

认证技术规范

大数据架构治理安全隐私管理体系 要求

Big Data Architecture Governance and Security-Privacy Management System

CTS-BQC-BDAGSP-2026

编制：王 雷

审批：杨小涛

北京质信认证有限公司

2026 年 5 月 1 日

目 录

前言

引言

1 范围

2 规范性引用文件

3 术语和定义

4 组织所处的环境

4.1 理解组织及其所处的环境

4.2 理解相关方的需求和期望

4.3 确定大数据架构治理安全隐私管理体系的范围

4.4 大数据架构治理安全隐私管理体系

5 领导作用

5.1 领导作用与承诺

5.2 大数据架构治理安全隐私方针

5.3 角色、职责和权限

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

6.1.2 大数据架构- 安全- 隐私风险评估

6.1.3 大数据风险处置

6.1.4 大数据生态系统影响评估

6.2 大数据目标及其实现的策划

6.3 变更的策划

7 支持

7.1 资源

7.2 能力

7.3 意识

7.4 沟通

7.5 成文信息

7.5.1 总则

7.5.2 成文信息的创建和更新

7.5.3 成文信息的控制

8 运行

8.1	运行的策划和控制
8.2	大数据架构治理过程
8.2.1	架构需求与 BDRA 框架应用
8.2.2	架构设计与架构评审
8.2.3	架构变更管理
8.2.4	架构资产与元数据管理
8.2.5	架构退役与处置
8.3	大数据安全与隐私运行过程
8.4	外部提供过程、产品和服务的控制
9	绩效评价
9.1	监视、测量、分析和评价
9.2	内部审核
9.2.1	总则
9.2.2	内部审核方案
9.3	管理评审
9.3.1	总则
9.3.2	管理评审输入
9.3.3	管理评审输出
10	改进
10.1	持续改进
10.2	不符合和纠正措施
附录 A (规范性)	参考控制目标与控制措施
域 1	大数据架构治理域
域 2	大数据安全与隐私域
附录 B (资料性)	大数据控制措施实施指南
附录 C (资料性)	潜在组织目标与风险来源
附录 D (资料性)	跨行业、跨领域本管理体系的应用
参考文献	

前 言

本规范按照 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》编制，采用 Annex- SL 管理体系高阶架构，实现与 GB/T 19001- 2016、ISO/IEC 27001、ISO/IEC 42001 管理体系兼容集成。

规范规范性引用 ISO/IEC 20547- 3:2020《信息技术- 大数据参考架构- 第 3 部分：参考架构》、ISO/IEC 20547- 4:2020《信息技术- 大数据参考架构- 第 4 部分：安全与隐私》。BDRA 大数据参考架构为本管理体系的技术基座；本标准不强制大数据系统的实现必须完全复刻 BDRA 用户视图、功能视图，强制要求组织在大数据系统全生命周期过程中应用 BDRA 作为分析框架。

本文件为认证技术规范，可用于组织建立、实施、保持、持续改进大数据架构治理安全隐私管理体系，可用于内部、第二方、第三方商业符合性审核。

引 言

大数据系统具备大容量、高速率、多类型、易变性特征，大数据生态包含多方当事方，对应 BDRA 用户视图下多类角色（大数据应用提供商 BDAP、大数据框架提供商 BDFP、大数据服务合作方 BDSP、大数据提供方 BDP、大数据消费方 BDC），横跨采集、预处理、分析、存储、可视化、访问全活动链条；同时横切方面包含安全、隐私、数据治理、系统管理。传统信息安全管理体系缺少针对大数据生态角色、大数据架构全生命周期的专项过程要求。

ISO/IEC 20547- 3 给出 BDRA 参考架构模型，ISO/IEC 20547- 4 给出安全隐私横切面的治理、管理、运行活动；但二者属于架构、指南类标准，缺少组织层面管理体系要素（领导、方针、内审、管理评审、持续改进），无法直接作为管理体系认证审核依据。

本规范解决上述缺口：

- 1) 遵循 Annex- SL 统一高阶架构，实现和现有管理体系兼容集成；
- 2) 以 BDRA (20547- 3) 作为组织大数据架构治理的分析框架，以 20547- 4 作为安全- 隐私技术活动输入；
- 3) 管控对象是**组织的管理过程**：架构设计、评审、变更、资产管控；大数据生态角色权责；大数据安全隐私风险、影响评估、控制措施；
- 4) 本规范不判定“大数据架构图纸设计方案的好坏”；审核判定重点：**组织是否建立并执行完整过程证据，使用 BDRA 开展架构分析、风险识别、安全隐私管控；架构设计决策本身的优劣不属于本体系的审核判定准则**；
- 5) 采用基于风险的方法，组织根据自身大数据业务场景，可在适用性声明 (SoA) 中论证部分控制措施的删减理由。

本管理体系可与 ISO/IEC 27001、ISO/IEC 27701、ISO/IEC 42001 协同使用。

本标准不设置 Annex- SL 原版 8.3 “设计和开发” 独立条款。大数据架构层面的需求分析、架构设计、评审、变更、退役等生命周期活动，整合纳入 8.2 大数据架构治理过程。本标准管控对象仅限于大数据系统架构治理活动，不管控软件源代码、单元测试、编码等软件产品实现细节。组织如完全外购 / 直接使用第三方现成大数据服务，无内部架构设计活动，允许在适用性声明 (SoA) 中基于风险论证，裁剪架构设计类子活动，仅保留架构集成评审、变更、退役相关要求。

1 范围

本规范规定组织建立、实施、保持和持续改进**大数据架构治理安全隐私管理体系**的要求。

本规范适用于开发、提供、运维、使用大数据系统、大数据平台的各类组织，无论组织规模、所有制形式。

本规范用于：

- a) 组织证明自身对大数据系统落实架构治理，同时对大数据场景的安全、隐私、数据治理风险进行管理；
- b) 内部、第二方、第三方开展符合性评价。

注：本规范不强制大数据系统的实现一比一复刻 ISO/IEC 20547- 3 的 BDRA 用户视图、功能视图；要求组织在大数据系统全生命周期过程中应用 **BDRA 框架**开展角色识别、活动识别、横切方面分析。

2 规范性引用文件

下列文件对于本规范的应用必不可少。凡是注日期引用仅引用该版本；未注日期引用使用最新版本（含修改单）。

ISO/IEC 20547- 3:2020 信息技术 大数据参考架构 第 3 部分：参考架构

ISO/IEC 20547- 4:2020 信息技术 大数据参考架构 第 4 部分：安全与隐私

ISO/IEC 20546 信息技术 大数据 概述与词汇

ISO 31000 风险管理 原则和指南

3 术语和定义

ISO/IEC 20546、ISO/IEC 20547- 3、ISO/IEC 20547- 4 给出的术语和定义，

注：本文件内容受到本机构版权保护，未经恰当的授权禁止复制。本机构客户及相关单位，如需获取文件完整内容，请通过电话 010-63265286 或邮箱 BQC@bqciso.com 获取。