扩展弹性池的网络访问的实例

**3.4 数据责任** data accountability

数据及其使用的责任,包括数据责任图中的：收集、存储、报告、决定、分发、处置

**3.5 去标识** de-identification

消除一组识别数据与数据主体之间关联的任何过程的通用术语

**3.6 机器学习** machine learning

使用算法而不是程序编码进行处理，从而能够从现有数据中学习，从而预测未来的结果。

假名化 pseudonymization

适用于个人可识别信息（PII）的流程，该流程使用别名替换识别信息

注 1：可由 PII 主体自己或 PII 控制者执行假名化。PII 主体可以使用假名来一致地使用资源或服务，而不向该资源或服务（或服务之间）透露其身份，同时仍对该使用负责。

注 2：假名化不排除除假名化数据的 PII 控制者外，可能存在（一组受限的）隐私利益相关者，这些利益相关者能够根据假名化的数据和与之相关的数据确定 PII 主体的身份。

**3.7 个人可识别信息** personally identifiable information PII

（a）可用于识别与该信息相关的 PII 主体的任何信息，或（b）与或可能与 PII 主体直接或间接关联的任何信息

注 1：为确定 PII 主体是否可识别，应考虑持有数据的隐私利益相关方或任何其他方可合理使用的识别特定自然人所有手段。

**3.8 PII 主体** PII principal

与个人身份信息（PII）关联的自然人

注 1：根据管辖权和特定的数据保护和隐私立法，也可以使用同义词“数据主体”代替术语“PII 主体”。

[来源：ISO/IEC 29100:2011，2.11]

GB/T 34960.1 界定的以及下列术语和定义适用于本文件。

**3.9 数据治理** data governance

数据资源及其应用过程中相关管控活动，绩效和风险管理的集合，包括“EDM”模型中的评估、指导、监控活动。

**3.10 数据管理** data management

数据资源获取，控制，价值提升等活动的集合，包括数据责任图中的：收集、存储、报告、决定、分发、处置。

**3.11 数据资产** data asset

组织拥有和控制的，能够产生效益的数据资源。

**3.12 数据战略** data strategy

组织开展数据工作的愿景和高阶指引。

**3.13 数据架构** data architecture

数据要素，结构和接口等抽象及其相互关系的框架。

**3.14 元数据** metadata

定义和描述其他数据的数据。

**3.15 数据生存周期** data life cycle

数据获取，存储，整合，分析，应用，呈现，归档和销毁等各种生存形态演变的过程。

**3.16 数据管理生命周期** Data Management Life Cycle

包括：收集、存储、处理、分发、共享、删除等。

## 4.数据治理机构和数据治理机制

### 4.1 数据治理机构的角色、岗位职责

数据治理机构的角色、岗位职责应包括“EDM”模型中的“评估—指导—监控”三个主要任务所需的角色和对应的岗位职责。

4.1.1 数据治理的指导角色，包括对数据战略和政策制定、实施、改进等管理活动的指导，具体职责应：

—包括解决当前和未来总体战略目标的数据使用计划；

—考虑到技术进步和市场预期；

—覆盖数据责任图的所有部分；

—考虑数据治理的特定方面（价值、风险、约束）；

—设定一个预期，即可能需要修改总体战略，以考虑新的机会或风险。

4.1.2 组织使用数据相关的责任的监督角色，其职责包括应确保组织内部人员理解并接受其责任。这些责任包括：

—扩展到整个组织，超出 IT 职能或部门，或 IT 发起的活动；

—包括与商业活动相关的关键数据，如营销，其中的数据用于通知产品计划，以及产品开发，其中的数据用于指导新产品的设计和制造；

—包括数据本身是组织提供的产品或服务的情况。这些情况包括音乐或电影等内容以及天气或股市报告等信息；

—覆盖数据的整个生命周期。

4.1.3 数据治理目标的治理角色，其职责包括对目标的策划、分解和考核进行治理，数据治理目标应包括：

—数据使用对组织内决策的支持程度；

—如果与供应商或客户共享数据，数据使用对其决策的支持程度；

—组织内新数据集和数据流的采用率；

—数据的投资回报，包括已分发的数据；

—组织利用的数据总价值与竞争对手或同类组织利用的价值之比。

4.1.4 数据及其使用相关合规义务管理的治理角色，其职责包括应确保组织了解并遵守外部义务，并正确定义、实施和确保遵守适当的内部政策。此类义务和政策应包括：

—所有数据集和数据流应根据满足组织需求和义务的安全策略进行安全保护；

—正确处理 PII；

—在整个组织内适当实施数据保留政策和做法；

—了解与数据相关的所有法律义务，并保证这些义务已在整个组织内得到履行。

4.1.5 组织内数据的使用评估角色，其职责包括审查并判断当前和未来数据的使用情况。这包括：

—数据及相关技术和流程的内部使用，

—竞争对手、其他组织、政府和个人使用数据，

—评估不断变化的法律、法规、社会期望以及

—控制和影响数据使用的其他因素。

4.1.6 组织内数据的使用监控角色，主要职责应包括对数据责任图中的收集、存储、报告、决定、分发、处置活动进行治理监控，治理监控应通过适当的测量体系，监控本组织数据使用的绩效。应测量报告和分析工具用于决策的情况，以了解数据的价值并改进决策过程。由于战略或法规的原因，治理机构的监督可能具有高度重要性的其他领域包括：

—PII 的使用，包括隐私问题、要求同意和数据使用的透明度（见 ISO/IEC 29100）；

—使用有效的信息安全管理体系（如 ISO/IEC 27001 所述），以反映数据的战略重要性。这应该扩展到包括第三方数据源和云计算服务中的数据管理（例如，ISO/IEC 27017）。这些国际标准为信息安全控制提供了指南，但在某些情况下，此类控制将不够充分，治理机构将需要依赖信任和验证；

—数据保留和处置要求；

—重复使用、共享或出售数据及其相关权利、许可或版权；

—在决策过程中适当考虑文化规范、偏见、歧视或压型（profiling）。

### 4.2 数据治理机构的角色权限

治理机构中各角色的权限应清晰、明确，应保持文件化信息，必要时应时行评审和更新。

### 4.3 数据治理机制

治理机构应建立适用于业务对数据依赖程度的数据管理监督机制。治理机构应该清楚地了解数据对组织业务战略的重要性，以及使用这些数据对组织的潜在战略风险。

治理机构对数据的关注程度应基于这些因素。治理机构应确保其成员和相关管理机制（如审计、风险管理和相关委员会）以及管理人员对数据的重要性具有必要的知识和理解。治理机构可设立一个小组委员会，以协助治理机构从战略角度监督组织对数据的使用。成立小组委员会的必要性将取决于数据对组织的重要性及其规模。治理机构应确保为数据的治理和管理建立适当的治理框架。治理机构应通过要求审计和独立评估等流程来确保治理有效，从而监测数据治理和管理机制的有效性。

## 5.数据治理的具体要求

### 5.1 总则

数据治理活动包括“EDM”模型中的评估、指导、监控活动，应分别从数据的价值、风险、限制 3 个特定方面（维度）对数据管理活动（收集、存储、报告、决定、分发、处置）进行数据治理。

### 5.2 评估

在评估组织的数据治理时，治理机构应考虑组织的内部要求和外部压力。

此外，治理机构应审查并判断当前和未来数据的使用情况。这包括：

—数据及相关技术和流程的内部使用，

—竞争对手、其他组织、政府和个人使用数据，

—评估不断变化的法律、法规、社会期望以及

—控制和影响数据使用的其他因素。

数据管理技术正在迅速变化，治理机构应征求管理人员的建议，以解释这些技术及其对组织的潜在影响。这些技术可以对所有数据方面产生重大影响，包括成本、洞察力和隐私。在许多情况下，这些影响可能超出数据管理的范围，并可能为组织提供新的商业机会，以及潜在的更大风险。由于不利用这些机会，治理机构可能会面临更多来自竞争对手的风险，改变市场预期，增加合规问题。

治理机构还应了解本组织的数据管理能力。例如：

—组织从数据泄露中恢复的程度；

—以正确的格式提供正确信息以帮助各级决策的容易程度；

—组织是否利用云计算等新技术来增强自身能力。只有当组织拥有实施这些策略所需的资源和能力时，才能实施数据治理的战略和策略。

### 5.3 指导

治理机构应指定责任人并指导战略和政策的制定和实施。组织当前和未来的数据使用战略和政策应旨在：

—最大化组织对数据的投资价值：与组织内的任何资产一样，数据也需要投资。无论数据是从组织外部收集、存储在第三方还是作为服务使用，都是如此。和任何投资一样，组织将希望确保从数据中获得良好的回报。数据的最终价值在于它的使用如何改善决策，但一个组织也可以出售数据供他人使用。

—根据数据风险偏好管理与数据相关的风险：一些数据（如产品研究或未披露的股市目标）具有较高的商业价值，需要应用适当的资源来利用和保护这些数据。与管理这些数据相关的价值和风险高于其他类型的数据，战略和政策应通过采用数据分类方案来反映这一点。

—确保数据管理的正确水平：治理机构对数据及其使用负责，包括根据这些数据做出的决策。因此，

数据活动相关责任应在组织内适当委派。

这些要素都有助于组织的“信息态度”，以及将数据应用于组织业务目标的有效性。这反映了一个组织的数据文化、整体战略、风险偏好、感知的安全级别、基于知识的工作量，以及对数据及其使用的衡量标准和价值。

### 5.4 监控

治理机构应通过适当的测量体系，监控本组织数据使用的绩效。他们应该能够向自己保证，与数据相关的策略正在正确实施，数据的使用和管理符合内部政策和外部要求，如法规和数据管理要求。

应测量报告和分析工具用于决策的情况，以了解数据的价值并改进决策过程。由于战略或法规的原因，治理机构的监督可能具有高度重要性的其他领域包括：

—PII 的使用，包括隐私问题、要求同意和数据使用的透明度（见 ISO/IEC 29100）；

—使用有效的信息安全管理体系（如 ISO/IEC 27001 所述），以反映数据的战略重要性。这应该扩展到包括第三方数据源和云计算服务中的数据管理（例如，ISO/IEC 27017）。这些国际标准为信息安全控制提供了指南，但在某些情况下，此类控制将不够充分，治理机构将需要依赖信任和验证；

—数据保留和处置要求；

—重复使用、共享或出售数据及其相关权利、许可或版权；

—在决策过程中适当考虑文化规范、偏见、歧视或压型（profiling）。

## 6.绩效评价

### 6.1 监视、测量、分析和评价

6.1.1 总则

组织应建立、实施和保持一个过程，用以监视、测量、分析和评价。

组织应确定：

a) 需要监视和测量的内容，包括：

1) 适用的法律法规要求和其它要求；

2) 内部要求和外部压力的变化；

3) 评估、指导、监控数据治理活动的实施情况：

4）数据治理目标的策划、考核情况；

b）组织评价其数据治理绩效所依据的准则；

c）适用时，监视、测拭、分析与评价的方法，以确保有效的结果；

d）何时应实施监视和测量；

e）何时应分析、评价和沟通监视和测量结果。

组织应评价其数据治理绩效并确定数据治理管理体系的有效性。

组织应保留适当的文件化信息，作为监视、测量、分析和评价结果的证据。

6.1.2 法律法规要求和其他要求的合规性评价

组织应策划、建立、实施和保持一个过程，以评价适用的法律法规要求和其他要求的符合性。（见6.1.3).

组织应：

a）确定评价合规性的频次和方法；

b）评价合规性；

c）必要时按照 7.1 采取措施；

d）保持其法律法规要求和其他要求的合规情况的知识和理解；

e）保留合规性评价结果的文件化信息。

## 6.2 内部审核

6.2.1 内部审核目标

组织应按计划的时间间隔实施内部审核，以提供下列数据治理管理体系的信息：

a）是否符合：

1）组织自身数据治理管理体系的要求，包括数据治理方针和数据治理目标；

2）本标准的要求；

b）是否得到了有效的实施和保持。

6.2.2 内部审核过程

组织应：

a）策划、建立、实施并保持一个或多个内部审核方案，包括实施审核的频次、方法、职责、协商、

策划要求和报告。策划、建立、实施和保持内部审核方案时，组织除了应考虑相关过程的重要性和以往审核的结果外，还应考虑：

1）影响组织的重要变更；

2）绩效评价和改进结果；

3）内部要求与外部压力相关的风险和机遇的应对措施的有效性；

b）规定每次审核的准则和范围；

c）选择胜任的审核员并实施审核，确保审核过程的客观性与公正性；

d）确保向相关管理者报告审核结果；

e）采取适当的措施应对不符合和持续改进其数据治理绩效；

g）组织应保留文件化信息，作为审核方案实施和审核结果的证据。

注： 有关审核的更多信息，参考 GB/T19011 管理体系审核指南。

**6.3 管理评审**

最高管理者应按计划的时间间隔对组织的数据治理管理体系进行评审，以确保其持续的适宜性、充分性和有效性。

管理评审应包括对下列事项的考虑：

a）以往管理评审所采取措施的状况；

b）与数据治理管理体系相关的内外部问题的变更，包括：

1）适用的法律法规要求和其他要求；

2）组织的数据治理风险和数据治理机遇；

c）数据治理方针和数据治理目标的满足程度；

d）数据治理绩效方面的信息，包括以下方面的趋势：

1）事件、不符合、纠正措施和持续改进；

2）员工参与和协商的输出；

3）监视和测量的结果；

4）审核结果；

S）合规性评价的结果；

6）数据治理风险和数据治理机遇。

e）与相关方的有关沟通；

f）持续改进的机遇；

g）为保持有效的数据治理管理体系所需的资源的充分性；

管理评审的输出应包括与以下方面相关的决策：

—对数据治理管理体系的待续适宜性、充分性和有效性的结论；

—持续改进机遇；

—数据治理管理体系变更的任何需求，包括所需的资源；

—目标未满足时需要采取的措施。

组织应向其相关的员工及员工代表（如有）沟通（见 7.4.)管理评审的相关输出。

组织应保留文件化信息，作为管理评审结果的证据。

## 7.改进

### 7.1 事件、不符合和纠正措施

组织应策划、建立、实施和保持一个过程，以管理事件和不符合，包括报告、调查和采取措施。

当发生串件或不符合时，组织应：

a）对事件或不符合作出及时反应，并且适用时：

1）直接采取措施控制并纠正该事件或不符合；

2）处理后果；

b）评价消除事件或不符合根本原因的措施需求，以防止不符合再次发生或在其他地方发生，通过以下方式评价：

1）评审事件或不符合；

2）确定事件或不符合的原因；

3）确定是否存在或是否可能发生类似的事件或不符合；

c）适当时，评审数据治理风险的评价请况

d）确定并实施与控制层级和变更管理相一致的任何所需的措施，包括纠正措施；

e）评审所采取的任何纠正措施的有效性；

f）必要时，对数据治理管理体系进行变更。

纠正措施应与所发生的事件或不符合造成的影响或潜在影响相适应。

组织应保留文件化信息作为下列事项的证据：

—事件或不符合的性质和所采取的任何后续措施；

—任何纠正措施的结果，包括所采取措施的有效性。

## 7.2 持续改进

7.2.1 持续改进目标

组织应持续改进数据治理管理体系的适宜性、充分性与有效性，以：

a）预防事件和不符合的发生；

b）宣传正面的数据治理文化；

c）提升数据治理绩效。

适当时，组织应确保员工参与实施其持续改进目标。

7.2.2 持续改进过程

组织应在考虑本标准描述的活动的输出的基础上，策划、建立、实施和保持一个或多个持续改进过程。

组织应与其相关的员工及员工代表（如有）沟通持续改进的结果。

组织应保留文件化信息，作为持续改进的证据。

## 附录 A:数据治理过程与数据管理过程的具体要求

| | 价值 | 风险 | 限制 |
|---|---|---|---|
| 收集 | [V1]治理机构应决定组织将在多大程度上利用或数据变现以实现其战略目标。 | [R1]治理机构应认识到与数据收集和使用相关的风险，并在组织的总体风险偏好范围内同意其数据风险的可接受水平。这应包括检查不收集和使用数据的风险。 | [C1]治理机构应在批准数据收集政策时，考虑质量、隐私、同意要求和使用透明度等约束。 |
| 存储 | [V2]治理机构应批准为数据存储和数据订阅分配适当资源的政策，以便提取数据的潜在价值。 | [R2]治理机构应指导管理人员确保 ISMS 已到位，并延伸至数据和技术供应商，拥有足够的资源、控制和信任，以确保不超过风险偏好水平。 | [C2]治理机构应指导管理人员确保数据存储实践（包括第三方数据订阅）符合数据收集限制。 |
| 报告 | [V3]治理机构应指导管理者使用必要的工具和技术，以确保数据的全部价值能够被提取出来。 | [R3]治理机构应确定数据背景（包括文化规范）的重要性及其潜在的总体误解。 | [C3]治理机构应确定数据及其约束之间关系的重要性，尤其是如果数据是从不同的数据集聚合而来的。 |
| 决定 | [V4]治理机构应确保组织的数据文化与其数据战略相一致，包括数据访问实践、数据支持决策制定和组织从决策过程中学习等行为。 | [R4]应在报告中提供适当的数据和格式，以便进行自动化或人工决策。在对这些决策负责的同时，治理机构应适当地为组织和可接受的数据风险水平委派决策责任。 | [C4]作为新数据，决定过程的输出将有其自身的价值、风险和约束，管理机构应设定对决定过程和相关责任的期望。 |
| 分发 | [V5]治理机构应制定数据分发策略，使组织能够满足组织的战略计划。 | [R5]治理机构应确保管理人员实施了充分的控制措施，以防止不当分配。 | [C5]治理机构应确保适当的分发权得到落实，并得到第三方的尊重。 |
| 处置 | [V6]治理机构应批准允许在数据不再有价值或无法保存时处置数据的策略。 | [R6]治理机构应指导管理人员实施适当的数据处置流程，包括安全和永久销毁数据等控制措施。 | [C6]治理机构应监控数据保留和处置义务，并确保实施了适当的流程。 |