ICS 03.060
CCS A 11

团 体 标 准

T/NIFA 29-2024

金融数据安全治理实施指南

Implementation guide for governance of financial data security

2024-11-28 发布 2024-11-28 实施

中国互联网金融协会 发布

目　　次

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》和GB/T 20004.1—2016《团体标准化 第1部分：良好行为指南》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专利的责任。

本文件由中国互联网金融协会提出。

本文件由中国互联网金融协会归口。

本文件起草单位：中国互联网金融协会、奇富科技股份有限公司、上海冰鉴信息科技有限公司、神州数码信息服务集团股份有限公司、农信银资金清算中心有限责任公司、平安银行股份有限公司、中金金融认证中心有限公司、济宁银行股份有限公司、京东科技控股股份有限公司、马上消费金融股份有限公司、中国投融资担保股份有限公司、潍坊银行股份有限公司、北京市海问律师事务所、花瓣支付（深圳）有限公司、百融云创科技股份有限公司、中国光大银行股份有限公司、厦门国际银行股份有限公司、中国农业银行股份有限公司、邯郸银行股份有限公司、中互金认证有限公司、北京国家金融科技认证中心有限公司、江苏省联合征信有限公司、重庆富民银行股份有限公司、百行征信有限公司、天星数科科技有限公司、武汉众邦银行股份有限公司、中国银联股份有限公司。

本文件主要起草人：单强、杨农、王新华、吴业超、李娜、邓康、马元朋、李阳、鲁广平、顾凌云、石祥汉、王诗强、张栌文、道日娜、江汝、董四杰、李坤、张自奇、关晓辉、母延燕、陈晓蓉、隆峰、李松涛、张蕊、王泽南、李梁、刘志强、李万军、郑明明、王承晖、牟江波、杨建媛、薛泽涵、胡琨、颜欣、李华华、余章馗、王佳晋、赖强、庞浩然、冯翊、李利杰、刘志刚、史汝辉、李振、张澍、陈康、袁轶慧、王睿、苏毅、田昆、刘远钊、王近朱、程峰、李耀、杨洋、门小骅。

金融数据安全治理实施指南

1 范围

本文件提出了金融数据安全治理的框架、实施及成果评估，明确了数据安全治理实施的主要内容和评估方法。

本文件适用于金融机构开展数据安全治理使用，为数据安全治理工作开展提供参考和指引。

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—2022 信息安全技术 术语

JR/T 0197—2020 金融数据安全 数据安全分级指南

3 术语与定义

GB/T 25069—2022中界定的以及下列术语和定义适用于本文件。

3.1

金融数据 financial data

金融业机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类数据。

[来源：JR/T 0197—2020，3.10]

3.2

数据资产 data asset

合法拥有或控制的，能进行计量的，为机构带来经济和社会价值的数据资源。

[来源：GB/T 40685—2021，有修改]

3.3

数据安全 data security

通过管理和技术措施，确保数据处于有效保护和合规使用的状态，以及具备保障持续安全状态的能力。

[来源：GB/T 37988—2019，有修改]

3.4

数据安全能力 data security capability

机构在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障能力。

[来源：GB/T 37988—2019，3.5，有修改]

3.5

数据生命周期管理 data life-cycle management

机构在开展业务和进行经营管理的过程中，对数据进行采集、传输、存储、使用、删除、销毁的整个过程。

[来源：JR/T 0223—2021，5.1，有修改]

3.6

数据安全事件 data security incident

由于人为原因、软硬件缺陷或故障、恶意程序攻击或自然灾害等因素，使得网络或信息系统中的数据遭篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成危害的事件。

4 金融数据安全治理概述

4.1 概述

金融数据安全治理，是金融机构为确保数据安全状态，以达到维护国家安全、金融安全和社会公共利益、保护个人、组织的合法权益的目的，由内外部相关方协作持续实施的一系列建立并保持数据安全能力的活动集合。

4.2 目的

金融数据安全治理旨在建立与组织机构业务发展目标相适应的、全面且有效的数据安全管理体系，保障数据开发、利用活动安全稳健开展，以确保金融数据得到妥善保护，符合法律法规、当地政策的要求，满足机构发展战略的需要。

4.3 实施

金融数据安全治理以“人”与数据为中心，通过平衡业务需求与风险，对数据进行分类分级管理，制定数据安全策略，对数据的全生命周期进行管理和保护，从管理层、技术层、运营层，全方位与组织机构的业务体系相融合，贯穿始终。

5 金融数据安全治理框架

5.1 概述

金融数据安全治理框架，是以法律法规、政策指引及公司战略为指导思想，以数据安全组织建设、数据分类分级管理为基础，以制度体系、技术体系、风险管理为治理核心，完整的、可实施的、可运营的、可追责的治理方案。

数据安全治理工作应以治理核心为基础，与机构业务战略同步发展。通过风险识别，进一步完善制度体系和技术体系，持续提升机构的数据安全治理核心能力。

5.2 框架构成

金融数据安全治理框架见图1，框架构成如下：

a） 法律、行政法规及相关政策和公司战略在金融数据安全治理中起着重要的指导作用。数据安全治理工作应以法律法规为底线，以政策指引为依托，与本机构业务发展战略相适应，保障数据安全治理工作方向的正确性。

b） 组织建设是开展数据安全治理工作的前提。机构宜成立数据安全治理工作组，主导数据安全治理工作的开展及实施，并对治理过程及结果负责。

c） 数据分类分级管理是金融数据安全治理工作的基础，是治理工作的重要支撑和抓手。机构应完成数据资产梳理，形成数据资产清单，并对其进行分类分级。

d） 金融数据安全治理工作的核心围绕制度体系、技术体系和风险管理开展，三者紧密协作，为保障数据安全提供了全方位的保护和管理；治理工作是持续动态的，需要根据风险变化、政策调整、数据资产变化进行动态调整，以确保治理工作的有效性。

1） 管理制度是治理工作的依据，包括制定数据安全规范、策略和流程，确保数据安全的全面管理和合规性；

2） 技术体系是指通过技术手段和措施，降低未授权访问、数据泄露等安全风险，并及时应对安全事件；

3） 风险管理是指通过风险识别、风险评估、风险处置等手段，发现和识别数据安全风险，并完成风险处置。

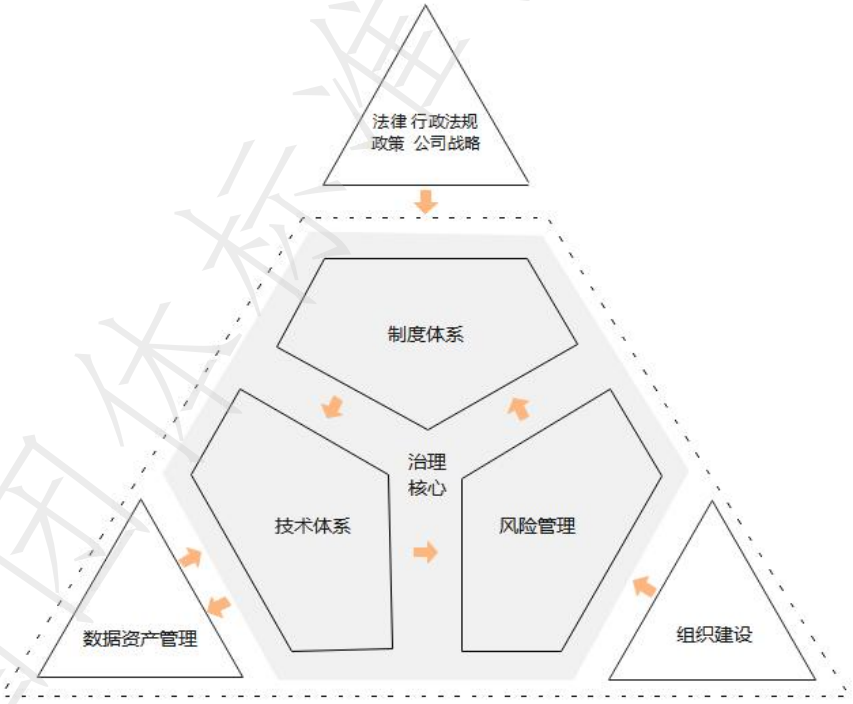

图1 数据安全治理框架

6 金融数据安全治理实施

6.1 组织建设

6.1.1 数据安全治理工作组

机构宜成立数据安全治理工作组，专项负责治理工作，并对机构数据安全负主要责任。下设数据安全治理领导小组、数据安全治理实施小组与数据安全治理监督小组，共同完成数据安全治理工作。

可由机构数据安全委员会承担，或由机构管理层进行任命。治理工作组参与部门有（各机构可根据机构内部的架构调整治理工作组的组成部门）：

a) 负责机构内数据安全归口管理、技术保护等工作的相关部门（以下简称数据安全部门）；
b) 负责机构内金融数据相关业务线的部门（以下简称业务部门）；
c) 负责机构内法务合规、内审等工作的相关部门（以下简称合规部门）。

6.1.2 数据安全治理工作组组成

6.1.2.1 数据安全治理领导小组

数据安全治理领导小组的人员组成和主要职责如下：

a) 人员组成：数据安全治理领导小组，一般由机构负责人及各参与部门负责人共同组成。
b) 主要职责：
   1） 数据安全治理工作的规划和目标设定，并将其上报董事会纳入机构的发展战略；
   2） 结合机构发展战略、经营策略，研究、提出、发布数据安全治理相关的重大决策和建议；
   3） 指导数据安全治理实施小组的工作；
   4） 对治理中发现的数据安全事件，参照T/NIFA 22—2023进行相关的内部发布、监管上报。

6.1.2.2 数据安全治理实施小组

数据安全治理实施小组的人员组成和主要职责如下：

a) 人员组成：数据安全治理实施小组，一般由数据安全部门和业务部门的具体实施人员组成，或可由数据安全领导小组任命。其中数据安全部门为主导方，业务部门为协同方，共同开展治理工作的执行落实。
b) 主导方职责：
   1） 根据领导小组决议、战略等制定数据安全管理、应急响应等制度规范及流程；
   2） 根据制度规范建立相应的防护能力，对敏感数据资产进行防护、对风险事件进行识别及拦截；
   3） 对数据全生命周期的风险识别负主要责任；
   4） 针对识别的数据安全风险，发起实施小组讨论会商议治理方案，跟进治理工作落实到位，并根据风险场景完善制度和规范、防护能力；
   5） 安全事件应急响应，数据泄露等事件响应，上报领导小组，带领协同方排查风险点；
   6） 对数据分类分级相关工作进行组织、协调、管理、审核、评审，并制定配套的安全管理规范制度及访问控制措施；
   7） 负责起草机构数据安全风险评估报告，经领导小组审核后报送上级管理部门。
c) 协同方职责：
   1） 对本部门内的业务数据负主要安全管理责任；
   2） 业务开展过程中，主动报告发现的风险，协同风险评估及优化治理；
   3） 协同或独立完成本部门内数据资产盘点，具体工作要求见6.2.2；
   4） 负责本部门风险的按期修复及治理；
   5） 配合主导方完成数据分类分级工作，并负责本部门数据的管控措施落实到位。

6.1.2.3 数据安全治理监督小组

数据安全治理监督小组的人员组成和主要职责如下：

a) 人员组成：数据安全治理监督小组，一般由合规部门人员担任，或可由机构管理层任命。
b) 主要职责：
   1) 负责对机构全员或数据安全治理工作组定期进行数据安全法律法规解读或培训；
   2) 参与数据安全相关管理制度的制定，确保制度内容的合法合规；

3） 依据数据安全相关管理制度制定治理成果的评估办法，并对数据安全治理工作进行定期审计及评估；
4） 根据领导小组决策监督实施小组治理执行工作。

6.2 数据分类分级管理

6.2.1 目标

数据分类分级管理旨在理清机构内部数据资产清单、完成数据分类分级，实现数据资产识别和及时更新，为数据安全治理工作提供基础。

6.2.2 数据资产盘点

6.2.2.1 盘点准备

数据资产盘点准备包括：

a） 明确盘点范围：数据资产盘点工作应覆盖机构内所有金融数据，包含但不限于服务器、数据库、云存储的金融数据，需要明确组织范围、业务范围和系统范围。
1） 组织范围：包含哪些组织和部门的数据，例如集团本部、子公司、具体业务部门等；
2） 业务范围：包含哪些业务的数据，例如采购业务、营销业务等；
3） 系统范围：包含哪些应用系统的数据，例如核心系统、CRM系统等。
b） 明确盘点内容：数据资产盘点的具体内容包括数据实体、数据项、数据文件等结构化和非结构化数据资产。需要明确数据资产的基本信息，例如名称、类型、格式、规模、存储位置，安全性和合规性以及相关方，例如持有者、使用者、管理者等；
c） 制定盘点模版：基于数据资产类型，确定数据资产盘点内容模板，明确每个模板的内容、格式、约束和填写规范等。并以此模板为基础，指导数据资产盘点人员高质量地完成数据资产盘点工作。在制定模板时应充分考虑数据资产相关的属性信息，包括但不限于基础属性、业务属性、管理属性。

6.2.2.2 资产盘点

数据资产盘点的必要性和工作内容包括：

a） 必要性：
数据资产盘点旨在对机构内存量数据进行系统化梳理，将数据资源转化为数据资产。
b） 工作内容：
1） 制定盘点计划：根据数据资产盘点范围，制定数据资产盘点计划，包括组织分工、盘点投入资源、时间、盘点工具、预期成果、里程碑计划等；
2） 选择盘点模式：选择合适的数据资产盘点模式，例如自上而下以业务视角进行梳理、自下而上以技术视角进行盘点等；
3） 盘点现有数据：对盘点范围内所有数据资源进行盘点，收集数据资源信息，按照数据资产盘点模板梳理数据资产的基础属性、业务属性、管理属性等信息。对数据生产链路的上下游关系进行整理，形成数据血缘；
4） 构建数据资产清单：根据盘点结果，对数据资产进行合理的梳理、归类和细分，建立机构级数据资产清单；
5） 资产发布与应用：通过平台工具落地数据资产目录，对于机构内存量的资产，进行规范化管理，实现数据资产变化及时更新。将数据资产以“服务”的形式进行发布。

6.2.3 数据分类分级

6.2.3.1 分类分级的必要性

数据分类分级是数据安全治理中的重要环节，通过对数据进行分类和分级，可以根据其重要性和敏感程度来采取相应的安全保护措施，进而实现数据资产的有效管理。

6.2.3.2 分类分级原则

数据分类分级的原则包括：

a) 对数据的分类应遵循以下几项原则：
   1) 系统性原则：基于对机构所有数据的考量，使整个机构范围内实现统一的数据管理；
   2) 规范性原则：分类中使用的词语能确切表达数据类目的实际内容范围，同时保证机构内不同团队或部门之间的统一；
   3) 稳定性原则：如果一个数据项需要由一个或者多个数据安全约束规则来描述，或者同一数据对象涉及多种分类的情况，应选择数据对象最稳定的特性作为数据分类的基础和依据；
   4) 适用性原则：应根据本机构的数据特征和应用场景选择适用性更强的分类方法；
   5) 可扩展性原则：在数据类目的设置或层级的划分上，允许随着机构的发展对数据分类进行适当扩展。
b) 数据安全分级应遵循以下几项原则：
   1) 合法合规性原则：数据分级应满足国家法律法规及行业主管部门有关规定，优先对国家或行业有专门管理要求的数据进行识别和管理，满足相应的数据安全管理要求；
   2) 可执行性原则：分级规则应避免过于复杂，以保证其在数据分级过程中的可行性；
   3) 时效性原则：数据所定级别具有一定的有效期限，应按照级别变更策略对数据级别进行及时调整；
   4) 差异性原则：应根据数据的类型、敏感程度等差异，划分不同的数据安全层级，并将数据划分至不同的级别中，不宜将所有数据集中划分到少数几个级别中；
   5) 客观性原则：数据定级规则应是客观并可以被校验的，即通过数据自身的属性和定级规则即可判定其级别，已定级的数据是可复核和检查的；
   6) 从高就严原则：如果数据项对应多个场景数据分类，按照数据分类对应最高级别对数据项进行定级。

6.2.3.3 分类分级实施

数据分类分级的实施步骤包括：

a) 确定数据分类标准：

机构典型数据类型建议参考 JR/T 0197—2020 附录 A。在实际应用过程中，机构宜根据其所管辖数据的类型、特性、规模以及机构特性等因素，综合考虑机构内数据安全管理的总体目标和安全策略要求，按照一定的颗粒度对数据资产进行合理的梳理、归类和细分，制定适用本机构的数据分类分级标准。

b) 划分数据安全等级：数据安全性遭到破坏后的影响是数据安全定级的主要评判依据，同时应考虑数据级别，其中一般数据可参照JR/T 0197—2020中1级-4级进行划分，核心数据和重要数据的安全级别不低于JR/T 0197—2020中的5级。安全影响评估主要从影响对象、影响程度两方面进行评估。
   1) 影响对象：即数据安全性遭受破坏后受到影响的对象，包括国家安全、公众权益、个人隐私、机构合法权益等；
   2) 影响程度：即数据安全性遭到破坏后所产生影响的大小，从高到低分为严重损害、一般损害、轻微损害和无损害。不同对象的相同类数据、相同对象的不同类数据，其数据安全性

遭到破坏后的影响程度可能不同。如交易信息中对实时性要求较高的数据安全性遭到破坏后产生的影响程度通常要高于实时性要求较低的数据。

c) 数据分类分级实施：机构应根据既定的数据分类分级标准，使用分类分级工具对机构内数据实施分类分级，实施过程应遵循分类分级原则，并对结果进行验证分析，保证分类分级结果达到预期。

d) 分类分级结果发布：

1） 结果发布流程发起：数据分类分级完成后，由实施小组主导方发起分类分级结果发布流程，发布流程须确保流程的透明性、可追溯性和合规性；

2） 数据安全定级审核：由实施小组和监督小组共同定级审核，审核过程需综合考虑数据规模、数据聚合、数据时效性、数据形态（如是否经汇总、加工、统计、脱敏或匿名化处理）等因素，对数据安全级别进行审核，调整形成数据安全级别评定结果及定级清单；

3） 数据安全级别批准：最终由数据安全治理领导小组对数据安全分级结果进行审议批准；

4） 数据安全分级发布：将审议批准后的定级清单进行发布。

e) 定期评估和更新：机构应对数据分类分级方案进行定期评估和更新，根据业务需求和风险的变化，及时调整和完善数据分类等级及相关安全措施。在数据分类分级完成后出现下列情形时，应对相关数据的安全级别进行主动变更。

1) 数据内容发生变化，导致原有数据的安全级别不适用于变化后的数据；

2) 数据内容未发生变化，但因数据时效性、数据规模、数据应用场景、数据加工处理方式等发生变化，导致原定的数据级别不再适用；

3) 不同数据类型经汇聚融合形成新的数据类别，使得原有的数据级别不适用，应重新进行级别判定；

4) 数据进行脱敏或删除关键字段，或者经过去标识化、匿名化处理；

5) 发生数据安全事件，导致数据敏感性发生变化；

6) 因国家或行业主管部门要求，导致原定的数据级别不再适用；

7) 需要对数据级别进行变更的其它情形。

6.3 数据安全风险管理

6.3.1 数据安全风险管理概述

数据安全风险是指可能对机构的数据资产造成潜在威胁和损害的各种风险因素，主要包括因违反相关法律法规要求所产生的风险，以及因主客观因素导致的对数据保密性、完整性和可用性产生影响的风险等。

数据安全风险管理是从风险识别到风险处理完成整个流程的闭环管理，其目的是在遵守相关法律法规要求的基础上，确保机构能够识别和处置数据安全风险，采取相应的管理和防护措施，确保数据的保密性、完整性和可用性，维护机构声誉，保护客户权益。

数据安全风险管理要求机构结合发展战略及业务需求，进行全面、客观的数据安全风险识别、对发现的风险进行评估并采取处置措施；要求机构通过建立风险清单的方式跟进风险处理及持续改进。

6.3.2 数据安全风险识别

6.3.2.1 数据安全风险识别的必要性

数据安全风险识别是通过识别和评估风险因素，对机构所面临的数据安全风险进行全面的认知和理解。它是数据安全风险管理的第一步，为后续的管理工作提供基础和依据。准确识别和理解风险，是有针对性地制定风险管理措施和策略的前提。

6.3.2.2 数据安全风险场景

根据数据不同生命周期阶段以及风险影响，常见的数据安全风险场景包括但不限于以下方面：

a) 数据采集阶段：
   1) 数据采集不当：违反法规、伦理标准，或非必要收集涉及个人隐私等敏感信息；
   2) 数据泄露：安全措施不到位导致的数据泄露，例如网络监听等；
   3) 数据篡改：安全措施不到位导致的数据篡改，例如数据劫持、身份欺骗等。
b) 数据传输阶段：
   1) 违规传输：未按照有关规定擅自传输数据，例如违规明文传输、违规数据出境等；
   2) 数据泄露：传输过程中未经授权的获取或披露，例如中间人攻击、未授权访问、网络监听等。
   3) 数据篡改：传输过程中未经授权的获取和篡改，例如 DNS 劫持、数据劫持修改等；
c) 数据存储阶段：
   1) 数据泄露：未经授权的披露或泄露敏感数据，例如网络攻击、员工泄露、设备失窃、业务链路缺陷、第三方供应商泄露等；
   2) 数据篡改：未经授权对数据的破坏行为，例如修改、增加、删除等；
   3) 数据存储不当：未采取适当的安全措施来保护存储的数据，使其容易受到非法访问或攻击。
d) 数据使用阶段：
   1) 非法访问：未经授权的或非预期的使用、披露、共享或篡改数据，例如数据遭受未授权访问等；
   2) 数据滥用：违反了数据所有者的意愿、权限或超出数据收集的合法目的范围，例如数据超范围、超用途、超时间使用等；
   3) 流量异常：数据流量异常，例如数据流量的规模异常、流量内容异常等。
e) 数据删除阶段：不完全删除，未能完全擦除或删除数据，导致数据仍然可被恢复或访问；
f) 数据销毁阶段：不完整销毁，数据或存储介质未被完全销毁，导致数据仍然可被恢复或访问，例如存储介质销毁不完全、备份数据未销毁等。

6.3.2.3 数据安全风险感知

机构应建立风险感知能力，包括主动感知数据处理活动中存在的风险，以及监测外部数据安全风险情报，一般的感知途径有：

a) 定期开展审计工作，审计应覆盖业务开展过程中数据采集、存储、传输、使用、删除、销毁各个环节，识别数据使用过程存在的合规风险；
b) 涉及敏感数据的业务活动，事先开展数据安全评估工作，评估数据处理的必要性和合规性，识别数据安全风险；
c) 业务流程数据验证，对篡改数据、验证异常数据进行标记；
d) 行为监测，对操作、请求等行为进行审计监测，识别敏感数据下载、爬取、敏感数据外发、非法请求等异常行为或异常请求；
e) 情报监测，对兜售本机构数据、机构非公开数据（如：客户数据、业务数据、经营数据等）泄露至互联网等情报持续监测；
f) 用户关于数据泄露投诉的事件的监测；
g) 上级单位的通报预警情况监测。

6.3.3 数据安全风险评估

基于已发现的数据安全风险，机构应对风险进行全面评估，以确定风险影响及优先级。

参考JR/T 0223—2021建立安全风险清单，列出所有可能影响数据安全的潜在风险因素。利用如风险矩阵、风险评分卡等风险评估工具，定量或定性地评估每个风险因素的可能性和影响，为每个风险因素分配适当的权重和优先级。风险因素评估过程中，可与历史安全事件和数据泄露案例关联分析。

6.3.4 数据安全风险处置

6.3.4.1 风险处置的必要性

风险处置是数据安全风险管理的重要环节，机构应当依据风险评估的结果，采取适当的措施来应对已识别的风险，将风险可能带来的影响控制在可接受范围内。

6.3.4.2 风险处置的目的和原则

风险处置过程中，机构应以风险降低、业务连续性、数据合规和声誉维护为目的，以风险优先、多层次防御、及时响应为原则，综合考虑风险的性质、机构的资源和能力、法规要求等因素，并基于此开展风险处置工作。

6.3.4.3 风险处置策略

机构应针对所列的数据安全风险，结合机构实际情况从管理、技术等方面制定具体的整改方案以及处置策略。常见的风险处置策略有：

a) 风险消除，是指通过采取一系列措施将风险彻底消除或避免潜在风险的发生，包括但不限于最小化采集与存储等措施，即非必要数据不采集，非必要数据不存储；

b) 风险减轻，指通过采取措施减少风险发生的概率或降低风险的影响程度，一般适用于无法避免或难以完全彻底消除的风险，常见的措施包括但不限于：
   1) 监测与检测：部署监测和检测系统，及时发现和应对潜在的风险事件；
   2) 备份和恢复：定期备份数据，并确保能够迅速恢复数据以应对数据丢失或损坏；
   3) 安全培训：对员工进行安全培训，提高员工的安全意识，减少人为风险；
   4) 数据分类与分级：对数据进行分类和分级，并采取差异化管控措施，确保高风险数据受到更严格的保护；
   5) 访问控制：限制数据访问权限，确保只有授权人员能够访问敏感数据；
   6) 敏感数据加密：对敏感数据进行加密，防止未授权的访问。

c) 风险接受，指机构明确意识到存在的风险，并选择接受其可能带来的损失或影响，一般适用于风险影响较小，且不会造成重大损失的风险。对于此类策略，机构需做好风险记录和报告，并定期开展可接受风险的再评估：
   1) 风险记录和报告：记录和报告已知的风险，同时明确风险的潜在损害和可能的后果；
   2) 定期评估：定期对风险接受项进行再评估，由于环境变化、业务调整等原因可能造成风险影响的变化或升级，应及时评估并适时处置，至少每年开展一次。

d) 风险转移，指机构意识到存在的风险，通过采取一定措施将风险转移至其他实体，需要注意的是，转移管理风险的责任是可能的，转移影响的责任通常是不可能的，机构进行风险转移时应充分考虑风险影响，转移过程可能产生新的风险或更改已识别的风险，机构需对额外的风险进行处置，常见的措施包括但不限于以下两个方面：
   1) 合同和法律保障：与合作伙伴或服务提供商建立明确的合同和法律协议，明确责任和权益；
   2) 数据安全保险：机构可以购买数据安全保险，以转移部分风险给保险公司承担，一旦遭受数据泄露或其他安全事件，可以通过保险索赔来得到一定经济赔偿。

6.3.4.4 风险处置的实施和监测

确定风险应对策略后，机构应积极实施处置并定期监测风险的状态，直至风险处置完成或达到可接受状态。

a) 处置实施：按照制定的计划，采取必要的措施来应对风险，包括制定制度流程、更新安全策略、部署新的安全工具、进行员工培训等；
b) 监测风险状态：定期监测已识别的风险的状态，包括定期的风险评估、漏洞扫描、安全事件、日志分析等；
c) 更新风险应对计划：随着情况的变化，机构应更新风险应对计划，以适应不断变化的风险环境，包括修改策略、重新评估风险、调整控制措施等。

6.4 数据安全制度体系

6.4.1 数据安全制度体系的建立

数据安全制度体系包含数据安全管理制度、员工信息安全管理制度、合作方管理制度、应急与响应制度等内容。

6.4.1.1 数据安全管理制度

应建立完善的数据安全管理制度，需覆盖数据全生命周期和全应用场景，应明确指出在不同数据类型或等级的管理要求，包括但不限于：数据安全管理、组织人员、合规评估、检查评价等制度；外部数据采购、合作引入的审批管理制度；数据分类分级管理制度；数据安全技术标准规范制度等。

6.4.1.2 建立员工信息安全管理制度

应在数据安全管理制度的基础上，建立员工信息安全管理细则，包含数据安全培训、考核、惩罚等信息安全管理要求。

针对三方人员参与本机构内业务的场景，三方人员除应遵守内部员工管理制度外，还应针对三方人员建立管理制度，包括出入场管理、权限管理、审计管理等。

6.4.1.3 建立合作方管理制度

针对与本机构有外部业务合作关系的机构，应建立合作方管理制度，包含数据需求、安全评估、数据引入、数据运维、登记备案和监督评价等管理机制，对数据来源的真实性、合法性进行调查，评估合作方的数据安全保障能力和数据安全风险管控能力，签订数据安全保密协议，明确双方数据安全责任及义务。

6.4.1.4 建立应急与事件响应制度

建立应急与事件响应制度的要求如下：

a) 应建立数据安全事件应急管理机制，建立机构内部协调联动机制，建立服务提供商、第三方合作机构数据安全事件的报告机制，及时处置风险隐患及安全事件；
b) 应制定数据安全事件应急预案，定期开展应急响应培训和应急演练；
c) 对已发生的数据安全事件，应当立即启动应急处置，分析事件原因、评估事件影响、开展事件定级，按照预案及时采取业务、技术等措施控制事态发展，并按相关要求报送上级管理部门。

6.4.2 数据安全管理制度体系实施细则

机构应在数据安全制度体系的基础上制定以下实施细则：

a) 建立相应的安全策略和流程控制机制：根据数据安全管理制度，对不同类型和级别的数据在其采集、传输、使用、存储、销毁与删除等环节建立管控或监测策略，并定期开展合规安全审计；

b） 建立可落地或可实施的操作指导：为员工或数据操作者制定的具体操作指南，以指导在工作中如何执行数据安全措施。应该清晰明确地描述各项安全措施的具体步骤和要求，以确保能够正确地执行安全策略和流程控制机制。例如，分类分级指南、数据安全技术标准规范、加密技术指导等；

c） 建立实施过程中需要用到的记录或清单模板：可以帮助机构记录在数据安全制度落实过程中的关键信息、跟踪执行进度和记录事件等。例如，访问日志、安全审计报告、数据备份记录等。

6.4.3 数据安全管理制度体系的完善

当机构出现以下场景时，应考虑优化和完善制度体系：

a） 制度体系无法及时应对新的威胁，例如新的漏洞或威胁；

b） 制度体系无法覆盖机构内所有业务场景，如业务拓展至新的领域等；

c） 制度体系无法满足法规和政策要求，如法律法规对数据安全的要求提高等；

d） 机构发生安全事件或漏洞；

e） 其他需要对制度体系进行完善的场景。

6.5 数据安全技术体系

6.5.1 概述

数据安全技术体系为治理工作提供技术支撑，实施小组宜在治理过程中根据不同的数据使用场景按需选择、灵活搭配，数据生命周期各阶段常见的防护技术见图 2。

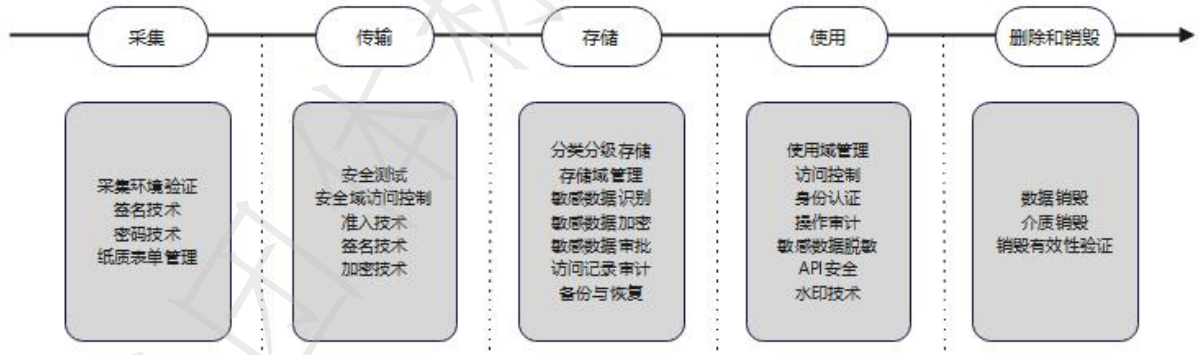

图2 数据全生命周期防护技术

6.5.2 数据生命周期防护技术

数据生命周期各阶段包括但不限于以下技术能力：

a） 数据采集：

1） 通过用户身份认证、IP 地址验证、验证码识别、人机交互验证等方式对数据源进行验证，以确保数据来源的真实性和合法性。涉及采集敏感信息时，结合口令密码、设备指纹、设备信息等多种因素进行增强验证；

2） 制定数据采集校验规则以自动检查数据的准确性和完整性，以确保采集数据的准确有效；

3） 采用哈希摘要、消息验证码、数字签名、数据证书等密码技术确保采集数据的完整性；

4） 对新采集的数据，使用分类分级工具自动添加数据资产安全标签；

5） 记录数据采集日志，确保采集数据的可追溯性；
6） 通过人工纸质表单形式采集数据时，应确保采集环境可控，防止采集过程中表单丢失与信息泄露；
7） 对采集的全流程进行加密通信，从发起采集需求，采集授权到传输，应采取全过程双向加密通信。

b） 数据传输：
1） 对传输双方进行身份认证，确保双方身份的真实可信；
2） 传输前对数据进行加密处理，应选用安全的密码算法，禁用 MD5、SHA-1、DES 等不安全算法；
3） 采用安全通道或安全传输协议进行数据传输，如采用安全传输协议应禁用 SSL 所有版本与 TLS1.2 版本以下的传输协议；
4） 使用数字签名技术以确保数据传输的抗抵赖性；
5） 对关键的网络传输链路、网络设备进行冗余建设，确保传输的可靠性；
6） 传输结束后及时清除传输过程中的历史缓存数据；
7） 记录传输日志，以确保传输过程的可追溯性；
8） 部署防火墙、防入侵等安全设备和技术，确保数据传输过程中的网络安全性。

c） 数据存储：
1） 根据数据安全级别，对数据进行分域分级存储；
2） 不同存储域之间进行物理或逻辑隔离，对不同域之间的数据流动进行安全管控；
3） 对金融数据的存储满足最小业务需求和法律法规或行业监管机构要求；
4） 对于去标识化的信息应与原始信息隔离存储，对于匿名化的信息，其原始信息不应再保留；
5） 数据安全级别为 4 级及以上数据进行加密存储；
6） 对存储设备的空间、性能进行监控，确保其满足业务增长需求；
7） 建立数据备份与恢复机制，支持海量数据的有效备份，定期对备份数据进行测试，确保备份数据的完整性和可用性；
8） 对于备份数据的保护要求应与源数据的安全级别保持一致；
9） 建立过期存储数据及其备份数据彻底删除或匿名化的处理机制，确保删除或匿名化的信息无法恢复或无法识别到个人；
10） 实体信息或信息载体运输必须通过可靠方式传输，在运输过程中，应维护对设备监督和记录，含有敏感信息的实体传输时，必须对实体进行封存，封存表面不能泄露实体的内容和保密分类。

d） 数据使用：
1） 数据处理环境隔离，开发测试环境原则上不允许使用生产环境的真实数据，如需使用须进行数据脱敏处理，脱敏方式包括不限于泛化、抑制、扰动、屏蔽，账号、卡号、协议号、支付指令等测试确需信息除外；
2） 对数据的处理包括访问、查询、分析、使用、导入导出等进行权限管控，仅赋予业务所必需的权限；
3） 建立数据处理身份认证机制，根据 JR/T 0197—2020 对定义为 3 级及以上数据进行双因素认证；
4） 对于有数据展示需求的业务系统，应对敏感数据进行脱敏展示，如因业务需求需要查询明文信息，应进行额外的安全控制如授权审批、二次身份验证、操作记录等，对于业务系统的导出、复制、打印等功能进行限制，并添加界面水印防止拍照截屏等；

5) 针对个人信息的数据处理时，应采用技术手段保护数据安全，包括差分隐私技术、安全多方计算、K 匿名等；
6) 对所有数据处理的操作进行日志记录，日志包括操作人、操作时间、操作行为、操作数据类型、操作结果等，日志应留存至少 6 个月（4 级数据操作日志应留存至少 1 年，5 级数据操作日志应留存至少 3 年）；
7) 采用身份验证、数据加密、脱敏、安全通道、共享交换区域等技术手段，对数据进行交换，确保数据交换安全；
8) 对于通过接口进行的数据交换，具备对接口输入参数有效性验证机制，为接口提供异常处理功能。

e) 数据删除与销毁：
1) 个人信息主体提出注销申请时，应在法律法规规定的时间内及时进行处理，确保数据在业务前台不可检索，不可用于其他任何业务活动；
2) 对于过期存储的数据本身及备份数据进行彻底删除或匿名化处理，应对彻底删除或匿名化处理数据进行验证，确保其不可用；
3) 存储个人金融信息的存储介质无须使用时，应进行消磁或物理破坏处理，并对销毁介质进行有效性验证。对于需要继续利用的存储介质，应采用数据多次覆写方式进行数据擦除，并检查确保擦除的数据不能恢复；
4) 纸件应用碎纸机销毁，禁止简单撕碎或随意丢弃；
5) 对数据删除及销毁的操作及过程进行记录，确保销毁过程可追溯、可审计。

7 金融数据安全治理成果评估

7.1 评估原则

金融数据安全治理成果评估的原则包括：

a) 合法合规原则：评估工作依照本文件及相关规范性文件合法合规地开展；
b) 客观公正原则：评估工作过程中，根据实际情况做出判断，根据真实情况客观评估，不夸大或掩盖发现的问题，评估结果客观、真实和公正；
c) 保密原则：评估参与方对评估过程中获得的信息严格保密，以保障数据安全；
d) 全覆盖原则：评估工作覆盖本文件中所有金融数据安全治理实施相关内容；
e) 最小影响原则：评估工作尽量最小化地影响机构业务和信息系统正常运行，最大程度地降低对机构造成的干扰和风险。

7.2 评估流程

金融数据安全治理成果评估包括以下流程：

a) 评估流程主要包括评估准备、评估执行、评估报告和评估审核四个阶段；
b) 评估准备：
1) 明确评估目标；
2) 根据评估目标组建评估团队，评估团队原则上由数据安全治理监督小组成员组成；
3) 明确评估范围，确定本次评估所涉及的金融数据、金融产品和服务、信息系统、人员及组织（含内、外部）等；
4) 根据评估目标和范围等情况编制并确定评估方案，明确本次评估工作的主要任务、任务分工、人员安排、时间计划等内容。

c） 评估执行：评估团队根据已确定的评估方案开展本次评估的具体实施工作，留存评估实施过程相关记录材料并形成各部分评估结果；

d） 评估报告：根据评估实施过程记录的材料，对评估内容、过程、结果、问题等进行总结和分析，并给出最终评估结论，形成评估报告；

e） 报告审核：由数据安全治理领导小组组建评审团队对评估报告进行审核，同时审核各评估事项及参与人员行为等是否公正、真实及合法合规等基本原则。

7.3 评估维度和指标

金融数据安全治理成果可从安全管理、安全保护技术和风险运营三个维度、14 个指标进行评估，见表 1。机构可根据内部情况对各个指标分值进行分配，并制定相应评级标准。

表1 金融数据安全治理评估表

评估维度和指标	安全管理评估				安全保护技术评估					安全风险运营评估			
	组织建设	制度流程建设	数据资产盘点	数据资产分类分级	数据采集	数据传输	数据存储	数据使用	数据删除与销毁	风险识别	风险清单	风险处置	应急响应

7.4 改进优化

数据安全治理工作组应根据评估报告和各单项指标的评估结果，对本次数据安全治理情况、存在问题和治理薄弱点进行分析和总结，提出相应改进建议和措施，并由实施小组制定工作计划加以落实。

改进优化后，应对治理成果再次根据本文件的要求进行评估，直至治理成果评估工作最终完成。

参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语
[2] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理
[3] GB/T 32923—2016 信息技术 安全技术 信息安全治理
[4] GB/T 35273—2020 信息安全技术 个人信息安全规范
[5] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[6] GB/T 39335—2020 信息安全技术 个人信息安全 影响评估指南
[7] GB/T 40685—2021 信息技术服务 数据资产 管理要求
[8] JR/T 0171—2020 个人金融信息保护技术规范
[9] JR/T 0197—2020 金融数据安全 数据安全分级指南
[10] JR/T 0223—2021 金融数据安全 数据生命周期安全规范
[11] T/NIFA 22—2023 金融数据安全应急响应和处置指引
[12] ISO/IEC 27014—2020 Information security, cybersecurity and privacy protection — Governance of information security
[13] 中华人民共和国数据安全法
[14] 数据资产管理实践白皮书 6.0 CCSATC601大数据技术标准推进委员会.2023年1月