数据治理应用管理体系

认证技术规范

文件编号：CTS TBGL145-2026

版本号：B/2

受控状态： （ 受控 ）

编写：技术部

审核：张辉根

批准：周春阳

首次发布：2022-12-20 **首次实施：2022-12-20** **修订实施日期：20260423**

江西腾标认证有限公司

目录

前言

本文件旨在为组织（以下简称“组织”）建立、实施、维护和持续改进数据治理应用管理体系（DGMS）提供要求和指南。本文件采用PDCA（策划-实施-检查-改进）循环模式，与 ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求》 的高阶结构保持一致，并充分融合了 GB/T 34960.5-2018《信息技术服务 治理 第5部分：数据治理规范》 的特定行业要求。

本文件旨在为组织在基于ISO/IEC 27001:2022建立和实施信息安全管理体系的过程中，提供一套专门的数据治理应用控制选择和实施指南。本文件的核心架构与ISO/IEC 27001:2022完全一致，组织可通过实施本文件，建立一个同时满足ISO/IEC 27001和GB/T 34960.5-2018要求的整合性管理体系。组织应首先建立满足ISO/IEC 27001要求的信息安全管理体系（ISMS），并在此基础上扩展数据治理应用管理要求。

1. 范围

本文件规定了组织建立、实施、保持和持续改进 数据治理应用管理体系 的要求。本文件适用于

1) 组织建立、实施、保持和改进 数据治理应用管理体系 管理方针和目标；
2) 认证机构对组织进行数据治理应用管理体系认证。

2. 规范性引用文件

下列文件对于本文件的应用必不可少。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 27000 信息技术 — 安全技术 — 信息安全管理体系 — 概述和词汇
- ISO/IEC 27001:2022 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 27002:2022 信息安全、网络安全和隐私保护 — 信息安全控制
- GB/T 34960.5-2018 信息技术服务 治理 第5部分：数据治理规范

注：认证审核时引用文件的有效性以审核实施时现行有效的最新版本为准。

3. 术语和定义

ISO/IEC 27000、ISO/IEC 27001:2022界定的以及下列术语和定义适用于本文件。ISO和IEC在以下地址维护用于标准化的术语数据库：

- ISO在线浏览平台：https://www.iso.org/obp
- IEC电子百科：https://www.electropedia.org/

3.1 数据治理

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。

[来源：GB/T 34960.5-2018, 3.1]

3.2 数据管理

数据资源获取、控制、价值提升等活动的集合。

[来源：GB/T 34960.5-2018, 3.2]

3.3 数据资产

组织拥有和控制的、能够产生效益的数据资源。

[来源：GB/T 34960.5-2018, 3.3]

3.4 数据战略

组织开展数据工作的愿景和高阶指引。

[来源：GB/T 34960.5-2018, 3.4]

3.5 数据架构

数据要素、结构和接口等抽象及其相互关系的框架。

[来源：GB/T 34960.5-2018, 3.5]

3.6 元数据

定义和描述其他数据的数据。

[来源：GB/T 34960.5-2018, 3.6]

3.7 数据生存周期

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。

[来源：GB/T 34960.5-2018, 3.7]

3.8 数据质量

数据满足规定或潜在需求的特性和特征的总和。

3.9 数据安全

通过采取必要的技术和管理措施，保护数据免受泄露、篡改、破坏和丢失。

4. 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其实现DGMS预期结果能力的外部和内部事项。

- **外部因素**：适用的数据保护法律和法规（如《数据安全法》、《个人信息保护法》、《网络安全法》等）、监管机构要求（如网信办、工信部、数据局等）、行业标准与最佳实践、市场对数据治理能力的要求、客户对数据安全和合规的期望、数据跨境传输的法律要求等。
- **内部因素**：组织的规模、治理结构、业务战略与数据战略的匹配度、数据资源的现状与价值、现有数据管理能力、人员数据意识与技能水平、组织文化对数据驱动决策的支持程度、以往数据相关风险事件记录等。

4.2 理解相关方的需求和期望

组织应确定：

a) 与DGMS有关的相关方；

b) 这些相关方的有关要求；

c) 哪些要求将通过DGMS予以解决。

相关方包括但不限于：监管机构、客户、合作伙伴、供应商、员工、股东、认证机构、公众。

组织应建立、实施并保持程序，以识别相关方，并促其参与到与DGMS相关的已识别的议题中。与相关方的沟通应为一个**持续的过程**。**组织应将促进相关方参与所产生的输出形成文件**。

4.3 确定DGMS的范围

组织应确定DGMS的边界及其适用性，以建立其范围。在确定范围时，组织应考虑：

a) 4.1中提到的外部和内部事项；

b) 4.2中提到的要求；

c) 组织实施的活动与其他组织实施的活动之间的接口和依赖关系（特别是与数据提供方、数据处理方之间的接口）。

范围应形成文件化信息并可用。

4.4 数据治理应用管理体系（DGMS）

4.4.1 组织应按照本标准的要求，建立、实施、保持和持续改进数据治理应用管理体系，包括所需过程及其相互作用。

组织应确定数据治理应用管理体系所需的过程及其在整个组织中的应用，且应：

a) 确定这些过程所需的输入和期望的输出；

b) 确定这些过程的顺序和相互作用；

c) 确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程的有效运行和控制；

d) 确定这些过程所需的资源并确保其可获得；

e) 分配这些过程的职责和权限；

f) 按照 6.1 的要求应对风险和机遇；

g) 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；

h) 改进过程和数据治理应用管理体系。

4.4.2 在必要的范围和程度上，组织应：

a) 保持成文信息以支持过程运行；

b) 保留成文信息以确信其过程按策划进行。

5. 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动，证实其在对DGMS的领导作用和承诺：

a) 确保建立数据治理方针和目标，并与组织战略方向一致；

b) 确保将DGMS要求融入组织的业务过程；

c) 确保DGMS所需的资源可获得；

d) 沟通有效的数据治理管理的重要性；

e) 确保DGMS达成其预期结果（如运营合规、风险可控、价值实现）；

f) 指导并支持相关人员为DGMS的有效性做出贡献；

g) 促进持续改进；

h) 支持其他相关管理角色在其职责范围内发挥领导作用。

5.2 方针

最高管理者应建立数据治理方针，该方针应：

a) 与组织的宗旨相适宜；

b) 包括信息安全目标（见6.2）或为设定信息安全目标提供框架；

c) 包括对满足适用数据治理相关要求的承诺；

d) 包括对持续改进DGMS的承诺；

e) **特别应包括对实现数据治理目标（运营合规、风险可控、价值实现）的承诺**。

数据治理方针应：

f) 形成文件化信息并可获取；

g) 在组织内得到沟通；

h) 适当时，可被相关方获取（如监管机构、客户）。

5.3 组织的岗位、职责和权限

最高管理者应确保与数据治理相关岗位、职责和权限在组织内得到分配和沟通。

最高管理者应**指定一名或多名管理者**（如首席数据官、数据治理委员会负责人），不论其是否负有其他职责，应使其具有以下方面的岗位、职责和权限：

a) 确保DGMS符合本文件的要求；

b) 向最高管理者报告DGMS绩效，供其评审并作为持续改进的依据；

c) 确保在整个组织内提高对数据治理重要性的意识；

d) 协调与DGMS有关的内部和外部沟通。

同时，最高管理者应**建立支撑数据战略的组织机构和组织机制**，明确决策和实施机构，设立岗位并明确角色，确保责权利的一致（根据GB/T 34960.5-2018第6.2条）。

6. 策划

6.1 应对风险和机会的措施

6.1.1 总则

当策划DGMS时，组织应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机会，以：

a) 确保DGMS可达到预期结果；

b) 预防或减少不良影响（如数据泄露、合规处罚、数据价值无法实现、战略决策失误）；

c) 达到持续改进。

组织应策划：

d) 应对这些风险和机会的措施；

e) 如何将此措施整合到DGMS过程中并予以实现及评价其有效性。

6.1.2 数据治理风险评估

组织应定义并应用风险评估过程，以建立并维护风险准则（包括风险接受准则和评估实施准则）；识别与数据治理相关的风险（如数据质量风险、数据安全风险、数据合规风险、数据

价值无法实现的业务风险、数据架构不匹配风险）；分析并评价风险。风险评估应特别考虑数据治理对实现组织战略目标的影响。组织应保留有关风险评估过程的文件化信息。

6.1.3 数据治理风险处置

组织应定义并应用风险处置过程，以选择适当的处置方案（通过 **ISO/IEC 27001:2022附录A** 及 **GB/T 34960.5-2018** 中的控制措施）。组织应**制定并维护一个《适用性声明》**，包含所选控制措施及删减的合理性说明，并制定正式的风险处置计划。组织应保留有关风险处置过程的文件化信息。

注： 组织应**建立并保持合规义务登记册**，以识别和跟踪与数据治理相关的法律法规、标准及其他要求。

6.2 数据治理目标及其实现的策划

组织应在相关职能和层级上建立数据治理目标。目标应：

a) 与数据治理方针一致；

b) 可测量（如数据质量指标、数据资产利用率、数据安全事件数、合规性评价通过率、数据治理成熟度等级）；

c) 考虑适用的要求；

d) 予以监视；

e) 予以沟通；

f) 视情况予以更新。

策划如何实现这些目标时，组织应确定要做什么、需要什么资源、由谁负责、何时完成、如何评价结果。

6.3 针对变更的规划

当组织确定需要对DGMS进行变更时（如组织架构调整、业务战略变更、法律法规更新、引入新技术、数据资产发生重大变化），变更应系统地予以策划和实施。

7. 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进DGMS所需的资源。资源包括：具备相应能力的人员（数据治理师、数据分析师、数据安全专家等）、技术基础设施（数据管理平台、数据分析工具、数据安全工具）、财务资源、技术资源等。

7.2 能力

组织应：确定从事会影响组织数据治理绩效的工作人员的必要能力（如数据治理方法、数据质量管理、元数据管理、数据安全技术）；基于适当的教育、培训或经验确保其胜任；适用时采取措施获得必要能力（如数据治理培训、认证），并评估有效性；保留适当的文件化信息作为能力的证据（如培训记录、认证证书）。

7.3 意识

在组织控制下工作的人员应了解：

a) 数据治理方针；

b) 其对DGMS有效性的贡献；

c) 不符合DGMS要求的潜在影响（如导致数据价值无法实现、合规处罚、决策失误）。

7.4 沟通

组织应确定与DGMS相关的内部和外部沟通的需求，包括：沟通什么（如数据治理政策、数据质量标准、数据安全事件、数据治理绩效）、何时沟通、与谁沟通、谁来沟通、怎么沟通。特别地，应建立与数据提供方、数据处理方和监管机构的沟通机制。

7.5 文件化信息

7.5.1 总则

组织的DGMS应包括：本文件要求的文件化信息（如DGMS手册、风险评估报告、风险处置计划、适用性声明等）；组织为DGMS有效性所确定的必要的文件化信息（如数据治理制度、数据标准、数据模型、元数据、数据质量报告）。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的标识和说明、形式、载体以及评审和批准。

7.5.3 文件化信息的控制

DGMS及本文件所要求的文件化信息应得到控制，以确保：在需要的场合和时机可获得并适用；予以妥善保护（避免泄密、不当使用或缺失）。为控制文件化信息，适用时，组织应分发、访问、检索和使用；存储和防护；更改控制；保留和处置。

8. 运行

8.1 运行的策划和控制

组织应策划、实施和控制为满足要求和实施第6章所确定的措施所需的过程，包括建立过程准则，并按照准则实施控制。组织应控制计划内和计划外的变更，确保外部提供的过程、产品和服务受控。

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发生时（如新业务上线、数据系统重大升级），执行数据治理风险评估。应保留风险评估结果的文件化信息。

8.3 数据治理风险处置

组织应实现数据治理风险处置计划。应保留风险处置结果的文件化信息。

8.4 数据治理特定控制措施（依据GB/T 34960.5-2018）

组织应按本章节要求实施和运行特定的数据治理控制措施，这些措施补充和细化了ISO/IEC 27001:2022附录A中的相关控制。

8.4.1 数据治理顶层设计（依据GB/T 34960.5-2018第6章）

控制

组织应进行数据治理的顶层设计，包括战略规划、组织构建和架构设计。

实施要求：

a) **战略规划**：制定与业务战略一致的数据战略，明确数据治理的目标、任务、实施路径和资源投入。

b) **组织构建**：建立支撑数据战略的组织机构（如数据治理委员会）和组织机制，明确决策和实施机构，设立岗位（如首席数据官、数据所有者、数据管家）并明确角色，确保责权利的一致，建立相关的授权、决策和沟通机制。

c) **架构设计**：建立与战略一致的数据架构，包括数据模型、数据分布、数据集成与共享架构，并确保其合理性和先进性。

8.4.2 数据治理环境管理（依据GB/T 34960.5-2018第7章）

控制

组织应识别和营造有利于数据治理的内外部环境，并识别促成因素。

实施要求：

a) **内外部环境**：分析业务、市场和利益相关方的需求，评估市场发展和竞争地位，遵循法律法规和监管要求。

b) **促成因素**：获得数据治理决策机构的授权和支持；明确人员的业务技能及职业发展路径，开展培训和能力提升；关注技术发展趋势，开展技术研发和创新；制定数据治理实施流程和制度；营造数据驱动的创新文化；评估数据资源的管理水平和数据资产的运营能力。

8.4.3 数据治理域管理——数据管理体系（依据GB/T 34960.5-2018第8.1条及附录A）

控制

组织应围绕数据标准、数据质量、数据安全、元数据管理和数据生存周期，开展数据管理体系的治理。

实施要求：

a) **数据标准管理**：建立数据标准和规范，确保数据的一致性和可理解性。

b) **数据质量管理**：建立数据质量度量体系，持续监控和改进数据质量，满足数据应用需求。

c) **数据安全管理**：制定数据安全策略，实施数据分类分级，建立数据访问控制、审计和脱敏机制，确保数据的保密性、完整性和可用性。定期开展安全审计和风险评估。

d) **元数据管理**：建立元数据管理机制，建立数据字典，确保元数据的完整性和准确性。

e) **数据生存周期管理**：定义数据生存周期，对数据获取、存储、使用、归档和销毁等各阶段进行管理，**确保数据的获取合法、归档可靠和销毁完全**，确保合规和安全。

8.4.4 数据治理域管理——数据价值体系（依据GB/T 34960.5-2018第8.2条及附录B）

控制

组织应围绕数据流通、数据服务和数据洞察，开展数据资产运营和应用的治理。

实施要求：

a) **数据流通管理**：建立数据共享和交换机制，确保数据在授权范围内的有效流转。**应建立数据资产的识别方法和机制，建立数据资产价值评估指标（如整体性、动态性、针对性、准确性等）**，并开展数据价值的评估。应明确可流通的数据权属和流通方式。应确保数据流通过程的可追溯，保存数据流通日志或记录，包含时间戳、参与方身份、数据内容描述等。

b) **数据服务管理**：提供数据服务，支持业务分析和决策。

c) **数据洞察管理**：通过数据分析挖掘数据价值，支持业务创新和优化。

d) **价值实现评估**：评估数据资产的运营和应用能力，监督数据价值实现的绩效和符合性。

8.4.5 数据治理过程管理（依据GB/T 34960.5-2018第9章）

控制

组织应通过统筹和规划、构建和运行、监控和评价、改进和优化的过程，实施数据治理。**组织应评估数据治理的现状和需求、数据治理环境、数据资源管理和数据资产运营能力。**

实施要求：

a) **统筹和规划**：评估数据治理现状、资源、环境，**评估数据管理的现状和能力**，分析与法律法规、行业发展的差距，制定数据治理方案（包括组织规划、范围任务、实施策略）。

b) **构建和运行**：根据方案构建数据治理体系（组织机构、责权利划分、实施路线图、管理制度），并确保有序运行。

c) **监控和评价**：构建绩效评估体系，监控评价数据治理过程，评价数据治理成效与目标的符合性，确保合规。

d) **改进和优化**：根据评价结果，改进数据治理方案，优化实施策略、方法和流程，促进治理体系完善。

8.4.6 数据安全与隐私保护（依据ISO/IEC 27001:2022附录A及GB/T 34960.5-2018附录A.4.3）

控制

应建立数据安全管理的目标、方针和策略，实施数据安全管控。

实施要求：

a) 建立数据安全管理机构，明确数据安全管理的角色和责任。

b) 建立数据安全分类分级规范，建立满足不同业务场景、不同级别的数据安全规范和保护机制。

c) 构建数据安全管理视图，识别数据应用过程中的风险，并建立数据泄露、应急响应、沟通协作和责任追究等安全管控机制。

d) 建立数据应用过程中的数据授权、访问和审计机制。

e) 定期开展安全审计和风险评估，对数据安全管理能力进行监督，并持续改进和优化。

9. 绩效评价

9.1 监视、测量、分析和评价

组织应确定：需要被监视和测量的内容（包括数据治理过程绩效、数据质量指标、数据安全事件、数据资产价值、数据治理目标完成度等）；适用的方法；何时执行；谁应执行；何时分析和评价结果。组织应评价数据治理绩效以及DGMS的有效性。**确保用于监视与测量的资源（如数据管理平台、分析工具）的准确性**。

9.1.2 合规性评价

组织应建立、实施并保持程序，以定期评价其对适用法律法规（特别是数据合规相关法律）、标准及自身DGMS要求的遵守情况。**合规性评价应至少每年进行一次**，并**保留合规性评价报告作为成文信息**。

9.2 内部审核

组织应按策划的时间间隔进行内部审核，以提供有关DGMS符合性及有效性的信息。审核员应确保客观性和公正性。审核结果应报告给相关管理层。

9.3 管理评审

最高管理者应按计划的时间间隔评审DGMS，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) 以往管理评审措施的状态；

b) 内外部的变化（如新的法规、业务战略调整、数据技术发展）；

c) 绩效信息（包括：数据治理目标完成度、数据质量趋势、数据安全事件、数据资产价值实现情况、**外部供方（如数据处理方）的绩效**、合规性偏差、风险评估与处置状态、改进机会等）；

d) 持续改进的机会。

评审输出应包括与持续改进机会及DGMS变更需求相关的决定。

10. 改进

10.1 持续改进

组织应持续改进DGMS的适宜性、充分性和有效性。

10.2 不符合与纠正措施

当发生不符合时，组织应：做出应对、控制并纠正，处置后果；评价是否需要采取措施消除原因；实施所需的措施并评审有效性；必要时对DGMS进行更改。应保留文件化信息作为不符合性质及后续采取措施的证据。**推荐预防措施**以防范潜在不符合的发生（例如，通过定期数据质量监控，预防数据质量下降导致业务决策失误）。

————————————————