金融领域数据安全能力体系构建方法研究

赵晓令，白惠文，李安伦
（中国软件评测中心，北京　100048）

摘　要：《中华人民共和国数据安全法》要求建立健全全流程数据安全管理制度，依照法律、法规开展数据处理活动。《中国人民银行业务领域数据安全管理办法（征求意见稿）》提出了金融领域的数据安全保护总体要求、数据分类分级、数据安全保护措施等方面的要求。为了帮助金融机构落实相关国家、行业数据安全要求，提出一种基于数据安全能力成熟度模型的数据安全能力体系构建方法，从组织建设、制度流程、技术工具和人员能力四个维度分别建设数据安全能力。所提方法可以帮助金融机构全面提升数据安全防护能力，从而满足合规需求以及自身发展需要。

关键词：数据安全法；数据安全能力成熟度模型；数据安全能力体系；数据安全防护能力
中图分类号：TP309.2　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097－1788.2024.05.004
引用格式：赵晓令，白惠文，李安伦. 金融领域数据安全能力体系构建方法研究［J］. 网络安全与数据治理，2024，43(5)：27－34.

Research on the construction method of data security capability system for financial domain

Zhao Xiaoling，Bai Huiwen，Li Anlun
（China Software Test Center（CSTC），Beijing 100048，China）

Abstract：The Data Security Law of the People′s Republic of China requires that institutions should establish and improve a whole-process data security management system and carry out data-processing activities in accordance with the provisions of laws and regulations. The Measures for the Management of Data Security in the Business Field of the People′s Bank of China（Draft for Public Comments）puts forward the general requirements for data security protection in the financial field，data classification and grading，and data security protection measures. In order to help financial institutions implement relevant national and industry data security requirements，this paper proposes a data security capability system construction method based on Data Security Capability Maturity Model（DSMM）. Building data security capabilities is carried out in four dimensions，such as organizational construction，institutional processes，technical tools and personnel capabilities，respectively. The proposed method can help financial institutions comprehensively improve their data security protection capabilities，so as to meet compliance requirements as well as their own development needs.

Key words：The Data Security Law；Data Security Capability Maturity Model；data security capability system；data security protection capabilities

0　引言

《中华人民共和国数据安全法》（以下简称《数据安全法》）要求建立健全全流程数据安全管理制度，依照法律、法规的规定开展数据处理活动。为贯彻落实《数据安全法》等国家法律、行政法规要求，加快推动自身业务监督管理职责范围内数据安全管理的法治化建设，2023年7月《中国人民银行业务领域数据安全管理办法（征求意见稿）》发布，为金融领域提供了数据安全保护总体要求、数据分类分级、数据安全保护管理措施、数据安全保护技术措施、风险监测、评估审计与事件处置措施等方面的要求。

随着数字金融的迅猛发展、金融数据的共享开发利用不断深化，金融数据安全治理面临巨大挑战，数据非法采集、数据贩卖、数据篡改、数据攻击、数据权限滥用等安全问题层出不穷[1-3]。当前金融机构的数据安全能力尚处于参差不齐的状态[4]，存在内部窃取、外部遭

受网络攻击等各种数据安全风险，因此金融领域亟需建立健全数据安全能力体系，从而合法合规地开展数据处理活动，抵御各种潜在的网络威胁。

为了帮助金融机构落实相关国家、行业数据安全要求，本文提出一种基于数据安全能力成熟度模型的数据安全能力体系构建方法，从组织建设、制度流程、技术工具和人员能力四个维度分别建设数据安全能力，从而帮助金融机构全面提升数据安全防护能力。

1　金融领域数据安全能力建设面临的挑战

金融数据安全对于国家经济安全和社会稳定具有重要意义。金融数据是指在金融领域中为进行风险分析、客户管理、投资决策等目的而收集、处理和分析的一系列数据，不仅具备数据的一般特性，更是包含了国民个人信息、企业资金流转、社会经济活动动态等重要内容，其安全防护能力建设尤为重要，当前金融领域数据安全能力建设面临多种挑战。

一是金融数据监管趋严。随着《网络安全法》《数据安全法》《个人信息保护法》等法律法规的落地实施，金融机构面临的数据安全合规难度加大，需要在合规前提下开展数据安全治理。

二是金融数据要素流通场景多样化。金融业数据要素流通场景具有多样化的特点，包括内部流通、外部流通、数据共享、数据交易等。每种流通场景都存在一定的安全风险，需要采取针对性的安全保护措施。

三是金融数据主体复杂。金融数据主体涉及个人、组织、企业、政府部门等多种类型，且数量庞大，其中蕴含着大量的金融敏感信息，因此需要厘清数据资产，根据数据属性、重要程度、敏感程度等多种因素进行分类分级管理。

四是金融数据滥用和泄露风险较高。金融行业业务复杂多样，作为数据处理者或使用者的业务人员较多，目前业务人员普遍缺乏数据安全意识，可能存在数据滥用或泄露等风险。此外，金融行业内部团队在使用数据工具分析数据的过程中，可能会发生误操作，造成严重的业务错误、数据丢失或泄露风险。

2　数据安全能力成熟度模型

GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》（以下简称 DSMM）是我国数据安全领域的首部国家标准，提出了从组织建设、制度流程、技术工具及人员能力四个方面构建数据安全能力成熟度的分级模型。该模型能力成熟度等级从低到高包括 1 至 5 级，依次为非正式执行、计划跟踪、充分定义、量化控制和持续优化；该模型数据安全过程包括数据生存周期安全和通用安全，其中数据生存周期包括数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全和数据销毁安全 6 个阶段，该模型也是组织开展数据安全能力建设的重要依据。

3　金融领域数据安全能力体系构建方法

金融数据安全防护体系建设初期需要自上而下进行推动，助力数据全生命周期安全建设和运行；在安全运营过程中自下而上进行优化，逐步完善数据全生命周期安全，最终构建完整的金融数据安全防护体系，如图 1 所示。

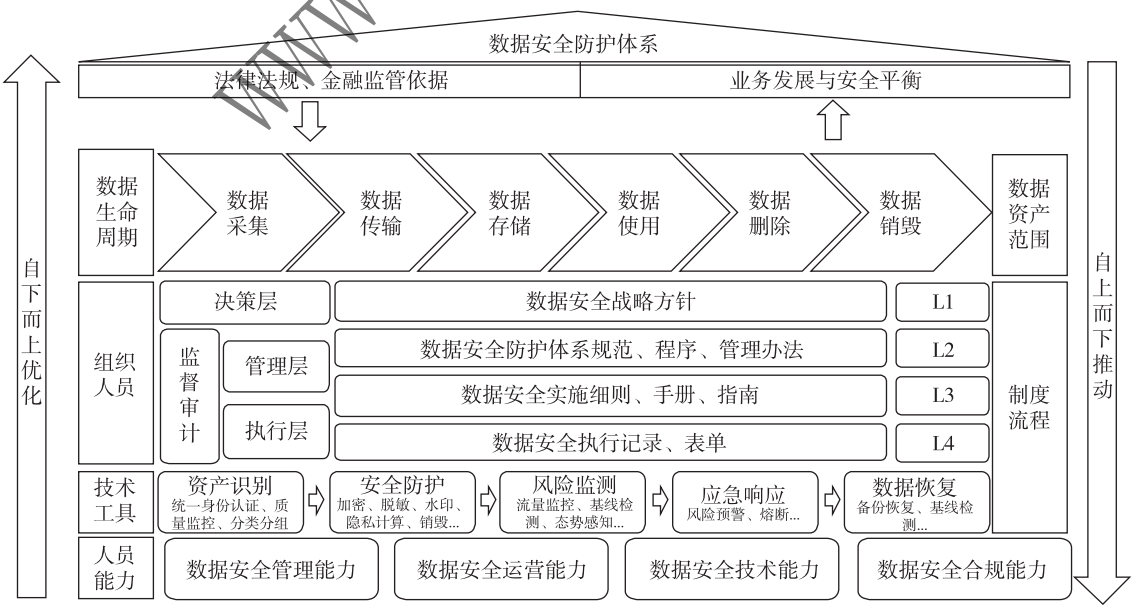

图 1　金融领域数据安全体系框架

3.1 数据安全原则

数据安全原则建立在对国家法律法规、金融行业监管规定基础上，遵循基本的数据安全管理原则，制定数据分类分级清单，并贯穿于金融数据生命周期安全过程，保障金融机构数据安全符合合规底线。

3.1.1 数据安全管理原则

数据安全工作遵循“谁管业务，谁管业务数据，谁管数据安全”的权责一致原则；在资源分配和监控审计层面，应具备系统管理员、数据安全管理员、数据安全审计员三员分立模式，其中数据安全管理员与数据安全审计员不能由同一人担任。

3.1.2 数据分类分级原则

全面梳理金融机构业务条线，收集、整理全部业务系统数据资产，分类过程中遵循科学实用、稳定性、明确性、可扩展性等原则，按照责任部门、描述对象、内容主题等进行分类，如一级子类按照描述对象分为客户数据、经营管理数据和监管数据等，其中客户数据可以细分为个人客户和企业客户等，三级子类可根据业务属性细化分类。数据分级按照数据安全性被破坏后的影响对象和影响程度进行划分，按照 GB/T 43697—2024《数据安全技术 数据分类分级规则》、JR/T 0197—2020《金融数据安全 数据安全分级指南》等文件要求，首先识别核心数据和重要数据，并实施重点保护措施，针对一般数据可根据需要划分敏感级别，如参考 JR/T 0171《个人金融信息保护技术规范》等划分个人信息，需要注意的是，当个人信息或敏感个人信息达到一定数量时，其级别应在原级别基础上进行升级，并实施更严格的保护措施。此外，数据分类分级应具备动态更新和监督评价流程，形成分类分级闭环管理。

3.1.3 数据全生命周期安全原则

JR/T 0223—2021《金融数据安全 数据生命周期安全规范》明确了金融数据的生命周期，包括数据采集、数据传输、数据存储、数据使用、数据删除及数据销毁过程。

按照分类分级结果，遵循数据处理的合法性、正当性、明确性原则，在数据生命周期各过程中采取对应的安全措施。数据采集过程对金融信息主体知情同意，明确采集范围、频度、类型、用途等，采用数据源鉴别、完整性校验等安全措施；数据传输过程采用主体身份鉴别、加密技术、网络冗余等安全措施；数据存储过程遵循“境内储存、出境评估”基本原则，采用数据加密、访问控制、备份恢复策略等安全措施；数据使用过程采用数据脱敏、数据挖掘、访问控制等安全措施；在数据删除与销毁过程中，采用匿名化处理、格式化、物理消磁、粉粹等安全措施。

总之，金融机构需要通过技术和管理手段保证数据全生命周期过程中的机密性、完整性和可用性，具备排查和处置数据安全隐患的能力，保证业务连续性。

3.2 组织能力构建

按照金融机构常规部门和岗位设置，数据安全组织可为虚拟团队；依据 DSMM 模型，数据安全组织建设分为决策层、管理层、执行层和监督审计层。

决策层至少包含企业战略和信息安全最高负责人，主要负责确定金融机构业务发展战略、确定数据安全的原则和目标以及数据安全的重大事项决策，为数据安全体系架构的建立提供支持和资源保障。

管理层应由专职的数据安全部门组成，例如金融科技部、数据管理与应用部等。管理层在全面理解决策层安全策略、完整掌握金融机构业务条线的基础上，主要负责牵头推动数据安全体系建设，包括依据安全原则、企业发展战略制定数据全生命周期安全制度，审核数据安全管理细则，向上汇报数据安全重大事项，向下协调数据安全日常工作，是组织架构中承上启下的关键层级。

执行层由各业务板块、IT 管理、运维服务、人力资源等各部门组成，主要负责协助管理层制定数据安全操作规程、实施细则等；负责按照数据安全制度要求执行安全运营日常工作，包括发现安全漏洞和潜在风险并及时处理；负责向管理层汇报数据安全运营情况和异常事件。其中人力资源主要负责将入职、离职、调岗等人员流动情况通知各相关部门，及时处理人员权限、回收资源等。

监督审计层由风险管理、审计等独立与其他部门的人员组成，主要负责定期对数据安全运营体系的监督和审查，包括制度执行情况、安全事件处理情况、安全问题分析情况以及运营体系改进情况；督促管理层和执行层整改数据安全运营体系，并定期向决策层汇报。

3.3 制度流程构建

数据安全制度规定各角色或岗位职责，约定管理流程，是金融机构安全体系有序运营的主要依据。数据安全制度主要由管理层和执行层根据决策层的数据安全原则、目标等制定，从上到下以此建立四层安全制度。

第一层根据决策层确定的金融机构业务发展规划，确定数据安全原则、目标、资源，由管理层建立数据安全战略相关文件（如数据安全管理总则），并由决策层批准下发。

第二层依据数据安全战略文件，由管理层与执行层共同讨论建立数据安全防护体系规范、程序和管理办法，如数据全生命周期安全管理办法、金融机构数据分类分级要求、员工管理办法、合作方管理办法、访问控制策

略等，并由决策层审批下发。

第三层依据数据安全防护体系文件，由管理层指导、执行层建立数据安全实施细则、手册和指南，如数据资产分类分级细则、数据访问控制设置手册、数据脱敏操作指南、数据接口接入指引、数据库备份与恢复策略等，发布至金融机构内部并确定意见收集、试运行、正式实施时间要求。

第四层依据数据安全防护系列指导书，由执行层按照安全体系规范输出运营过程中的各类文件，如数据资产分类分级清单、数据库备份与恢复记录表、数据销毁申请/记录、数据接口设计文档、系统运维权限清单、系统安全报告等。

3.4 技术工具构建

金融机构数据安全组织和制度的建立，为数据安全体系构建了管理责任机制，引入和借助安全工具辅助，以数据资产分类分级为基础，依据安全原则、管理制度以及应用场景实现“数据资产识别－安全防护－风险检测－应急响应－数据恢复”的全闭环过程，形成管理与技术并行的数据安全运营体系。

（1）资产识别。使用统一身份认证系统实现数据源鉴别，数据访问控制，使用检测数据规则/密码技术实现数据完整性、机密性、准确性等质量要求，在数据采集阶段保证数据源真实、数据质量合规；利用资产管理工具实现分类分级的自动识别，为数据在全生命周期的安全做基础。

（2）安全防护。依据资产分级安全要求，应必须对重要数据、敏感信息采用加密传输、加密存储、脱敏显示等安全措施，对提供第三方进行使用的数据采取脱敏/水印技术、隐私计算等方式加强安全管控，依据合规原则保护数据全生命周期安全。

（3）风险检测。采用流量监控、基线检测、防泄漏、态势感知等安全工具，检测数据在终端、服务器的安全状态；检测恶意攻击等事件发生；通过统一日志系统、安全审计工具等发现异常操作行为；风险检测过程根据数据安全管理制度，实时检测风险，并按照策略发出预警，为应急响应做基础。

（4）应急响应。依据金融机构应急管理要求，发现风险后，在技术上可采用熔断等策略尽可能保护数据资产，同时金融机构应按应急演练过程及时调集相关岗位人员，依据风险场景及时作出响应，并按数据安全原则验证响应结果。

（5）数据恢复。对于引起的数据损坏、业务中断等风险情况，通过数据备份恢复、基线检测等工具恢复数据，保证业务连续性。

3.5 人员能力构建

金融机构人员能力主要针对管理层和执行层相关岗位，针对管理层应在充分理解决策层数据安全方针政策基础上，具备数据合规分析能力和数据安全管理能力，同时具备数据安全运营的管理能力；针对执行层，在充分理解管理层要求基础上，具备数据安全运营执行能力和数据安全技术能力。

在数据安全合规能力方面，管理层应具备对国家有关法律法规和行业监管规定的分析解读能力，具备基于相关规定形成契合金融机构发展的数据安全合规策略能力，具备指导金融机构数据安全架构建设、制度制定、方案改进等能力。

在数据安全管理能力方面，管理层应具备推动数据安全相关要求、制度、工具的落地，并及时有效解决金融机构在安全与业务发展冲突的能力。

在数据安全运营能力方面，管理层应具备数据安全运营与数据安全策略的一致性检查能力，在管理上促进数据安全有效运营；执行层应在管理制度和策略要求上，具备正确执行数据安全运营过程的能力，并及时发现和反馈问题。

在数据安全技术能力方面，执行层各岗位应具备熟练使用各种安全平台、安全分析等的技术能力，具备学习和吸收企业相关数据安全要求、制度的能力，并具备按照要求通过技术协助实现数据安全措施落地的能力。

3.6 持续优化能力构建

3.6.1 自上而下推动

金融数据安全防护体系建设初期需要自上而下进行推动，助力数据全生命周期安全建设和运行。

数据安全建设存在被动因素，例如由外部攻击造成的数据泄漏、由监管要求提出的数据安全改进或由系统改造升级相应的安全要求等。这些被动因素可能引起在数据安全建设过程进度缓慢，效果不佳等。决策层应在体系建设初期起到引领作用，例如规划安全体系建设的投入，主动安装安全工具等；管理层应全面支持体系建设，除制定基本制度流程外，还应在早期进行数据安全培训、宣传示范优秀安全行为，全面推动数据安全体系建设和落实。

3.6.2 自下而上优化

在安全运营过程中自下而上进行优化，逐步完善金融数据全生命周期安全，达到持续安全运营。

在数据安全落地运行过程中，由执行层按照安全制度和安全策略执行安全过程，并定期输出相关数据，包括运营数据、分析数据、问题清单等，提交管理层进行汇总分析。管理层与执行层深入分析安全运营体系的优

缺点，改进流程、策略，在合规的基础上，发挥数据安全对业务发展的正向作用，例如打通流程环节，助力数据要素有效流转，提高数据利用价值等。

3.7 数据安全能力成熟度评价

根据 DSMM 模型中 1 至 5 级的最佳实践要求，收集和检验金融机构数据安全佐证材料，包括数据资产关联图、人员岗位设置、制度流程清单、技术工具清单、人员培训记录等，通过综合得分得出金融机构数据安全能力成熟度等级。

DSMM 由 30 个过程域（PA）组成，每个 PA 包含不同等级的基本实践（BP）；BP 的分数之和的算数平均值为 PA 得分，PA 等级取决于 PA 得分与修正因子（基于对某一 PA 数据安全风险的接受程度，可对等级结果进行修订因子不超过 0.5～1.5 区间的修订）之和，金融机构最终 DSMM 等级由 PA 等级决定，可以跨级别进行评价；其中 1～3 级单独评价，4～5 级应包含 3 级。例如 2 级评价必须包含 94 项 2 级要求的基本实践；3 级评价必须包含 263 项 3 级要求的基本实践，可包含 4 级基本实践；4 级评价必须包含 3 级和 4 级的基本实践；5 级评价必须包含 3 级、4 级和 5 级的基本实践。该模型依据组织实际情况检查所有适用过程域，并记录不适用过程域及原因，评分公式为：

if（BP≤3 级）

$$\text{PA 分值} = \frac{\sum_{1}^{n} \text{BP 分值} \times \text{BP 符合率}(\text{BP} \leq 3\ \text{级})}{n}$$

if（BP=4 级）

$$\text{PA 分值} = \frac{3 \times \sum_{1}^{n} \text{BP 符合率}(\text{BP} = 3\ \text{级})}{n} + \frac{\sum_{1}^{n} \text{BP 符合率}(\text{BP} = 4\ \text{级})}{n}$$

if（BP=5 级）

$$\text{PA 分值} = \frac{3 \times \sum_{1}^{n} \text{BP 符合率}(\text{BP} = 3\ \text{级})}{n} + \frac{\sum_{1}^{n} \text{BP 符合率}(\text{BP} = 4\ \text{级})}{n}$$

$$\text{DSMM 等级} = \frac{\sum_{1}^{n} \text{Min}(\text{PAm 分值} + \text{PAm 修正因子})}{m}$$

备注：n 为 PA 不同等级包含的 BP 数量，不包含不适用项；m（$1 \leq m \leq 30$）为 PA 数，且不包含不适用过程域。BP 默认分值 1 级 1 分，2 级 2 分，3 级 3 分，4 级 1 分，5 级 1 分。

数据安全能力成熟度评价是对金融机构数据安全现状的了解，也是制定优化方案的依据。根据评价过程中发现的问题，制定解决方案，及时优化数据安全过程，不断提升数据安全水平，并形成契合金融机构的数据安全体系架构，促进行业共同进步。

3.8 数据安全能力评估案例

以某保险公司年金业务为例，收集数据安全组织架构、制度流程、安全技术与平台等材料，如表 1 所示。

表 1 某保险公司年金业务数据安全材料概览表

序号	数据安全属性	证据材料	概况
1	组织架构	某保险公司组织架构图	决策层→保险公司级副总裁：负责明确数据安全目标、数据安全投入等重大事项的决策和审批 管理层→科技发展部、各团队负责人（综合数据团队、开发团队、创新团队、投资团队、应用团队、安全团队、人力资源部）：负责本部门数据安全场景、制度、流程等梳理、建设、优化 执行层→各团队人员（综合数据团队、开发团队、创新团队、投资团队、应用管理团队、安全团队、人力资源部）：负责按照规定执行数据安全过程、提出优化方案
2		人力资源部岗位职责要求	
3	数据资产	集团公司数据分类分级表	数据包含 4 个类别、4 个级级别，涵盖数据的采集、传输、存储、处理、交换、销毁场景
4		年金系统数据流转图	
5	制度流程	《某保险公司数据安全管理目标》	一级制度，数据安全的战略方针指导
6		《某保险公司数据分类分级管理办法》	二级制度，管理层按某保险公司部门、业务环境建立管理级制度集合
7		《员工安全管理办法》	
8		《数据生命周期安全管理办法》	

（续表）

序号	数据安全属性	证据材料	概况
9		《权限管理办法》	
10		《数据脱敏原则和制度》	
11		《数据存储介质安全管理办法》	二级制度，管理层按某保险公司部门、业务环境建立管理级制度集合
12		《数据发布管理办法》	
13		《用数环境安全规范》……	
14		《XX 外部接口管理平台数据接入细则》	
15		《XX 资产管理平台使用规范》	
16		《数据脱敏操作指南》	
17		《数据使用申请表》	
18		《数据加密管理规范》	三级制度：管理层与执行层按照各个业务系统、管理规范等制定的具有实操指导的文件集合
19		《数据备份与恢复管理规范》	
20	制度流程	《IT 管理规范》	
21		《XX 受托系统权限管理规定》	
22		《XX 账管系统权限管理规定》	
23		《数据安全合规指引文件》	
24		《数据资产分类分级清单》	
25		《业务合作方清单》	
26		《数据销毁记录》	
27		《账号权限申请》	四级制度：由执行层在数据全生命周期过程中执行的安全记录，用于安全优化和审计的记录集合
28		《数据备份与恢复记录》	
29		《数据接口清单》	
30		《XX 系统数据加密细则》	
31		《XX 客户采集系统需求评审会议纪要》	
32		安全职位人员 CISP 证书 5、CISSP 证书	
33	人员能力	《员工数据安全能力考评记录》	用于保持和提升员工的数据安全意识的培训计划和能力验证
34		《数据安全培训计划表》……	
35		XX 身份认证平台	
36		XX 数据资产综合管理平台	
37		XXAPI 数据安全网关	用于辅助管理数据安全过程，安全工具与人工管理过程结合，可涵盖数据的采集、传输、存储、处理、交换、销毁过程
38	技术工具	XX 数据安全态势感知平台	
39		XX 数据脱敏系统（DW）	
40		XX 外部接口管理平台……	

依据佐证材料，通过调研访谈、平台验证、配置检查、记录核查等方式，初步判别按照 DSMM3 级进行符合性评估，BP 等级包含 3 级与 4 级项，按照评价计算方法得到某保险公司安全水平。表 2 和表 3 分别为 PA01 数据分类分级过程域结果和 DSMM 等级一览表。

4 结论

金融数据涉及大量个人信息、企业敏感信息，数据安全是金融机构数据安全合规处理的保障，更是数据要素市场有序发展的前提。本文借鉴 DSMM 模型，建立金融机构安全组织和制度，并从数据安全运营角度，以数据资产识别、安全防护、风险监控、应急响应和数据恢复的数据安全运营方式，将管理和技术结合，通过自上而下的推动执行、自下而上的优化改进，持续完善金融机构数据安全防护体系。

表 2　PA01 数据分类分级过程域结果

过程域	基本实践	能力维度	级别	适用	符合度	分值	修正因子	等级
PA01 数据分类分级	组织应设立负责数据安全分类分级工作的管理岗位和人员，主要负责定义组织整体的数据分类分级的安全原则（BP. 01. 04）	组织建设	3	是	100%	3. 2	0	3
	应明确数据分类分级原则、方法和操作指南（BP. 01. 05）	制度流程	3	是	75%			
	应对组织的数据进行分类分级标识和管理（BP. 01. 06）	制度流程	3	是	100%			
	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（BP. 01. 07）	制度流程	3	是	75%			
	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对数据分类分级的变更操作及其结果符合组织的要求（BP. 01. 08）	制度流程	3	是	75%			
	应建立数据分类分级打标或数据资产管理工具，实现对数据的分类分级自动标识、标识结果发布、审核等功能（BP. 01. 09）	技术工具	3	是	100%			
	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（BP. 01. 10）	人员能力	3	是	100%			
	应记录自动分类分级结果与人工审核后的分类分级结果之间的差异，定期分析改进分类分级标识工具，提升工具处理的准确度（BP. 01. 11）	技术工具	4	是	50%			
	应对数据分类分级的操作、变更过程进行日志记录和分析，定期通过日志分析等技术手段进行变更操作审计。数据分类分级可追溯（BP. 01. 12）	技术工具	4	是	50%			

表 3　某保险公司 DSMM 等级一览表

过程维度	过程域	过程域等级	修正因子	修正后等级	综合等级
数据采集	PA01 数据分类分级	3. 0	0. 0	3	3. 0
	PA02 数据采集安全管理	2. 7	0. 5	3	
	PA03 数据源鉴别及记录	3. 0	0. 0	3	
	PA04 数据质量管理	2. 9	0. 5	3	
数据传输	PA05 数据传输加密	2. 5	0. 5	3	
	PA06 网络可用性管理	2. 8	0. 5	3	
数据存储	PA07 存储媒体安全	2. 8	0. 5	3	
	PA08 逻辑存储安全	2. 5	0. 5	3	
	PA09 数据备份和恢复	2. 9	0. 5	3	
数据处理	PA10 数据脱敏	2. 7	0. 5	3	
	PA11 数据分析安全	2. 7	0. 5	3	
	PA12 数据正当使用	2. 5	0. 5	3	
	PA13 数据处理环境安全	3. 0	0. 0	3	
	PA14 数据导入导出安全	2. 8	0. 5	3	
数据交换	PA15 数据共享安全	3. 0	0. 0	3	
	PA16 数据发布安全	3. 2	0. 0	3	
	PA17 数据接口安全	3. 1	0. 0	3	
数据销毁	PA18 数据销毁处置	2. 6	0. 5	3	
	PA19 存储媒体销毁处置	2. 7	0. 5	3	
通用安全	PA20 数据安全策略规划	3. 0	0. 0	3	
	PA21 组织和人员管理	3. 0	0. 0	3	
	PA22 合规管理	2. 6	0. 5	3	
	PA23 数据资产管理	3. 0	0. 0	3	

（续表）

过程维度	过程域	过程域等级	修正因子	修正后等级	综合等级
通用安全	PA24 数据供应链安全	2.8	0.5	3	3.0
	PA25 元数据管理	3.0	0.0	3	
	PA26 终端数据安全	3.0	0.0	3	
	PA27 监控与审计	2.8	0.5	3	
	PA28 鉴别与访问控制	2.8	0.5	3	
	PA29 需求分析	2.5	0.5	3	
	PA30 安全事件应急	2.8	0.5	3	

参考文献

[1] 杨立文. 运用前沿科技促进供应链金融数字化发展的机遇、挑战和对策研究 [J]. 金融科技时代，2022（7）：36－42.

[2] 王京晶. 新形势下金融数据安全面临的挑战与思考 [J]. 金融科技时代，2020（8）：53－54，58.

[3] 李松涛，谢宗晓. 数据资产化时代的金融数据安全 [J]. 中国信息安全，2021（5）：37－38.

[4] 张凤娜，刘金波. 安全视角下金融数据要素流通共享研究 [J]. 商业经济，2023（3）：161－164.

（收稿日期：2024－03－26）

作者简介：

赵晓令（1984－），女，硕士，工程师，主要研究方向：数据安全治理、云计算安全。

白惠文（1992－），男，博士，工程师，主要研究方向：数据安全治理、数据空间技术、网络流量分析。

李安伦（1985－），男，硕士，高级工程师，主要研究方向：数据治理、数据要素、云计算安全。

（上接第 10 页）

[66] IMRAN M, MITRA P, CASTILLO C. Twitter as a lifeline: human-annotated twitter corpora for NLP of crisis-related messages [J]. arXiv preprint arXiv：1605.05894，2016.

[67] IMRAN M，CASTILLO C，DIAZ F，et al. Processing social media messages in mass emergency：survey summary [C]// www18：Companion Proceedings of the Web Conference 2018，2018.

[68] 白华，林勋国. 基于中文短文本分类的社交媒体灾害事件检测系统研究 [J]. 灾害学，2016，31（2）：19－23.

[69] 闫家滕，栾翠菊. 微博意图分类在地震事件应急中的应用研究 [J]. 现代计算机（专业版），2018（23）：38－41.

[70] 刘晓. 基于文本挖掘的灾害多级联动分析与预测研究 [D]. 武汉：中国地质大学，2021.

[71] 刘淑涵，王艳东，付小康. 利用卷积神经网络提取微博中的暴雨灾害信息 [J]. 地球信息科学学报，2019，21（7）：1009－1017.

[72] 吴雪华，毛进，陈思菁，等. 突发事件应急行动支撑信息的自动识别与分类研究 [J]. 情报学报，2021，40（8）：817－830.

[73] 林佳瑞，程志刚，韩宇，等. 基于 BERT 预训练模型的灾害推文分类方法 [J]. 图学学报，2022，43（3）：530－536.

（收稿日期：2024－03－18）

作者简介：

姜钰棋（1998－），女，硕士研究生，主要研究方向：网络空间安全、自然语言处理等。

强子珊（1999－），女，硕士研究生，主要研究方向：网络空间安全等。

卜凡亮（1965－），通信作者，男，博士，教授，主要研究方向：安全和保护系统工程。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部