ICS 35.030

CCS L80

DB21

辽 宁 省 地 方 标 准

DB21/T xxx.xx—XXXX

数据流通安全审计服务规范

Technical Specification for Data Circulation Security Audit Service

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

本部分按照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。

本部分由辽宁省数据和政务服务局提出并归口。

本部分起草单位：北方实验室（沈阳）股份有限公司、辽宁北实数据科技有限公司、辽宁省数据中心、辽宁省工业和信息化发展研究院。

本部分主要起草人：张健楠、韩晓娜、张建宇、李琳、王明俊、魏凤娇、孙辉航、王启光、冯玉佳、周淼、苏建宇、孙愈、王旭东、罗有喆、陆建松、徐帅、王新明、曹明、闫丽杰、梁爽、赵鑫、曹阳、张秀娟、王艺桥。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通讯地址：辽宁省数据和政务服务局（沈阳市皇姑区崇山中路109号），联系电话：024-86916223。

标准起草单位通讯地址：北方实验室（沈阳）股份有限公司（辽宁省沈阳市浑南区智慧三街199号），联系电话：400-664-5588。

数据流通安全审计服务规范（征求意见稿）

1 范围

本文件规定了数据流通场景下数据安全审计的服务内容、审计流程、审计方法以及第三方审计服务机构的能力要求。数据流通场景包括数据共享、数据交易、数据授权使用、数据开放等跨主体数据流动活动。

本文件适用于在辽宁省行政区域内，第三方专业技术服务机构对数据共享、数据交易、数据授权使用、数据开放等数据流通活动开展的安全审计服务。本文件不适用于网络安全等级保护测评、数据出境安全评估、涉密信息系统安全评估，上述活动按照国家相关规定执行。

本文件适用于非涉密数据流通活动的安全审计，不适用于涉密数据及涉密信息系统。

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/T 36073-2018 数据管理能力成熟度评估模型

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 45577-2025 数据安全技术 数据安全风险评估方法

GB/T 43697-2024 数据安全技术 数据分类分级规则

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

3 术语和定义

下列术语和定义适用于本文件。

数据安全审计：第三方服务机构依据法律法规及标准规范，对组织数据安全管理、数据安全技术等活动进行合规性和安全性审查与评价，形成审计意见并出具审计报告的监督活动。

数据流通安全审计：第三方服务机构依据法律法规及标准规范，对数据共享、数据交易、数据授权使用、数据开放等数据流通活动中数据提供方、数据接收方及相关方的数据安全管理和技术防护措施进行合规性、安全性审查与评价，形成审计意见并出具审计报告的专业服务活动。

数据资产：是指特定主体合法拥有或者控制的，能进行货币计量的，且能带来经济利益或社会效益的数据资源。

数据处理：包括数据的收集、存储、使用、加工、传输、提供、公开、删除等。

数据交换：不同组织机构之间或组织机构与个人之间，因业务需要按照约定方式进行数据双向或单向传递的行为。

数据流通：是指数据在不同主体之间流动的过程，包括数据开放、共享、交易、交换等。

数据治理：是指提升数据的质量、安全、合规性，推动数据有效利用的过程，包含组织数据治理、行业数据治理、社会数据治理等。

数据安全：是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

原始数据：对于数据持有方而言，未经加工处理的数据。

审计委托方：委托第三方审计机构开展数据流通安全审计的组织或个人，通常为数据提供方、数据接收方或监管部门。

被审计对象：数据流通安全审计所指向的组织、系统、流程或活动，包括数据提供方、数据接收方及流通相关系统。

审计证据：审计人员在审计过程中获取的，用于支撑审计发现和审计结论的各种资料、记录、数据和事实。

审计发现：在审计过程中识别的，被审计对象在数据安全管理或技术防护方面存在的合规偏差、控制缺陷或安全隐患。

审计整改：被审计对象针对审计发现的问题，采取管理措施或技术措施进行纠正和完善的过程。

个人信息：以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

4　安全审计概述

4.1 安全审计目标

数据流通安全审计通过对数据流通活动中各方主体的数据安全管理和技术防护措施进行合规性、安全性审查与评价，识别数据流通全生命周期中的安全风险和控制缺陷，提出整改建议，促进数据流通安全保障能力的持续提升。

数据流通安全审计应遵循以下原则：

a）独立性原则：审计机构和审计人员应独立于被审计对象的数据安全建设活动，不受任何组织和个人的不当干预；

b）客观性原则：审计应以事实为依据，以法律法规和标准规范为准绳，客观公正地作出审计判断；

c）保密性原则：审计机构和审计人员应对审计过程中知悉的国家秘密、商业秘密、个人信息及敏感数据严格保密；

d）风险导向原则：审计应根据数据流通场景、数据级别和风险状况，合理确定审计范围、审计深度和审计方法。

4.2 安全审计架构

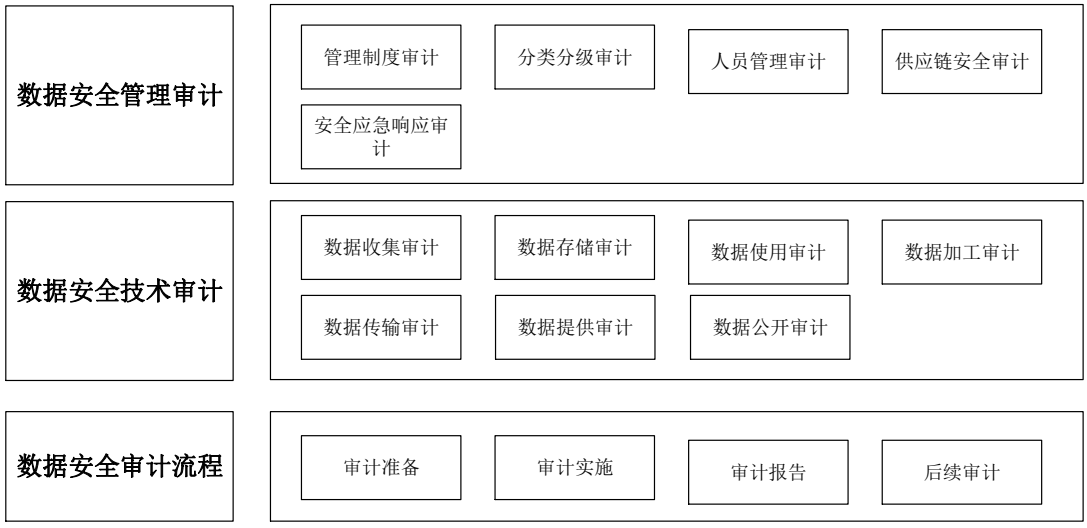

图1 数据安全审计框架

数据流通安全审计框架包括审计主体层、审计对象层、审计内容层和审计成果层四个层次。审计主体层为第三方审计服务机构；审计对象层为数据提供方、数据接收方及流通相关系统；审计内容层涵盖数据安全管理审计和数据安全技术审计；审计成果层包括审计报告、风险提示函和整改建议清单。

4.3 安全审计规范要求

数据安全审计规范要求包括：

a) 数据安全审计工作流程：包括审计准备、审计实施、审计报告、后续审计等。

b） 数据安全管理审计：包括管理制度安全审计、分类分级安全审计、人员管理安全审计、供应链安全审计、安全应急审计等。

c） 数据安全技术审计：包括数据收集审计、数据存储审计、数据使用审计、数据加工审计、数据传输审计、数据提供审计、数据公开审计、数据删除审计等。

5 安全审计工作流程规范

数据流通安全审计程序一般包括审计准备、审计实施、审计报告和后续审计四个阶段。

5.1 审计准备

审计准备工作包括但不限于：

a） 明确审计目的及任务；

b） 组建审计项目组，明确角色和责任，并确保所有人员均具备完成该项目相应的专业胜任能力；

c） 开展审计前调查，收集法规、制度及相关资料；

d） 编制审计项目计划及审计程序。

e） 进行利益冲突评估，审计机构及审计人员与被审计对象存在可能影响审计独立性的利益关系时，应主动声明并回避；

f） 与委托方签订审计服务合同或审计业务约定书，明确审计目的、审计范围、审计期限、双方权利义务及保密责任；

g） 编制审计实施方案，明确审计目标、审计范围、审计内容、审计方法、人员分工、时间安排和审计证据采集要求；

h） 向被审计对象发送审计通知书，告知审计目的、审计范围、审计时间及需要配合的事项。

5.2 审计实施

审计实施工作至少应包括：

a） 依据审计计划实施现场审计；

b） 了解被审计组织的内部控制管理制度及流程，并根据实际情况调整审计计划；

c） 开展控制测试；

d） 开展实质性测试。

e） 按照审计实施方案采集审计证据，审计证据应具备充分性、相关性和可靠性；

f） 编制审计工作底稿，如实记录审计过程、审计发现、审计证据来源及审计判断依据；

g） 对审计发现的问题进行初步确认，与被审计对象沟通核实，听取被审计对象的说明和申辩；

h） 根据审计实施情况，必要时调整审计范围和审计程序。

5.3 审计报告

审计报告工作至少应包括：

a） 整理与复核审计工作底稿；

b） 整理审计证据；

c） 判断并报告审计发现；

d） 沟通审计结果，形成审计意见和结论；

e） 出具审计报告，审计报告应包括以下基本要素：审计项目名称、审计委托方、被审计对象、审计依据、审计范围、审计方法、审计发现、审计结论、整改建议、审计机构签章、审计日期。

f） 审计报告仅作为委托方数据安全管理和决策的参考依据，不替代监管部门的行政执法结论。

5.4 后续审计

后续审计是审计机构对被审计对象整改情况进行跟踪验证的活动，包括整改跟踪和闭环验证两个环节。审计机构应在审计报告出具后，对被审计对象的整改计划制定、整改措施落实情况进行跟踪；对审计发现的重大问题和高风险缺陷，应在整改完成后开展闭环验证，确认整改措施的有效性，形成整改验证记录。对整改不到位或整改效果不明显的，应向委托方出具风险提示函并建议开展再次审计。

6 数据安全审计内容

6.1 数据安全管理审计

6.1.1 管理制度流程审计

审计管理制度流程时，审计范围包括但不限于：

a） 审查数据安全管理制度的建立情况及持续更新优化和发布的情况；

b） 对数据安全管理制度发布时的控制政策与流程的建立情况进行审计；

c） 对数据安全相关管理制度发布时的授权与审批控制进行审计；

d） 审查数据安全管理制度是否符合国家相关法律法规、技术标准及主管部门安全要求；

e） 应定期开展针对各岗位人员的数据安全相关管理规范、流程、制度培训，并进行考核。

f） 应统筹实施数据安全管理工作，监督落实数据安全管理制度及技术防护措施执行情况。

g） 应审查数据流通合约或数据处理协议的合规性，检查合约是否明确数据流通的目的、范围、方式、期限、数据安全责任、保密义务、违约责任及数据销毁要求；

h） 应审查数据流通各方的数据安全责任划分情况，检查数据提供方、数据接收方在数据安全保护方面的权利义务是否明确。

6.1.2 分类分级审计

审计分类分级时，审计范围包括但不限于：

a） 应参照国家标准和行业标准，结合自身业务对数据进行分类分级，形成目录清单并采取相匹配的保护和管理措施；

b） 应从元数据角度，对数据资源目录中的数据在数据管理、业务、安全、对象等维度的分类分级情况进行审计；

c） 应建立数据全生命周期安全管理制度，针对不同类型和级别数据，实施数据收集、存储、使用、加工、传输、提供、销毁等环节的保护与管理，保障数据的保密性、完整性、可用性和合规性。

d） 应结合数据全生命周期以及具体的分类实施流程，如明确实施步骤、启动实施工作、开展实施工作、总结实施等过程进行审计。

e） 应根据分类主体制定安全管理方案的情况进行审计；

f） 按照数据敏感性、保密性、重要性的程度对数据分类的情况进行审计。

g） 应对数据分类维度和方法的合理性进行审计，检查是否符合业务场景变化和分类视角变化；

h） 应根据数据应用场景以及数据分类分级情况，建立覆盖数据全生命周期的安全防护机制，采取数据加密、数据脱敏、身份认证、入侵防护、安全监测等技术保护措施，提高数据安全保障能力；

i） 应对数据分类分级实施过程进行审查，确保数据分类分级过程的合规性和安全性。

j） 应审查数据来源的合法性，检查数据提供方是否对流通数据拥有合法权利或已获得合法授权，数据来源是否清晰可追溯；

k） 应审查数据获取方式的合规性，检查数据收集是否符合合法、正当、必要原则，是否存在非法获取、爬取数据的情形；

l） 涉及个人信息的，应审查是否已取得个人信息主体的同意，或具备其他合法处理事由。

6.1.3 安全应急响应审计

审计安全应急响应时，审计范围包括但不限于：

a) 应对数据安全应急管理工作纳入整体应急管理工作框架之内的情况进行审计；

b) 应对建立数据安全事件处置的指挥体系，明确管理组织架构、应急技术队伍架构的情况进行审计；

c) 应对突发网络与数据安全事件制定的一整套应急处置方案的有效性情况进行审计；

d) 应对定期开展应急演练工作情况进行审计；

e) 应对处置机构人员的配合度与应急处置方案的掌握情况进行审计；

f) 应对重要业务恢复目标和恢复策略的制定情况进行审计；

g) 根据应急预案修订的基本要求、修订周期及应急预案评审周期的规定情况进行审计；

h) 应对数据安全教育培训工作记录进行审计，应总结数据安全事件的经验教训，提升应急能力；

i) 应对数据安全整改、安全加固等方面的改进方案和计划进行审计，明确改进的管理措施、技术措施、人员队伍等内容，强化数据安全能力。

6.1.4 人员管理审计

审计人员管理时，审计范围包括但不限于：

a) 应成立数据安全工作委员会或领导小组，其最高领导由单位主管领导担任或授权。

b) 应设立数据保护官、数据管理员、数据审计员、数据安全员等负责人岗位，明确岗位职责；

c) 应加强人员管理，明确在人员录用、人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面的管理规定并严格落实；

d) 应对数据业务关键岗位人员进行任用前的考核、签订岗位责任协议、背景调查、能力调查；

e) 应加强对外部单位技术人员和外协人员的安全管理，必须签署保密协议，做好人员背景调查，严格实施权限管理，定期进行人员活动审查；

a) 应定期开展针对各岗位人员的数据安全知识和技能培训，并进行考核；

b) 应定期开展针对各岗位人员的数据安全相关管理规范、流程、制度培训，并进行考核；

c) 应对人员离岗进行权限回收、设备回收等情况进行审计。

6.1.5 供应链审计

审计供应链时，审计范围包括但不限于：

a） 应建立供应商安全管理体系，明确安全管理工作的总体目标、范围、原则和各类安全策略；

b） 应建立内部安全控制和安全管理工作的责任部门，并明确相关岗位的责任人的岗位职责；

c） 审查安全管理制度类文档中各项安全管理制度是否覆盖产品/服务涉及的数据安全管理以及供应链生命周期中各类数据安全管理等管理内容；

d） 审查对供应商的管理情况，包括供应商的选择、签约、管理制度及服务能力的评估情况等；

e） 应定期评价供应商管理制度，并评价制度和流程的可操作性、合理性和适用性；

f） 应对供应商尽职审查，评估供应商管理制度是否得到有效执行；

g） 应定期对参与的供应活动全流程的各个环节进行供应链风险评估并生成供应链风险评估报告、风险处置预案以及整改记录等；

h） 应严格控制数据处理相关系统平台特权账号设置和使用；

i） 应对供应商建立严格的访问控制措施，限制数据采集、抓取和抽取的权限，确保只有授权人员能够进行数据操作；

j） 应定期对数据服务供应商当前数据的加工和使用情况进行检查，并查看应用系统和配置，确认符合合规协议约定内容；

k） 应审查数据服务供应商在服务过程中对数据操作的加工、使用等重要活动。

6.1.6 其他审计

审计其他相关控制时，审计范围包括但不限于：

a） 应明确数据资产登记机制，明确数据资产管理范围和属性，确保组织内部重要的数据资产有明确的管理者或责任部门；

b） 审查资产清单的建立情况，包括资产责任部门、重要程度和所处位置等内容；

c） 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理；

d） 基于制定的数据基础安全要求、数据生命周期保护、数据安全管理要求，对落实情况进行监管。

6.2 数据安全技术审计

6.2.1 数据采集安全审计

审计数据采集安全时，审计范围包括但不限于：

a) 应明确数据采集源、采集范围、采集方式、采集周期和频率，确保数据采集的合法性、必要性、正当性，防范捆绑和高频的数据采集；

b) 应对数据采集终端、数据导入服务组件等的使用进行身份鉴别，并实现采集账号权限最小化原则；

c) 数据源选择应根据需要采集数据的数据源类型(如：文件、数据库、传感器等)，确定数据源连接通信的方式，明确采集标准范围及属性；

d) 应采用加密传输协议、可信通道，禁止通过公共社交平台传输敏感数据；

e) 应审查数据分类分级存储和管理应用的安全使用、防护、存储情况，实施差异化采集策略；

f) 应验证或确保数据来源的可追踪、可溯源，来源清晰，包括交易获得、合法授权、自主生产等；

g) 应建立数据来源可靠性验证机制，其中包括建立校验机制、异常数据纠偏机制、来源黑名单机制等；

h) 应对采集的数据进行完整性、一致性和真实性校验，避免数据遭受泄露、篡改、丢失；

i) 应对数据处理工具进行审计，该工具应支持不同数据源、不同安全域之间数据访问控制；

j) 应对采集的原始数据进行清洗、转换、分析等处理，确保数据的完整性、准确性和时效性；

k) 数据采集应具备复杂网络环境下、不同异构数据源之间高速、稳定、弹性伸缩的数据移动及同步能力；

l) 应采取技术措施对数据采集过程进行实时监控，及时发现和告警异常数据，并及时进行更正。

6.2.2 数据传输安全审计

审计数据传输安全时，审计范围包括但不限于：

a) 应采用国家密码管理部门核准密码技术保证传输过程中数据的完整性、一致性和保密性；

b) 应建立安全策略变更的审核制度，落实数据传输接口的安全管理工作；

c) 应具备对传输通道两端主体身份进行鉴别和认证的技术工具；

d) 应具备对传输数据完整性进行检测的能力并拥有执行恢复控制的措施；

e) 应使用网络传输专用通道（如VPN），规避公共互联网传输敏感数据；

f) 应定期评估传输渠道风险（如VPN漏洞、供应商安全事件），更新加密算法及认证方式。

6.2.3 数据存储安全审计

审计数据存储安全时，审计范围包括但不限于：

a) 应采用国家密码管理部门核准的密码技术保证数据在存储过程中的保密性、完整性、一致性和可用性要求；

b) 对数据建立分层的逻辑存储授权管理规则和授权操作规范进行审计，是否具备对数据逻辑存储结构的分层和分级保护能力；

c) 应周期性地备份数据，实现对数据的冗余性管理，保证副本数据的有效性；

d) 应基于数据存储的安全性需求和合规性要求，建立数据访问控制机制；

e) 对数据库安全防护系统进行审计，确保安全日志可溯源；

f) 涉及个人信息存储，其期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外。

g) 应将去标识化的个人信息与可用于恢复识别个人的信息分开存储；

h) 应将个人生物识别信息与其他信息分开存储。

6.2.4 数据加工安全审计

审计数据加工安全时，审计范围包括但不限于：

a) 应对数据加工处理审核流程机制进行审计，确保数据分析、数据脱敏等处理的安全性与合理性；

b) 应根据国家及行业对数据分类分级的要求，结合自身数据业务特性，对数据进行分类分级；

c) 应制定严格的访问控制规则防止非授权的加工、分析操作；

d) 对数据加工处理过程中数据文件鉴别和访问用户身份认证等技术进行审计；

e) 应明确数据加工、分析的目标和范围，确保加工前后数据映射关系；

f) 应对加工、分析产生的新数据设置级别标签；

g) 应建立数据加工、分析操作专区，并采取技术措施禁止远程加工、分析数据；

h) 对数据处理过程中的调用、处理的监控措施进行审计；

i) 审查数据脱敏的记录，证明采取了适用的数据脱敏规则及方法；

j) 审查数据脱敏工具，确保数据脱敏与数据处理权限的一致性；

k) 审查个人数据执行去标识化处理的措施；

l） 敏感数据应采用匿名化或去标识化处理，确保匿名化或去标识化后的数据不可逆；

m） 数据加工不应超出合理范围使用，且行为不存在违反法律法规等强制性规定、危害国家利益、社会公共利益或侵害第三方合法权益的情形；

n） 数据加工应确保衍生数据不超过原始数据的授权范围和安全使用要求；

o） 数据加工算法应符合《中华人民共和国个人信息保护法》相关要求，禁止基于种族、性别、宗教信仰等敏感特征进行自动化决策；

p） 数据加工应该满足数据质量评价规范，包括数据规范性、完整性、准确性、一致性、及时性和可用性6个维度。

6.2.5 数据使用安全审计

审计数据使用安全时，审计范围包括但不限于：

a） 应建立数据使用的管理规范，涉及数据类型、数据内容、数据格式及分场景使用管理细则等；

b） 应建立数据使用的安全策略，包括访问控制策略、不一致处理策略、流程控制策略、审批策略等；

c） 应建立有效的内部控制机制，确保其仅按照供需双方约定的使用目的、范围、方式和期限使用数据；如涉及个人信息去标识化处理的，是否采取有效措施以防止对个人信息进行重新溯源或再识别；

d） 应建立数据资产使用变更机制，明确数据资产变更触发条件，并有效管控变更过程；

e） 应建立数据脱敏制度、流程和方法，指导数据脱敏操作；

f） 应建立数据分析相关数据源获取规范和使用机制，明确数据获取方式、访问接口、授权机制、数据使用等；

g） 应建立数据分析结果的安全机制和授权访问机制，保证数据分析结果不泄露个人信息、重要数据等敏感信息；

h） 应建立数据使用导入导出的安全制度或审批流程。

6.2.6 数据提供安全审计

审计数据提供安全时，审计范围包括但不限于：

a） 数据提供方应建立对外数据使用政策、服务规范等；

b） 数据提供应确保数据的合规性、准确性，并保证数据质量；

c） 数据提供方在归集共享数据过程中应采用身份鉴别、数据源认证等安全机制保障共享数据来源的真实性；

d） 应具备对传输通道两端主体身份进行鉴别和认证的技术工具；

e） 应具备不同业务场景下数据提供执行相应安全策略的能力；

f） 应验证数据提供方提供数据获取渠道合法、权利清晰无争议的承诺或证明材料，确保来源主体具备数据所有权或合法授权；

g） 应按照数据级别明确使用方对共享数据的使用权限和责任；

h） 涉及个人隐私数据、企业商业秘密等敏感数据的，应提供个人、企业明确的同意证明；或经脱敏处理无法识别到特定的个人或机构，且不能复原；

i） 应采取技术措施防止所有数据在未授权条件下的下载、复制、截屏等方式的数据输出，同时应采取措施防止敏感数据泄露；

j） 审查数据提供方流通交易数据的限定用途、使用范围、流通交易方式和使用期限的明确情况；

k） 审查数据提供方对数据的安全评估并出具安全风险评估报告的情况，确保其安全风险不构成对可交易性的阻碍。

6.2.7 数据公开安全审计

审计数据公开安全时，审计范围包括但不限于：

a） 数据公开前应当开展数据安全风险评估，明确公开数据的内容与种类、公开方式、公开范围、安全保障措施、可能的风险与影响范围以及更新频率等，并进行动态调整；

b） 数据公开应当按照相应规定实施数据公开管控措施，保障公共数据的公开范围、公开渠道、公开流程、公开内容和公开时效等合法、正确、有效；

c） 梳理数据共享开放的目录，明确应用场景和数据责任主体以及共享开放数据的级别；

d） 应构建数据公开资源目录发布的审核机制，明确发布审核流程；

e） 数据公开应满足数据源鉴别安全技术要求；

f） 应采取技术措施对异常或高风险数据访问行为进行自动化识别和实时预警，对违规行为及时进行阻断。

g） 应设置数据专区的访问控制规则，实现基于角色的访问控制，并在此基础上建立属性的访问控制。

h） 应采取技术措施严格限制个人敏感信息的公开操作，仅允许特定对象、特定方式的公开操作。

i） 应确保数据流通在个人数据安全保护方面满足GB/T 35273中的关于个人数据的委托处理、共享、转让、公开披露安全要求，并提供数据安全风险评估报告。

6.2.8 审计数据删除审计

审计数据删除安全时，审计范围包括但不限于：

a） 审计数据流通相关合约、协议中是否明确约定数据删除触发条件：包括流通期限届满、委托处理终止、授权撤回、业务终止、合约解除、个人信息主体行使删除权等场景，明确删除时限、删除对象、删除责任方、验证方式。

b） 审计数据删除对象覆盖完整性，核查是否对原始流通数据、备份副本、缓存数据、中间处理数据集、导出副本、共享给内部子部门或第三方的二次分发数据、流通产生的衍生数据集全部纳入删除范围，不应仅删除主库数据而遗漏各类副本。

c） 审计数据删除审批流程落实情况：流通场景下批量数据删除操作是否履行审批，留存审批记录，记录应包含删除原因、数据范围、数据级别、执行人、执行时间、复核人。

d） 审计不同类别数据的删除处置措施：

1）个人信息：应区分直接个人信息、去标识化信息，核查个人信息主体行使删除权时的响应流程、处理时限；去标识化信息如仍可重识别，应按照个人信息要求执行删除；

2）重要数据：核查删除操作是否留存处置记录，重要数据删除后开展有效性复核；

3）匿名化数据：按照合约约定执行，匿名化且不可复原的，可按协议不强制删除，但应留存协议依据。

e） 审计技术删除执行有效性：核查是否采用不可逆删除手段；禁止仅做逻辑标记、仅修改访问权限替代物理或逻辑彻底删除；对于云平台、SaaS 服务流通的数据，审计应确认云侧存储、快照、备份实例中的对应数据完成处置。

f） 审计删除操作日志审计留存：数据删除全过程操作日志应完整留存，日志包含操作账号、时间、数据对象、操作类型、结果，日志本身不得被随意删除，留存周期符合法规及合约要求。

g） 审计删除效果验证机制：被审计方是否建立删除后复核验证手段；高敏感、重要数据流通场景，应抽样开展删除结果核验；发现未彻底删除残留数据，应纳入审计发现问题，提出整改要求。

6.2.9 其他审计

审计其他相关控制时，审计范围包括但不限于：

a） 共享数据提供方应基于国家相关法律法规对数据使用和分析处理的相关要求建立数据使用监管机制，约束数据使用方对共享数据的正当使用；

b） 应确保以不可逆方式销毁数据及其副本内容；

c） 应建立符合数据销毁策略和管理制度的销毁审批机制，记录审批过程；

d） 应对数据销毁处理过程相关的操作进行记录，以满足安全审计的要求。

7 数据安全审计机构能力

7.1 数据安全审计体系

数据安全审计服务机构应具备以下要求：

a） 在中华人民共和国境内依法注册，具有独立法人资格，近三年内无重大违法违规记录和严重失信行为；

b） 数据安全审计服务机构应制定管理制度，包括机构人员管理中的相关职责、仪器设备的购置、使用和运行维护的各项规定等。

c） 机构应严格遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国认证认可条例》及网络与数据安全相关行业监管文件等相关法律法规；

d） 机构及其从业人员开展相关业务时，应当遵守法律法规的规定，诚实守信，勤勉尽责，遵守职业道德规范，不得危害国家安全、公共利益以及企业和个人的合法权益。

e） 机构及其从业人员开展数据安全审计相关业务，应当坚持独立、客观、公正原则，对于任何组织和个人的不当干预应当予以拒绝。

f） 机构及其从业人员应当遵守保密原则，妥善保存客户委托文件、数据资料、审计底稿等信息和资料，任何人不得泄露、隐匿、伪造、篡改或者毁损。

g） 数据安全审计服务机构应确保数据安全审计设备和工具运行状态良好，并通过持续更新、升级等手段保证其提供准确的测评数据。

h） 数据安全审计服务专业机构应具备开展数据安全审计的技术能力，能够真实、有效、充分地开展数据安全审计。

7.2 数据安全审计能力

7.2.1 数据安全审计方法

a） 访谈法

通过面对面或在线视频、音频等方式交谈来了解被审计对象的信息。依据不同问题的性质、目的或对象，采用不同的访谈形式。

b） 调查法

通过发放调查问卷、查阅统计资料、函证等方式，对审计事项进行调查核实，获取审计证据。调查法适用于对被审计对象数据安全管理状况的全面了解和对特定事项的函证确认。

c） 检查法

审查书面资料的真实性、合法性，如政策、制度、流程等；审查各种相关资料的一致性，对各类资料之间的相关数据，按照其内在联系进行相互对照检查，以获取审计证据；对书面资料或信息系统的相关数据进行重新计算，以验证原计算结果是否正确；对重要的比率或趋势进行的分析，包括调查异常变动以及这些重要比率或趋势与预期数额和相关信息的差异，以获取审计证据。

d） 观察法

观察相关人员正在从事的活动或实施的程序。观察法所提供的审计证据仅限于观察发生的地点，由于观察人员的行为可能因被观察而受影响，从而导致观察提供的审计证据受到限制。

e） 测试法

基本原理是从计算机输入开始，跟踪某项业务直至输出，以检验计算机应用程序、控制程序和系统可靠性。执行此类方法使用的是用于测试目的的业务数据，称之为测试数据。

f） 验证法

可验证系统的控制是否有效和计算逻辑的正确性；对系统采集数据、转换数据及处理数据的过程和结果进行控制和实质性测试，验证系统数据的合规性、一致性及准确性，并对系统的相关指标进行分析和评价。

7.2.2 数据安全审计人员能力

数据安全审计人员应具备以下能力要求

a） 数据安全审计人员应经过网络与数据安全专业培训，具备相应的专业知识和技能，鼓励取得数据安全、网络安全相关专业认证；

b） 数据安全审计服务机构应持续开展对数据安全审计人员的培训，培训内容应包括政策法规及标准规范、实践经验、数据安全审计案例、工具使用等，培训方式可采用内训、外训相结合的方式，每年培训时间应不少于20学时。

c） 掌握与数据合规相关的专业知识和技能，包括数据安全、信息安全、安全风险及应对措施等；

d） 根据获取的审计证据，具备评估审计风险是否降低至可以接受水平的能力，并形成审计意见。

e） 对数据安全审计人员进行背景审查，审查结果长期留存并可供认证认可相关机构查看。

7.2.3 数据安全审计其他能力

数据安全审计应具备以下其他能力要求

a） 机构应通过多种措施对被审计单位可能面临的风险加以规避和控制；

b） 机构应建立安全应急处置机制，防范发生审计风险。

c） 机构应制定完备的、符合自身特点的数据安全审计项目管理程序，主要包括审计工作的组织形式、工作职责，审计各阶段的工作内容和管理要求等。