

团 体 标 准

T/QGCML XXXX—2024

企业大数据信息运维处理软件技术规范

Technical specifications for enterprise big data information operation and
maintenance processing software

2024 – XX – XX 发布

2024 – XX – XX 实施

全国城市工业品贸易中心联合会 发 布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 通用服务内容 1

5 维护管理 3

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。

本文件由提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件起草单位：。

本文件主要起草人：。

本文件为首次发布。

企业大数据信息运维处理软件技术规范

1 范围

本文件规定了企业大数据信息运维处理软件技术规范的术语和定义、通用服务内容、维护管理。
本文件适用于企业大数据信息运维处理软件技术规范。

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 17859 计算机信息系统 安全保护等级划分准则

3 术语和定义

本文件没有需要界定的术语和定义。

4 通用服务内容

4.1 基础服务内容

4.1.1 规划设计

为保证系统运维的科学性、有效性和完整性，信息服务提供者应确定规划设计的合理性、可用性：
——研究、分析规划设计中所有要素和关联因素的有效性；
——评估规划设计的合理性、有效性和可用性，及对运维的影响；
——提出规划设计中不合理因素和影响运维的因子，提出修正建议；
——在运维过程中尝试修正等。

4.1.2 信息资源

信息资源主要应包括：
——应确认信息资源相关需求和实现；
——确认信息资源实现的方法、路径等的合理性和可行性；
——识别信息资源需求实现的缺陷和改进方法；
——提供信息资源管理和修正管理建议；
——在运维过程中尝试修正等。

4.1.3 物理环境管理和维护

4.1.3.1 机房管理和维护

为保证机房内所有设备的安全、稳定、无故障运行，监控机房的环境、监测并定期检查电源、通风、接地等所有机房设施的工作状态，发现并报告问题和提出变更建议，包括以下内容：

——电源管理：将电源有效分配到系统中不同的设备组件。应考虑电源设备参数对设备的影响，如过压、过流、浪涌、短路等；
——等电位管理：设置配电系统、各类电子设备及附属设施、防雷等的接地等电位体，应考虑静电防护、感应雷电可能形成的电磁脉冲和过电压的干扰和毁坏等；
——设备管理：计算机信息系统、信息网络系统设施的日常运行和管理、可靠性评价；
——环境管理：应考虑机房内通风、温度、湿度、灰尘、灯光等的配置；考虑机柜放置与冷却效率和制冷单元热点的关系；以及可能因功能扩大引起的冷却效率问题等；

——灾害预防：应考虑物理和自然灾害发生的可能性，制定应急预案。

4.1.3.2 其它管理和维护

其他管理和维护包括：

- 布线系统管理和维护：监控、诊断、分析设备间、弱电井等区域配线设备、线缆、信息插座等设施，及网络通信线路的工作状态和可能的故障状态，发现并报告问题，提出维护建议，保证系统运行的高可靠性和维护的高效率；
- 监控系统管理和维护：监控、诊断、分析门禁系统和各类监控设备等的运行状态、参数变化、提示信息等，发现并报告问题，及时变更、维护，保证监控系统的可靠性。

4.1.4 网络基础设施管理和维护

为保证网络基础平台的高可靠性、高可用性，网络基础设施管理和维护，主要应包括：

- 网络拓扑结构的诊断、优化；
- 基础设施的诊断、评估；
- 根据系统规划目标评估系统承载能力；
- 制定网络基础设施管理服务计划；
- 制定故障维护预案，及时消除可能的故障隐患；
- 制定应急预案等。

4.1.5 系统平台管理和维护

为保障系统的安全、稳定、持续运行，系统平台管理主要应包括：

- 系统平台应包括操作系统、数据库系统、中间件、其它支撑系统应用的软件系统及各种协议等；
- 系统平台的诊断、评估；
- 系统平台配置、部署的合理性、可靠性、健壮性；
- 评估系统平台安全风险；
- 评估系统平台性能、性能变化，保证系统平台的可靠性和可用性；
- 根据应用规划评估系统平台容量、支撑能力；
- 制定系统平台管理服务计划；
- 制定系统故障维护处理预案，及时消除故障隐患；
- 制定应急预案等。

4.1.6 应用系统管理和维护

应用系统管理和维护，主要应包括：

- 应用需求、规划的充分性、完整性；
- 应用系统架构设计的可靠性、安全性、前瞻性；
- 应用系统的安全性、可靠性和可用性；
- 应用系统部署的合理性、可靠性和可用性；
- 评估应用系统性能、性能缺陷；
- 评估应用系统功能完整性、功能缺陷；
- 评估应用系统代码效率、系统运行效率；
- 评估应用系统安全风险、安全缺陷，并及时与开发商沟通消除可能存在的安全隐患和威胁；
- 提供应用系统更新、升级等，及技术支持方案；
- 根据需求变化，更新、变更应用系统功能；
- 评估业务融合度等。

4.1.7 数据管理和维护

4.1.7.1 要求

数据管理是系统应用的核心。为保证数据存储、数据访问、数据通信、数据交换的安全，定期评估数据的完整性、安全性、可靠性；制定备份、容灾策略和数据恢复策略，消除可能存在的安全隐患和威胁。

4.1.7.2 数据存储设施

数据存储设施的管理和维护，主要应包括：

- 数据存储设施应包括服务器设备、集群系统、虚拟系统、存储阵列、存储网络等，以及支撑数据存储设施运行的软件平台等；
- 存储设施的诊断、评估；
- 数据存储设施的参数配置、性能要求、容量设定、软件平台的性能等的安全性、可靠性、可用性和可扩展性；
- 评估虚拟系统的适用性、支撑能力等；
- 评估存储系统的安全风险，确认数据存储的安全等级；
- 评估虚拟系统的安全风险；
- 制定故障应急预案，及时消除故障隐患等。

4.1.7.3 数据安全性管理和维护

数据安全性管理和维护，主要应包括：

- 安全评估：评估数据的完整性、可靠性、可用性和保密性等要素，制定数据管理和数据恢复策略，保证数据的安全；
- 数据访问控制：制定数据访问控制策略、访问权限控制策略、非授权访问处理策略，防止未经授权的数据访问、修改、移动、删除、毁损等；
- 数据存储与容灾：制定数据存储、数据容灾策略，评估数据存储的安全性，保证数据存储的完整性、可靠性；制定数据存储事件处理预案；
- 数据通信安全：评估数据通信的安全性，制定数据通信的安全策略，保证数据的完整性、可靠性、保密性和不可抵赖性；制定数据通信应急处理预案。

4.1.7.4 媒介安全性管理和维护

制定媒介管理、权限策略，制定媒介泄露的处理策略，明确责任，保证数据保管的安全。

4.1.7.5 风险评估

评估系统的安全威胁、脆弱性、漏洞，评估安全管理，制定风险应对策略和风险处理机制，及时消除或弱化风险，并将残余风险控制在可控范围内。

4.1.7.6 安全策略

制定物理环境、基础平台、数据、应用软件、事件管理等的信息安全策略，实行信息安全教育，明确责任，采取相应的安全措施，实施安全策略的综合管理。

5 维护管理

5.1 目标

利用各种技术手段，检测、监控系统的运行，分析、优化系统性能，及时发现故障、处理故障，保证系统和业务系统的持续、稳定运行。

5.2 需求分析

应识别、整合、定义、分类信息资源和相关资源，检测、分析系统性能，确定维护服务需求和范畴。

5.3 维护计划

应根据维护服务需求、业务需求、服务水平管理、服务能力管理，制定维护计划，确定管理流程，建立维护体系。

5.4 沟通与协调

在维护服务中，应随时与用户沟通、交流，了解可能的需求变更，听取用户的意见，不断改进和完善服务过程。

5.5 问题管理

5.5.1 问题识别

应监测、记录、识别、分析系统出现的或潜在的问题，建立问题处理流程，查找引起问题的原因，降低系统运行的风险。

5.5.2 问题控制

应根据问题的性质分类，确定问题的影响和程度，按照优先级定义排队，定义问题解决方案。

5.5.3 问题跟踪

应跟踪问题处理流程，及时改进和完善。

5.5.4 协调管理

在问题管理中，应协调服务台、变更管理和问题管理，促进问题的预防、解决和管理。

5.6 维护方式

5.6.1 需求确定

应依据用户需求，确定系统维护服务的类型、内容，明确维护服务的目标，和对服务能力的要求，建立维护服务管理流程。

5.6.2 维护支持

应依据用户需求及服务类型、服务内容和 service 管理流程，采取不同层次的维护服务和技术支持：

- 定期与非定期维护；
- 远程维护；
- 现场维护等。

5.7 维护跟踪

应在维护工作完成后，跟踪、监测维护效果，及时改进、弥补各类缺陷、不足。
