ICS 35.030
CCS L80

团　　体　　标　　准

T/ISC-0011-2021

数据安全治理能力评估方法

Evaluation method of data security governance capability

2021－04－27 发布　　2021－07－01 实施

中　国　互　联　网　协　会　　发 布

目　　次

前　言

本文件按照GB/T 1.1-2020给出的规则起草。

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这些专利的责任。

本文件由中国互联网协会提出并归口。

本文件主要起草单位：中国信息通信研究院、联通数字科技有限公司、北京百度网讯科技有限公司、奇安信科技集团股份有限公司、蚂蚁科技集团股份有限公司、京东数字科技集团、北京爱奇艺科技有限公司、北京小米移动软件有限公司、北京三快在线科技有限公司、中国联合网络通信集团有限公司、中国联通研究院、恒安嘉新（北京）科技股份公司、中国移动通信集团有限公司、天翼云科技有限公司、闪捷信息科技有限公司、北京快手科技有限公司、同盾科技有限公司、北京天融信网络安全技术有限公司、北京字节跳动科技有限公司、贝壳找房（北京）科技有限公司、OPPO广东移动通信有限公司、杭州安恒信息技术股份有限公司、启明星辰信息技术集团股份有限公司等。

本文件主要起草人：李雪妮、闫树、魏凯、姜春宇、范东媛、裴超、田涛、钟舒翔、孙硕、聂君、孙晶、王新华、马天羿、王昕、陆平、李龙、樊庆君、朱玲凤、刘大千、张振涛、李鹏超、孟娟、叶串、吴斌、孙艺、吴连勇、曹咪、娄涛、温暖、李文琦、刘飞龙、蓝宇娜、陈广辉、赵皓星、王峰、曲远汶、陈洪运、安潇羽、刘扬、孙瑶、李根、高柱、周瑞群

引　言

随着大数据技术和产业的不断发展壮大，数据跃升为生产要素，以推动数字经济的高质量发展。新形势下的数据安全上升到国家安全层面，事关国家安全与经济社会发展。然而，当前行业数据安全认识稍显不足，数据安全治理能力参差不齐，数据安全标准实际落地效果欠佳。为指导行业数据安全治理能力建设，帮助企业发现数据安全治理能力不足，促进行业数据安全治理能力发展，需要推出数据安全治理能力评估标准及配套评估方法。本文件以数据全生命周期的安全治理能力建设为切入点，关注数据安全治理要点和关键环节的建设情况，梳理治理能力级别并分级制定考核指标，以对电信互联网企业的数据安全治理能力进行度量，为企业不断提升数据安全治理能力提供可操作的实施指南。

数据安全治理能力评估方法

1 范围

本文件描述了各类数据治理活动及其相关平台应遵循的数据安全治理能力要求和评估方法，包括评估等级划分方法，以及数据安全战略、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、基础安全等能力的具体评估等级确定原则。

本文件适用于电信网和互联网等企业开展数据治理工作，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—2010 信息安全技术 术语

GB/T 29765—2013 信息安全技术 数据备份与恢复产品技术要求与测试评价方法 术语和定义

GB/T 29246—2017 信息技术 安全技术信息安全管理体系 概述和词汇

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型 术语和定义

GB/T 35273—2020 信息安全技术 个人信息安全规范 术语和定义

3 术语和定义

GB/T 25069—2010、GB/T 29765—2013、GB/T 29246—2017、GB/T 37988—2019和GB/T 35273—2020界定的以及下列术语和定义适用于本文件。

3.1

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019，3.1]

3.2

保密性 confidentiality

使信息不泄漏给未授权的个人、实体、进程，或不被其利用的特性。

[来源：GB/T 25069—2010，2.1.1]

3.3

完整性 integrity

准确和完备的特性。

[来源：GB/T 29246—2017，2.40]

3.4

备份数据 backup data

存储在（通常可移动的）非易失性存储介质上某一时间点的数据集合，用于原数据丢失或不可访问时的数据恢复。

[来源：GB/T 29765-2013，3.1]

3.5

备份 backup

创建备份数据的过程。

[来源：GB/T 29765-2013，3.2]

3.6

技术工具technical tool

通过技术手段或平台工具等方式支撑组织数据安全治理能力的建设。

3.7

内部共享internal sharing

在单个组织内部环境下的数据交换过程。

3.8

外部共享external sharing

在任意两个或多个组织之间的数据交换过程。

3.9

数据血缘data consanguinity

记录了对原始数据的处理步骤，标明了数据产生的链路关系。

3.10

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。

注1： 个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，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，属于个人信息。

[来源：GB/T 35273-2020，3.1，有修改]

3.11

个人敏感信息 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 35273-2020，3.2]

4 概述

4.1 评估原则

（1）标准性原则：评估工作应依据本文件展开。

（2）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。

（3）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

主要通过文档查验、人员访谈、系统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。

系统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，评估实施过程见图1

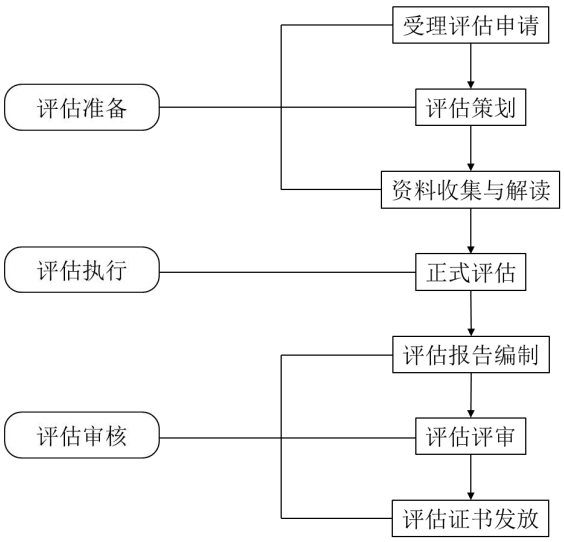

图1 评估实施过程

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，并进行评估的等级证书发放。

5 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，见图2所示。

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、鉴别与访问、风险和需求分析、安全事件应急。

	数据安全战略		数据生命周期安全									基础安全						
能力项	数据安全规划	机构人员管理	数据采集安全	数据传输安全	存储安全	数据备份与恢复	使用安全	数据处理环境安全	数据内部共享安全	数据外部共享安全	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	鉴别与访问	风险和需求分析	安全事件应急

图2 数据安全治理能力评估框架

6 评估等级

数据安全治理能力评估等级将从组织建设的完备程度、制度流程覆盖面、技术工具支撑力度、人员能力培养四个维度划分为三级，分别是基础级、优秀级、先进级，每个后一级的标准均是在前一级基础上的加强。

6.1 第一级：基础级

数据安全治理能力主要是体现在离散的项目中，建立了基本的管理流程和初步的体系，具体特征如下：

a) 一般由各业务团队人员负责数据安全相关工作；
b) 制定了初步的数据安全制度规范和管理流程，以保障组织核心业务的安全执行及故障恢复，并能基本满足监管要求；
c) 尝试采用技术手段和产品工具落实安全要求，但对业务和数据全生命周期的覆盖范围及支撑能力有限；
d) 开始关注组织内人员的数据安全意识，进行定期培训。

6.2 第二级：优秀级

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，能够促进数据安全的规范化落地，具体特征如下：

a) 设立了专门的数据安全管理部门、岗位、人员，主要负责制定实施组织的数据安全战略规划、数据安全制度流程，以覆盖数据全生命周期相关的业务、系统和应用；
b) 具备完善的数据安全管理制度和流程，以保障组织全部业务的安全执行及故障恢复，并能完全满足监管要求；
c) 具备较强的技术能力，积累了大量的技术手段和产品工具，对数据全生命周期的安全过程和组织内全业务流程的开展进行有效支撑；
d) 对组织内部人员的安全意识和安全能力制定了相应的培训及考核机制，注重组织内部数据安全的人才培养。

6.3 第三级：先进级

数据安全治理能力体现在拥有完善的数据安全治理能力量化评估体系和持续优化策略，具体特征如下：

a) 建立了统一的技术工具，能够为组织的数据安全治理提供支撑；
b) 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，并根据评估结果及时对组织建设情况进行调整优化；
c) 当监管要求、组织架构、业务需求等发生变化时，能够及时调整相应的数据安全策略及规范。

7 数据安全战略

7.1 数据安全规划

7.1.1 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。

7.1.2 等级要求

7.1.2.1 基础级

从组织建设、制度流程方面进行要求。

a) 组织建设：应设置相关岗位和人员负责核心业务的数据安全规划，推进规划的开展实施。
b) 制度流程：应对核心业务进行数据安全规划，明确基本的合规要求。

7.1.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

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、技术工具、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，明确安全方针、安全目标和安全原则，其中方针和策略应明确对组织的价值和意义、应以数据为核心围绕数据工作；
    2) 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；
    3) 应制定数据保护计划，明确需要执行的活动、所需资源、支持岗位、时间安排和实施步骤。
c) 技术工具：应建立数据安全规划分发及管理平台在组织内部对数据安全规划进行推广。

d) 人员能力：
   1) 应了解组织的业务发展目标，能够将数据安全工作的目标和业务发展的目标进行有机结合；
   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计划实施；
   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。

7.1.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
   1) 应在组织架构发生重大调整或数据服务业务发生重大变化时，及时评估数据安全制度与规程的实施效果，并将效果反应到安全制度和规程文件的修订过程中；
   2) 应对数据安全制度和规程进行体系化的评估，制定数据安全治理能力提升计划；
   3) 应对数据安全战略规划进行评估，确保数据安全总体策略、安全目标和战略规划内容的合规性。
b) 技术工具：应建立数据安全规划动态调整机制，通过信息化系统执行对数据安全规划的动态管理。

7.1.3 评估方法

7.1.3.1 基础级

根据基础级要求，从组织建设、制度流程方面进行查验。

a) 查验业务团队是否明确了负责本业务数据安全规划的岗位和人员。
b) 查验是否在核心业务层级制定了数据安全规划相关制度文件：
   1) 查验该文件是否明确了相关数据全生命周期的数据安全策略；
   2) 查验该文件是否定义了合规要求。

7.1.3.2 优秀级

根据优秀级要求，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安全安全规划的部门、岗位和人员，并规定了职责范围。
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) 查验该文件的制定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) 查验该文件是否制定了组织的数据安全总体策略，明确了安全方针、安全目标和安全原则等内容；
   3) 查验该文件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、工作重点，并保障其与业务规划相适应；
   4) 查验该文件是否明确了数据保护机制；
   5) 查验该文件是否规定了数据安全规划制度的编制、评审、发布、更新流程。
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) 查验该文件是否明确了数据安全管理的目的、范围、岗位、责任、管理层承诺、内外部协调机制及合规目标等；
   2) 查验该文件是否规定了数据安全制度的分发机制；
   3) 查验该文件是否明确了数据安全制度的编制、评审、发布、更新流程；
   4) 由数据安全规划组织对数据安全策略进行统一规划、发布、更新。
d) 查验组织技术工具：
   1) 是否开展数据安全规划研讨会；

2) 是否具备数据安全规划推广平台，且能正常运行。

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。

7.1.3.3 先进级

根据先进级要求，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安全管理制度、规划效果的量化评估方式：
   1) 是否定义了量化评估指标；
   2) 是否规定了量化评估频率。
b) 查验组织是否明确了数据安全规划的优化工作机制：
   1) 是否支持根据政策变化、架构调整、业务发展等需求优化规划制度；
   2) 是否支持根据评估结果优化管理制度。
c) 查验组织的技术工具：是否具备安全规划管理平台，动态调整机制，通过信息化对于数据安全规划进行动态管理。

7.2 机构人员管理

7.2.1 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。

7.2.2 等级要求

7.2.2.1 基础级

从组织建设、制度流程、人员能力方面进行要求。

a) 组织建设：应设置具有数据安全职能的岗位和人员，以实现对关键业务环节数据安全风险的有效管理。
b) 制度流程：
   1) 应明确核心业务数据安全违规的纪律处理制度；
   2) 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；
   3) 应明确核心业务数据安全岗位的职责；
   4) 应明确核心业务数据安全培训计划，并按计划对相关人员开展数据安全培训；
   5) 应与所有涉及数据服务的人员签订安全责任协议和保密协议。
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。

7.2.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a)组织建设：
   1) 应明确组织层面负责数据安全管理的部门、岗位和人员，具备数据安全管理责任体系，并指定机构最高管理者或授权代表担任责任人，明确其责任与权力；
   2) 应建立组织的监督管理职能部门，负责对组织内部的数据操作行为进行监督；

3) 应制定组织的数据安全规划、安全建设、安全运营和系统维护工作的责任部门；
4) 应明确组织层面担任机构人员数据安全培训职责的岗位和人员，负责对数据安全培训需求的分析及落地方案的制定和推进。

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，以及职能部门之间的协作关系和配合机制；
2) 应明确数据安全追责机制，定期对责任部门和安全岗位组织安全检查，形成检查报告；
3) 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；
4) 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；
5) 应明确数据服务涉敏岗位的权限分离、多人共管等安全管理要求；
6) 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) 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) 应开展针对员工入职过程中的数据安全教育，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。

7.2.2.3 先进级

在优秀级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a)组织建设：

1) 应根据职责分离原则设置数据安全管理的岗位和人员；
2) 应建立覆盖各业务部门的体系化的数据安全管理部门，且配备必要的管理人员和技术人员；

b)制度流程：

1) 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；
2) 应定期对数据安全培训内容、计划审核更新，对数据安全培训效果进行量化评估；
3) 应定期对机构人员的管理效果进行量化评估；
4) 应对数据安全职能的运行效果以量化指标的形式进行定期衡量，并出具相关报告持续改进数据安全计划；
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：应建立人员数据安全意识或能力的客观评价工具，定期更新反馈结果。

b)人员能力：

1) 应具备较强的数据安全保护意识，形成组织的数据安全保护品牌；
2) 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。

7.2.3 评估方法

7.2.3.1 基础级

根据基础级要求，从组织建设、制度流程、人员能力方面进行查验。

a) 查验业务团队是否明确了负责数据安全管理的岗位和人员，及其职责范围。
b) 查验是否在核心业务层级制定了数据安全管理办法。
c) 查验是否制定了数据安全管理人员的培训计划。
d) 查验组织是否明确了针对数据安全违规的处理制度。
e) 查验组织是否签订了数据安全泄露相关的保密协议。
f) 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。

7.2.3.2 优秀级

根据优秀级要求，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数据安全管理责任部门、岗位及领导人员，明确规定了其职责范围。
b) 查验组织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。
c) 查验组织是否建立了数据安全责任体系，包括安全规划、建设、运营等在内的各责任部门。
d) 查验是否建立组织层面的数据安全治理绩效评价体系，对数据安全岗位人员的履职情况制定绩效考核方法。
e) 查验组织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。
f) 查验组织是否设立了数据安全的监督部门，该部门负责对于组织内部数据安全操作行为进行监督。
g) 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) 是否实现了安全规划的公开查询。
h) 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。

7.2.3.3 先进级

根据先进级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验。

a) 查验组织是否支持职责分离的数据安全管理岗位和人员设置。
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；
    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；
    2) 是否规定了量化评估频率。
d) 查验组织是否明确了人员管理的优化工作机制：
    1) 是否支持人员能力的定期考核；
    2) 是否支持根据评估结果优化培训、考核等管理制度；
e) 查验组织的技术工具：是否具备对人员数据安全意识或能力进行客观评价的工具。
f) 查验组织的人员能力：是否具备完善的人才培养体系。

8 数据全生命周期安全

8.1 数据采集安全

8.1.1 概述

在直接采集或间接收集外部数据的过程中，组织应明确采集数据目的和用途的真实性、有效性，满足采集最小必要等原则要求，并明确数据采集渠道、规范数据采集格式以及相关的流程，从而保证数据采集的合法性、合规性、正当性。

8.1.2 等级要求

8.1.2.1 基础级

从组织建设、制度流程方面进行要求。

a) 组织建设：应设置相关岗位和人员负责数据采集安全的管理，配合推动相关要求的执行。
b) 制度流程：
   1) 应定义核心业务的数据采集规则，如采集原则、采集渠道等，以保证该业务数据采集的合法、正当；
   2) 应明确核心业务的数据采集合规性评估工作机制；
   3) 核心业务应明确个人信息采集的目的、方式、范围、保存期限，当涉及个人敏感信息时，应明确采集的必要性及对个人的影响。
   4) 应明确个人信息的采集需要用户授权同意。
   5) 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。

8.1.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：应设立相关部门、岗位和人员，负责统一制定相关的数据采集安全管理的制度，配合推动相关要求的执行。
b) 制度流程：
   1) 应明确数据采集安全管理要求，包括组织采集数据时的原则，定义业务数据的直接或间接采集流程和方法；
   2) 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；
   3) 应规定数据采集的渠道及外部数据源鉴定方式，并对采集来源方式、数据范围和类型进行记录，确保不收集与提供服务无关的个人信息；
   4) 应规定数据采集过程中个人信息的知悉范围和需要采取的控制措施，确保采集过程中的个人信息不被泄漏，尤其是个人敏感信息。
   5) 应规定当用户注销账户时，不得设置过多不合理的注销条件。
c) 技术工具：
   1) 应建立数据采集工具，具备详细的日志记录功能，保障数据采集授权过程的完整记录；
   2) 应采取相应的技术手段，保证数据采集过程中个人信息不被泄漏。
d) 人员能力：
   1) 应能充分理解数据采集的法律要求、安全和业务需求，并能根据组织的业务提出针对性的解

决方案，能就具体业务场景开展评估；
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。

8.1.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
   1) 应规定数据采集安全管理效果的量化评估方式；
   2) 应规定相关流程确保对行业新技术、最佳实践、法律法规要求、行业标准等合规要求新变化的持续跟踪，并及时修正数据采集安全管理工作。
b) 技术工具：
   1) 应根据制度流程的更新，不断升级优化数据采集工具；
   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) 应具备对采集工具进行统一管理的平台。

8.1.3 评估方法

8.1.3.1 基础级

根据基础级要求，从组织建设、制度流程方面进行查验。

a) 查验业务团队是否明确了负责本业务数据采集安全管理的岗位和人员。
b) 查验是否在核心业务层级制定了数据采集安全相关制度文件：
   1) 查验该文件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) 查验该文件是否规定了数据采集的合规性评估流程；
   3) 查验该文件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、到处理方式等。
   4) 查验该文件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) 查验该文件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) 查验该业务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) 查验该文件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、到处理方式等。
   3) 查验该文件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。
   4) 查验该文件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。

8.1.3.2 优秀级

根据优秀级要求，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) 查验该文件是否覆盖了组织内涉及采集活动的全部业务；
   2) 查验该文件是否对直接和间接采集进行区分管理；
   3) 查验该文件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) 查验该文件是否规定了数据采集的合规性评估流程。

c) 查验组织隐私政策文件及用户协议：
   5) 是否符合国家法律法规和监管要求；
   6) 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、用途、范围、保存时限、到期处理方式等；
   7) 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；
   8) 是否规定了个人信息采集过程中防泄漏措施；
   9) 是否规定了用户提出终止服务时的停止采集要求。
d) 查验组织的技术工具：
   1) 是否支持数据采集过程的自动化实现及日志记录；
   2) 是否实现了对采集环境，如采集设备、采集接口等的安全管控，防止数据泄露；
   3) 是否采用了有效的防护手段，保障用户个人信息采集的安全性。
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。

8.1.3.3 先进级

根据先进级要求，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；
   2) 是否规定了量化评估频率。
b) 查验组织是否明确了数据采集安全的优化工作机制：
   1) 是否支持根据政策变化、业务发展等需求优化管理制度；
   2) 是否支持根据评估结果优化管理制度。
c) 验证组织的技术工具：
   1) 是否定期对采集工具进行安全测试、适用性评估、合规性评估等；
   2) 是否支持数据合规性的监控与告警；
   3) 是否具备统一的数据采集工具管理平台。

8.2 数据传输安全

8.2.1 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。

8.2.2 等级要求

8.2.2.1 基础级

从组织建设、制度流程、技术工具方面进行要求。

a) 组织建设：应设置相关岗位和人员负责数据传输安全的管理，配合推动相关要求的执行。
b) 制度流程：应根据合规要求和业务性能的需求，明确核心业务中需要加密传输的数据范围和加密算法。
c) 技术工具：
   1) 应实现对传输通道两端的主体身份鉴别和认证；
   2) 应建立传输数据加密的技术方案和工具，包括针对关键的数据传输通道的加密方案（如采用

TLS/SSL 方式），及对传输数据内容进行加密等；

3) 传输个人敏感信息时，应实施加密技术进行保护。

8.2.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：应设置相关部门、岗位和人员，负责数据传输安全的解决方案制定，配合推动相关要求的执行。

b) 制度流程：

1) 在数据分类分级定义的基础上制定数据传输安全管理规范，明确各业务场景下的数据传输安全要求（如传输通道加密、数据内容加密、签名验签、身份鉴别、数据传输接口安全等）；

2) 应明确境内或跨境传输个人信息，尤其是个人敏感信息时的安全管理规范；

3) 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；

4) 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相应的安全控制技术方案，包括安全通道、可信通道、数据加密等；

2) 应提供对数据传输安全策略的变更进行审核和监控的技术方案和工具；

3) 应部署对通道安全配置、密码算法配置等保护措施进行审核及监控的技术工具。

4) 应提供对数据传输接口的审核及监控手段。

d) 人员能力：

1) 应了解市场上主流的安全通道和可信通道建立方案、身份鉴别和认证技术、数据加密算法和国家推荐的数据加密算法，从而能够基于具体的业务场景选择合适的数据传输安全管理方式，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。

8.2.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：

1) 应规定数据传输安全效果的量化评估方式；

2) 应规定根据政策变化和业务需求等对数据传输制度进行优化的机制；

3) 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。

3) 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。

4) 应对输入输出的数据进行安全拦截，及时发现数据传输中的安全问题，能够自动化应急处理。

8.2.3 评估方法

8.2.3.1 基础级

根据基础级要求，从组织建设、制度流程、技术工具方面进行查验。

a) 查验业务团队是否明确了负责本业务数据传输安全管理的岗位和人员。
b) 查验是否在核心业务层级制定了数据传输安全相关制度文件：
   1) 查验该文件是否明确规定了数据传输的加密要求及加密方案；
   2) 查验该文件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；
   3) 查验该文件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) 是否支持对传输通道两侧的身份验证。

8.2.3.2 优秀级

根据优秀级要求，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整体数据传输安全防护的部门、岗位和人员。
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) 查验该文件的制定是否结合了组织的数据分类分级策略，并明确提出相匹配的数据加密传输要求；
   2) 查验该文件是否对组织内、外的传输场景进行了区分，并规定了差异化的加密措施；
   3) 查验该文件是否定义了传输策略变更的审批和监控机制；
   4) 查验该文件是否明确了数据跨境传输的管理要求，尤其是个人信息的跨境传输，以符合国家规定及监管要求。
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) 查验该文件是否规定了新增接口、变更接口、废弃接口等的处理流程；
   2) 查验该文件是否定义了传输流程的技术管控及安全防护措施；
   3) 查验该文件是否规定了接口梳理的工作制度；
   4) 查看该文件是否规定了对涉及个人信息传输的接口应实施调用监控制度。
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评估；
   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鉴别与认证；
   6) 是否支持对传输通道缓存的自动删除；
   7) 是否支持对传输安全策略变更的审核及监控。
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。

8.2.3.3 先进级

根据先进级要求，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；
   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) 查验组织是否明确了根据评估结果、业务需要、监管要求等进行传输方案优化的制度。

c) 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。
d) 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。

8.3 存储安全

8.3.1 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。

8.3.2 等级要求

8.3.2.1 基础级

从组织建设、制度流程、技术工具方面进行要求。
a) 组织建设：应设置相关岗位和人员负责数据存储安全工作，负责各项制度的推进落实。
b) 制度流程：应在核心业务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。
c) 技术工具：应提供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、存储空间的身份鉴别、逻辑访问控制以及运维管理的基本能力。

8.3.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。
a) 组织建设：应建立体系化的存储管理部门，在存储介质和逻辑存储管理设置专门的安全管理岗位和人员，遵循组织层面统一的安全管理原则，并执行推进实施。
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，尤其是个人信息存储相关规范；
   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) 应建立存储介质的保存环境制度规范，明确存储介质引入流程、出入库规范、保存环境要求、以及可用性保障要求；
   4) 应建立存储介质的环境变更机制、逻辑存储资源的配置变更机制，对配置规则、操作流程、发布要求、授权管理等标准进行规范；
   5) 应定义存储介质、逻辑存储、存储系统架构的设计及安全要求。
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) 存储空间应根据数据的保密性提供完善的加密存储能力。
d) 人员能力：应熟悉存储结构，组织应定期对人员进行培训，并考核人员能力与岗位的匹配程度。

8.3.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
   1) 应制定数据存储的操作流程手册和配置规则，确立可遵照执行、有准确描述的操作步骤、配置指标。
   2) 应规定相关流程确保对行业新技术、最佳实践、法律法规要求、行业标准等合规要求新变化的持续跟踪，并及时修正数据存储安全管理工作。
   3) 应制定数据存储安全的量化评估机制，定期对存储安全管理效果进行量化评估。
b) 技术工具：
   1) 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、传递追踪等；
   2) 应采用可扩展的数据存储架构；
   3) 应根据数据敏感度，提供不同的安全存储管理能力。
   4) 应提供数据审查、保护系统，能够实时发现敏感数据信息，保障在查询、输出时及时脱敏处理。

8.3.3 评估方法

8.3.3.1 基础级

根据基础级要求，从组织建设、制度流程、技术工具方面进行查验。

a) 查验业务团队是否明确了负责本业务数据存储安全的岗位和人员。
b) 查验是否在核心业务层级制定了数据存储策略相关制度文件：
   1) 查验该文件是否明确了数据安全存储的配置规则；
   2) 查验该文件是否明确了存储媒体的购买、标记、使用等安全制度。
c) 查验组织的技术工具：是否实现了存储系统的访问控制、身份鉴别、运维管理等。

8.3.3.2 优秀级

根据优秀级要求，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整体负责数据存储安全的部门、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，并规定了差异化的安全存储保护方式等；
   2) 查验该文件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) 查验该文件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) 查验该文件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。
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) 查验该文件是否规定了存储介质的登记、审批、标记、接入、保存环境、可用性要求等安全管理措施；
   2) 查验该文件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；
   3) 查验该文件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) 是否提供多种加密存储手段（如磁盘加密、文档加密、数据库表行级加密等），满足不同的数据保密要求；
   3) 是否支持分类分级的差异化数据存储管理；

4) 是否能够对存储系统的安全配置进行定期扫描。

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。

8.3.3.3 先进级

根据先进级要求，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存储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；
   2) 是否规定了量化评估频率。
b) 查验组织是否明确了数据存储安全的优化工作机制：
   1) 是否支持根据政策变化、业务发展等需求优化管理制度；
   2) 是否支持根据评估结果优化管理制度。
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) 是否支持可扩展的数据存储架构；
   3) 是否支持根据数据的敏感度，提供不同的安全存储管理能力；
   4) 是否支持定期更新加密密钥；
   5) 是否具备敏感数据识别、保护的工具或平台。

8.4 数据备份与恢复

8.4.1 概述

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。

8.4.2 等级要求

8.4.2.1 基础级

从组织建设、制度流程、技术工具、人员能力方面进行要求。

a) 组织建设：应设置相关岗位和人员负责核心业务的数据备份与恢复工作，负责各项制度的推进落实。
b) 制度流程：应建立关于核心业务的数据存储冗余策略和恢复管理机制。
c) 技术工具：存储系统应具备数据备份与恢复功能。
d) 人员能力：
   1) 应了解数据备份和恢复的重要性。
   2) 应熟练操作系统自身备份与恢复功能。

8.4.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：应在组织层面设立负责数据备份和恢复工作的部门、岗位，并配备人员负责建立相应的制度流程并部署相关的安全措施。
b) 制度流程：
   1) 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；
   2) 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；

3) 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、一致性检查等；

4) 应根据数据生命周期和业务规范，建立数据生命周期各阶段数据归档的操作流程；

5) 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。

c) 技术工具：

1) 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；

2) 应建立备份数据安全的技术手段，包括但不限于对备份数据的访问控制、压缩或加密管理、完整性和可用性管理，确保对备份数据的安全性、存储空间的有效利用、安全存储和安全访问；

3) 应采取必要的技术措施定期查验备份数据完整性和可用性；

4) 应建立过期存储数据及其备份数据彻底删除或匿名化的方法和机制，能够验证数据已被完全删除、无法恢复或无法识别到个人；

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

6) 应确保存储架构具备数据存储跨机柜或跨机房容错部署能力。

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) 应了解数据存储时效性相关的合规性要求，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，考核人员能力与岗位的匹配程度。

8.4.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：

1) 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；

2) 应定期统计组织内数据备份的场景、数量、频率，对组织内部数据备份与恢复工作进行量化评估。

b) 技术工具：

1) 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；

2) 存储系统应具备数据存储跨地域的容灾能力；

3) 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。

8.4.3 评估方法

8.4.3.1 基础级

根据基础级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务数据备份与恢复的岗位和人员。

b) 查验是否在核心业务层级制定了数据备份与恢复相关制度文件。

c) 查验存储系统是否具备自动备份与恢复的功能。

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。

8.4.3.2 优秀级

根据优秀级要求，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整体负责数据备份与恢复的部门、岗位和人员。
b) 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) 查验该文件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) 查验该文件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；
   3) 规定了生命周期各阶段的数据归档操作流程；
   4) 查验该文件是否规定了使用第三方备份服务时的协同工作机制；
   5) 查验该文件是否明确了备份数据的压缩或加密要求；
   6) 查验该文件是否结合国家法律法规和监管要求等，规定了个人信息的备份制度。
c) 查验组织的技术工具：
   1) 是否支持数据的备份和恢复；
   2) 是否提供备份数据的安全防护手段（如加密或压缩算法、访问控制机制等）、过期删除机制、误删除恢复机制；
   3) 是否支持备份数据的完整性和可用性验证；
   4) 是否支持误删除的恢复机制；
   5) 是否具备数据存储跨机柜/机房的容错部署能力。
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。

8.4.3.3 先进级

根据先进级要求，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备份与恢复的管理效果的量化评估方式：
   1) 是否定义了量化评估指标；
   2) 是否规定了量化评估频率。
b) 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。
c) 查验组织的技术工具：
   1) 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；
   2) 是否支持跨地域容灾；
   3) 是否支持备份数据的时效性检测。

8.5 使用安全

8.5.1 概述

根据数据分析、数据挖掘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。

8.5.2 等级要求

8.5.2.1 基础级

从组织建设、制度流程、人员能力方面进行要求。

a) 组织建设：应设置相关工作岗位和人员负责核心业务的数据使用安全，配合推动相关要求的执行。
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范围和权限、合规要求、使用安全防护要求（例如数据脱敏、访问控制）、数据使用限制等；
   2) 应明确业务平台在不同目的下数据使用审批要求，留存审批记录。
c) 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。

8.5.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：
   1) 应设立数据安全部门、岗位和人员，负责制定数据使用的安全原则和要求，建立数据权限使用、申请评估机制；
   2) 在数据权限的申请阶段，应明确有相关人员评估数据使用的真实性、必要性、合规性，确定该场景下的安全要求。
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范围和权限、合规要求、使用安全防护要求（例如数据脱敏、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) 应建立业务结果数据输出的安全审核、合规评估的流程。
c) 技术工具
   1) 应部署数据脱敏工具，确保脱敏有效性；
   2) 应记录、保存数据使用过程中对个人信息等敏感数据的操作行为；
   3) 应部署数据权限管控工具，依据安全使用规范的要求建立相应强度或粒度的访问控制机制，限定用户可访问数据范围；
   4) 应支持对违规使用行为的有效识别和监控。
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) 应定期对人员进行培训，考核人员能力与岗位的匹配程度。

8.5.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：应明确数据使用安全的量化评估机制。
b) 技术工具：
   1) 应具备技术手段或机制，对数据滥用行为进行有效的自动识别、监控和预警；
   2) 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；
   3) 应具备数据管理平台，提供完整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。

8.5.3 评估方法

8.5.3.1 基础级

根据基础级要求，从组织建设、制度流程、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务数据使用安全的岗位和人员。

b) 查验是否在核心业务层级制定了数据使用安全相关制度文件：

1) 查验该文件是否明确了数据的脱敏规范；

2) 查验该文件是否明确了数据使用的范围、权限、合规要求等；

3) 查验该文件是否明确了不同目的下的数据使用审批流程；

4) 查验该文件是否明确了数据使用者的权限管理及访问控制机制。

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。

8.5.3.2 优秀级

根据优秀级要求，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整体数据使用安全的部门、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) 查验该文件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) 查验该文件是否规定了数据使用相关平台系统的访问控制措施；

4) 查验该文件是否定义了违规使用数据的操作；

5) 查验该文件是否明确了个人信息的使用安全保护规范，以符合国家法律法规及监管要求。

c) 查验是否在组织层级制定了数据脱敏规范：

1) 查验该文件是否明确了脱敏处理使用场景；

2) 查验该文件是否规定了数据脱敏规则、方法、处理流程等。

d) 查验组织的技术工具：

1) 是否部署了脱敏工具，并对敏感数据的脱敏操作进行日志记录；

2) 是否支持账号权限管理、访问控制等管控要求；

3) 是否支持数据脱敏处理的安全审计；

4) 是否支持数据违规使用行为的有效识别、监控。

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。

8.5.3.3 先进级

根据先进级要求，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使用安全的量化评估方式：

1) 是否定义了量化评估指标；

2) 是否规定了量化评估频率。

b) 查验组织的技术工具：

1) 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；

2) 是否支持对输出信息的检测，避免存在可恢复的个人信息；

3) 是否具备对数据滥用行为的自动监控和预警功能。

8.6 数据处理环境安全

8.6.1 概述

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建立安全保护机制，确保数据处理过程的安全管控和技术支撑。

8.6.2 等级要求

8.6.2.1 基础级

从组织建设、制度流程方面进行要求。

a) 组织建设：应设置相关工作岗位和人员负责数据处理环境安全工作，配合推动相关要求的执行。
b) 制度流程：应明确核心业务的数据处理环境安全管理要求，制定满足核心业务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环境安全。

8.6.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：
   1) 应设立组织层面的部门、岗位和人员，负责制定各业务场景数据处理环境的安全原则和要求；
   2) 各业务团队应明确相关人员负责数据处理环境安全管控实施工作。
b) 制度流程：
   1) 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；
   2) 应明确数据处理环境的安全管理要求；
   3) 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。
c) 技术工具
   1) 应基于核心业务场景、数据重要性等，对数据、系统功能、运营环境等资源实现隔离控制；
   2) 应建立数据处理日志管理工具，记录用户在数据处理系统上的加工操作；
   3) 应建立处理过程中的数据防泄漏技术工具，防止数据处理过程中的敏感数据的泄露。
d) 人员能力：
   1) 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的有效配置规避相关风险；
   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。

8.6.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：应规定数据处理环境安全的量化评估方式，可实现数据处理环境设计阶段和运维阶段的安全手段不断优化。
b) 技术工具：
   1) 应建立数据分布式处理节点的服务组件自动维护和管控措施，包括虚假节点监测、故障用户节点确认和自动修复的技术机制；
   2) 应建立不同环境下的数据防泄漏技术工具。

8.6.3 评估方法

8.6.3.1 基础级

根据基础级要求，从组织建设、制度流程方面进行查验。

a) 查验业务团队是否明确了负责本业务数据处理环境安全的岗位和人员。

b) 查验是否在核心业务层级制定了数据处理环境安全相关制度文件：

1) 查验该文件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) 查验该文件是否规定了数据在不同使用场景下的环境安全；

3) 查验该文件是否规定了终端环境的管理要求。

8.6.3.2 优秀级

根据优秀级要求，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处理环境安全的部门、岗位和人员。

b) 查验是否在组织层级制定了数据处理环境安全相关制度文件：

1) 查验该文件是否明确了系统设计、开发、运维阶段的安全控制措施；

2) 查验该文件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) 查验该文件是否规定了终端环境的管理规范；

4) 查验该文件是否规定了分布式处理场景下的环境安全要求。

c) 查验组织的技术工具：

1) 具备数据处理的日志管理工具；

2) 具备数据处理过程的防泄漏工具；

3) 支持不同业务场景下的资源隔离控制。

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。

8.6.3.3 先进级

根据先进级要求，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处理环境安全的量化评估方式：

1) 是否定义了量化评估指标；

2) 是否规定了量化评估频率。

b) 查验组织的技术工具：

1) 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；

2) 是否支持分布式处理节点的服务监测与修复。

8.7 数据内部共享安全

8.7.1 概述

通过对组织的数据内部共享进行安全性管理，防止数据内部共享中可能对数据自身的可用性和完整性构成的危害，降低可能存在的数据泄漏风险。

8.7.2 等级要求

8.7.2.1 基础级

从组织建设、制度流程、技术工具、人员能力方面进行要求。

a) 组织建设：应设置相关岗位和人员负责对数据内部共享执行安全管理。

b) 制度流程：应建立核心业务数据内部共享原则、范围、安全制度或审批流程。

c) 技术工具：应采取技术措施记录组织的数据内部共享行为，确保数据内部共享行为可追溯。
d) 人员能力：应具备对数据内部共享业务的理解能力，掌握数据内部共享规程，并能够针对具体场景提出有效的解决方案。

8.7.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：应设立数据内部共享安全管理部门、岗位和人员，负责制定规则和提供技术能力，配合推动相关要求的执行。
b) 制度流程：
   1) 应依据数据分类分级要求建立了符合业务规则的数据内部共享安全策略，如授权策略、流程控制策略、不一致处理策略等；
   2) 应建立数据内部共享安全评估和授权审批流程，评估数据内部共享的安全风险，并对大量或敏感数据的内部共享进行授权审批；
   3) 在采用存储介质及设备导出数据的情况下，应建立针对导出存储介质及设备的标识规范，明确存储介质及设备的命名规则、标识属性等重要信息，定期验证导出数据的完整性和可用性；
   4) 应制定数据内部共享审计策略和日志管理规程，并保存内部共享过程中的出错数据处理记录；
   5) 应建立数据内部共享清单，定期对各项数据内部共享进行安全审查。
c) 技术工具：
   1) 应采用审计工具记录并定期审计组织内部的数据内部共享行为，避免超出数据授权使用范围；
   2) 应对数据内部共享终端设备、用户或服务组件执行有效的访问控制，保障其身份的真实性和合法性；
   3) 在内部共享完成后对数据内部共享通道缓存的数据进行删除，以保证内部共享过程中涉及的数据不会被恢复；
   4) 应建立对导出生产系统的敏感数据进行脱敏、溯源的技术能力。
d) 人员能力：
   1) 应能够充分理解组织的数据内部共享规程，并根据数据内部共享的业务执行相应的风险评估，从而提出实际的解决方案；
   2) 定期开展数据内部共享规程等相关培训，考核人员能力与岗位的匹配程度。

8.7.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：应定期评估内部共享服务组件和内部共享通道的安全性，对数据内部共享的风险控制方案进行持续的优化调整。
b) 技术工具：
   1) 应建立统一的数据内部共享管理系统，提示数据内部共享的安全风险并进行在线审核；
   2) 应配置规范的数据内部共享机制或服务组件，明确数据内部共享域最低安全防护要求；
   3) 应监控并记录数据的流转过程，能够及时发现异常情况，具备预警、溯源排查、精确定位等能力。

8.7.3 评估方法

8.7.3.1 基础级

根据基础级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务数据内部共享安全的岗位和人员。
b) 查验是否在核心业务层级制定了数据内部共享安全相关制度文件：
   1) 查验该文件是否明确了数据内部共享的原则、范围、审批流程、共享流程等；
   2) 查验该文件是否规定了内部共享的安全策略。
c) 查验组织的技术工具：是否支持共享行为的日志记录功能。
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。

8.7.3.2 优秀级

根据优秀级要求，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内部共享安全的部门、岗位和人员。
b) 查验是否在组织层级制定了数据内部共享安全相关制度文件：
   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) 查验该文件是否建立了符合业务规则的内部数据共享安全策略，如授权策略、流程控制策略等；
   3) 查验该文件是否明确了使用存储介质导出数据时的管理规范及操作规程；
   4) 查验该文件是否规定了内容共享审计和日志管理策略；
   5) 查验该文件是否规定了内部共享的授权审批及安全评估流程，尤其当存在大量或敏感数据共享的场景；
   6) 查验该文件是否规定建立数据内部共享清单。
c) 查验组织的技术工具：
   1) 是否具备数据内部共享清单；
   2) 是否支持对共享两侧的设备、用户、系统之间的身份鉴别与访问控制；
   3) 是否支持内部共享的风险评估；
   4) 是否对导出的敏感数据采取了脱敏措施；
   5) 是否支持对导出数据文件的溯源；
   6) 是否支持共享通道的缓存删除。
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。

8.7.3.3 先进级

根据先进级要求，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内部共享安全管理效果的量化评估方式：
   1) 是否定义了共享服务组件、共享通道的量化评估指标；
   2) 是否规定了共享服务组件、共享通道的量化评估频率。
b) 查验组织的技术工具：
   1) 是否建立了统一的数据内部共享管理系统；
   2) 提供配置规范的服务组件和共享机制；
   3) 是否支持共享流转过程的监控记录。

8.8 数据外部共享安全

8.8.1 概述

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

8.8.2 等级要求

8.8.2.1 基础级

从组织建设、制度流程、人员能力方面进行要求。

a) 组织建设：应设置相关工作岗位和人员负责对数据外部共享、外部合作等场景的数据共享方案执行安全风险管控，明确数据服务提供者与共享数据使用者的数据保护责任。
b) 制度流程：
   1) 应明确数据外部共享的原则、范围和安全规范，明确数据外部共享内容范围和数据外部共享的管控措施，及数据外部共享涉及机构或部门相关用户职责和权限；
   2) 应与数据外部共享方签署保密和合作协议，明确数据的使用目的、供应方式、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，包括告知个人第三方相关信息，并取得个人同意等。
   4) 应保证共享内容符合数据合规和监管要求，明确数据挖掘和应用范围。
c) 人员能力：应具备对数据外部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。

8.8.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：应在组织层面设立数据外部共享交换安全管理的部门、岗位和人员，负责相关原则和技术能力的提供，配合推动相关要求的执行。
b) 制度流程：
   1) 应制定数据外部共享的原则及数据保护措施，尤其是个人信息的外部共享，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；
   2) 应明确数据外部共享审计规程和审计日志管理要求，明确审计记录要求，为数据外部共享安全事件的处置、应急响应和事后调查提供帮助；
   3) 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；
   4) 应明确共享的数据留存期限，并提供有效方式，证明数据的销毁情况。
c) 技术工具：
   1) 应采取措施保障个人信息在委托处理、共享、转让等对外提供场景的安全合规，如数据脱敏、数据加密、安全通道、共享交换区域等；
   2) 应对外部共享数据及数据外部共享过程进行监控审计，避免超范围共享；
   3) 应对跨安全域间的数据接口调用采用安全通道、加密传输、时间戳等安全措施；
   4) 应支持对外共享场景下的数据溯源技术。
d) 人员能力：
   1) 应能充分理解组织的数据外部共享规程，并根据数据外部共享的业务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。

8.8.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
   1) 应定期评估数据外部共享机制、接口组件和共享通道的安全性，对数据共享的风险控制方案进行持续的优化调整；
   2) 在数据外部共享时，应对数据接收方的数据安全防护能力开展评估工作。
b) 技术工具
   1) 应跟进数据加密和共享通道加密保护的技术发展，评估新技术对安全方案的影响，适当引入新技术以应对最新的安全风险；
   2) 应建立长线的数据外部共享溯源能力；
   3) 应对数据外部共享接口进行异常监控及自动化处理。

8.8.3 评估方法

8.8.3.1 基础级

根据基础级要求，从组织建设、制度流程、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务数据外部共享安全的岗位和人员。
b) 查验是否在核心业务层级制定了数据外部共享安全相关制度文件：
   1) 查验该文件是否明确了数据外部共享的原则、范围、审批流程、共享流程、审计流程等；
   2) 查验该文件是否规定了数据外部共享的安全策略；
   3) 查验该文件是否明确了与外部共享方的保密合作协议；
   4) 查验该文件是否明确了共享安全合规评估机制；
   5) 查验该文件是否明确了个人信息对外共享的操作规范，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。

8.8.3.2 优秀级

根据优秀级要求，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外部共享安全的部门、岗位和人员。
b) 查验是否在组织层级制定了数据外部共享安全相关制度文件：
   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) 查验该文件是否明确了分组织机构、分共享场景的外部数据共享安全策略；
   3) 查验该文件是否规定了对数据共享需求、共享范围、共享内容、共享流程的审核控制机制；
   4) 查验该文件是否规定了共享操作的审计规范及日志规范；
   5) 查验该文件是否规定了共享双方的安全责任；
   6) 查验该文件是否明确了数据共享接口的安全控制策略；
   7) 对个人信息的对外共享提出了明确要求，以符合国家法律法规和监管要求；
   8) 明确了数据共享接口的安全控制策略。
c) 查验组织的技术工具：
   1) 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；
   2) 是否支持个人信息在不同场景下的共享安全防护；
   3) 是否支持对共享过程的监控审计；

4) 是否实现了对数据接口调用的安全管控。

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。

8.8.3.3 先进级

根据先进级要求，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外部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；
   2) 是否规定了量化评估频率。
b) 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。
c) 查验组织的技术工具：
   1) 是否支持引入新的加密技术，并能够进行引入风险评估；
   2) 是否支持数据外部共享长线溯源能力；
   3) 是否支持对共享接口异常的有效监控，并实现自动关停。

8.9 数据销毁安全

8.9.1 概述

通过制定数据销毁机制，实现有效的数据删除管控，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。

8.9.2 等级要求

8.9.2.1 基础级

从组织建设、制度流程、技术工具、人员能力方面进行要求。

a) 组织建设：应设置相关工作岗位和人员负责核心业务的数据销毁和存储介质销毁工作。
b) 制度流程：应规定核心业务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、以及有效性验证标准。
c) 技术工具：
   1) 应采用技术工具对核心业务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核心业务的存储媒体；
   2) 应采用数据销毁技术手段，保证删除数据的不可恢复。
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。

8.9.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：
   1) 应设立负责数据销毁管理的部门、岗位和人员，负责制定数据销毁处置规范、媒体销毁管理的制度，明确销毁对象和流程，配合推动相关要求的执行；
   2) 应设置数据销毁监督角色，监督数据销毁过程。
b) 制度流程：
   1) 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媒

体销毁的场景、销毁对象、销毁方式和销毁结果；
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销毁个人信息等敏感数据；
5) 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。

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；
4) 数据资产管理系统应能够对数据的销毁需求进行明确的标识，并可通过该系统提醒数据管理者及时发起对数据的销毁。

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、媒体销毁工具。

8.9.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
1) 应定期审核数据存储合理性，并及时根据法律法规和最新合同的要求，对销毁的整体方案进行及时更新；
2) 应明确数据销毁、媒体销毁效果的量化评估指标和机制，定期对销毁效果进行抽样认定。

b) 技术工具：
1) 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；
2) 应提供销毁记录归档手段，记录销毁过程及验证结果。

8.9.3 评估方法

8.9.3.1 基础级

根据基础级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务数据销毁安全和存储介质销毁安全的岗位和人员。

b) 查验是否在核心业务层级制定了数据销毁和存储介质销毁相关制度文件：
1) 查验该文件是否明确了数据销毁的原则、流程、方式、工具、有效性验证等；
2) 查验该文件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) 是否支持对存储介质的擦除；
2) 是否支持对涉及核心业务的存储介质进行物理销毁；
3) 是否实现了不可恢复的数据销毁。

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。

8.9.3.2 优秀级

根据优秀级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验。

a) 查验组织的部门、岗位和人员：
1) 是否设立了负责数据销毁安全部门、岗位和人员；

2) 是否设置的数据销毁的监督人员。

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) 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) 查验该文件是否规定了数据销毁流程、销毁场景、销毁原因、销毁方式、销毁工具、销毁对象等；
3) 查验该文件是否规定了数据销毁的审批机制；
4) 查验该文件是否规定了个人信息的销毁安全保护措施，以符合国家法律法规和监管要求；
5) 查验该文件是否明确了第三方存储的销毁规范；
6) 查验该文件是否明确了已外部共享的数据的销毁机制。

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) 查验该文件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) 查验该文件是否规定了不同的销毁措施（硬销毁和软销毁等）；
3) 查验该文件是否规范了登记、审批、交接等介质销毁流程；
4) 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；
2) 是否提供存储介质销毁工具；
3) 是否支持销毁效果验证；
4) 是否支持销毁过程日志记录。

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。

8.9.3.3 先进级

根据先进级要求，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；
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) 是否支持销毁过程的日志记录及结果验证。

9 基础安全

9.1 数据分类分级

9.1.1 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。

9.1.2 等级要求

9.1.2.1 基础级

从组织建设、制度流程方面进行要求。

a) 组织建设：应设置相关岗位和人员负责核心业务的数据分类分级。

b) 制度流程：

1） 应根据业务特性和外部合规要求，对核心业务的数据进行分类分级管理；

2） 应定义组织内部核心业务的数据资产的分类分级方法，能够提供业务数据资产被合理正确的标识。

9.1.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：组织应设立负责数据安全分类分级工作的部门、岗位和人员，主要负责定义组织整体的数据分类分级的安全原则，配合推动相关要求的执行。

b) 制度流程：

1) 应结合数据类型特点、业务运营需求等，明确数据分类分级原则、方法和操作指南；

2) 应对组织的数据进行分类分级标识和管理，建立数据保护清单；

3) 应对不同类别和级别的数据建立相应的访问控制、数据加解密、数据脱敏等安全管理和控制措施；

4) 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。

c) 技术工具：

1） 应建立数据分类分级工具，保证组织数据分类分级管理的准确性和一致性；

2） 应具备对数据分类分级结果进行标识的技术手段；

3） 应具备数据分类分级策略变更的监控手段。

d) 人员能力：

1） 负责该项工作的人员应了解数据分类分级的合规要求，能够识别哪些数据属于敏感数据；

2） 组织的数据安全教育培训中包含了对数据分级分类管理安全要求的宣贯内容；

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。

9.1.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：

1) 规定了数据分类管理效果的量化评估方式；

2) 规定了数据分级管理效果的量化评估方式。

b) 技术工具：

1) 通过建立数据资产的分类分级工具，保证组织数据的分类分级准确性和一致性，能够自动化的对分类分级后的数据进行量化统计；

2) 应建立相应的技术手段，保证一定类别和一定敏感级别的数据在被使用时不被泄露。

9.1.3 评估方法

9.1.3.1 基础级

根据基础级要求，从组织建设、制度流程方面进行查验。

a) 查验业务团队是否明确了负责本业务数据分类分级的岗位和人员。

b) 查验是否在核心业务层级制定了数据分类分级相关制度文件：

1) 查验该文件是否明确了不同类别不同级别数据的安全管理要求；
2) 查验该文件是否定义了数据资产的标识规范。

9.1.3.2 优秀级

根据优秀级要求，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分类分级工作的部门、岗位和人员。
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) 查验该文件的制定是否结合了业务需求、数据的重要性、敏感程度以及安全防护需求；
   3) 查验该文件是否定义了分类分级的原则、方法、操作指南等；
   4) 查验该文件的制定是否完整覆盖组织的业务需求及数据全生命周期的处理活动；
   5) 查验该文件是否明确了分类分级策略实施及变更流程；
   6) 查验该文件是否对分类分级数据设置了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、数据备份与恢复、访问控制权限等技术能力和措施。
c) 查验组织技术工具：
   1) 是否支持数据的分类分级；
   2) 是否建立了数据分类分级保护清单；
   3) 是否支持对分类分级策略变更的监控；
   4) 是否支持分类分级数据的打标。
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。

9.1.3.3 先进级

根据先进级要求，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；
   2) 是否规定了分类、分级的量化评估频率。
b) 查验组织的技术工具：
   1) 是否支持数据资产的自动分类分级；
   2) 是否支持分类分级结果数据的量化统计。

9.2 合规管理

9.2.1 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。

9.2.2 等级要求

9.2.2.1 基础级

从组织建设、制度流程、人员能力方面进行要求。

a) 组织建设：应设置相关工作岗位和人员，根据业务需求开展合规管理工作。
b) 制度流程：应明确个人信息保护、跨境数据传输等方面的数据安全合规管理制度规范。

c) 人员能力：负责该项工作的人员应基本理解个人信息保护、跨境数据传输等方面的安全合规要求。

9.2.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：应设置负责个人信息保护、跨境数据传输等方面的安全合规的部门、岗位和人员，负责制定组织及业务的数据安全合规的规范要求和解决方案，配合推动相关要求的执行。

b) 制度流程：
   1) 应依据组织或机构所适用的相关法律法规及标准规范的要求，建立统一的个人信息保护、跨境数据传输等方面的管理制度；
   2) 应在个人信息采集、使用、存储、共享、跨境数据传输等核心环节设置相应的管控措施和流程，对个人信息合规使用提供有效保护；
   3) 应通过员工入职安全意识培训、全员安全意识培训、安全意识宣贯海报、安全周等方式加强组织内部员工在个人信息保护、隐私合规等方面的安全意识，并对产品、开发、客服等重要部门的相关岗位人员开展安全合规专项培训；
   4) 应明确组织的外部合规要求并形成清单，能够定期通过跟进监管机构合规要求的动态对该清单进行更新和宣贯；
   5) 应在业务功能上线、个人数据共享、跨境数据传输等关键环节实施前开展合规风险评估。

c) 技术工具：
   1) 能够采取技术手段和控制措施实现个人信息的安全保护，例如在个人信息处理过程中进行匿名化、去标识化；
   2) 建立有对个人信息的监控机制，防范数据安全事件发生；
   3) 建立合规要求清单，支持清单的定期更新。

d) 人员能力：
   1) 负责该项工作的人员能够对个人信息保护、跨境数据传输等方面的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) 能够依据外部合规要求，建立覆盖组织的数据安全和隐私保护的管理体系和机制，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。

9.2.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
   1) 应建立整改和考核规范，用于指导发现和整改情况追踪、报告管理、问题管理等；
   2) 应规定发生数据安全合规事件的量化方式，通过数据指标定义安全事件风险的严重程度。

b) 技术工具：
   1) 建立可量化的合规情况评估体系，将合规结果上报管理层，以保证对组织整体的合规运行情况得到有效了解；
   2) 能够基于针对个人信息保护、数据跨境传输的风险进行监控，定期审核相关操作记录，统计安全风险发生情况；
   3) 建立合规资料库或提供外部合规资料库查询渠道。

9.2.3 评估方法

9.2.3.1 基础级

根据基础级要求，从组织建设、制度流程、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务合规管理的岗位和人员。
b) 查验是否在核心业务层级制定了数据合规管理的相关制度文件：
   1) 查验该文件是否明确了用户个人信息和核心业务数据保护的合规要求；
   2) 查验该文件是否明确了数据跨境传输的合规要求；
   3) 查验该文件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。

9.2.3.2 优秀级

根据优秀级要求，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规管理的部门、岗位和人员。
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) 查验该文件是否明确了个人信息保护、跨境数据传输等在数据全生命周期的合规管理要求；
   3) 查验该文件是否明确要求建立合规清单，定期进行更新和宣贯；
   4) 查验该文件是否规定了合规培训的计划；
   5) 查验该文件是否明确了合规性评估的业务场景；
   6) 查验该文件是否规定了合规性评估的具体内容，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；
   7) 查验该文件是否规定了合规性评估的开展时机、频次等内容。
c) 查验组织的技术工具：
   1) 是否记录了各业务场景的数据安全合规性评估报告；
   2) 是否支持对个人信息使用过程的合规监控机制，以及使用过程的安全保护；
   3) 是否建立了可定期更新的合规要求清单。
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。

9.2.3.3 先进级

根据先进级要求，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效果的量化评估方式：
   1) 是否定义了量化评估指标；
   2) 是否规定了量化评估的时机、频率。
b) 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。
c) 查验组织的技术工具：
   1) 是否具备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。

9.3 合作方管理

9.3.1 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。

9.3.2 等级要求

9.3.2.1 基础级

从组织建设、制度流程、人员能力方面进行要求。

a) 组织机构：应设置相关岗位和人员，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：组织内核心业务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。

9.3.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：应明确负责合作方管理的部门、岗位和人员，推动合作方管理相关制度文件的落地实施。
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，对接触个人信息等数据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。
c) 技术工具：
   1) 应建立合作方管理平台，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) 应建立对合作方的风险评估工具，支持业务开展前的风险评估。
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。

9.3.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

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) 能够定期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进行评估；
   3) 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；

4) 组织整体的数据合作方管理方案能够根据国内外数据合作方管理领域的监管动态和行业时间进行及时调整。

5) 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) 应建立合作方管理资料库，相关人员可以通过该资料库查询合作方评估考核情况；

2) 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；

3) 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。

9.3.3 评估方法

9.3.3.1 基础级

根据基础级要求，从组织建设、制度流程、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务合作方管理的岗位和人员。

b) 查验是否对核心业务的数据合作制定了合作方管理的相关制度文件：

1) 查验该文件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。

9.3.3.2 优秀级

根据优秀级要求，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) 查验该文件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；

2) 查验该文件是否规定了对合作方的数据安全保护能力进行资质审核；

3) 查验该文件是否规定了合作期间的数据安全定期风险评估机制；

4) 查验该文件是否规定了涉及个人信息时的合规性评估工作；

5) 查验该文件是否规定了合作方的管理台账机制；

6) 查验该文件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) 是否建立合作方管理平台；

2) 是否支持合作方接口的监控审核；

3) 是否支持对合作方的风险评估。

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。

9.3.3.3 先进级

根据先进级要求，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；

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) 是否对合作方的数据安全治理能力等开展持续了评估、审核，并记录评估、审核结果。

2) 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；

3) 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) 是否建立了合作方管理资料库；

2) 是否具备合作方发生安全事件时的应急响应能力；

3) 是否支持对合作方数据安全治理、合规等内容的持续监控。

9.4 监控审计

9.4.1 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。

9.4.2 等级要求

9.4.2.1 基础级

从组织建设、制度流程、技术工具、人员能力方面进行要求。

a) 组织建设：应设置相关工作岗位和人员，负责数据全生命周期流转过程的安全监控。

b) 制度流程：核心业务应建立数据安全监控和审计相关规则，如对数据生命周期各阶段的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。

c) 技术工具：应提供技术手段对数据的高风险操作进行监控。

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。

9.4.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：应设置组织层面的部门、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的安全风险进行监控和审计。

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，并制定数据安全风险行为识别和评估规则；

3) 应定期对组织内部员工数据操作行为进行人工审计。

c) 技术工具：

1) 应建立针对数据访问和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，高敏感数据以及特权账户对数据的访问和操作都纳入重点的监控范围；

2) 应采用技术工具对数据交换服务流量数据进行安全监控和分析。

d) 人员能力：

1) 应充分理解数据监控和审计的要求，能够识别数据泄漏风险，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。

9.4.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：应规定数据的访问和操作发生安全风险的量化指标，通过对比与正常数据访问和操作的偏离度识别安全事件的发生。

b) 技术工具：

1) 应建立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；

2) 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。

9.4.3 评估方法

9.4.3.1 基础级

根据基础级要求，从组织建设、制度流程、技术工具、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务监控审计的岗位和人员。

b) 查验是否在核心业务层级制定了监控审计的相关制度文件：

1) 查验该文件是否规定了全生命周期的监控审计的规则；

2) 查验该文件是否规定了对异常操作的监控审计；

3) 查验该文件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) 是否建立了数据高风险操作清单，并定期更新；

2) 是否支持对数据高风险操作的监控。

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。

9.4.3.2 优秀级

根据优秀级要求，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) 查验该文件是否明确了监控审计工作的牵头及配合执行部门；

2) 查验该文件是否明确了数据安全风险行为的识别和评估规则；

3) 查验该文件是否明确了数据相关操作的日志记录和安全监控要求；

4) 查验该文件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；

5) 查验该文件是否覆盖了对组织全业务数据处理活动的审计操作；

6) 查验该文件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) 是否建立了异常操作清单，并定期更新；

2) 是否支持异常操作的监控分析；

3) 是否留存相关监控审计报告。

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。

9.4.3.3 先进级

根据先进级要求，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；
2) 是否规定了量化评估频率。

b) 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) 是否支持对异常或高风险操作的自动识别与预警。

9.5 鉴别与访问

9.5.1 概述

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

9.5.2 等级要求

9.5.2.1 基础级

从组织建设、制度流程、技术工具方面进行要求。

a) 组织建设：应明确核心业务系统的用户身份管理及数据权限管理的岗位和人员。
b) 制度流程：核心业务应明确重要系统和数据库的身份鉴别、访问控制和权限管理的安全要求。
c) 技术工具：
1) 应对核心业务系统的登录用户进行身份标识和鉴别，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) 应提供核心业务系统的访问控制功能，对登录的用户分配账户和权限；
3) 应提供并启用核心业务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。

9.5.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

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) 应明确对身份标识与鉴别、访问控制及权限的分配、变更、撤销等方面管理的要求；
2) 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；
3) 应明确数据权限授权审批流程，对数据权限申请和变更进行审核；
c) 技术工具：
1) 应建立身份鉴别管理系统，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) 应建立权限管理系统，支持组织主要应用接入，对人员访问数据资源进行访问控制和权限管理；
3) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；
4) 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。
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。

9.5.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
   1) 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；
   2) 应定期对组织的鉴别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取证机制；
   2) 应建立定期更新和审核的敏感数据权限清单；

9.5.3 评估方法

9.5.3.1 基础级

根据基础级要求，从组织建设、制度流程、技术工具方面进行查验。

a) 查验业务团队是否明确了负责本业务用户身份和权限管理的岗位和人员。
b) 查验是否在核心业务层级制定了鉴别与访问控制的相关制度文件：查验该文件是否明确了身份鉴别、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) 是否支持用户登录身份鉴别；
   2) 是否支持核心业务的访问权限控制；
   3) 是否支持身份鉴别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。

9.5.3.2 优秀级

根据优秀级要求，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鉴别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鉴别与访问控制相关制度文件：
   1) 查验该文件是否明确了组织内各部门各员工以及外包人员及实习生等的身份鉴别、访问控制及权限管理等要求；
   2) 查验该文件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；
   3) 查验该文件是否规定了账号权限等的定期审核制度；
   4) 查验该文件是否规定了账号口令的访问控制复杂度要求；
   5) 查验该文件是否规定了不同业务数据的访问控制粒度。
c) 查验组织的技术手段和工具：
   1) 是否具备身份鉴别管理系统；
   2) 是否具备权限管理系统；
   3) 是否提供口令、密码技术、生物技术等多种鉴别技术；
   4) 是否支持不同访问控制粒度的实现。

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。

9.5.3.3 先进级

根据先进级要求，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鉴别与访问控制效果的量化评估方式：
   1) 是否定义了量化评估指标；
   2) 是否规定了量化评估频率。
b) 查验组织的技术工具：
   1) 是否建立了敏感数据权限清单，明确安全角色的安全要求、分配策略、授权机制、权限范围等；
   2) 是否建立了敏感数据权限清单的定期更新和审核工具。

9.6 风险和需求分析

9.6.1 概述

根据组织的业务场景和数据安全需求，建立数据安全风险分析和需求分析体系，有效应对组织内数据和业务的安全需求和风险。

9.6.2 等级要求

9.6.2.1 基础级

从组织建设、制度流程、人员能力方面进行要求。

a) 组织建设：应设置相关岗位和人员负责数据安全风险和需求分析的工作。
b) 制度流程：
   1) 核心业务应明确数据安全风险分析的管理制度；
   2) 核心业务应明确数据安全需求分析的管理制度。
c) 人员能力：
   1) 应熟悉业务自身数据应用场景，数据调用逻辑，并对数据安全法律合规知识体系具有一定概念；
   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。

9.6.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：
   1) 应设立负责数据安全需求分析的部门、岗位和人员，负责对数据业务设计开发等阶段开展数据安全需求分析工作，确保安全需求的有效制定和规范化表达；
   2) 应设立负责数据安全风险的岗位和人员，负责对各业务线开展数据安全风险识别工作，确保数据安全策略和工具等对数据安全风险的有效覆盖。
b) 制度流程：
   1) 应结合国家法律法规和监管要求等，分析数据安全合规性需求；
   2) 应识别数据服务面临的威胁和自身脆弱性，分析数据安全风险和应对措施需求；

3) 应明确数据安全需求和风险分析的制定流程和评审机制，明确安全需求和风险分析文档内容要求，流程实施过程以及评审应保留记录。

c) 技术工具：
1) 应建立需求管理工具，记录业务数据安全需求的申请、分析以及相关安全方案，以保证业务的安全需求分析过程可有效追溯；
2) 应建立风险分析库，用于线上风险评估。

d) 人员能力：应在数据风险管理及业务实践方向具备一定经验，能够判断风险程度和需求紧迫性。

9.6.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
1) 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；
2) 应量化数据安全需求分析，以保证符合组织发展战略和业务发展的实际需要；
3) 应明确风险和需求分析工作的持续优化开展机制，风险和需求分析应具备一定前瞻性。

b) 技术工具：应提供量化分析工具。

9.6.3 评估方法

9.6.3.1 基础级

根据基础级要求，从组织建设、制度流程、人员能力方面进行查验。

a) 查验业务团队是否明确了负责本业务风险和需求分析的岗位和人员。
b) 查验是否在核心业务层级制定了风险和需求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。

9.6.3.2 优秀级

根据优秀级要求，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风险分析和需求分析的部门、岗位和人员。
b) 查验是否在组织层面制定了风险和需求分析相关制度文件：
1) 查验该文件是否明确了风险和需求分析的申请流程、评审机制、开展时机等；
2) 查验该文件是否结合了法律法规和监管要求等，明确具体数据安全的合规需求；
3) 查验该文件是否结合组织安全规划、业务特点等因素，明确了风险和需求分析的优先级；
4) 查验该文件是否根据组织自身数据服务的脆弱性和面临的威胁，明确安全风险场景和应对措施。

c) 查验组织技术工具：
1) 是否建立了需求管理工具；
2) 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；
3) 是否具备需求分析、风险分析的报告。

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。

9.6.3.3 先进级

根据先进级要求，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和需求分析效果的量化评估方式：

1) 是否定义了风险及需求分析的量化评估指标；
2) 是否规定了风险及需求分析的量化评估频率。

b) 查验组织是否制定了持续开展并优化风险和需求分析制度的管理机制。
c) 查验组织的技术工具：是否提供了量化分析工具。

9.7 安全事件应急

9.7.1 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。

9.7.2 等级要求

9.7.2.1 基础级

从组织建设、制度流程、技术工具、人员能力方面进行要求。

a) 组织建设：应设置相关工作岗位和人员负责在核心业务层面根据业务需求建立安全应急响应机制，当出现数据安全事件时，能够根据工作相关性组织应急工作。
b) 制度流程：明确核心业务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：应提供技术平台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方案，并按照指定的策略开展相应的应急活动。

9.7.2.2 优秀级

在基础级的等级要求基础上，从组织建设、制度流程、技术工具、人员能力方面进行强化。

a) 组织建设：组织设立负责数据安全事件管理和应急响应的部门、岗位和人员。
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。
c) 技术工具：应建立统一的安全事件管理系统，对日志、流量等内容进行关联分析。
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。

9.7.2.3 先进级

在优秀级的等级要求基础上，从制度流程、技术工具方面进行强化。

a) 制度流程：
   1) 应建立对数据安全事件管理及执行的有效性量化评估，向管理层呈现数据安全事件应急处置效果；
   2) 应根据法律法规政策、公司业务调整对数据安全事件管理、应急响应制度进行优化，定期复核制度流程有效性，复核周期不低于每年一次；

3) 建立数据安全事件复盘机制，总结应急响应经验。

b) 技术工具：

1) 能够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) 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。

9.7.3 评估方法

9.7.3.1 基础级

根据基础级要求，从组织建设、制度流程、技术工具、人力能力方面进行查验。

a) 查验业务团队是否明确了负责本业务安全事件应急的部门和人员。

b) 查验是否在核心业务层级制定了安全事件应急的相关制度文件：

1) 查验该文件是否明确了安全事件管理方案；

2) 查验该文件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。

9.7.3.2 优秀级

根据优秀级要求，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安全事件应急的部门、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及等级划分是否参考了国家法律法规及监管部门要求；

2) 查验该文件的数据安全事件类型及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) 查验该文件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) 查验该文件是否明确了不同类型及等级的数据安全事件的应急预案。

c) 查验组织技术工具：

1) 是否具备数据安全事件管理系统，对日志、流量等进行关联分析；

2) 是否支持数据安全事件处置、应急响应制度的推广和宣贯；

3) 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。

9.7.3.3 先进级

根据先进级要求，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；

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。

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。

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 37988-2019 信息安全技术 数据安全能力成熟度模型
[4] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求
[5] GB/T 35273-2020 信息安全技术 个人信息安全规范