Q/BJKB

北京坤标检验认证有限公司企业标准

Q/BJKB 003-2026

数据治理管理体系 基本要求

Data Governance Management System - Basic Requirements

2026-4-1 发布　　2026-4-1 实施

北京坤标检验认证有限公司　　发　布

目　　次

前　言

所有组织均会使用数据，且大部分数据通过信息技术系统以电子形式存储。随着云计算的出现、物联网潜力的释放以及大数据分析的日益普及，数据的生成、收集、存储和挖掘以获取有用信息的过程变得愈发便捷。海量数据的涌现，要求治理机构切实履行职责，抓住宝贵机遇，同时保护和保障敏感数据安全，这一要求与职责已刻不容缓。

制定本文件，旨在为治理机构成员提供指导，使其采用基于原则的方法开展数据治理，提升数据价值，降低与数据相关的风险。ISO/IEC 38500 为组织治理机构提供了指导其当前信息技术（IT）使用及规划未来 IT 应用的原则和模型，本文件是对该标准的管理体系的基本要求。

本文件以落实数据治理义务为目标，以构建数据治理管理体系为核心，提出组织、领导作用、策划、支持、运行、绩效评价、改进等方面的数据治理管理要求，对组织及其最高管理者、员工、第三方合作伙伴开展数据治理工作确立了行为规范和边界。

本文件的主要适用对象为组织的治理机构，且适用于各类规模、各行业和领域的组织。本文件可以作为组织开展数据治理管理活动的依据，也可作为认证机构开展认证、法律从业者开展数据治理业务、组织开展第三方监督评估、政府开展数据治理的参考依据。同时，本文件可以作为数据治理能力成熟度评价有关数据合规方面的补充要求。

本标准按 GB/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》给出的规则起草。

本标准主要起草人：陈刚辉、杨英者、李英华。

数据治理管理体系 基本要求

1 范围

本标准规定了数据治理管理体系的术语和定义、基本要求等内容。

本标准适用于采用本标准在企业内部建立数据治理管理体系，也适用于北京坤标检验认证有限公司作为第三方认证机构对企业进行数据治理管理体系的评价。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本（包括所有的修改单）适用于本文件。

ISO/IEC 27001 信息安全、网络安全和隐私保护—信息安全管理体系 要求

ISO/IEC 38505-1 信息技术-信息技术的治理-数据治理-第 1 部分：ISO/IEC 38500 对数据管理的应用

ISO/IEC 38500 Information technology — Governance of IT for the organization

3 术语和定义

下列术语和定义适用于本文件。

GB/T 27000、ISO/IEC 38505-1（第 3 章）界定的术语和定义适用于本文件。

4 组织的背景

4.1 了解组织和其背景

组织应确定与其目的相关的、影响其实现数据治理管理体系预期结果能力的外部和内部问题。

4.2 了解有关各方的需求和期望

组织应确定:

a) 与数据治理管理体系有关的有关各方。

b) 这些相关方的相关要求。

c) 这些要求中的哪些将通过数据治理管理体系来解决。

4.3 确定数据治理管理体系范围

4.1.1 组织应确定数据治理管理体系的边界和适用性以建立其范围。

4.1.2 当确定范围时，组织应考虑组织实施活动之间及与其他组织间实际活动的接口和依赖关系。

4.1.3 范围应形成文件化信息并可获得。

4.4 数据治理管理体系

4.2.1 组织应根据本文件要求，建立、实施、维护和持续改进数据治理管理体系，包括所需过程及其相互作用。

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，证实其对数据治理管理体系的领导作用和承诺：

a) 确保建立数据治理方针和数据治理目标，并与组织的战略方向相一致；
b) 确保将数据治理管理体系的要求融入组织的过程中；
c) 确保数据治理管理体系所需的资源是可获得的；
d) 沟通有效的数据治理管理和符合数据治理管理体系要求的重要性；
e) 确保数据治理管理体系实现其预期结果；
f) 促使人员积极参与，指导和支持他们为数据治理管理体系的有效性作出贡献；
g) 推动改进；
h) 支持其他相关管理者在其职责范围内发挥领导作用。

组织应满足 ISO/IEC 38505-1 第 4 章对数据的良好管理 4.2 理事机构的责任、4.3 理事机构和监督机制中要求。

5.2 方针

最高管理者应制定、实施和保持数据治理方针，数据治理方针应：

a) 与组织的宗旨相事宜；
b) 为建立数据治理目标提供框架；
c) 包括满足适用要求的承诺；
d) 包括持续改进数据治理管理体系的承诺。

数据治理方针应：

a) 可获取并保持成文信息；
b) 在组织内得到沟通、理解和应用；
c) 适宜时，可为有关相关方所获取。

5.3 组织的岗位、职责和权限

5.3.1 最高管理者应确保组织相关岗位的职责、权限得到分配、沟通和理解。

5.3.2 最高管理者应分配职责和权限，以：

a) 确保数据治理管理体系符合本文件的要求；
b) 报告数据治理管理体系的绩效以及改进机会，特别是向最高管理者报告。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

在策划数据治理管理体系时，组织应确定需要应对的风险和机遇，以：

a) 确保数据治理管理体系能够实现其预期结果；
b) 预防或减少不利影响；
c) 实现改进。

组织应策划：

a) 应对这些风险和机遇的措施；
b) 如何 ：
    1) 在数据治理管理体系过程中整合并实施这些措施；

2） 评价这些措施的有效性。

6.1.2 数据治理风险评价

组织应确定和实施数据治理风险评估过程，以：

a） 建立并维护数据治理风险准则，包括：

1）风险可接受准则；

2）实施数据治理风险评估准则。

b） 确保重复的数据治理风险评估产生一致、有效和可比较的结果。

c） 识别数据治理风险：

1） 实施数据治理风险评估过程以识别以数据治理管理体系范围内与数据的保密性、完整性和可用性损失有关的风险；

2）识别风险所有者。

d） 分析数据治理风险：

1）评估 6.1.2c)1)中所识别的风险发生后，可能导致的潜在后果；

2）评估 6.1.2c)1)中所识别的风险实际发生的可能性；

3）确定风险级别。

e） 评价数据治理风险：

1）将风险分析的结果与 6.1.2a)中建立的风险准则进行比较；

2）为风险处置排序已分析风险的优先级。

组织应保留有关数据治理风险评估过程的文件化信息。

6.1.3 数据治理风险处置

组织应确定并实施数据治理风险处置过程，以：

a） 在风险评估结果的基础上，选择适当的数据治理风险处置选项；

b） 确定实现已选的数据治理风险处置选项所必需的所有控制；

注 1：当需要时，组织可设计控制，或识别来自任何来源的控制。

c） 制定一个适用性声明，包括：

——必要的控制；

——包含这些控制的正当理由；

——是否实施了所必需的控制；

d） 制定正式的数据治理风险处置计划；

e） 获得风险所有者对数据治理风险处置计划以及对数据治理残余风险接受的批准。

组织应保留有关数据治理风险处置过程的文件化信息。

注 4：本文件中的数据治理风险评估与处置过程与 ISO 31000 中给出的原则和通用指南相匹配。

6.1.4 组织应满足 ISO/IEC 38505-1 第 5 章数据良好治理的原则、模型和特定方面中要求。

6.2 数据治理目标及实现的策划

组织应针对相关职能、层次和数据治理管理体系所需的过程建立数据治理目标。

数据治理目标应：

a） 与数据治理方针保持一致；

b） 可测量；

c） 考虑适用的要求，以及数据治理评估和数据治理处置的结果；

d） 予以监视；

e） 予以沟通；

f） 适时更新；

g） 作为文件化信息可获取。

组织应保持有关数据治理目标的成文信息。

策划如何实现数据治理目标时，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。

6.3 变更的策划

当组织确定需要变更数据治理管理体系时，变更应按计划的方式实施。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进数据治理管理体系所需的资源。

7.2 能力

组织应：

a) 确定在其控制下工作的人员所需具备的能力，这些人员从事的工作影响数据治理管理体系绩效和有效性；
b) 基于适当的教育、培训或经验，确保这些人员是胜任的；
c) 适用时，采取措施以获得所需的能力，并评价措施的有效性；
d) 保留适当的成文信息，作为人员能力的证据。

注：适用措施可包括对在职人员进行培训、辅导或重新分配工作，或者聘用、外包胜任的人员。

7.3 意识

组织应确保在其控制下工作的人员知晓：

a) 数据治理方针；
b) 他们对数据治理管理体系有效性的贡献，包括改进绩效的益处；
c) 不符合数据治理管理体系要求的后果。

7.4 沟通

组织应确定与数据治理管理体系相关的内部和外部沟通，包括：

a) 沟通什么；
b) 何时沟通；
c) 与谁沟通；
d) 怎么沟通。

7.5 成文信息

7.5.1 总则

组织的数据治理管理体系应包括：

a) 本文件要求的成文信息；
b) 组织所确定的、为确保数据治理管理体系有效性所需的成文信息。

注：对于不同组织，数据治理管理体系成文信息的多少与详路程度可以不同，取决于：

——组织的规模，以及活动、过程、产品和服务的类型；

——过程及其相互作用的复杂程度；

——人员的能力。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保适当的：

a) 标识和说明(如标题、日期、作者、索引编号)；

b) 形式(如语言、软件版本、图表)和载体(如纸质的、电子的)；

c) 评审和批准，以保持适宜性和充分性。

7.5.3 成文信息的控制

应控制数据治理管理体系和本文件所要求的成文信息，以确保：

a) 在需要的场合和时机，均可获得并适用；

b) 予以妥善保护(如防止泄密、不当使用或缺失)。

为控制成文信息，适用时，组织应进行下列活动：

a) 分发、访问、检索和使用；

b) 存储和防护，包括保持可读性；

c) 更改控制(如版本控制)；

d) 保留和处置。

对于组织确定的策划和运行数据治理管理体系所必需的来自外部的成文信息，组织应进行适当识别，并 予以控制。

注：对成文信息的“访问”可能意味着仅允许查阅，或者意味着允许查阅并授权修改。

8 运行

8.1 运行的策划和控制

8.1.1 为满足产品和服务提供的要求，并实施第 6 章所确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：

——建立过程准则；

——按照过程准则实施过程控制。

8.1.2 应在必要的范围和程度上提供文件化信息，以确信这些过程按计划得到执行。

8.1.3 组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

8.1.4 组织应确保外包过程是确定的和受控的。

8.1.4 组织应满足 ISO/IEC 38505-1 第 6 章数据责任中要求，数据环节包括不限于收集、存储、报告、决策、分发处置。

8.1.5 组织应满足 ISO/IEC 38505-1 第 7 章数据治理指南—原则中要求。

8.1.6 组织应满足 ISO/IEC 38505-1 第 9 章数据治理指南—数据特定方面中要求，包括价值、风险、约束三个数据特定方面的要求。

8.2 数据治理风险评估

组织应考虑 6.1.2a)所建立的准则，按计划的时间间隔，或当重大变更提出或发生时，执行数据治理风险评估。

组织应保留数据治理风险评估结果的文件化信息。

8.3 数据治理风险处置

组织应实施数据治理处置计划。

组织应保留数据治理风险处置结果的文件化信息。

8.4 符合性

组织应满足 ISO/IEC 38505-1 第 8 章数据治理指南—模型的要求。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 总则

组织应确定：

a) 需要监视和测量什么，包括数据治理过程和控制；

b) 适用时的监视、测量、分析和评价的方法，以确保结果有效。选择的方法应能产生可比较与可重现的结果以被认为是有效的；

c) 何时实施监视和测量；

d) 谁应监视和测量；

e) 何时对监视和测量的结果进行分析和评价；

f) 应分析和评价这些结果。

应提供文件化信息以作为结果的证据。

组织应评价数据治理绩效和数据治理管理体系的有效性。

组织应满足 ISO/IEC 38505-1 第 10 章对数据责任图谱的应用中要求。

9.2 内部审核

9.2.1 总则

组织应按照策划的时间间隔实施内部审核，以提供有关数据治理管理体系的以下信息，是否：

a) 符合：

1) 组织自身对数据治理管理体系要求；

2) 本文件的要求；

b) 得到有效的实施和保持。

9.2.2 内部审核

组织应策划、制定、实施和维护审核方案，包括审核频次、方法、职责、策划要求和报告；

制定内部审核方案时，组织应考虑相关过程的重要性和以往审核的结果。

组织应：

a) 规定每次审核的审核准则和范围；

b) 选择审核员并实施审核，确保审核过程的客观公正；

c) 确保将审核结果报告至相关管理者。

应提供文件化信息，作为实施审核方案以及审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理者应按照策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。

9.3.2 管理评审输入

策划和实施管理评审时应考虑下列内容：

a) 以往管理评审所采取措施的情况；

b) 与数据治理管理体系相关的相关方需求和期望的变化；

c) 下列有关数据治理管理体系绩效和有效性的信息，包括其趋势：

1） 不合格及纠正措施；
2） 监视和测量结果；
3） 审核结果；
4） 数据治理目标完成情况。

d） 相关方反馈；
e） 风险评估及风险处置计划的情况；
f） 持续改进的机会。

9.3.3 管理评审输出

管理评审的结果应包括与持续改进机会相关的决定以及变更数据治理管理体系的任何需求。

组织应提供文件化信息，以作为管理评审结果的证据。

10 改进

10.1 持续改进

组织应持续改进数据治理管理体系的适宜性、充分性和有效性。

10.2 不合格和纠正措施

10.2.1 当发生不符合时，组织应：

a） 对不符合做出应对，适用时：
1） 采取措施，以控制和纠正不符合；
2） 处理后果；

b） 通过下列活动，评价是否需要采取措施，以消除产生不符合的原因，避免其再次发生或在其他场合发生：
1） 评审不符合；
2） 确定不符合的原因；
3） 确定是否存在或可能发生类似的不符合；

c） 实施任何所需的措施；
d） 评审任何所采取纠正措施的有效性；
e） 必要时，对数据治理管理体系进行变更；

10.2.2 纠正措施应对不符合所产生的影响相适应。

10.2.3 应提供文件化信息以作为下列事项的证据：

a） 不符合的性质以及所采取的任何后续措施；
b） 任何纠正措施的结果。

参 考 文 献

[1] GB/T 19000 质量管理体系 基础和术语

[2] GB/T 19001—2016/ISO 质量管理体系 要求

[3] GB/T 19011 管理体系审核指南

[4] GB/T 27011 合格评定 认可机构要求

[5] GB/T 27021.1 合格评定 管理体系审核认证机构要求 第 1 部分：要求

[6] 国家认证认可监督管理委员会 2006 年第 3 号公告 认证技术规范管理办法

[7] GB/T 22081 信息技术 安全技术 信息安全控制实践指南

[8] ISO/IEC 27001 信息安全、网络安全和隐私保护—信息安全管理体系 要求

[9] ISO/IEC 27002 信息安全、网络安全和隐私保护-信息安全控制

[10] ISO/IEC 27003 信息技术 安全技术 信息安全管理体系实施指南

[11] ISO/IEC 27004 信息技术 安全技术 信息安全管理 测量

[12] ISO/IEC 27005 信息技术 安全技术 信息安全风险管理

[13] ISO 31000 风险管理 原则和指南

[14] ISO/IEC 27000 信息技术-安全技术-信息安全管理体系-概述和词汇

[15] ISO/IEC 38505-1 信息技术-信息技术的治理-数据治理-第 1 部分：ISO/IEC 38500 对数据管理的应用