ICS 35.030
CCS L70

YD

中华人民共和国通信行业标准

YD/T xxxx—2023

数据安全治理能力通用评估方法

General evaluation method of data security governance capability

（报批稿）

2022 年 10 月 8 日

[××××]-[××]-[××]发布　　[××××]-[××]-[××]实施

中华人民共和国工业和信息化部　发 布

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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、中国移动通信集团有限公司、奇安信科技集团股份有限公司、杭州安恒信息技术股份有限公司、蚂蚁科技集团股份有限公司、北京百度网讯科技有限公司、上海观安信息技术股份有限公司、北京数牍科技有限公司、杭州美创科技有限公司、郑州信大捷安信息技术股份有限公司、联通华盛通信有限公司、北京天融信网络安全技术有限公司、OPPO广东移动通信有限公司、中国移动通信集团有限公司、联通数字科技有限公司、浪潮云信息技术股份公司、北京数安行科技有限公司、北京国双科技有限公司、北京亿赛通科技发展有限责任公司、恒安嘉新（北京）科技股份公司、中兴通讯股份有限公司、深圳市和讯华谷信息技术有限公司、上海新炬网络信息技术股份有限公司。

本文件主要起草人：刘雪花、李雪妮、龚诗然、闫树、魏凯、姜春宇、李天阳、郝志婧、张越、张亚兰、范东媛、王新华、梁伟、马冰珂、孟小楠、郭建领、孙硕、谢江、裴超、王泽、刘为华、尚晶、 陈卓、郑涛、陈洪运、付艳艳、温暖、李文琦、刘飞龙、何晓倩、周庆勇、刘玉红、张柏、李楷、孟娟、王文娟、马超、张艺伟、黄国标。

目　次

数据安全治理能力通用评估方法

1 范围

本文件规定了数据安全治理能力通用评估方法，包括评估实施方法，评估结果等级划分和数据安全治理能力在各等级的具体要求和评估细则。

本文件适用于企业针对其拥有的数据开展数据安全治理工作，为其数据安全治理能力评估提供参考和指引。

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 25069 信息安全技术 术语

GB/T 29246—2017 信息技术 安全技术信息安全管理体系

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 37988—2019和GB/T 35273界定的以及下列术语和定义适用于本文件。

3.1

数据安全治理 data security governance

在组织数据安全战略的指导下，为确保组织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，内外部相关方协作实施的一系列活动集合。

注：活动包括建立数据安全治理组织架构，制定数据安全制度规范，构建数据安全技术体系，建设数据安全人才梯队等。

3.2

数据使用 data using

在组织内部开展的数据开发利用活动的过程。

3.3

数据共享 data disclosing and sharing

在组织之间、组织与外部个人之间进行数据提供或交换的过程。

3.4

合规 compliance

对数据安全所适用的法律法规的符合程度。

[来源：GB/T 37988—2019,3.16]

3.5

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[来源：GB/T 35273,3.1,有修改]

3.6

敏感个人信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

[来源：GB/T 35273,3.2]

4 概述

4.1 评估原则

数据安全治理能力评估应遵守如下原则：

a) 标准性原则：评估工作应依据本文件展开；

b) 客观公正原则：评估发现、评估结论和评估报告应真实和准确地反映评估活动，不带评估人员个人偏见，以确保评估发现和评估结论仅建立在评估证据的基础上；

c) 保密原则：评估人员应审慎使用和保护在评估过程获得的信息，以保障被评估方数据安全。可以在评估前与被评估单位就数据安全保密责任义务进行认定与划分，包括不限于保密协议签署等。

4.2 评估实施方法

评估实施方法主要通过文档查验、人员访谈、工具演示等方式对评估对象的实际建设情况进行评估。

文档查验是指评估人员查阅数据安全相关文件资料，如组织数据安全管理制度、业务技术资料和其他相关文件，用以评估数据安全治理相关制度文件是否符合标准要求。评估对象需要事先完整准备上述文档以供评估人员查阅。

人员访谈是指评估人员通过与评估对象相关人员进行交流、讨论、询问等活动，以评估数据安全保障措施是否有效。评估对象需要安排熟悉数据流转过程，以及承载数据的应用、系统、规划等情况的人员参加访谈。

工具演示是指由评估对象相关人员进行展示，评估人员查看承载数据的应用、系统等，以评估数据安全保障措施是否有效。评估对象需要安排相关人员进行现场演示，评估人员根据系统演示情况进行查验。

4.3 评估实施过程

评估实施过程主要包括评估准备、评估执行和评估审核三个阶段，与评估对象的沟通和洽谈贯穿整个过程，评估实施过程如图1所示。

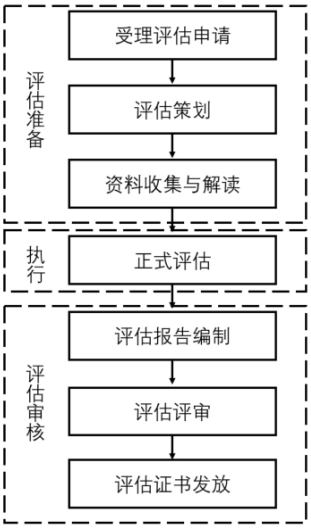

图1 评估实施过程

评估准备阶段由评估机构受理评估对象的评估申请，确定评估小组成员，并进行评估策划，通过对评估对象进行资料收集与解读，了解评估对象的基本情况，如评估对象的组织架构、评估对象的数据安全治理系统清单、数据安全治理制度清单、数据安全治理的工具使用情况、数据安全治理部门职责和人员角色等。

评估执行阶段由评估小组进入评估对象现场进行正式评估，由评估对象安排相关工作人员按照评估等级要求逐项展示相关资料，供评估小组成员审阅及询问。

评估审核阶段由评审专家通过评审会的形式对评估报告的编制进行审核，以最终确定评估等级，并进行评估等级证书的发放。

5 数据安全治理体系框架

数据安全治理体系框架是组织的数据安全治理建设蓝图，也是组织数据安全治理能力的集中体现和主要成果转化。如图2，给出了一种较为典型的数据安全治理体系框架，主要包括数据安全管理体系、数据安全通用技术体系和数据安全运营体系。

数据安全管理体系包括组织架构的建设、制度流程的建设和人员能力的建设三方面。组织架构方面，建议建成决策层、管理层、执行层和监督层的组织架构，以保障数据安全治理的有效落地实施。制度流程方面，建议在遵循现有相关国家要求的基础上，结合组织业务发展需要，建成4级数据安全制度体系，涵盖数据安全方针政策、管控策略、操作指南和模板清单，以指导数据安全治理工作的开展。人员能力方面，建议建成从数据安全意识、数据安全技能到数据安全技术逐层递进的人员能力体系，以形成良好的数据安全企业文化，建立完善的数据安全人才队伍。

数据安全通用技术体系围绕数据全生命周期的安全防护技术体系，实现各项数据安全制度要求的落实，为实现数据安全防护总体目标提供技术支撑。数据安全治理技术工具可分基础安全技术工具和数据生命周期安全技术工具。其中基础安全技术工具建议包括数据分类分级、身份认证与访问控制、日志管理、监控审计和安全评估等技术工具。数据生命周期安全技术为数据生命周期特定环节适用的

技术，以保障这些环节的数据安全，建议包括敏感数据识别、备份与恢复、数据加密、数据脱敏、数据水印、API管控、数据防泄漏、隐私计算、数据删除、介质销毁等技术。

数据安全运营体系建议包括数据运营、安全运营和合规运营三方面。数据运营包括数据资产的持续梳理和数据分类分级管理，数据资产的梳理实现对组织持续产生的数据的资产化管理，数据分类分级管理实现对存量数据资产、新增数据资产或者因使用场景、汇聚融合、脱敏等原因发生变化的数据资产的分类分级管理。安全运营包括数据安全策略管理、安全风险监测审计、安全事件应急响应三方面，通过安全运营实现事前防范、事中监控预警、事后应急处置的全链条管理，保障数据安全治理体系持续安全有效。合规运营包括合规库管理和合规评估，合规库管理通过持续跟进最新监管要求，结合组织实际情况进行解读和内化，形成企业合规管理的基线，合规评估依据合规基线定期开展组织各业务线合规评估，促进业务高质量发展。

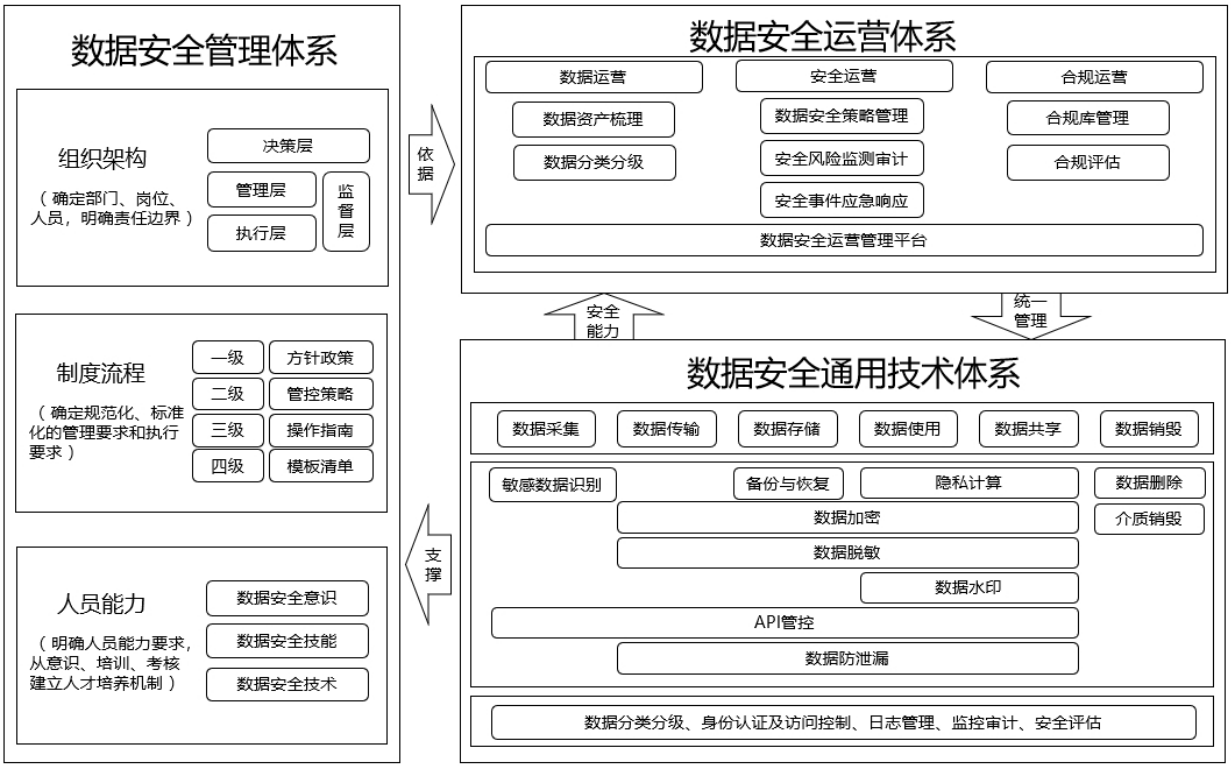

图2 数据安全治理体系框架

6 数据安全治理能力总体要求

数据安全治理能力包括数据安全战略、数据全生命周期安全、基础安全三部分，如表1所示。

表1 数据安全治理能力体系

评估维度	安全战略		数据全生命周期安全						基础安全						
	数据安全规划	机构人员管理	数据采集安全	数据传输安全	数据存储安全	数据使用安全	数据共享安全	数据销毁安全	数据分类分级	合规管理	合作方管理	监控审计	身份认证与访问控制	安全风险分析	安全事件应急
组织建设	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1
制度流程	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1	S1
技术工具	S3	S3	S3	S3	S3	S3	S3	S3	S2	S1	S1	S4	S4	S4	S4
人员能力	S1	S1	S3	S3	S3	S3	S3	S3	S2	S1	S1	S4	S4	S4	S4

数据安全战略能力包括：数据安全规划、机构人员管理。

数据全生命周期安全能力包括：数据采集安全、数据传输安全、数据存储安全、数据使用安全、数据共享安全、数据销毁安全。

基础安全能力包括：数据分类分级、合规管理、合作方管理、监控审计、身份认证与访问控制、安全风险分析、安全事件应急。

数据安全治理能力评估划分为4个评估域，见图3，分别是数据安全管理（S1）、数据分类分级（S2）、数据全生命周期安全保护（S3）和数据安全运营（S4），评估域与数据安全治理能力体系对应关系见表1。

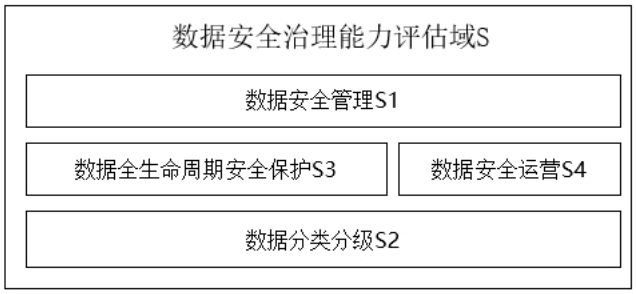

图3 数据安全治理能力评估域示意图

7 评估等级

7.1 第一级 初始级

数据安全治理能力体现在个别项目中，没有正式的数据安全治理组织、制度流程，没有完整的技术体系，主要是被动式管理，较依赖个人能力。具体特征如下：

a) 没有正式的数据安全组织架构、制度流程、技术工具或人才体系；

b) 仅根据临时需求在个别项目中体现了数据安全相关工作；

c) 数据安全意识不足。

7.2 第二级 重点执行级

数据安全治理能力主要是体现在部门或者数据职能领域中，建立了基本的制度流程及技术工具，对部门或者数据职能领域的数据安全保护满足合规要求。具体特征如下：

a) 一般由各部门人员负责数据安全相关工作；
b) 初步制定了数据安全管理制度流程，以保障组织部门或者数据职能领域安全执行及故障恢复；
c) 尝试采用技术工具落实数据安全要求，但对数据全生命周期的覆盖范围及保护能力有限；
d) 开始关注组织内人员的数据安全意识，开展了数据安全相关培训。

7.3 第三级 全面治理级

数据安全治理能力体现在组织层面，具备完善的标准化管理机制和技术体系，能够促进数据安全的规范化落地，能完全满足合规要求。具体特征如下：

a) 成立了专门的数据安全管理团队，并设置了数据安全相关岗位、明确了人员；
b) 具备了完善的数据安全管理制度和流程，以保障组织内各业务的安全执行及故障恢复；
c) 具备了较强的技术能力，配备了足够的技术工具，以有效保障组织内各业务的数据全生命周期安全；
d) 制定了数据安全培训计划，并定期开展培训。

7.4 第四级 量化评估级

数据安全治理能力体现在组织的数据安全治理的效率、效果能量化分析和监控。具体特征如下：

a) 建立了可量化的评估指标体系，能够准确评估数据安全的治理效果并及时做出调整；
b) 建立了统一的技术工具和平台，能够为组织的数据安全治理提供有效支撑；
c) 制定了数据安全培训计划及考核机制，提升组织数据安全意识并营造数据安全文化。

7.5 第五级 持续优化级

数据安全治理能力体现在能根据最新的外部监管要求、内部发展需要和相关技术的发展，持续改进和优化数据安全治理体系,成为行业标杆并推广至行业。具体特征如下：

a) 实现了数据安全制度、规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进；
b) 实现了数据安全技术体系的持续优化，能够根据组织数据安全治理的战略目标和规划的变化和相关技术的发展进行持续优化；
c) 主导国际、国家和行业标准的制定，具备数据安全研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

8 数据安全战略

8.1 数据安全规划

8.1.1 概述

根据数据安全风险状况建立组织整体数据安全规划，数据安全规划的内容应覆盖数据全生命周期的安全风险管控。

8.1.2 等级要求

8.1.2.1 第一级

第一级应从制度流程方面满足如下要求：

a) 制度流程：应在项目的建设过程中反映了数据安全管理的目标和范围。

8.1.2.2 第二级

第二级应从组织建设、制度流程方面满足如下要求：

a) 组织建设：应设置核心部门的数据安全规划相关的岗位和人员，负责制定核心部门的数据安全规划，并推进规划的开展和实施。

b) 制度流程：应对核心部门进行数据安全规划，并明确基本的合规要求。

8.1.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据安全管理部门、岗位和人员，负责协调安全管理、推进技术工具建设、推进规划开展执行。

b) 制度流程：

1) 应明确符合组织数据战略规划的数据安全战略，明确安全策略、方针、目标、原则，其中方针和策略应明确对组织的价值和意义；

2) 应制定数据安全规划，明确需要执行的活动、所需资源和实施计划；

3) 应明确数据安全规划活动的执行频率、审核机制及发布流程等；

4) 应在组织层面制定了数据安全管理相关的制度体系，如管理办法和操作规程等文件。

c) 技术工具：应在内部管理平台设置数据安全制度文件分发及管理渠道，在组织内部对数据安全制度文件进行推广。

d) 人员能力：

1) 应了解组织的业务发展目标，规划工作中能够将其与数据安全目标进行有机结合；

2) 应具备资源统筹协调能力，定期开展宣贯工作在组织内推进规划的实施；

3) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

8.1.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具和人员能力方面满足如下要求：

a) 制度流程：

1) 应对安全规划效果、数据安全制度完善情况进行量化评估，制定数据安全治理能力提升计划；

2) 应定期评估数据安全战略规划、数据安全总体策略、目标、方针、策略对组织生产运营、业务发展目标、IT 目标的和合规要求适应性，并进行适度调整。

b) 技术工具：应实现数据安全规划效果和数据安全制度完善情况量化评估方法。

c) 人员能力：负责人员应具备评估规划实施效果的能力，并可根据既定标准对规划文件进一步修订。

8.1.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持数据安全制度流程的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。
b) 技术工具：
   1) 应能够通过技术工具执行对数据安全规划的动态管理；
   2) 应支数据安全技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；
   3) 应能主导国际、国家和行业标准的制定，具备数据安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

8.1.3 评估方法

8.1.3.1 第一级

根据第一级要求，从制度流程方面进行查验：
a) 查验是否在项目建设过程中考虑了数据安全管理要求。

8.1.3.2 第二级

根据第二级要求，从组织建设、制度流程方面进行查验：
a) 查验是否在核心部门设置了数据安全规划相关的岗位和人员，并在岗位职责描述中明确了数据安全规划相关职责。
b) 查验是否在核心部门制定了数据安全相关制度文件：
   1) 是否明确了部门的数据安全策略、规划和保护机制等；
   2) 是否定义了合规要求。

8.1.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：
a) 查验是否在组织层面设置了数据安全规划相关的部门、岗位和人员，并在部门和岗位的职责描述中明确了数据安全规划相关职责。
b) 查验是否在组织层面制定了数据安全规划相关制度文件：
   1) 是否考虑了国家法律法规和监管要求，以及组织的数据安全需求；
   2) 是否制定了组织的安全策略、方针、安全目标和安全原则等内容；
   3) 是否明确了组织的数据安全战略规划，包括各阶段目标、任务、所需资源、支持岗位、时间安排和实施步骤等内容；
c) 查验是否在组织层面制定了数据安全管理相关制度文件：
   1) 是否明确了数据安全工作的基本原则，数据安全管理规则和程序以及围绕数据全生命周期进行保护的具体的操作流程、规范、内外部协调机制等；
   2) 是否明确了数据安全制度的编制、评审、发布、更新流程。
d) 查验组织技术工具：
   1) 是否开展数据安全规划研讨会；
   2) 是否在内部管理平台设置数据安全制度文件分发及管理渠道。
e) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

8.1.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 查验组织的制度文件：
   1) 是否明确了安全规划实施效果评估指标,如数据安全规划覆盖面、完善程度等；
   2) 是否明确了数据安全制度的评估指标，如数据安全制度完备比率，数据安全制度执行率等；
   3) 是否明确了量化评估开展的频率；
   4) 是否进行量化评估结果分析，并根据分析结论要求优化数据安全规划、修订数据安全制度等。
b) 查验组织的技术工具：是否有安全规划和数据安全体制体系评估和改进记录。
c) 查验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

8.1.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验是否具有数据安全制度、规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b) 查验组织的技术工具：
   1) 是否能够对于数据安全规划和制度流程进行动态管理；
   2) 是否具有数据安全技术持续优化升级的记录，其优化动机体现了外部监管要求、内部发展需要或者最新技术的发展等；
   3) 是否主导国际、国家和行业标准的制定；
   4) 是否具备数据安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

8.2 机构人员管理

8.2.1 概述

建立负责组织内部数据安全工作的部门、岗位和人员，并与人力资源管理部门进行联动，防范机构人员管理过程中存在的数据安全风险。

8.2.2 等级要求

8.2.2.1 第一级

第一级应从组织建设和人员能力方面满足如下要求：

a) 组织建设：应在具体的项目中体现出数据安全管理的角色及职责。
b) 人员能力：应具备依据个人经验解决数据安全问题的能力。

8.2.2.2 第二级

第二级应从组织建设、制度流程、人员能力方面满足如下要求：

a) 组织建设：应设置核心部门的数据安全治理相关的岗位和人员，负责核心部门的数据安全治理，并推进相关工作的开展和实施。
b) 制度流程：

1) 应明确核心部门数据安全岗位的职责规定；
2) 应对安全负责人和关键岗位的人员进行安全背景审查；
3) 应与所有涉及数据服务的人员签订保密协议；
4) 应明确核心部门数据安全培训制度，对相关人员开展数据安全培训；
5) 应明确核心部门数据安全违规的内部处理制度。

c) 人员能力：
1) 应能够充分了解目前数据安全在组织整体业务目标中的定位；
2) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

8.2.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a)组织建设：
1) 应设置组织层面的数据安全治理相关的部门、岗位和人员，负责组织层面的数据安全治理，与其他部门协同工作，推进相关工作的开展和实施；
2) 应指定机构最高管理者或授权代表担任数据安全责任人，负责统筹数据安全治理工作；
3) 应建立数据安全监督管理职能部门，负责对组织内部的数据操作行为进行监督；
4) 应设置数据安全培训相关岗位和人员，负责对数据安全培训进行统筹管理，包括培训需求分析及落地方案的制定和实施；
5) 当组织处理个人信息达到国家网信部门规定数量时，应指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

b)制度流程：
1) 应明确数据安全岗位和人员的要求，明确其工作职责，以及部门之间的协作关系和配合机制；
2) 应明确数据安全责任体系和追责机制，定期对责任部门和安全岗位组织安全检查，形成检查报告；
3) 应明确组织层面的数据服务人员招聘、录用、上岗、调岗、离岗、考核、选拔等人员安全管理制度；
4) 应于数据处理关键岗位及人员签订数据安全责任书；
5) 应对核心业务岗位候选者从法律法规、行业道德准则等层面执行背景调查；
6) 应明确数据服务涉敏岗位的职权分离、多人共管等安全管理要求；
7) 应根据组织内部员工的岗位职责，制定相应的数据安全培训计划，按计划定期对员工开展数据安全培训。

c)技术工具：
1) 应具备工具及时终止或变更离岗和转岗员工的数据操作权限，并及时将人员的变更通知到相关方；
2) 应具备工具在员工入职时应按最小必要原则分配初始权限；
3) 应以公开信息且可查询的形式，面向组织全员公布数据安全职能部门的组织架构。

d)人员能力：
1) 负责机构人员管理的员工应充分理解人力资源管理流程中可对安全风险进行把控的环节；
2) 应对员工开展数据安全教育，通过培训、考试等手段提升其整体的数据安全意识，形成组织的数据安全保护文化；

3) 负责设置数据安全职能的人员应能够明确组织的数据安全工作目标及组织的战略发展方向。

8.2.2.4 第四级

第四级应在第三级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：
   1) 当组织为重要互联网平台服务、用户数量巨大、业务类型复杂类型企业时，应成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；
   2) 境外的个人信息处理者，应在境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。
b) 制度流程：
   1) 应明确数据服务人力资源安全策略，明确不同岗位人员在数据生命周期各阶段相关的工作范畴和安全管控措施；
   2) 应明确重要岗位人员安全能力要求，并确定其培训技能考核内容与考核指标，定期对重要岗位人员进行审查和能力考核；
   3) 应明确对人员管理效果的量化评估方式、频率和调整计划；
   4) 应明确对数据安全培训效果的量化评估方式、频率和调整计划；
   5) 应定期评估在当前组织职能架构下，数据安全职能岗位与业务职能岗位之间的关系是否平衡，是否能够保证安全需求在业务中的推广。
c) 技术工具：应实现人员管理效果、数据安全培训效果的量化评估方法。
d) 人员能力：
   1) 负责组织和人员管理的人员应定期反馈数据安全培训和考核情况，及时和数据安全管理部门有关领导汇报；
   2) 应具备结合公司数据安全职能人员培训和考试的考核情况，挖掘出提高能力水平的改进点，建立改进目标，优化培训内容和方式的能力。

8.2.2.5 第五级

第五级应在第四级的等级要求上，从组织建设、制度流程、人员能力方面满足如下要求：

a) 组织建设：应能够持续优化组织的数据安全职能设置，确保组织建设的健全，以满足最新的外部监管要求和内部的发展需要。
b) 制度流程：
   1) 应能够持续优化组织和人员管理的相关流程，确保人员管理的完善，以满足最新的外部监管要求和内部的发展需要；
   2) 应能够定期对数据安全相关人员根据外部监管要求、内部发展需要和技术的发展进行人员安全能力优化、能力提升。
c) 人员能力：应具备数据安全政策、标准、产业动态、技术趋势的研究分析能力，并具有根据分析成果对组织的数据安全治理体系进行持续优化的能力。

8.2.3 评估方法

8.2.3.1 第一级

根据第一级要求，从组织建设和人员能力方面进行查验：

a) 查验组织的组织建设：是否在具体项目建设中临时指定人员负责数据安全相关工作；

b) 查验组织的人员能力：个别人员是否具有解决数据安全问题的相关经验。

8.2.3.2 第二级

根据第二级要求，从组织建设、制度流程、人员能力方面进行查验：

a) 查验是否在核心部门层级制定了相关制度文件明确数据安全部门和岗位的职责。

b) 查验组织的制度流程：

1) 查验是否制定了数据安全管理人员的培训计划，包含数据安全意识培训，合规培训等内容；

2) 查验是否与涉及数据服务的人员签订了保密协议；

3) 查验是否明确了数据安全违规的内部处理制度。

c) 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

8.2.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验组织建设：

1) 查验是否设立了数据安全管理责任部门、岗位及人员，明确规定了其职责范围；

2) 查验是否根据职责分离原则设置数据安全管理的岗位和人员；

3) 查验是否指定了机构最高管理者或授权代表担任数据安全责任人；

4) 查验是否在各部门配备了数据安全岗位和人员，具体执行落实部门内数据安全工作；

5) 查验是否设立了数据安全的监督部门，该部门负责对组织内部数据安全操作行为进行监督；

6) 查验是否设立了相关岗位和人员负责数据安全培训工作；

7) 查验是否依据合规要求指定个人信息保护负责人，查验其职责是否包含对个人信息处理活动以及采取的保护措施等的监督要求。

b) 查验组织的制度流程：

1) 查验是否在人力资源安全管理相关制度明确了人员招聘、录用、上岗、调岗、离岗、考核、选拔过程中的相关安全要求；

2) 查验是否与数据处理关键岗位及人员签订了数据安全责任书；

3) 查验是否在录用核心业务岗位人员时，从法律法规、行业道德准则等层面执行背景调查；

4) 查验组织是否建立了数据安全责任体系和包括安全规划、建设、运营等在内的各责任部门；

5) 查验是否建立了数据安全追责机制，定期对责任部门和安全岗位组织安全检查，形成检查报告；

6) 查验是否在岗位职责相关制度文件中明确了数据服务涉敏岗位的职权分离、多人共管等安全管理要求；

7) 查验是否制定了团队培训、能力提升计划，通过引入内部、外部资源定期开展人员培训，提升团队人员的数据安全治理技能。

c) 查验组织的技术工具：

1) 是否支持人员流动与数据操作权限的联动管理；

2) 是否实现了数据安全组织架构的公开查询。

d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

8.2.3.4 第四级

根据第四级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验组织：
   1) 是否成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；
   2) 境外的个人信息处理者是否在境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。
b) 查验组织是否明确了人员管理效果的量化评估方式：
   1) 是否定义了量化评估指标，如数据安全岗位设置完整度，团队人员与公司规模的比例等；
   2) 是否规定了量化评估频率。
c) 查验组织是否明确了数据安全培训效果的量化评估方式：
   1) 是否定义了量化评估指标，如数据安全培训的人员参与率、通过率等；
   2) 是否规定了量化评估频率。
d) 查验组织的技术工具：
   1) 是否具备对机构人员管理和数据安全培训效果进行量化评估的工具；
   2) 是否定期开展量化评估；
   3) 是否进行量化评估结果分析，并根据分析结论要求对人员管理流程和数据安全培训内容和计划等做出调整。
e) 查验组织的人员能力：
   1) 通过访谈、查验工作记录等方式，查验职能人员是否具备相应的人员管理和培训计划、执行能力；
   2) 通过访谈、考察输出成果等方式，查验数据安全专业人员是否具备完善的数据安全知识体系和实践能力。

8.2.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了人员管理的优化工作机制：
   1) 是否支持根据政策变化、架构调整、业务发展等需求优化组织的数据安全职能设置；
   2) 是否支持根据政策变化、架构调整、业务发展等需求优化组织人员管理的相关流程；
   3) 查验组织的团队培训、能力提升计划是否依据组织安全战略规划、安全治理体系建设和发展的需要不断优化。
b) 查验组织的人员能力：
   1) 是否根据最新的监管要求和技术发展更新、优化培训课程设置，配置相应培训资源；
   2) 通过访谈、考察输出成果等方式，查验相关人员是否具备完善的数据安全知识体系，并具有全球视野，能根据全球技术发展动态及时调整、优化所在组织的数据安全治理体系和人才培养体系。

9 数据全生命周期安全

9.1 数据采集安全

9.1.1 概述

根据组织对数据采集的安全要求，建立数据采集安全管理措施和安全防护措施，规范数据采集相关的流程，从而保证数据采集的合法、合规、正当和诚信。

9.1.2 等级要求

9.1.2.1 第一级

第一级应从制度流程方面满足如下要求：

a) 制度流程：未建立数据采集安全管理制度和流程，仅根据个别业务临时需要或项目人员经验考虑了数据采集安全管理。

9.1.2.2 第二级

第二级应从组织建设、制度流程方面满足如下要求：

a) 组织建设：应设置核心部门的数据采集安全相关的岗位和人员，负责核心部门的数据采集安全管理，并配合推进相关工作的开展和实施。

b) 制度流程：

1) 应定义核心部门的数据采集管理规范，明确数据采集的合法、正当、必要和诚信原则；
2) 个人信息采集应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围，并提供隐私政策与用户协议；
3) 应明确个人信息的采集需要用户授权同意，法律规定可授权豁免的情况除外；
4) 应明确当已知采集的个人信息为不满十四周岁未成年人个人信息时的采集规范，并应取得监护人同意。

9.1.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据采集安全相关的部门、岗位和人员，负责组织层面的数据采集安全管理，与其他部门协同工作，配合推进相关工作的开展和实施。

b) 制度流程：

1) 应明确数据采集安全管理要求，定义数据的直接或间接采集流程和方法；
2) 应梳理本企业数据采集渠道，针对直接采集和间接采集，分别明确安全合规要求及安全审核流程；
3) 应规定涉及个人信息采集授权同意及合规性评估流程；
4) 应明确外部数据源已获得的个人信息处理的授权同意范围，包括使用目的、采集范围、个人信息主体是否授权同意共享等；
5) 应规定个人信息的处理目的、处理方式和处理的个人信息种类发生变更时需重新取得个人同意；
6) 针对外部数据源采集时，应与数据提供方签订协议，明确数据提供方数据采集渠道、合作数据范围及类型、双方权利义务等。涉及个人信息的，应审核用户隐私协议是否涵盖合作的数据内容以及用户授权流程和方式的合理性；
7) 应规定数据采集过程中需要采取的控制措施，确保采集过程中的数据不被泄漏，尤其是

个人敏感信息；

8) 应规定用户提出撤回同意和终止服务时的停止采集的要求，当用户撤销同意或者注销账户时，不得设置过多不合理的条件；

9) 应明确个人敏感信息处理的单独同意要求。

c) 技术工具：

1) 应具备技术工具保证数据采集过程中个人信息的保密性、完整性、可用性；

2) 应具备数据采集工具，具备详细的日志记录功能，保障数据采集过程的完整记录；

3) 应具备数据采集审计工具，检测数据采集范围、类别、频度等的合理性，检测采集过程的安全性；

4) 应具备便捷的个人信息查询、纠正和撤回同意、账号注销的方式和权益申诉机制。

d) 人员能力：

1) 应能充分理解数据采集相关的法律、行政法规要求和业务需求中的数据安全要求，并能根据数据安全需求提出针对性的解决方案；

2) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

9.1.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应规定数据采集安全管理效果的量化评估方式、频率和调整计划。

b) 技术工具：

1) 应实现数据采集安全管理效果的量化评估方法；

2) 应基于合规评估的数据采集策略（如原则、频度、范围等），实现数据合规性监控与告警；

3) 应具备对采集工具和渠道进行统一管理的平台。

9.1.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持数据采集安全规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。

b) 技术工具：

1) 应支数据采集安全技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；

2) 应能主导国际、国家和行业标准的制定，具备数据采集安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.1.3 评估方法

9.1.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别项目中考虑了数据采集的合规性要求。

9.1.3.2 第二级

根据第二级要求，从组织建设、制度流程方面进行查验：

a) 查验是否在核心部门设置了数据采集安全相关的岗位和人员，并在岗位职责描述中明确了数据采集安全相关职责。
b) 查验是否在核心部门层级制定了数据采集安全相关制度文件：
   1) 是否明确规定了数据采集原则、采集渠道、采集流程、采集方式、采集频度、采集类型、采集范围、采集数据格式及停止采集等要求；
   2) 是否规定了数据采集的合规性评估流程；
   3) 是否明确了个人信息采集，尤其是个人敏感信息采集的目的、方式、范围、保存时限、到期处理方式等；
   4) 是否规定了个人敏感信息的采集应明确必要性及对个人的影响；
   5) 是否明确了个人信息采集的授权同意规定；
   6) 是否明确了未满十四周岁未成年人的个人信息采集规范，及监护人的授权同意。
c) 查验该部门的隐私政策文件及用户协议：
   1) 是否符合国家法律法规和监管要求；
   2) 是否明确告知个人信息处理者的姓名和联系方式，采集的目的、方式、用途、范围、保存时限、到期理方式等；
   3) 是否明确告知个人敏感信息的采集的必要性及对个人的影响；
   4) 是否明确告知未满十四周岁未成年人的个人信息采集规范，及监护人的授权同意。

9.1.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：
a) 查验组织是否设立了负责数据采集安全管理的部门、岗位、人员。
b) 查验是否在组织层级制定了数据采集安全相关制度文件：
   1) 是否覆盖了组织内涉及采集活动的全部业务；
   2) 是否对直接和间接采集进行区分管理；
   3) 是否明确规定了数据采集原则、采集渠道、采集流程、采集方式、采集频度、采集类型、采集范围、采集数据格式及停止采集等要求；
   4) 是否规定了数据采集的合规性评估流程；
   5) 查验与数据提供方签订协议，是否明确数据提供方数据采集渠道、合作数据范围及类型、双方权利义务等；
   6) 是否规定了涉及个人信息采集授权同意及合规性评估流程；
   7) 是否明确规定了当个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意；
   8) 是否明确了个人敏感信息的处理的单独同意要求；
   9) 是否规定了用户提出撤回同意和终止服务时的停止采集的要求。
c) 查验组织隐私政策文件及用户协议：
   1) 是否告知涉及个人信息采集授权同意要求；
   2) 是否告知个人信息采集过程中防泄漏措施；
   3) 是否告知用户提出撤回同意和终止服务时的停止采集的方式；
   4) 是否以显著的方式公开，是否以明显方式（如弹窗）提示用户阅读，是否难以访问（如进入 App 主界面后，需多于 4 次点击等操作才能访问到），是否难以阅读（如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等）等。
d) 查验组织的技术工具：

1) 是否记录数据采集日志，包括采集渠道、采集来源方式、数据范围和类型、采集时间、有效期期限等内容；
2) 是否采用了身份认证、授权、数据加密、安全传输通道等保证采集数据保密性；
3) 是否采用了校验码等技术验证采集数据的完整性；
4) 是否采用了负载均衡、冗余设计等技术保证采集功能的可用性；
5) 是否提供了便捷的个人信息查询、纠正和撤回同意、账号注销的方式和权益申诉机制；
6) 当业务涉及外部数据源采集时，是否签订了采集协议。

e) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

9.1.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了数据采集安全管理效果的量化评估方式：
   1) 是否定义了量化评估指标，如采集活动开始前进行合规检测的比例，间接采集个人时对第三方个人信息主体授权文件的审核率等；
   2) 是否规定了量化评估频率。
b) 验证组织的技术工具：
   1) 是否实现数据采集安全管理效果的量化评估工具；
   2) 是否定期进行数据采集安全管理效果量化评估；
   3) 是否根据量化评估结果进行及时的调整；
   4) 是否具备工具进行数据合规性的监控与告警，有效监控数据采集范围、类别、频度等，确保采集行为符合隐私政策及相关法律法规要求；
   5) 是否具备统一的数据采集工具管理平台。

9.1.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验是否具有数据采集安全规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b) 验证组织的技术工具：
   1) 是否具有数据采集安全技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；
   2) 是否主导国际、国家和行业标准的制定；
   3) 是否具备数据采集安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.2 数据传输安全

9.2.1 概述

根据组织对内和对外的数据传输需求，建立不同的数据加密保护策略和安全防护措施，防止传输过程中的数据泄漏等风险。

9.2.2 等级要求

9.2.2.1 第一级

第一级应从制度流程方面满足如下要求：

制度流程：未在任何业务中建立成熟稳定的数据传输安全管理制度，仅根据个别业务临时需要或项目人员经验采取了传输保护措施。

9.2.2.2 第二级

第二级应从组织建设、制度流程、技术工具方面满足如下要求：

a) 组织建设：应设置核心部门的数据传输安全相关的岗位和人员，负责核心部门的数据传输安全管理，并配合推进相关工作的开展和实施。

b) 制度流程：应根据合规要求和业务性能需求，明确核心业务中需要加密传输、完整性保护的数据范围。

c) 技术工具：

1) 应在数据传输前对通信双方主体进行身份认证；

2) 应具备传输数据加密、校验码、签名等技术工具。

9.2.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据传输安全相关的部门、岗位和人员，负责组织层面的数据传输安全管理，与其他部门协同工作，配合推进相关工作的开展和实施。

b) 制度流程：

1) 应明确在数据分类分级定义的基础上数据跨组织机构或者使用公共信息网络传输的安全管理要求，尤其明确个人信息、重要数据、核心数据的传输安全要求（如传输加密通道、数据内容加密、签名验签、身份认证、数据传输接口安全等）；

2) 应建立数据传输接口安全管理工作规范，包括安全域内、安全域间等数据传输接口规范；

3) 应建立对数据传输安全策略变更进行审核和监控的制度。

c) 技术工具：

1) 应提供满足数据传输安全策略的全面的安全控制技术方案；

2) 传输个人敏感信息和重要数据、核心数据时，应实施全面的保护措施，避免信息的泄露；

3) 应支持对数据传输事件进行登记和审批的机制；

4) 应支持对数据传输安全策略的变更进行审核和监控；

5) 应提供对数据传输接口的审核及监控手段。

d) 人员能力：

1) 应熟悉行业主流的安全通道建立方案、身份认证技术、数据加密算法等，从而能够基于具体的业务场景选择合适的数据传输安全实现方式，并具备针对数据传输安全管理要求在实际业务场景中制定解决方案的能力；

2) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

9.2.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：

1) 应规定数据传输安全效果的量化评估方式、频率和调整计划；

2) 应制定密钥管理规范，对不同场景的密钥使用，明确全生命周期的安全管理措施。

b) 技术工具：
   1) 应提供数据加密模块供开发传输功能的人员调用，能够根据不同数据类型和级别进行数据加密处理；
   2) 应提供全链路的数据流转的监控体系，能够实时了解数据的流向，传输情况；
   3) 应对输入输出的数据进行内容分析，及时发现数据传输中的安全问题，发现安全问题后应根据预案进行自动化应急处理；
   4) 应实现数据传输安全管理效果的量化评估方法。

9.2.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：
   1) 应能够综合量化敏感数据加密和数据传输通道加密的实现效果和成本，定期审核并调整数据加密的实现方案；
   2) 应支持数据传输安全规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。
b) 技术工具：
   1) 应支持数据传输安全技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；
   2) 应能主导国际、国家和行业标准的制定，具备数据传输安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.2.3 评估方法

9.2.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别业务中根据临时需求采取加密传输或完整性保护措施。

9.2.3.2 第二级

根据第二级要求，从组织建设、制度流程、技术工具方面进行查验：

a) 查验是否在核心部门设置了数据传输安全相关的岗位和人员，并在岗位职责描述中明确了数据传输安全相关职责。
b) 查验是否在核心部门层级制定了数据传输安全相关制度文件：
   1) 是否规定了数据传输的加密要求及加密方案；
   2) 是否规定了数据传输的完整性保护要求及方案；
   3) 规定的加密要求及加密方案是否结合了合规要求及业务性能需求；
   4) 是否规定了传输通道两侧的身份鉴别与认证。
c) 查验组织的技术工具：
   1) 是否支持对传输数据（尤其是个人敏感信息）、传输通道的加密；
   2) 是否支持对传输数据（尤其是个人敏感信息）的完整性验证；
   3) 是否支持对传输通道两侧的身份验证。

9.2.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设置了数据传输安全相关的部门、岗位和人员，并在部门和岗位的职责描述中明确了数据传输安全相关职责。

b) 查验是否在组织层级制定了数据传输安全相关制度文件：
   1) 是否明确了数据跨组织机构或者使用公共信息网络传输的安全管理要求，尤其是个人信息、重要数据、核心数据的传输，以符合国家规定及监管要求；
   2) 是否明确个人信息、重要数据、核心数据的安全传输要求，制定相应安全策略并采取保护措施（如传输加密通道、数据内容加密、签名验签、身份认证、数据传输接口安全等）；
   3) 是否明确，以符合国家规定及监管要求；
   4) 是否定义了传输策略变更的审批和监控机制。

c) 查验是否在组织层级制定了数据传输接口安全管理规范：
   1) 是否规定了新增接口、变更接口、废弃接口等的处理流程；
   2) 是否规定了传输接口的安全防护措施；
   3) 是否规定了接口梳理的工作制度；
   4) 是否规定了对涉及个人信息传输的接口应实施监控制度。

d) 查验组织的技术工具：
   1) 是否支持对接口调用的监控，尤其是涉及个人信息传输的接口，包括权限控制、流量监控、调用过载保护等；
   2) 是否支持接口调用的自动化的日志记录；
   3) 是否支持定期对接口权限控制等相关功能的安全审计；
   4) 是否支持安全通道、可信通道、加密算法等多种安全控制措施；
   5) 是否支持系统间接口的身份认证；
   6) 是否支持对传输通道缓存的自动删除；
   7) 是否支持对数据传输事件进行登记和审批的机制；
   8) 是否支持对传输安全策略变更的审核及监控；
   9) 是否支持对个人敏感信息的安全传输，如采用加密、去标识化、匿名化、传输通道的加密等技术，应符合 GB/T 35273 6.3 的要求；
   10) 是否支持对传输内容的签名验签等。

e) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

9.2.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了数据传输安全防护效果的量化评估方式：
   1) 是否定义了传输数据、传输通道加密效果的量化评估指标，如数据传输安全风险识别数量、级别、处理量等；
   2) 是否规定了传输数据、传输通道加密效果的量化评估频率。

b) 查验相关数据安全传输制度文件是否明确了密钥全生命周期管理的相关要求。

c) 查验组织的技术工具：
   1) 是否实现了分数据类型、分重要级别的数据加密模块；
   2) 是否实现了全链路的数据流转监控体系；

3) 是否支持数据传输过程的安全问题自动发现及处理；
4) 是否实现数据传输安全管理效果的量化评估方法；
5) 是否定期进行数据传输安全管理效果量化评估；
6) 是否根据量化评估结果进行及时的调整。

9.2.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否具有数据传输安全规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b) 查验组织的技术工具：
   1) 是否具有数据传输安全技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；
   2) 是否主导国际、国家和行业标准的制定；
   3) 是否具备数据传输安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.3 数据存储安全

9.3.1 概述

根据组织内部数据存储介质的访问和使用场景，以及业务特性和数据存储安全要求，提供有效的技术和管理手段，防止对存储介质的不当使用而可能引发的数据泄漏风险，实现对数据逻辑存储、存储容器等的有效安全控制。并规范数据存储的冗余管理流程，实现定期数据备份与恢复，保障数据可用性。

9.3.2 等级要求

9.3.2.1 第一级

第一级应从制度流程方面满足如下要求：

a) 制度流程：未在任何业务中建立数据存储安全管理制度，仅根据个别业务临时需要或项目人员经验考虑了存储系统的安全管理。

9.3.2.2 第二级

第二级应从组织建设、制度流程、技术工具方面满足如下要求：

a) 组织建设：应设置核心部门的数据存储安全相关的岗位和人员，负责核心部门的数据存储安全管理，并配合推进相关工作的开展和实施。
b) 制度流程：
   1) 应在核心部门建立数据存储安全的制度规范，对存储环境变更、存储介质、逻辑存储访问控制规则进行基本约束；
   2) 应建立关于核心系统的数据存储冗余策略和恢复管理机制。
c) 技术工具：
   1) 应具备工具支撑存储介质及逻辑存储空间的安全管理工作，提供如权限控制、身份认证、逻辑访问控制以及运维管理的基本能力；
   2) 应支持数据备份与恢复。

d) 人员能力：应熟悉组织的存储实现方案，并能正确使用。

9.3.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据存储安全相关的部门、岗位和人员，负责组织层面的数据存储安全管理，与其他部门协同工作，配合推进相关工作的开展和实施。

b) 制度流程：

1) 应建立存储介质及逻辑存储管理遵循的安全管理制度体系，包括安全管理政策、实施细则及指导方案，并明确个人信息、重要数据、核心数据等的存储相关规范；

2) 应建立存储介质及逻辑存储的资产管理机制，对于数据存储介质及其类型进行定义，如物理实体介质、虚拟存储介质等，资源应具备资产标识，并能够识别存储内容敏感度和数据属主；

3) 应制定数据备份与恢复的管理制度，以满足数据服务可靠性、可用性等安全目标；

4) 应制定数据备份与恢复的操作规程，明确定义数据备份和恢复的范围、频率、工具、过程、 日志记录、数据保存时长等；

5) 应建立数据备份与恢复的定期检查和更新工作规程，包括数据副本的更新频率、保存期限、一致性检查、定期演练等；

6) 应根据业务规范和合规要求，建立数据归档的操作流程；

7) 应明确组织适用的合规要求，按照法律法规和监管规定对相关数据予以记录和保存；

8) 应结合数据分类分级，明确各类各级数据的加密存储要求。

c) 技术工具：

1) 应提供逻辑存储的安全配置扫描工具，并定期扫描；

2) 应提供完善的加密存储能力，确保数据的保密性；

3) 应部署数据备份与恢复的技术工具，保证相关工作的有效执行；

4) 应定期对备份数据的有效性和可用性进行检查，定期对主要备份业务数据进行恢复验证；

5) 应通过风险提示和技术手段避免非过期数据的删除，确保在一定的时间窗口内的删除数据可以恢复；

6) 应确保存储架构具备数据存储在本地域的跨机柜或跨机房容错部署能力；

7) 应确保相关系统的网络安全建设及监督管理满足网络安全等级保护制度要求。

d) 人员能力：

1) 应了解数据备份介质的性能和相关数据的业务特性，能够确定有效的数据备份和恢复机制；

2) 应了解数据存储相关的合规性要求，并具备对合规要求的解读能力和实施能力；

3) 应定期对人员进行培训，并定期考核人员能力与岗位的匹配程度。

9.3.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：

1) 应定义存储介质、逻辑存储、存储系统架构的统一设计及安全要求；

2) 应明确数据冗余强一致性、弱一致性等控制要求，以满足不同一致性水平需求的数据副本多样性和多变性存储管理要求；

3) 应制定数据存储安全的量化评估机制，包括评估方式、频率和调整计划。

b) 技术工具：

1) 应结合数据分类分级，提供针对性的数据存储安全控制能力；
2) 应提供平台化工具支撑存储介质管理，支持存储介质的使用授权、转移、报废、维修等流程跟踪及对应存储数据的管理流程；
3) 应提供数据审查、保护系统，能够实时发现个人敏感数据信息，保障在查询、输出时及时脱敏处理；
4) 应提供为不同时效性的数据建立安全分层的数据备份方法，具备按时效性自动迁移数据的分层存储能力；
5) 存储系统应具备数据存储跨地域的容灾能力；
6) 应具备数据时效性的检测能力，以保证数据的及时删除、更新和有效性；
7) 应实现数据存储安全管理效果的量化评估方法。

9.3.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持数据存储安全规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。

b) 技术工具：

1) 应支持数据存储安全技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；
2) 应能主导国际、国家和行业标准的制定；
3) 具备数据存储安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.3.3 评估方法

9.3.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别业务中根据需求临时采取一些数据存储保护措施。

9.3.3.2 第二级

根据第二级要求，从组织建设、制度流程、技术工具方面进行查验：

a) 查验是否在核心部门设置了数据存储安全相关的岗位和人员，并在岗位职责描述中明确了数据存储安全相关职责。

b) 查验是否在核心部门层级制定了数据存储策略相关制度文件：

1) 是否明确了数据安全存储的配置规则；
2) 是否明确了存储媒体的购买、标记、使用等安全制度。

c) 是否明确了数据备份与恢复相关制度文件。

d) 查验组织的技术工具：

1) 是否实现了存储系统的访问控制、身份鉴别、运维管理等；
2) 是否实现了存储系统的自动备份与恢复的功能。

e) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

9.3.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设置了数据存储安全相关的部门、岗位和人员，并在部门和岗位的职责描述中明确了数据存储安全相关职责。

b) 查验是否在组织层级制定了数据存储策略相关制度文件：
   1) 查验该文件的制定是否结合了组织的数据分类分级策略，并规定了针对性的安全存储方案等；
   2) 是否规定了数据存储系统的安全配置规则，如权限管理、访问控制、加密管理等；
   3) 是否规定了逻辑存储资源的配置变更机制，对操作流程、安全配置进行规范；
   4) 是否明确了个人信息存储的相关规定，以符合国家法律法规和监管要求；
   5) 是否明确了重要数据、核心数据存储的相关规定，以符合国家法律法规和监管要求。

c) 查验是否在组织层面制定了数据存储介质安全相关制度文件：
   1) 是否明确了存储介质的安全配置规则、配置变更流程及授权管理规范等；
   2) 是否定义了存储介质的获取（购买）、使用、维护、销毁等流程。

d) 查验是否在组织层面制定了数据备份与恢复的相关制度文件：
   1) 是否明确了数据备份范围、备份频率、备份方式、备份工具、备份地点、日志记录、保存时长、数据恢复性验证机制等内容；
   2) 是否明确了备份数据的安全存储要求；
   3) 是否规定了备份数据的定期检查工作制度，以满足数据服务可靠性、可用性等安全目标；
   4) 是否规定了生命周期各阶段的数据归档操作流程；
   5) 是否规定了使用第三方备份服务时的协同工作机制。

e) 查验组织的技术工具：
   1) 是否实现了逻辑存储系统和存储介质的权限管理、访问控制等技术手段；
   2) 是否提供加密存储手段，满足不同的数据保密要求，如如磁盘加密、文档加密、数据库加密等；
   3) 是否能够对存储系统的安全配置进行定期扫描；
   4) 是否支持数据的自动备份和恢复；
   5) 是否定期对备份数据的有效性和可用性进行检查，并定期对主要备份业务数据进行恢复验证；
   6) 是否具备数据存储跨机柜/机房的容错部署能力；
   7) 查验储存系统是否满足网络安全等级保护要求。

f) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

9.3.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 查制度流程：
   1) 是否明确了存储介质的安全配置规则、配置变更流程及授权管理规范等；
   2) 查验组织是否明确了数据备份与恢复的优化工作机制：是否支持根据不同的数据冗余要求，提供多样性和多变性副本存储管理要求；
   3) 是否具备支持分类分级的差异化数据安全存储管理能力，如数据的分域分级存储、差异化的加密方案和权限控制方案等。

b） 是否明确了数据存储安全管理效果的量化评估方式：
   1） 是否定义并应用量化指标，如数据存储安全方案有效性，如数据存储访问控制有效性、数据脱敏存储有效性、数据加密存储有效率性等；
   2） 是否规定了量化评估频率。
c） 查验组织的技术工具：
   1） 是否具备存储介质的统一管理工具，对存储介质的使用授权等进行管理；
   2） 是否具备敏感数据识别、保护的工具或平台；
   3） 是否具备按照时效性分层的自动数据备份与快速恢复系统；
   4） 是否支持跨地域容灾；
   5） 是否支持备份数据的时效性检测；
   6） 是否实现数据传输存储安全管理效果的量化评估方法；
   7） 是否定期进行数据存储安全管理效果量化评估；
   8） 是否根据量化评估结果进行及时的调整。

9.3.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：
a） 查验是否具有数据存储安全规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b） 查验组织的技术工具：
   1） 查验是否具有数据存储安全技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；
   2） 查验是否主导国际、国家和行业标准的制定；
   3） 查验是否具备数据存储安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.4 数据使用安全

9.4.1 概述

根据数据使用过程面临的安全风险，建立有效的安全管控措施，防止数据泄露。根据组织内部数据处理过程面临的安全威胁，建立适用的数据处理环境的安全保护机制，确保数据处理过程的安全性。

9.4.2 等级要求

9.4.2.1 第一级

第一级应从制度流程方面满足如下要求：
制度流程：未在任何业务中建立数据使用安全制度，仅根据临时需要或基于个人经验，在个别数据使用场景中考虑了数据安全需求。

9.4.2.2 第二级

第二级应从组织建设、制度流程、人员能力方面满足如下要求：
a） 组织建设：应设置核心部门的数据使用安全相关的岗位和人员，负责核心部门的数据使用安全管理，并配合推进相关工作的开展和实施。
b） 制度流程：

1) 应制定数据使用规范，明确核心业务场景数据使用原则、范围和权限、合规要求、使用安全防护要求、数据使用限制等；
2) 应明确数据使用审批要求，针对不同级别数据制定不同的审批流程；
3) 应明确核心部门的数据处理环境安全管理要求，制定满足核心部门数据安全要求的对处理环境的相关规定,如数据使用环境、数据开发测试环境下的安全要求。

c) 技术工具：
1) 应部署数据脱敏工具，确保数据在脱离生产系统时进行了脱敏保护；
2) 应记录数据处理操作日志，如用户在数据处理系统上的加工操作。

d) 人员能力：针对核心业务场景需求，应能提出有效的数据安全合规使用的解决方案。

9.4.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据使用安全相关的部门、岗位和人员，负责组织层面的数据使用安全管理，与其他部门协同工作，配合推进相关工作的开展和实施。

b) 制度流程：
1) 应制定数据使用规范，明确各业务场景数据使用原则、范围和权限、合规要求、使用安全防护要求（例如数据脱敏、加密、访问控制）、数据使用限制等；
2) 应建立数据权限申请审核流程，对数据源、数据使用场景、数据使用范围、数据使用逻辑、个人信息安全影响情况进行审核，以确保数据使用的真实性、必要性、合规性；
3) 应建立个人信息、重要数据、核心数据使用和加工的保护规定；
4) 应针对数据处理环境的系统设计、开发和运维阶段制定相应的安全控制措施，实现对安全风险的管理；
5) 应明确数据处理环境的安全管理要求。

c) 技术工具
1) 应建立日志管理工具，记录数据处理过程中的操作行为；
2) 应建立防泄漏技术工具，防止数据处理过程中数据泄露；
3) 应部署数据权限管控工具，通过访问控制机制限定用户可访问数据范围；
4) 应具备数字水印技术，防止数据的泄露；
5) 应建立审计工具，支持对安全事件的追踪溯源。

d) 人员能力：
1) 应能基于业务场景要求、相关标准对数据使用过程中所可能引发的安全风险进行有效的评估，并能够针对各业务场景提出有效的解决方案；
2) 应了解在数据环境下的数据处理系统的主要安全风险，并能够在相关的系统设计、开发阶段通过合理的设计以及运维阶段进行有效配置规避相关风险；
3) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

9.4.2.4 第四级

第四级应在第三级的等级要求上，从组织建设、制度流程、技术工具方面满足如下要求：

a) 组织建设：
1) 应建立数据使用安全监督管理职能部门，负责对组织内部的数据使用行为进行监督；
2) 应在各部门、各条线建立数据使用接口人团队，承接和落地数据安全各项工作。

b) 制度流程：
   1) 应制定数据使用审计制度，定期对用户的数据进行审计，确定用户的数据使用未超出前期申请数据时的目的；
   2) 应基于数据处理环境需求，建立分布式处理安全要求，对外部服务组件注册与使用审核、分布式处理节点间可信连接认证、节点和用户安全属性周期性确认、数据文件标识和用户身份鉴权、数据副本节点更新检测及防止数据泄漏等方面进行安全要求和控制；
   3) 应明确数据使用安全的量化评估机制，包括评估方式、频率和调整计划。
c) 技术工具：
   1) 应具备数据监控审计工具，对数据泄露、滥用等违规操作行为进行监控、识别和告警；
   2) 应采取必要的技术手段，实现各个环节的防泄漏；
   3) 应具备统一数据管理平台，支撑数据血缘和生命周期等管理，实现数据处理前后数据间的映射关系；
   4) 应采取必要的技术手段，避免输出的业务结果数据包含可恢复的个人信息数据和结构标识；
   5) 应实现数据使用安全管理效果的量化评估方法。

9.4.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持数据使用安全规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。
b) 技术工具：
   1) 应支持对数据使用的安全风险进行自动化分析和处理；
   2) 应支持数据使用安全技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；
   3) 应能主导国际、国家和行业标准的制定，具备数据使用安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.4.3 评估方法

9.4.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别数据使用场景中临时采用了一些数据保护技术，如数据加密。

9.4.3.2 第二级

根据第二级要求，从组织建设、制度流程、技术工具和人员能力方面进行查验：

a) 查验是否在核心部门设置了数据使用安全相关的岗位和人员，并在岗位职责描述中明确了数据使用安全相关职责。
b) 查验是否在核心部门层级制定了数据使用安全相关制度文件：
   1) 是否明确了数据使用的原则、范围、权限、合规要求等；
   2) 是否明确了数据使用审批流程；
   3) 是否明确了数据使用者的权限管理及访问控制机制。
c) 查验是否在核心部门层级制定了数据处理环境安全相关制度文件：

1) 是否明确了数据处理过程中的身份鉴别、访问控制等要求；
2) 是否规定了数据在不同使用场景下的环境安全；
3) 是否规定了终端环境的管理要求。

d) 查验技术工具：
1) 是否部署了脱敏工具，支持静态脱敏、动态脱敏并对敏感数据的脱敏操作进行日志记录；
2) 是否对数据处理系统上的加工操作等进行了日志记录。

e) 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

9.4.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设置了数据使用安全相关的部门、岗位和人员，并在部门和岗位的职责描述中明确了数据使用安全相关职责。

b) 查验是否在组织层级制定了数据使用安全相关制度文件：
1) 查验该文件的制定是否结合了组织数据分类分级策略；
2) 是否明确了各业务场景下的数据使用审批流程、数据权限申请流程、数据脱敏规范、数据访问控制、数据结果发布审核、数据保护要求等内容；
3) 是否规定了数据使用相关平台系统的访问控制措施；
4) 是否建立数据使用者安全责任制度，定义违规使用数据的操作；
5) 是否明确了个人信息的使用安全保护规定；
6) 是否明确了重要数据、核心数据的使用安全保护规定，并建立登记、审批机制，留存记录。

c) 查验是否在组织层级制定了数据脱敏规范：
1) 是否明确了脱敏处理使用场景；
2) 是否规定了数据脱敏规则、方法、处理流程等。

d) 查验是否在组织层级制定了数据处理环境安全相关制度文件：
1) 是否明确了系统设计、开发、运维阶段的安全控制措施；
2) 是否规定了身份鉴别、访问控制、安全配置等环境管理要求；
3) 是否规定了终端环境的管理规范。

e) 查验组织的技术工具：
1) 是否具备脱敏工具，对导出生产系统的敏感数据进行脱敏；
2) 是否具备水印工具，支持事后追踪溯源；
3) 是否支持账号权限管理、访问控制等管控要求；
4) 是否具备日志管理工具，对数据处理过程的操作日志进行统一管理；
5) 是否具备防泄漏工具，防止数据处理过程中的泄露；
6) 是否具备审计工具，支持对安全事件的追踪溯源；
7) 是否支持不同使用环境的资源隔离控制和用户隔离。

f) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

9.4.3.4 第四级

根据第四级要求，从组织建设、制度流程、技术工具方面进行查验：

a) 查验组织：

1) 是否设立数据使用安全监督管理职能部门，并在制度文件中明确监督职责范围；
2) 是否在各部门或各条线设立数据使用接口人。

b) 数据使用安全监督管理职能部门，并在制度文件中明确监督职责范围。
c) 查验制度中是否明确了数据使用定期审计的要求。
d) 是否规定了分布式处理场景下的环境安全要求。
e) 查验组织是否明确了数据使用安全管理的量化评估方式：
1) 是否定义了量化评估指标，如数据使用安全风险识别数量、级别、处理量等；
2) 是否规定了量化评估频率。
f) 查验组织的技术工具：
1) 是否部署了数据监控与审计工具，对数据使用量、使用频次、导出下载量等设置了使用规则并进行监控，支持数据违规使用行为的有效识别与预警；
2) 是否具备相应管理平台，支持数据血缘分析，构建数据使用链路；
3) 是否支持对输出信息的检测，避免存在可恢复的个人信息；
4) 是否支持终端、网络、应用、数据库等不同环境下的数据防泄漏工具；
5) 是否支持分布式处理节点的服务监测与修复；
6) 是否实现数据使用安全管理效果的量化评估方法；
7) 是否定期进行数据使用安全管理效果量化评估；
8) 是否根据量化评估结果进行及时的调整。

9.4.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验是否具有数据使用安全规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b) 查验组织的技术工具：
1) 是否具有数据使用安全风险自动化分析和处理工具；
2) 是否具有数据使用安全技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；
3) 是否主导国际、国家和行业标准的制定；
4) 是否具备数据使用安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.5 数据共享安全

9.5.1 概述

根据组织对外提供或交换数据的需求，建立有效的数据共享的安全防护措施，以降低数据共享场景下的安全风险。

9.5.2 等级要求

9.5.2.1 第一级

第一级从制度流程方面满足如下要求：

制度流程：未在任何业务建立成熟稳定的数据共享安全风险管控，仅根据临时需求或基于个人经验对个别数据共享场景考虑了安全需求。

9.5.2.2 第二级

第二级从组织建设、制度流程、人员能力方面满足如下要求：

a) 组织建设：应设置核心部门的数据共享安全相关的岗位和人员，负责核心部门的数据共享安全管理，并配合推进相关工作的开展和实施。

b) 制度流程：

1) 应明确数据共享的原则、范围和安全规范，明确数据共享内容范围和数据共享的管控措施，及数据共享涉及机构或部门相关用户职责和权限；

2) 应与数据共享方签署数据保密和合作协议，明确数据的使用目的、供应方式、可能存在的安全风险、保密约定、数据安全责任等；

3) 应明确向第三方共享个人信息时的操作规范，包括告知个人信息接收方的姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；

4) 应保证共享内容符合数据合规和监管要求，明确数据使用的范围。

c) 人员能力：应具备对数据共享业务场景的理解能力，能够结合合规性要求给出适当的安全解决方案。

9.5.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据共享安全相关的部门、岗位和人员，负责组织层面的数据共享安全管理，与其他部门协同工作，配合推进相关工作的开展和实施。

b) 制度流程：

1) 应结合组织数据分类分级策略，规定数据的共享原则、范围、类别、条件、程序及数据安全保护措施；

2) 应针对不同类别的数据共享场景，建立针对性的数据共享需求、范围、内容、流程的审核控制机制；

3) 应确保数据使用的相关方具有对共享数据的足够的保护能力，从而保障数据共享安全策略的有效性；

4) 应通过协议等形式明确共享双方的数据安全责任；

5) 应明确个人信息共享时的安全管控要求；

6) 应梳理各类共享场景，建立对应的安全管控机制；

7) 应明确数据接口安全控制策略，明确规定使用数据接口的安全限制和安全控制措施，如身份鉴别、访问控制、授权策略、签名、时间戳、安全协议等；

8) 应明确共享的数据留存期限，并提供有效方式证明数据的销毁的情况；

9) 应明确数据转移的数据安全管理规范，明确发生数据转移的具体场景，在发生数据转移时应明确数据转移方案，通知受影响用户并记录,涉及重要数据和核心数据转移的，应及时向主管部门更新备案等。

c) 技术工具：

1) 应采取措施保障数据共享过程安全，尤其是个人信息在共享场景中的安全；

2) 应对共享数据及数据接口进行监控审计，避免超范围共享等问题；

3) 应对跨安全域的数据接口调用采用安全通道、加密传输、时间戳以及签名等安全措施。

d) 人员能力：

1) 应能充分理解组织的数据共享规范，并根据数据共享的场景执行相应的风险评估，从而

提出实际的解决方案；

2) 应能充分理解数据接口调用业务的使用场景，具备充分的数据接口调用的安全意识、技术能力和风险控制能力；

3) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

9.5.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：

1) 应建立数据共享的目录，包括共享的源机构、目的机构、共享方式、共享数据内容、共享数据量、共享频率等；

2) 应定期盘点数据共享合作的必要性，数据共享使用的必要性，减少非必要字段的使用；

3) 在数据共享时，应对数据接收方的数据安全防护能力开展评估工作；

4) 应制定数据共享安全的量化评估机制，包括评估方式、频率和调整计划。

b) 技术工具

1) 应对数据共享接口进行异常监控及自动化处理；

2) 应支持对外共享场景下的数据溯源技术；

3) 应建立统一的数据共享技术工具，支持统一的安全管理等；

4) 应实现数据共享安全管理效果的量化评估方法。

9.5.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持数据共享安全规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。

b) 技术工具

1) 应支数据共享安全技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；

2) 应能主导国际、国家和行业标准的制定，具备数据共享安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.5.3 评估方法

9.5.3.1 第一级

根据第一级要求，从制度流程方面进行查验：

查验是否在个别数据共享场景中临时采用了一些数据保护流程，如数据加密等。

9.5.3.2 第二级

根据第二级要求，从组织建设、制度流程、人员能力方面进行查验：

a) 查验是否在核心部门设置了数据共享安全相关的岗位和人员，并在岗位职责描述中明确了数据共享安全相关职责。

b) 查验是否在核心部门层级制定了数据共享安全相关制度文件：

1) 是否明确了数据共享的原则、范围、审批流程、共享流程、审计流程等；

2) 是否规定了数据共享的安全策略；

3) 是否明确了通过协议等形式明确共享方的数据安全责任；
4) 是否明确了共享安全合规评估机制；
5) 是否明确了个人信息共享的操作规范，是否明确告知个人信息接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意等，以符合国家法律法规和监管要求。

c) 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

9.5.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验组织是否设立了负责数据共享安全的部门、岗位和人员。
b) 查验是否在组织层级制定了数据共享安全相关制度文件：
   1) 查验是否结合了组织数据分类分级策略，规定数据的共享范围、类别、条件、程序及数据安全保护措施；
   2) 是否明确了分共享场景的数据共享安全策略，针对不同类别的数据共享场景，规定了针对性的数据共享需求、共享范围、共享内容、共享流程的审核控制机制；
   3) 是明确了通过协议等形式明确共享双方的数据安全责任；
   4) 是否明确了数据共享接口的安全控制策略；
   5) 是否明确了个人信息共享场景（第三方共享、委托处理、转移、公开等）的安全合规管理，以符合国家法律法规和监管要求；
   6) 涉及因兼并、重组、破产等原因需要转移数据的，是否明确了数据转移方案，通知受影响用户并记录；涉及重要数据和核心数据转移的，是否及时向主管部门更新备案。
c) 查验组织的技术工具：
   1) 是否采取措施支持数据共享安全，尤其是个人信息、重要数据、核心数据在不同场景下的共享安全防护，如数据脱敏降级、去标识、隐私计算、数据加密、安全通道、安全共享交换区域、安全授权网关、数据水印等；
   2) 是否支持数据接口的监控审计，避免超范围共享等问题；
   3) 是否支持数据接口调用的安全管控，如身份鉴别、访问控制、授权策略、签名、时间戳、安全协议等。
d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

9.5.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 检查数据共享目录，是否对源机构、目的机构共享方式、共享数据内容、共享数据量、共享频率等信息进行了记录。
b) 检查一年内的数据共享盘点记录，包括盘点事项的发起记录、盘点结果等。
c) 查验组织是否明确了数据接收方的数据安全防护能力定期评估机制。
d) 查验组织是否明确了数据共享安全管理效果的量化评估方式：
   1) 是否定义了量化评估指标，如数据共享安全风险识别数量、级别、处理量等；
   2) 是否规定了量化评估频率。
e) 查验组织的技术工具：
   1) 是否支持对共享接口异常的有效监控，并实现自动关停；

2) 是否支持对外共享场景下的数据溯源技术，如数字签名、数字水印；
3) 是否支持数据集共享统一安全管理和审核等；
4) 是否支持数据共享与交换工台，实现数据集中处理和共享，限定数据共享方式，记录数据共享日志；
5) 是否实现数据共享安全管理效果的量化评估方法；
6) 是否定期进行数据共享安全管理效果量化评估；
7) 是否根据量化评估结果进行及时的调整。

9.5.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验是否具有数据共享安全规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b) 查验组织的技术工具：
   1) 是否具有数据共享安全技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；
   2) 是否主导国际、国家和行业标准的制定；
   3) 是否具备数据共享安全技术研究能力，形成一系列卓越的研究成果，并将自身的数据安全建设经验作为行业最佳案例进行推广，获得行业认可。

9.6 数据销毁安全

9.6.1 概述

通过制定数据销毁机制，实现有效的数据销毁管控，防止因对存储介质中的数据进行恢复而导致的数据泄漏风险。

9.6.2 等级要求

9.6.2.1 第一级

第一级从制度流程方面满足如下要求：

制度流程：未建立的数据销毁安全制度，仅根据临时需求对指定的数据进行逻辑删除。

9.6.2.2 第二级

第二级从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置核心部门的数据销毁安全相关的岗位和人员，负责核心部门的数据销毁安全管理，并配合推进相关工作的开展和实施；
b) 制度流程：应规定核心部门数据销毁方案和存储介质销毁方案，包括销毁原则、操作流程；
c) 技术工具：应采用技术工具对存储介质的数据内容进行擦除销毁。在必要时能够采用物理销毁的形式销毁存储介质；
d) 人员能力：应具备针对销毁需求制定对应的销毁方案的能力，能够明确判断存储媒体销毁的必要性。

9.6.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据销毁安全相关的部门、岗位和人员，负责组织层面的数据销毁安全管理，与其他部门协同工作，配合推进相关工作的开展和实施。

b) 制度流程：

1) 应规定数据销毁对象、规则、流程和技术等；

2) 应建立规范的数据销毁、存储介质销毁流程和审批机制，对审批和销毁过程进行记录控制；

3) 针对不同的存储介质，应建立针对性的销毁流程和检验标准；

4) 应按国家相关法律和标准要求销毁或删除个人信息和敏感数据；

5) 应在重要数据和核心数据的销毁及时向主管部门更新备案。

c) 技术工具：

1) 应针对存储数据、存储介质等，建立硬销毁和软销毁的销毁方法和技术；

2) 应配置必要的数据销毁技术手段与管控措施，确保以不可恢复的方式销毁敏感数据及其副本内容；

3) 应提供存储介质销毁工具，包括但不限于物理销毁、消磁设备等工具。

d) 人员能力：应能够定期接受安全培训，熟悉数据销毁的相关合规要求，能够根据需求使用相应的数据销毁技术、存储介质销毁工具。

9.6.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：

1) 应按国家相关法律法规和标准销毁重要数据、核心数据；

2) 应依照数据分类分级建立数据销毁、存储介质销毁策略和管理制度，明确数据销毁和存储介质销毁的场景、销毁对象、销毁方式和销毁结果；

3) 应明确已共享或者已被其他用户使用的数据销毁管控措施。

b) 技术工具：

1) 应能够验证数据已被完全删除、无法恢复或无法识别到个人；

2) 应对销毁记录进行归档，记录销毁过程及验证结果。

9.6.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应明确数据销毁、媒体销毁效果的量化评估机制，包括评估方式、频率和调整计划。

b) 技术工具：

1) 应实现数据销毁安全管理效果的量化评估方法；

2) 应持续更新组织的数据销毁、存储媒体销毁工具，以保证销毁的效果。

9.6.3 评估方法

9.6.3.1 第一级

根据第一级要求，从制度流程方面进行查验：

查验是否在个别数据删除场景中临时采用了一些逻辑删除方法。

9.6.3.2 第二级

根据第二级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在核心部门设置了数据销毁安全相关的岗位和人员，并在岗位职责描述中明确了数据销毁安全相关职责。
b) 查验是否在核心部门层级制定了数据销毁和存储介质销毁相关制度文件：
   1) 是否明确了数据销毁的销毁机制和管控措施；
   2) 是否规定了存储介质的销毁机制和管控措施。
c) 验证组织的技术工具：
   1) 是否支持数据的销毁；
   2) 是否支持存储介质的销毁。
d) 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

9.6.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设置了数据销毁安全相关的部门、岗位和人员，并在部门和岗位的职责描述中明确了数据销毁安全相关职责。
b) 查验是否在组织层级制定了数据销毁安全相关制度文件：
   1) 是否规定了数据销毁对象、规则、流程和技术等；
   2) 是否对重要数据和核心数据的销毁及时向主管部门更新备案；
   3) 是否规定了数据销毁的审批机制；
   4) 是否规定了个人信息的销毁、删除或者匿名化，以符合国家法律法规、监管要求。
c) 查验是否在组织层级制定了存储介质的销毁机制和管控措施：
   1) 是否明确了对存储不同重要性内容的各类介质的销毁方法；
   2) 是否规范了登记、审批、交接等介质销毁流程；
   3) 是否规定了销毁后的核验和资源回收措施。
d) 查验组织的技术工具：
   1) 是否具备销毁工具，包括逻辑销毁和物理销毁工具；
   2) 是否支持销毁过程记录；
   3) 是否支持销毁的有效性验证。
e) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

9.6.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 查验是否在组织层级制定了数据销毁安全相关制度文件：
   1) 查验该文件的制定是否结合了组织的数据分类分级制度；
   2) 是否明确了第三方存储的销毁规范；
   3) 是否明确了已共享的数据的销毁机制。
b) 查验组织的技术工具：
   1) 是否支持通过系统向管理员发起数据销毁提醒；

2) 是否支持销毁记录归档；
3) 是否支持销毁过程的结果验证。

9.6.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了数据销毁安全管理效果的量化评估方式：
   1) 是否定义了量化评估指标，如数据销毁有效性，数据销毁执行率；
   2) 是否规定了量化评估频率。
b) 查验组织是否明确了数据销毁安全的优化工作机制：是否支持根据法律法规和合同要求，更新优化销毁方案。
c) 查验组织的技术工具：
   1) 是否支持销毁工具的迭代更新；
   2) 是否实现数据销毁安全管理效果的量化评估方法；
   3) 是否定期进行数据销毁安全管理效果量化评估；
   4) 是否根据量化评估结果进行及时的调整。

10 基础安全

10.1 数据分类分级

10.1.1 概述

根据法律法规以及业务需求明确组织内部的数据分类分级原则及方法，并对数据进行分类分级标识。

10.1.2 等级要求

10.1.2.1 第一级

第一级应从制度流程方面满足如下要求：

制度流程：未在任何业务建立成熟稳定的数据分类分级制度，仅根据临时需求在个别业务场景下考虑了数据分类分级。

10.1.2.2 第二级

第二级应从组织建设、制度流程方面满足如下要求：

a) 组织建设：应设置核心部门的数据分类分级相关的岗位和人员，负责核心部门的数据分类分级管理，并配合推进相关工作的开展和实施。
b) 制度流程：
   1) 应建立数据分类分级规范，包括分类分级的原则、方法等；
   2) 应根据业务特性和外部合规要求，对核心部门的数据进行分类分级管理；
   3) 应定义核心部门的数据资产的分类分级方法，能够支持部门数据资产合理正确的标识。

10.1.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据分类分级相关的部门、岗位和人员，负责组织层面的数据分类分级管理，与其他部门协同工作，配合推进相关工作的开展和实施。
b) 制度流程：
   1) 应建立分类分级的原则、方法、操作指南等，并符合国家法律法规和监管要求和行业管理规定；
   2) 应明确数据资产梳理统一规范要求；
   3) 应对组织的数据进行分类分级标识，建立数据保护清单；
   4) 应针对不同级别数据，制定数据生命周期各环节的不同的安全管理要求及技术保障措施；
   5) 应建立重要数据和核心数据目录，并按要求向主管部门备案机制；
   6) 应明确数据分类分级变更审批流程和机制，通过该流程保证数据分类分级的变更操作及其结果符合组织的要求；
   7) 应对个人信息实施分类分级管理；
   8) 应对未成年人数据进行识别，并制定专门的未成年人个人信息处理规则。
c) 技术工具：
   1) 应支持数据资产的识别，形成数据资产清单；
   2) 应具备数据分类分级工具，实现数据分类分级打标；
   3) 应支持数据分类分级策略的变更管理。
d) 人员能力：
   1) 负责数据分类分级人员应了解数据分类分级的合规要求，了解组织数据分类分级方法及相关原则标准，如数据类型、级别设置等；
   2) 应定期对人员进行考核，验证人员能力与岗位的匹配程度；
   3) 应能够识别哪些数据属于个人信息，哪些数据属于重要数据、核心数据。

10.1.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：
a) 组织建设：应在组织各业务部门设置接口人负责对接数据分类分级工作，承接数据分类分级工作的变更维护。
b) 制度流程：应制定数据分类分级的量化评估机制，包括评估方式、频率和调整计划。
c) 技术工具：
   1) 应支持自定义分类分级、自动分类分级、人工标签处理、分类分级结果审核的技术手段，以能保证数据分类分级的覆盖范围和准确性；
   2) 应具备数据级别变更降级能力；
   3) 应具备对分类分级结果进行对外输出的技术手段，将数据分类分级结果提供给其他系统；
   4) 应实现数据分类分级管理效果的量化评估方法。

10.1.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：
a) 制度流程：应支持数据分类分级规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。
b) 技术工具：
   1) 应支持数据分类分级技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；

2) 应能主导国际、国家和行业标准的制定，具备数据分类分级技术研究能力，形成一系列卓越的研究成果，并将自身的数据分类分级建设经验作为行业最佳案例进行推广，获得行业认可。

10.1.3 评估方法

10.1.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别业务场景中对部分数据进行业务数据和非业务数据或者敏感数据和非敏感数据的划分。

10.1.3.2 第二级

根据第二级要求，从组织建设、制度流程方面进行查验：

a) 查验是否在核心部门设置了数据分类分级相关的岗位和人员，并在岗位职责描述中明确了数据分类分级相关职责。

b) 查验是否在核心部门层级制定了数据分类分级相关制度文件：
   1) 是否明确了数据分类分级规范，包括分类分级的原则、方法等；
   2) 是否明确了不同类别不同级别数据的安全管理要求；
   3) 是否定义了数据资产的标识规范。

10.1.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设置了数据分类分级相关的部门、岗位和人员，并在部门和岗位的职责描述中明确了数据分类分级相关职责。

b) 查验是否在组织层面制定了数据分类分级相关制度文件：
   1) 查验该文件的制定是否考虑了国家法律法规和监管要求；
   2) 是否定义了分类分级的原则、方法、操作指南等，并符合国家法律法规和监管要求和行业管理规定；
   3) 是否明确数据资产梳理统一规范要求；
   4) 是否对组织的数据进行分类分级标识，并建立数据保护清单；
   5) 是否对不同级别数据，制定数据生命周期各环节的不同的安全管理要求及技术保障措施，如数据加密、数据脱敏、加强访问控制权限等措施；
   6) 是否具有重要数据和核心数据目录，并按要求向主管部门备案；
   7) 是否明确了分类分级策略实施及变更流程；
   8) 是否对个人信息实施分类分级管理；
   9) 查验是否明确了未成年人数据处理的安全管理要求。

c) 查验组织技术工具：
   1) 是否支持数据资产的识别，形成数据资产清单；
   2) 是否支持数据的分类分级，对数据进行分类分级打标；
   3) 是否支持对分类分级策略变更管理。

d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

10.1.3.4 第四级

根据第四级要求，从组织建设、制度流程、技术工具方面进行查验：

a) 查验是否在各业务部门设置了数据分类分级接口人，并在个人职责描述中明确了对接和承接数据分类分级工作的相关职责。

b) 查看接口人清单，查看接口人对数据分类分级工作的相关工作记录。

c) 查验组织是否明确了数据分类分级管理效果的量化评估方式：

1) 是否定义了分类、分级的量化评估指标，如数据分类分级对数据类型的覆盖率，数据分类分级的准确性等；

2) 是否规定了分类、分级的量化评估频率。

d) 查验组织的技术工具：

1) 是否支持针对用户需要自定义分类分级；

2) 是否支持结合业务、资产梳理情况等自动分类分级能力；

3) 是否支持用户自定义分类分级规则；

4) 是否支持通过脱敏、去标识、加密手段处理后，安全级别可以调整，降级后的数据可以有效使用；

5) 是否支持分类分级结果的输出能力；

6) 是否实现数据分类分级管理效果的量化评估方法；

7) 是否定期进行数据分类分级管理效果量化评估；

8) 是否根据量化评估结果进行及时的调整。

10.1.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了数据分类分级的优化工作机制：是否具有数据分类分级规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。

b) 是查验组织的技术工具：

1) 是否具有数据分类分级技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；

2) 是否主导国际、国家和行业标准的制定；

3) 是否具备数据分类分级技术研究能力，形成一系列卓越的研究成果，并将自身的数据分类分级建设经验作为行业最佳案例进行推广，获得行业认可。

10.2 合规管理

10.2.1 概述

根据组织内部的业务需求和业务开展场景，明确相关法律法规要求，通过制定管理措施降低组织面临的合规风险。

10.2.2 等级要求

10.2.2.1 第一级

第一级应从制度流程方面满足如下要求：

制度流程：未在任何业务中建立成熟稳定的安全合规工作流程或规范，仅根据临时需求或基于个人经验在个别业务中考虑了合规要求。

10.2.2.2 第二级

第二级应从组织建设、制度流程、人员能力方面满足如下要求：

a) 组织建设：应设置核心部门的合规管理相关的岗位和人员，负责核心部门的合规管理，并配合推进相关工作的开展和实施。

b) 制度流程：应对核心部门建立的数据合规管理制度，覆盖外部法规、行业监管要求和内部数据安全运营策略。

c) 人员能力：负责该项工作的人员应基本理解本组织相关数据安全合规要求。

10.2.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应结合国家相关法律法规要求和地方、行业监管等要求，设置组织层面的合规管理相关的部门、岗位和人员，负责组织层面的合规管理，与其他部门协同工作，配合推进相关工作的开展和实施。

b) 制度流程：

1) 应建立组织层面的数据合规管理制度，覆盖外部法规、行业监管要求和内部数据安全运营策略；

2) 应明确组织的数据安全合规要求，如个人信息合规要求、重要数据合规要求、核心数据合规要求，数据跨境合规要求等；

3) 应能定期通过跟进监管机构合规要求对合规管理制度、清单进行更新和宣贯；

4) 应明确个人信息保护影响评估的场景和具体要求；

5) 应建立数据出境的安全管控机制，明确数据出境前的安全评估等要求；

6) 应明确各类数据安全评估的具体场景、具体内容和开展评估的具体要求；

7) 应定期开数据安全评估工作，重点梳理存在问题并通报评估结果，并按照主管部门要求进行数据安全评估上报；

8) 应建立合规培训的计划，进行全员的安全合规意识培训和重点部门的安全合规专项培训。

c) 技术工具：

1) 应具备平台工具支撑合规管理；

2) 应具备各类数据安全评估标准或者工具。

d) 人员能力：

1) 负负责该项工作的人员应能对数据安全合规要求的进行解读和分析，能够识别核心业务中存在的风险，并可基于业务实际情况制定和推进数据安全合规方案；

2) 应能够依据外部合规要求，建立覆盖组织的数据安全管理体系和机制，并推动多方参与，落地执行；

3) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

10.2.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 组织建设：应在组织各业务部门设置合规管理接口人负责对接数据处理、流转等过程中的合规管理，并与合规部门形成协同机制，共同推动组织合规工作。

b) 制度流程：

1) 应建立合规问题整改和合规管理考核规范，明确问题管理、整改情况追踪等规范性要求；

2) 应规定数据安全合规风险的量化方式，通过数据指标定义安全事件风险的严重程度；

3) 应定期评审组织的合规规范和流程，考虑其内容是否满足最新的监管要求，是否完全覆盖了当前业务，并执行持续的改进优化工作；
4) 应制定合规管理的量化评估机制，包括评估方式、频率和调整计划。

c) 技术工具：
1) 应实现合规管理的量化评估机制方法；
2) 应能够针对个人信息保护、重要数据、核心数据保护、数据跨境传输的合规状况进行监控，定期审核相关操作记录，统计安全风险发生情况；
3) 应建立合规资料库或提供外部合规资料库查询渠道。

10.2.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持合规管理规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进；
b) 技术工具：应能主导国际、国家和行业标准的制定，并将自身的合规管理建设经验作为行业最佳案例进行推广，获得行业认可。

10.2.3 评估方法

10.2.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别业务中尝试了合规管理。

10.2.3.2 第二级

根据第二级要求，从组织建设、制度流程、人员能力方面进行查验：

a) 查验是否在核心部门设置了合规管理相关的岗位和人员，并在岗位职责描述中明确了合规管理相关职责。
b) 查验是否在核心部门层级制定了数据合规管理的相关制度文件：
1) 是否明确了核心部门数据保护的合规要求；
2) 是否明确了合规评估流程。
c) 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

10.2.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设置了合规管理相关的部门、岗位和人员，并在部门和岗位的职责描述中明确了合规管理相关职责。
b) 查验是否在组织层面制定了合规管理相关制度文件：
1) 查验该文件的制定是否参考了法律法规、标准规范、监管要求；
2) 是否明确了数据保护合规要求，建立合规清单；
3) 是否支持根据外部合规要求及时更新合规清单；
4) 是否明确了个人信息保护影响评估的场景和具体要求，如对个人权益有重大影响的各类个人信息处理活动场景，评估方法、评估范围、评估报告等具体要求；
5) 是否明确了数据出境的安全管控要求以符合法律法规要求，如依法定期进行安全评估及数据出境前的安全评估等；
6) 是否明确了开展各类数据安全评估的业务场景；

7) 是否规定了各类数据安全评估的具体内容，如数据安全风险情况、数据合规使用提供情况、数据安全保障措施配备情况与完善程度，以及如开展时机、频次等；
8) 是否定期开展数据安全评估及整改，并按照主管部门规定进行数据安全评估上报；
9) 是否规定了合规培训的计划，并定期开展合规主题的培训，对合规要求进行宣贯。

c) 查验组织的技术工具：
1) 是否记录了各业务场景的各类数据安全评估报告；
2) 是否具备平台工具支撑合规管理；
3) 是否具备各类数据安全评估标准或者工具。

d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

10.2.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 查验组织建设：
1) 是否在各业务部门设置了合规管理接口人，并在个人职责描述中明确了合规管理相关职责；
2) 是否建立了合规管理部门与各业务部门的协同机制。

b) 查验组织是否明确了合规管理效果的量化评估方式：
1) 是否定义了量化评估指标，如相关法律法规及标准对标覆盖率、更新频率等；
2) 是否规定了量化评估的时机、频率。

c) 查验组织是否明确了合规管理的优化工作机制：
1) 是否明确了合规管理的考核规范；
2) 是否明确了评估后的整改措施及复核机制。

d) 查验组织的技术工具：
1) 是否具备个人信息保护、重要信息保护、跨境数据传输等的合规风险的自动监控预警能力；
2) 是否建立了数据合规资料库。

10.2.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了合规管理的优化工作机制：是否具有合规管理规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。

b) 是查验组织的技术工具：
1) 是否主导国际、国家和行业标准的制定；
2) 否将自身的合规管理建设经验作为行业最佳案例进行推广，获得行业认可。

10.3 合作方管理

10.3.1 概述

通过建立组织的合作方管理机制，防范组织对外合作中的数据安全风险。

10.3.2 等级要求

10.3.2.1 第一级

第一级应从制度流程方面满足如下要求：

制度流程：未在任何业务建立成熟稳定的合作方数据安全管理制度，仅根据临时需求在个别合作场景中考虑了合作方的安全保障能力。

10.3.2.2 第二级

第二级应从组织建设、制度流程、人员能力方面满足如下要求：

a) 组织机构：应设置核心部门的合作方管理相关的岗位和人员，负责对合作方进行管理，监督合作方是否遵守其企业内部的数据安全流程。
b) 制度建设：核心部门与组织外机构开展数据合作时，应以合同、协议等方式明确数据的使用目的、使用范围、保密约定、安全责任和安全保护措施等内容。
c) 人员能力：
   1) 合作方管理负责人能够清晰理解组织数据安全管理目标，理解与合作方签订的数据安全合作条款的内容，合作方需要承担的安全责任，以及常规安全流程；
   2) 负责该项过程的人员应具备对具体数据合作场景的风险评估能力。

10.3.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的合作方管理相关的部门、岗位和人员，负责组织层面的合作方管理，与其他部门协同工作，配合推进相关工作的开展和实施。
b) 制度流程：
   1) 应明确数据安全主管部门、人力资源部门、合作方管理部门等的联动机制，对合作方引入、现场工作、合作方/合作方人员退场/离岗等环节进行管理，明确规范及监督流程；
   2) 应建立组织内通用的合作方管理规范，至少包括合作方安全管理要求、组织内部数据资源及网络环境接入要求、开发及运维管理要求、组织内部的审核原则、风险评估等；
   3) 应明确针对合作方的安全管理制度，对接触个人信息、重要数据、核心数据等的人员进行审批和登记，并要求签署保密协议，定期对相关人员行为进行安全审查；
   4) 应建立对数据合作方数据活动的安全风险和数据合作方的数据安全管理能力和资质的定期评估机制。
c) 技术工具：
   1) 应具备平台工具支持合作方管理，对合作方的接入、审批、权限管理、人员培训等内容进行统一管理；
   2) 应建立组织整体的数据合作方库，管理数据合作方目录、清单和相关数据源数据字典；
   3) 应具备对合作方的数据安全风险评估标准或者工具，支持数据相关业务开展前的数据安全风险评估。
d) 人员能力：
   1) 应了解组织数据合作方的整体情况，熟悉合作方安全方面的法规和标准，并具备推进合作方管理方案执行的能力；
   2) 应具备对个人信息保护、跨境数据传输、数据共享风险等方面的理解能力和开展数据共享安全风险评估的能力；
   3) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

10.3.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a）制度流程：

1） 应建立对合作方的持续化监控和应急处理流程，对合作方数据安全治理能力、安全合规事件等进行记录和应急响应；

2） 应建立组织整体的数据合作方库，用于管理数据合作方目录、清单和相关数据源数据字典，便于及时查看并更新合作方的整体情况，并用于事后追踪分析数据合作方合规情况；

3） 应规定合作方管理效果的量化评估方式，通过数据指标定义合作方管理的安全效果。

b）技术工具：

1） 应具备工具支持对合作方人员敏感数据使用情况的安全检查；

2） 合作方管理资料库应支持相关人员通过该资料库查询合作方信用考核情况；

3） 应能对合作方在开展合作过程中数据安全治理能力、安全合规情况、数据保护能力进行持续化监控；

4） 应建立应急响应机制，对合作过程中数据安全事件及时响应；

5） 应实现合作方管理效果的量化评估方法。

10.3.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a） 制度流程：应支持合作方管理规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进；

b） 技术工具：应能主导国际、国家和行业标准的制定，并将自身的合作方管理建设经验作为行业最佳案例进行推广，获得行业认可。

10.3.3 评估方法

10.3.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别合作场景中考虑了合作方的安全保障能力，如具备相关资质和证书。

10.3.3.2 第二级

根据第二级要求，从组织建设、制度流程、人员能力方面进行查验：

a） 查验核心部门是否明确了负责本部门合作方管理的岗位和人员。

b） 查验是否对核心部门的数据合作制定了合作方管理的相关制度文件：

1） 是否明确了合作方的数据使用目的、保密约定等；

2） 查验合作方签署的合同、协议是否对数据内容的使用目的、使用范围、安全责任、安全保护措施等进行了规定。

c） 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

10.3.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a） 查验组织是否设立了负责合作方管理的部门、岗位和人员。

b) 查验是否在组织层面制定了相关合作方管理制度文件：
   1) 是否规定了合作方数据安全管理的责任部门、管理机制、监督机制，是否覆盖对对合作方引入、现场工作、合作方/合作方人员退场/离岗等环节的安全管理；
   2) 是否规定了对合作方的数据安全保护能力、资质进行评估和核实；
   3) 是否建立对数据合作方数据活动的安全风险和数据合作方的数据安全管理能力和资质的定期评估机制，例如进行调研，形成评估报告；
   4) 是否规定了涉及个人信息时的合规性评估工作；
   5) 是否规定了合作方的管理台账机制；
   6) 是否对合作方驻场情形下的环境接入、账号分配回收、权限管理等内容进行了规范。
c) 查验组织的技术工具：
   1) 是否支持合作方管理，并建立合作方资料管理库；
   2) 是否支持对合作方的数据安全风险评估。
d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

10.3.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：
a) 查验组织是否明确了合作方管理效果的量化评估方式：
   1) 是否定义了量化评估指标，如签署保密协议的覆盖率等；
   2) 是否规定了量化评估频率。
b) 查验组织的合作方管理机制：
   1) 是否支持根据政策变化、业务发展等需求优化合作方管理制度；
   2) 是否规定了对合作方的持续化监控审计机制。
c) 查验组织的技术工具：
   1) 是否支持对合作方人员敏感数据使用情况的安全检查；
   2) 是否建立了合作方管理资料库，且支持相关人员通过该资料库查询合作方信用考核情况；
   3) 是否具备合作方发生安全事件时的应急响应能力；
   4) 是否支持对合作方数据安全治理、合规等内容的持续监控；
   5) 是否实现合作方管理效果的量化评估方法；
   6) 是否定期进行合作方管理效果量化评估；
   7) 是否根据量化评估结果进行及时的调整。

10.3.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：
a) 查验组织的合作方管理技术：是否具有合作方管理规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b) 是查验组织的技术工具：
   1) 是否主导国际、国家和行业标准的制定；
   2) 是否将自身的合作方管理建设经验作为行业最佳案例进行推广，获得行业认可。

10.4 监控审计

10.4.1 概述

通过建立监控审计的工作机制，有效防范不正当的数据访问和操作行为，降低数据全生命周期未授权访问、数据滥用、数据泄漏等安全风险。

10.4.2 等级要求

10.4.2.1 第一级

第一级应从制度流程方面满足如下要求：

制度流程：未在任何业务中建立成熟和稳定的监控审计制度，仅根据临时需要或基于个人经验考虑了监控审计要求。

10.4.2.2 第二级

第二级应从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置核心部门的监控审计相关的岗位和人员，负责数据全生命周期流转过程的安全监控；
b) 制度流程：核心部门应建立较完整的监控审计工作流程制度，包括事前监控规则制定、事中告警以及事后溯源分析；
c) 技术工具：应支持对异常操作的监控和审计；
d) 人员能力：应了解数据访问和操作涉及的数据范围，具备对安全风险的判断能力。

10.4.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的监控审计相关的部门、岗位和人员，负责对数据生命周期各阶段的数据访问和操作进行监控和审计。
b) 制度流程：
    1) 应明确对组织内部各类数据访问和操作的日志记录要求、安全监控要求和审计要求；
    2) 应记录数据操作事件，并制定数据安全违规行为识别和审计规则；
    3) 应明确对组织内部员工数据操作行为进行审计的方式和频率。
c) 技术工具：
    1) 应具备数据安全监控审计的工具或技术；
    2) 应具备针对数据操作的日志监控技术工具，实现对数据异常访问和操作进行告警，并将敏感数据的操作以及特权账户的数据操作纳入重点的监控范围；
    3) 应采用技术工具对数据流量数据进行安全监控和预警。
d) 人员能力：
    1) 应充分理解数据监控和审计的要求，能够识别数据安全风险，并及时应对；
    2) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

10.4.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：
    1) 应制定监控审计效果的量化评估机制，包括评估方式、频率和调整计划；

2) 应建立日志的定期盘点机制，保障日志的及时性和完整性，确保有效性。

b) 技术工具：

1) 应建立完善的数据安全审计平台，围绕数据的全生命周期过程的数据访问和操作进行监控、审计、分析，及时发现异常数据流向、异常数据操作行为，并进行告警和追溯，输出审计报告；

2) 应具备统一的数据访问和操作日志监控技术手段，可对各类数据访问和操作的日志进行处理和分析，并量化数据异常访问和操作引发的数据安全风险，实现对数据安全风险的整体感知；

3) 应具备对数据的异常或高风险操作进行自动识别和预警的能力；

4) 应实现监控审计效果的量化评估方法。

10.4.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持监控审计规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。

b) 技术工具：

1) 应支持监控审计技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；

2) 应能主导国际、国家和行业标准的制定，具备监控审计技术研究能力，形成一系列卓越的研究成果，并将自身的监控审计建设经验作为行业最佳案例进行推广，获得行业认可。

10.4.3 评估方法

10.4.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别业务进行了较粗粒度监控审计，如系统和网络层的监控和审计。

10.4.3.2 第二级

根据第二级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在核心部门设置了监控审计相关的岗位和人员。

b) 查验是否在核心部门层级制定了监控审计的相关制度文件：

1) 是否规定了监控的规则，如对数据访问和操作进行监控的方案（如实时监控、定期批量监控等）、对异常操作的监控方案等；

2) 是否规定了对异常操作的审计规则；

3) 是否规定了监控审计的工作流程、工作方案。

c) 查验组织的技术工具：

1) 是否支持对异常操作的监控；

2) 是否支持对异常操作的审计。

d) 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

10.4.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设立了负责数据监控审计的部门、岗位和人员。

b) 查验是否在组织层级制定了监控审计相关制度文件：
   1) 是否明确了数据相关操作的日志记录和安全监控要求，明确日志记录应包含数据处理、权限管理、人员操作等内容；
   2) 是否明确了审计目的、审计对象、审计内容（异常操作的定义）、审计流程、审计频度、审计报告、审计问题整改跟踪等内容；
   3) 是否覆盖了对组织各数据处理活动的审计操作；
   4) 是否明确了数据安全违规行为的识别和审计规则；
   5) 是否规定了对员工数据操作行为的定期审计。
c) 查验组织的技术工具：
   1) 是否具备工具支持数据异常操作的监控分析；
   2) 是否建立了全面的数据异常操作的预警策略；
   3) 是否具备工具支持数据安全审计，对数据异常访问和操作进行审计；
   4) 是否将敏感数据的操作，以及特权账户的数据操作纳入重点的监控范围；
   5) 是否留存相关数据安全事件审计报告。
d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

10.4.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：
a) 查验组织是否明确了监控审计效果的量化评估方式：
   1) 是否定义了量化评估指标，如日志系统的完整性，数据监控系统的覆盖范围、对员工数据操作行为审计的执行频度等；
   2) 是否规定了量化评估频率。
b) 检查是否有定期盘点的要求和盘点记录。
c) 查验组织的技术工具：
   1) 是否具备统一的监控审计系统或平台；
   2) 是否具备涵盖数据全生命周期的数据安全监控审计；
   3) 是否支持对异常或高风险操作的自动识别与预警；
   4) 是否实现监控审计管理效果的量化评估方法；
   5) 是否定期进行监控审计管理效果量化评估；
   6) 是否根据量化评估结果进行及时的调整。

10.4.3.5 第五级

根据第五要求，从制度流程、技术工具方面进行查验：
a) 查验组织是否明确了监控审计的优化工作机制：
   1) 查验是否具有监控审计规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b) 查验组织的技术工具：
   1) 是否具有监控审计技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；
   2) 是否主导国际、国家和行业标准的制定；
   3) 是否具备监控审计技术研究能力，形成一系列卓越的研究成果，并将自身的监控审计建

设经验作为行业最佳案例进行推广，获得行业认可。

10.5 身份认证与访问控制

10.5.1 概述

根据组织的安全合规要求，建立用户身份认证和访问控制管理机制，防止对数据的未授权访问风险。

10.5.2 等级要求

10.5.2.1 第一级

第一级应从制度流程方面满足如下要求：

制度流程：应对核心业务系统的登录用户进行基本的身份认证与权限管理。

10.5.2.2 第二级

第二级应从组织建设、制度流程、技术工具方面满足如下要求：

a) 组织建设：应设置核心部门的身份认证与访问控制相关的岗位和人员，负责部门各系统的身份认证与访问控制，并配合推进相关工作的开展和实施。
b) 制度流程：核心部门应明确重要系统和数据库的身份认证、访问控制和权限管理的安全要求。
c) 技术工具：
   1) 应对部门各系统的用户进行身份认证，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
   2) 应提供部门各系统的访问控制功能，对用户分配账户和权限；
   3) 应提供并启用部门各系统的登录失败处理功能，多次登录失败后应采取必要的保护措施；
   4) 应建立人力资源管理与身份鉴别管理、权限管理的联动控制，能够及时删除离岗、转岗人员的权限。

10.5.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：组织应设立相关的部门、岗位和人员，负责制定组织内用户身份鉴别、访问控制和权限管理的策略，提供相关技术能力或进行统一管理。
b) 制度流程：
   1) 应明确身份认证、权限管理、访问控制等方面的管理要求；涉及重要数据和核心数据的，应加强访问控制；
   2) 应明确对身份认证、访问控制及权限的分配、变更、撤销等方面管理的要求；
   3) 应按最小必要、职权分离等原则，授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
   4) 应明确数据资产授权审批流程，对数据资产权限申请和变更进行审核。
c) 技术工具：
   1) 应建立身份认证管理系统，支持组织主要应用接入，实现对人员访问数据资源的统一身份鉴别；

2) 应建立人力资源管理与身份认证管理、权限管理的关联控制，能够及时删除离岗、转岗人员的权限；
3) 应采多因子技术对用户进行身份鉴别；
4) 应建立权限管理系统，支持组织主要应用接入，实现数据资产的表级、字段级的访问控制和权限管理；
5) 应支持三权分立的权限管理，避免超级用户。

d) 人员能力：
1) 负责该项工作的人员应熟悉相关的数据访问控制的技术知识，并能够根据组织数据安全管理制度对数据权限进行审批管理；
2) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

10.5.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：
1) 应针对敏感数据以及重大操作行为建立加强的授权流程；
2) 应建立敏感数据权限清单，明确了数据权限的安全要求、分配策略、授权机制和权限范围；
3) 访问控制的粒度应达到主体为用户级，客体为系统、文件、数据库表级和字段级；
4) 应具备鉴权凭据保护能力，凭据应与人员分离，采用凭据托管、混淆等方式对凭据进行管理；
5) 应定期对组织的认证和访问控制效果进行量化评估。

b) 技术工具：
1) 应建立面向数据应用的访问控制机制，包括访问控制时效的管理和验证，以及数据应用接入的合法性和安全性认证机制；
2) 应建立定期更新和审核的敏感数据权限清单；
3) 应实现身份认证与访问控制管理效果的量化评估方法。

10.5.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持身份认证与访问控制规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。

b) 技术工具：
1) 应支持身份认证与访问控制技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；
2) 应能主导国际、国家和行业标准的制定，具备身份认证与访问控制技术研究能力，形成一系列卓越的研究成果，并将自身的身份认证与访问控制建设经验作为行业最佳案例进行推广，获得行业认可。

10.5.3 评估方法

10.5.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在核心业务系统实现了基本的身份认证与权限管理。

10.5.3.2 第二级

根据第二级要求，从组织建设、制度流程、技术工具方面进行查验：

a) 查验是否在核心部门设置了身份认证与访问控制相关的岗位和人员。
b) 查验是否在核心部门层级制定了身份认证与访问控制控制的相关制度文件：是否明确了身份认证、权限管理、访问控制等方面的管理要求。
c) 查验组织的技术工具：
   1) 是否支持用户身份认证；
   2) 是否支持各系统的访问权限控制；
   3) 是否支持身份认证和权限管理的联动控制；
   4) 是否支持对访问控制时效的管理和验证。

10.5.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验组织是否设立了负责身份认证与访问控制安全部门、岗位和人员。
b) 查验是否在组织层面制定了身份认证与访问控制控制相关制度文件：
   1) 是否明确了身份认证、权限管理、访问控制等方面的管理要求；涉及重要数据和核心数据的，是否加强访问控制；
   2) 是否明确了组织内员工以及外包人员及实习生等的身份认证、访问控制及权限管理等要求；
   3) 是否规定了账号口令的复杂度要求；
   4) 是否规定了账号权限等的定期审核制度；
   5) 是否明确了权限申请和分配原则、变更制度、撤销流程等内容；
   6) 是否规定了数据资产的授权审批流程，对数据权限申请和变更进行审核。
c) 查验组织的技术手段和工具：
   1) 是否具备身份认证管理系统；
   2) 是否具备权限管理系统；
   3) 是否支持身份认证和权限管理的关联控制；
   4) 是否提供多因子鉴别技术；
   5) 是否支持数据资产表级、字段级的授权管理；
   6) 是否支持三权分立（系统管理员、安全管理员、审计员）。
d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

10.5.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 检查授权流程是否针对敏感信息和重大操作行为（数量超过组织规定的安全基线的）单独进行设置，加强审批流程和审批粒度。
b) 是否支持不同访问控制粒度，如系统级、库级、表级、字段级。
c) 查验组织是否明确了身份认证与访问控制控制效果的量化评估方式：
   1) 是否定义了量化评估指标，如多因子身份认证方式覆盖率等；
   2) 是否规定了量化评估频率。
d) 查验组织的技术工具：

1) 是否存在凭据托管系统(如密钥托管)，避免凭据写死代码等行为；
2) 是否具备敏感数据权限清单，明确安全角色的安全要求、分配策略、授权机制、权限范围等；
3) 是否支持敏感数据权限清单的定期更新和审核；
4) 是否实现身份认证与访问控制管理效果的量化评估方法；
5) 是否定期进行身份认证与访问控制管理效果量化评估；
6) 是否根据量化评估结果进行及时的调整。

10.5.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了身份认证与访问控制安全的优化工作机制：是查验是否具有身份认证与访问控制规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。
b) 查验组织的技术工具：
   1) 是否具有身份认证与访问控制技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；
   2) 是否主导国际、国家和行业标准的制定；
   3) 是否具备身份认证与访问控制技术研究能力，形成一系列卓越的研究成果，并将自身的身份认证与访问控制建设经验作为行业最佳案例进行推广，获得行业认可。

10.6 安全风险分析

10.6.1 概述

根据组织的业务场景建立数据安全风险分析体系，有效应对组织内数据和业务的安全风险。

10.6.2 等级要求

10.6.2.1 第一级

第一级应从制度流程方面满足如下要求：

制度流程：未在任何业务中建立成熟和稳定的安全风险分析制度，仅根据临时需要或基于个人经验考虑了安全风险。

10.6.2.2 第二级

第二级应从组织建设、制度流程、人员能力方面满足如下要求：

a) 组织建设：应设置核心部门的数据安全风险分析相关的岗位和人员，负责核心部门的数据安全风险分析，并配合推进相关工作的开展和实施；
b) 制度流程：核心部门应明确数据安全风险分析的管理制度与流程；
c) 人员能力：应了解常见的数据应用场景和安全风险，并对数据安全法律合规知识体系具有一定概念。

10.6.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据安全风险分析相关的部门、岗位和人员，负责组织层面的数据安全风险分析，与其他部门协同工作，配合推进相关工作的开展和实施。
b) 制度流程：
   1) 应建立数据安全风险监测机制，及时排查安全隐患，采取必要的措施防范数据安全风险；
   2) 应明确数据安全风险分析方法、优先级计算规则和风险处置跟踪机制；
   3) 应明确数据安全风险评估方法、评估报告内容和上报机制，按照主管部门要求向其报送风险评估报告。
c) 技术工具：
   1) 应建立风险分析库，用于风险评估；
   2) 应支持识别数据资产及其面临的威胁和自身脆弱性，并分析数据安全风险；
   3) 应具备数据安全风险监测技术手段；
   4) 应具备数据风险评估标准或工具。
d) 人员能力：
   1) 应在数据风险管理及业务实践方向具备一定经验，能够判断风险程度；
   2) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

10.6.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：
a) 制度流程：
   1) 应建立完善的数据安全风险分析体系；
   2) 应量化数据安全风险分析，以保证符合组织发展战略和业务发展的实际需要，并定期更新相关制度、流程。
b) 技术工具：
   1) 应建立完善的数据安全风险分析系统；
   2) 应提供量化分析工具，对数据安全风险管理效果进行量化评估。

10.6.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：
a) 制度流程：应支持安全风险分析规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。
b) 技术工具：
   1) 应支持安全风险分析技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；
   2) 应能主导国际、国家和行业标准的制定，具备安全风险分析技术研究能力，形成一系列卓越的研究成果，并将自身的安全风险分析建设经验作为行业最佳案例进行推广，获得行业认可。

10.6.3 评估方法

10.6.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别业务中根据临时需求进行风险感知。

10.6.3.2 第二级

根据第二级要求，从组织建设、制度流程、人员能力方面进行查验：

a) 查验是否在核心业务部门设置了数据安全风险分析相关的岗位和人员；

b) 查验是否在核心部门层级制定了数据安全风险分析的相关制度文件；

c) 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

10.6.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设置了数据安全风险分析相关的部门、岗位和人员。

b) 查验是否在组织层面制定了数据安全风险分析相关制度文件：

1) 是否建立数据安全风险监测机制，及时排查安全隐患，采取必要的措施防范数据安全风险；

2) 是否明确数据安全风险分析方法、优先级计算规则和风险处置跟踪机制；

3) 是否明确数据安全风险评估方法、评估报告内容和上报机制，并定期开展数据安风险评估，按照主管部门要求向其报送风险评估报告。

c) 查验组织技术工具：

1) 是否建立了风险分析库，明确风险评估场景，尤其是个人信息处理场景，并定期更新；

2) 是否具备数据安全风险监测技术工具，能够实时发现数据安全风险，包括但不限于数据异常访问、数据泄露等风险；

3) 是否具备数据安全风险可视化展示功能；

4) 是否具备数据安全风险评估标准或工具，并每年至少一次开展全面的数据安全风险评估。

d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

10.6.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是建立了围绕数据全生命周期的数据安全风险分析体系。

b) 查验组织是否明确了风险分析效果的量化评估方式：

1) 是否定义了风险分析的量化评估指标,如数据安全风险识别数量、级别、处理量等；

2) 是否规定了风险分析的量化评估频率。

c) 查验组织的技术工具：

1) 是否实现了围绕数据全生命周期的安全风险分析体系；

2) 是否实现安全风险分析管理效果的量化评估方法；

3) 是否定期进行安全风险分析管理效果量化评估；

4) 是否根据量化评估结果进行及时的调整。

10.6.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了风险分析的优化工作机制：

1) 是否具有安全风险分析规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。

b) 查验组织的技术工具：

1) 是否具有安全风险分析技术持续优化升级的记录，其优化动机体现了企业数据安全治理

战略目标和规划的调整或者最新技术的发展等；

2) 是否主导国际、国家和行业标准的制定；

3) 是否具备安全风险分析技术研究能力，形成一系列卓越的研究成果，并将自身的安全风险分析建设经验作为行业最佳案例进行推广，获得行业认可。

10.7 安全事件应急

10.7.1 概述

建立数据安全应急响应体系，对各类数据安全事件进行及时响应和处置。

10.7.2 等级要求

10.7.2.1 第一级

第一级应从制度流程方面满足如下要求：

制度流程：未在任何业务中建立成熟和稳定的安全事件应急制度，仅根据临时需要或基于个人经验考虑了安全事件应急。

10.7.2.2 第二级

第二级应从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置核心部门的数据安全事件应急相关的岗位和人员，负责核心部门的数据安全事件应急，并配合推进相关工作的开展和实施；

b) 制度流程：明确核心部门中数据安全事件的管理，以及应急响应策略和具体方案的制定；

c) 技术工具：应记录数据安全事件处理情况、应急演练情况；

d) 人员能力：能够按准确理解应急响应方案，并按照指定的策略开展相应的应急活动。

10.7.2.3 第三级

第三级应在第二级的等级要求上，从组织建设、制度流程、技术工具、人员能力方面满足如下要求：

a) 组织建设：应设置组织层面的数据安全事件应急相关的部门、岗位和人员，负责组织层面的数据安全事件应急，与其他部门协同工作，配合推进相关工作的开展和实施。

b) 制度流程：

1) 应明确数据安全事件管理和应急响应工作指南，定义数据安全事件类型，明确不同类别事件的处置流程和方法；

2) 应在组织内部对应急响应、数据安全事件处置工作制度、策略、方法进行培训宣传，培养人员的基本应急响应意识；

3) 应制定数据安全事件应急预案，并定期开展应急演练活动；

4) 应明确规定涉及个人信息安全事件的应急响应机制及应急预案；

5) 发生数据安全事件时，应按照行业主管部门有关规定，向行业主管部门上报数据安全事件及其处置情况；

6) 发生数据安全事件且涉及个人信息时，应按照法律法规要求告知个人；

7) 应定期开展应急演练。

c) 技术工具：应具备安全事件管理工具，对安全事件告警进行处置和响应。

d) 人员能力：

1) 应能够进行安全事件的分析判断，熟悉安全事件应急响应措施；
2) 应具备实践经验，能够应对应急事件处理过程中的决策工作；
3) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

10.7.2.4 第四级

第四级应在第三级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：
   1) 应建立数据安全事件复盘机制，总结应急响应经验；
   2) 应根据不同安全事件类型建立差异化的应急流程，明确不同应急流程应采取的溯源、阻断、删除等响应动作；
   3) 应规定安全事件应急响应管理效果的量化评估方式、频率和调整计划。
b) 技术工具：
   1) 应能基于分析的内容实现预警及自动化响应决策，及时辅助安全事件应急响应；
   2) 应提供知识库平台，记录应急演练安全事件处置结果和应急策略；
   3) 应在应急事件处理中具备拦截、阻断数据外发能力，及其数据清除的能力；
   4) 应实现安全事件应急效果的量化评估方法。

10.7.2.5 第五级

第五级应在第四级的等级要求上，从制度流程、技术工具方面满足如下要求：

a) 制度流程：应支持安全事件应急规范和流程等的持续优化，能根据外部监管要求和内部发展需要做出及时的优化和改进。
b) 技术工具：
   1) 应支持安全事件应急技术的持续优化，能够根据数据安全治理的战略目标和规划的变化和技术的发展进行持续优化；
   2) 应能主导国际、国家和行业标准的制定，具备安全事件应急技术研究能力，形成一系列卓越的研究成果，并将自身的安全事件应急建设经验作为行业最佳案例进行推广，获得行业认可。

10.7.3 评估方法

10.7.3.1 第一级

根据第一级要求，从制度流程方面进行查验：查验是否在个别业务中根据安全事件的发生进行了安全事件的及时处置。

10.7.3.2 第二级

根据第二级要求，从组织建设、制度流程、技术工具、人力能力方面进行查验：

a) 查验是否在核心部门设置了数据安全事件应急相关的岗位和人员。
b) 查验是否在核心部门层级制定了安全事件应急的相关制度文件：
   1) 是否明确了安全事件管理方案；
   2) 是否规定了安全应急预案。
c) 查验组织的技术工具：是否支持对数据安全事件处理和应急演练的记录。
d) 验证组织的人员能力：通过培训记录、考试记录，验证组织的人员能力。

10.7.3.3 第三级

根据第三级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验：

a) 查验是否在组织层面设置了数据安全事件应急相关的部门、岗位和人员。

b) 查验是否在组织层面制定了安全事件应急相关制度文件：

1) 查验该文件的数据安全事件类型划分是否参考了国家法律法规及监管部门要求，如泄露、篡改、非法访问、非法利用、重大数据操作行为等；

2) 查验该文件的数据安全事件等级划分是否结合了对国家安全、经济发展、社会公共利益、企业和个人信息主体合法权益的影响程度；

3) 是否明确了不同类型及等级的数据安全事件处置流程和方法；

4) 是否明确了不同类型及等级的数据安全事件的应急预案；

5) 是否明确了按照法律法规要求进行用户告知和上报关主管部门的规定；

6) 如有发生数据安全事件且涉及个人信息情况，是否按照法律法规要求告知个人；

7) 是否定期开展应急演练。

c) 查验组织技术工具：

1) 是否具备数据安全事件管理系统，对告警进行处置和响应；

2) 是否留存应急响应处置记录、演练记录。

d) 验证组织的人员能力：通过访谈、查验培训记录、查验考试记录或查验相关人员制定的解决方案等方式，验证组织的人员具备相应的能力。

10.7.3.4 第四级

根据第四级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了安全事件应急管理效果的量化评估方式：

1) 是否定义了量化评估指标，如数据安全事件统计、监控报警处理及时度等；

2) 是否规定了量化评估频率。

b) 查验组织是否明确了安全事件应急的优化工作机制：

1) 是否根据政策、业务等的需求，对组织的安全事件管理和应急响应机制进行优化调整，并复核有效性；

2) 是否明确了数据安全事件的总结分享机制；

3) 是否根据不同安全事件类型建立差异化的应急流程。

c) 查验组织的技术工具：

1) 是否支持数据安全事件的预警与自动化响应；

2) 是否具备数据安全应急演练知识库；

3) 是否具备拦截、阻断数据外发能力，及其数据清除的能力；

4) 是否实现安全事件应急管理效果的量化评估方法；

5) 是否定期进行安全事件应急管理效果量化评估；

6) 是否根据量化评估结果进行及时的调整。

10.7.3.5 第五级

根据第五级要求，从制度流程、技术工具方面进行查验：

a) 查验组织是否明确了安全事件应急的优化工作机制：是否具有安全事件应急规范和流程的持续优化的记录，其优化动机体现了外部监管要求和内部发展需要等。

b) 查验组织的技术工具：

1) 是否具有安全事件应急技术持续优化升级的记录，其优化动机体现了企业数据安全治理战略目标和规划的调整或者最新技术的发展等；
2) 是否主导国际、国家和行业标准的制定；
3) 是否具备安全事件应急技术研究能力，形成一系列卓越的研究成果，并将自身的安全事件应急建设经验作为行业最佳案例进行推广，获得行业认可。

参 考 文 献

[1] GB/T 36073-2019 数据管理能力成熟度评估模型
[2] GB/T 37973-2019 信息安全技术 大数据安全管理指南
[3] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求