

ICS 03.060

CCS A 11

团体标准

T/NIFA 22—2023

金融数据安全应急响应和处置 指引

Guidelines for financial data security emergency
response and disposal

2023-11-10 发布

2023-11-10 实施

中国互联网金融协会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语与定义 1

4 缩略语 2

5 应急响应与处置框架 2

6 应急响应处置能力建设 3

 6.1 组织建设 3

 6.2 制度流程 5

 6.3 技术工具 7

 6.4 人员能力 7

7 金融数据安全事件分类分级 7

 7.1 事件分类 7

 7.2 事件分级 8

8 应急响应流程 10

 8.1 安全监测 10

 8.2 分级响应 10

 8.3 溯源分析 10

 8.4 影响评估 11

 8.5 处置恢复 11

 8.6 上报主管部门 12

 8.7 复盘总结 12

附录 A（资料性）数据安全事件向主管部门报告相关要求 13

参考文献 16

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、蚂蚁科技集团股份有限公司、奇富科技股份有限公司、奇安信科技集团股份有限公司、中国金融认证中心、济宁银行股份有限公司、重庆银行股份有限公司、维沃移动通信有限公司、北京三快科技有限公司。

本文件主要起草人：单强、陆书春、朱勇、王新华、白晓媛、李亮、马余静、高吉兴、周杨、彭晋、冯朝、王嵩贺、邓康、李娜、崔新炜、安锦程、隆峰、焦凡、张蕊、刘畅、唐福喜、秦雪、宋文娣。

金融数据安全应急响应和处置指引

1 范围

本文件规定了金融数据安全应急响应和处置的整体框架，明确了金融数据安全事件应急响应处置能力建设要素和指南、金融数据安全事件分类分级的原则和定义以及安全事件应急响应流程。

本文件适用于指导金融机构开展金融数据安全应急响应和处置工作，并为主管部门和第三方测评机构等单位开展金融数据安全应急处置检查和评估工作提供参考。

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。

JR/T 0197—2020 金融数据安全 数据安全分级指南

3 术语与定义

下列术语和定义适用于本文件。

3.1

金融数据 financial data

金融机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类金融数据。

注：该类金融数据可用传统金融数据处理技术或大金融数据处理技术进行组织、存储、计算、分析和管理。

[来源：JR/T 0197—2020，3.10]

3.2

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被篡改、泄漏、窃取或滥用、丢失，对国家安全、公共利益或个人、机构合法权益造成负面影响的事件。

3.3

数据安全事件应急响应 data security emergency response

机构为了应对数据安全事件的发生所做的准备，以及在事件发生后所采取的措施。

3.4

数据安全事件应急响应演练 data security incident emergency exercises

机构针对设定的数据安全事件模拟情形,按照应急预案所规定的职责和程序,在特定的时间和地域,开展应急处置的活动。

4 缩略语

下列缩略语适用于本文件。

BIA: 业务影响分析 (business impact analysis)

DLP: 数据泄漏防护 (data loss prevention)

DRP: 灾难恢复计划 (disaster recovery planning)

SRC: 安全响应中心 (security response center)

5 应急响应与处置框架

金融数据安全应急响应与处置框架如图1所示。

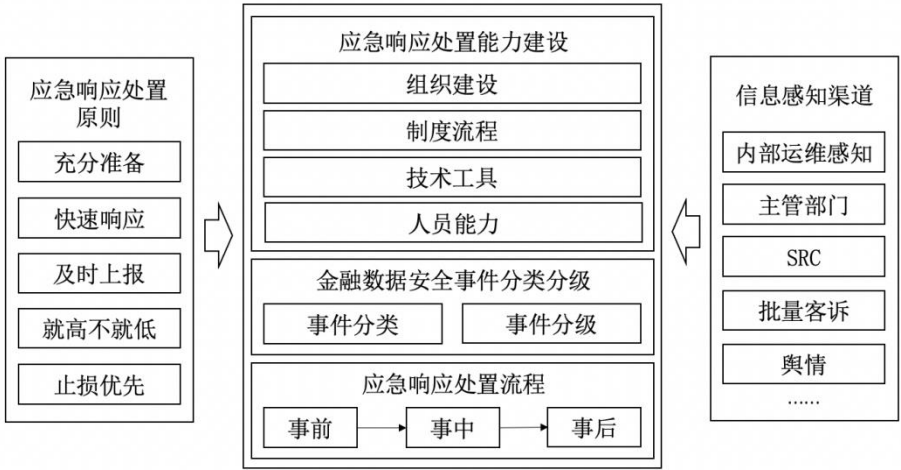


图1 应急响应与处置框架

金融数据安全应急响应与处置框架由如下五部分组成：

- a) 应急响应原则：
- 1) 充分准备：重视金融数据安全事件应急准备工作，包括应急响应处置能力建设、信息感知渠道建设等，并通过开展应急演练提高数据安全事件应对的能力；
 - 2) 快速响应：建立金融数据安全事件快速反应的机制，果断决策，即时处理，最大程度地降低事件对内对外的危害和影响；
 - 3) 及时上报：在金融数据安全事件处置过程中，针对事件影响进一步扩大的情况，及时对内升级，如有需要，上报主管部门，以决策处置方式调度更多的资源，防止风险进一步泛化和蔓延；
 - 4) 就高不就低：当金融数据安全事件等级判定指标覆盖不同的等级，难以判断级别时，按照较高一级数据安全事件进行定级处理；
 - 5) 止损优先：处置金融数据安全突发事件所采取的措施应以风险止损为首要目标，在最短时间内阻止数据风险的继续扩大，降低金融数据安全事件的负面影响。
- b) 应急响应处置能力建设：明确机构在金融数据安全应急领域应具备的能力：
- 1) 组织建设：金融数据安全事件应急相关组织和团队的设立、职责分工和沟通协作；

- 2) 制度流程：相关组织在金融数据安全事件应急方面的制度和执行流程；
- 3) 技术工具：通过技术手段和产品工具落实金融数据安全事件应急要求或自动化实现安全事件应急响应工作；
- 4) 人员能力：从事金融数据安全应急和处置的人员需要具备的知识和技能等。
- c) 金融数据安全事件分类分级：对金融数据安全事件进行分类分级，以便对不同类别和级别的事件制定有针对性的应急处置策略和流程，是快速有效处置事件的基础：
 - 1) 事件分类：金融数据安全事件可从产生原因、攻击方式、损害后果等方面进行分类，本文件主要将损害后果作为主要的分类原则；
 - 2) 事件分级：金融数据安全事件分级主要基于数据等级、影响对象、影响程度等要素，采用定性与定量相结合的方式。
- d) 应急响应处置流程：
 - 1) 事前：通过风险排查、总结历史突发事件应对情况、建立应急预案和定期应急演练等程序，全面梳理机构的金融数据安全应急场景。同时建立突发事件的监控、预警及应急联动处置机制；
 - 2) 事中：根据应急预案和事件的定级，采用分级的应急响应和处置；
 - 3) 事后：处置完金融数据安全事件后，尽快组织复盘，沉淀应急手段、落实整改方案并完善应急预案。如需要向主管部门或其他数据安全机构上报的，进行及时上报。
- e) 信息感知渠道：从多个渠道获取金融数据安全相关信息，作为事件预警的输入，以便有效应对，快速响应：
 - 1) 内部运维感知：通过安全审计等方式对可能导致数据安全事件的风险进行预警；
 - 2) 主管部门信息：主管部门下发的金融数据安全相关信息，如：风险提示、案例通报、通知要求等；
 - 3) SRC：与其他SRC建立沟通协作机制，互通金融数据安全相关信息，如：协助进行漏洞验证修复等；
 - 4) 批量客诉：从机构相关业务的客诉信息中，获取和分析金融数据安全相关信息；
 - 5) 舆情：通过对互联网上的数据安全相关事件和舆论的监测和分析，进行数据安全风险预警。

6 应急响应处置能力建设

6.1 组织建设

6.1.1 组织架构

机构应制定金融数据安全应急和处置的组织架构，明确应急响应的相关组织或团队的职责分工及相互协作关系，确保及时有效的实施应急响应工作。金融数据安全应急响应与处置组织架构如图2所示。

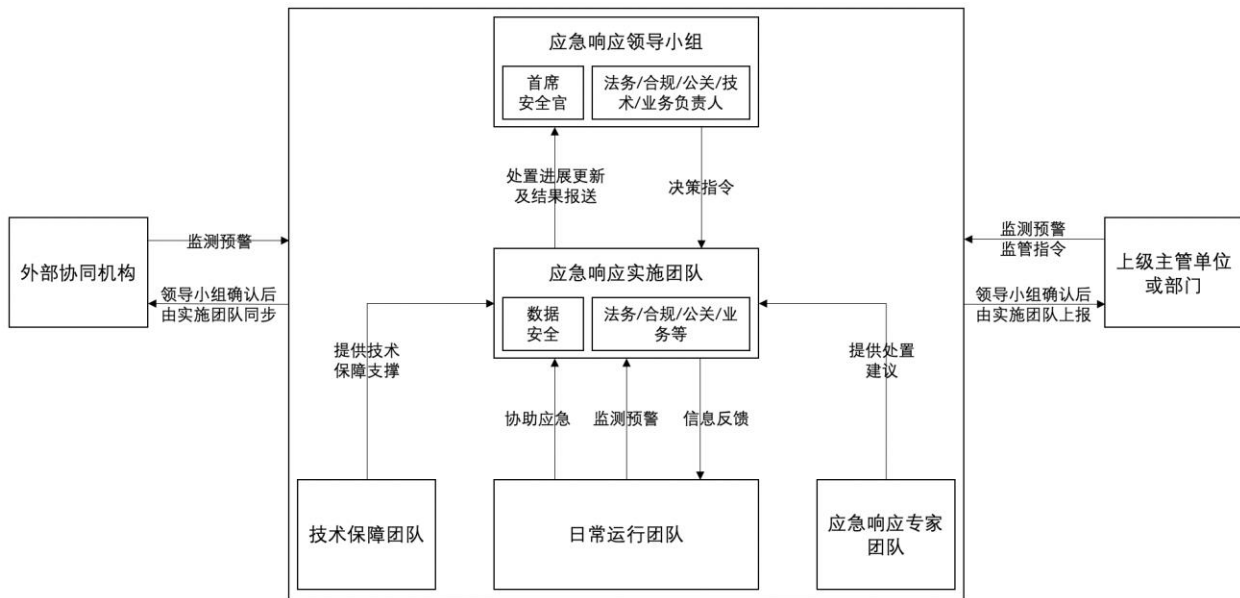


图2 应急响应组织架构

金融数据安全应急和处置组织架构分为外部组织和内部组织两大部分。外部组织包括上级主管单位或部门、外部协同机构：

- 上级主管单位或部门主要负责下发应急响应指令给机构内部的应急响应领导小组，接收机构上报的金融数据安全事件报告或应急处置结果等；
- 外部协同机构主要包括上下游利益相关方、新闻媒体、第三方服务机构等，与机构保持信息沟通和协作，以进行信息互补，必要时协作开展联合应急处置。在事件发生时，能及时通报准确情况并获得相应的支持。

内部组织划分基于GB/T 24363—2009中6.3节的描述，包括应急响应领导小组、应急响应实施团队、技术保障团队、日常运行团队、应急响应专家团队。

6.1.2 应急响应领导小组

应急响应领导小组应至少包含首席安全官、法务负责人、合规负责人、公关负责人、技术负责人、业务负责人，并由首席安全官牵头推进相关工作。主要职责包括：

- 对应急响应工作的承诺和支持，包括发布正式文件、提供必要资源等；
- 审核并批准应急响应策略和计划；
- 批准和监督应急响应计划的执行；
- 负责机构内外部的协调工作；
- 负责高等级安全事件应急处置方案的决策；
- 宣布重大应急响应状态的降级或解除；
- 决定重大的处置措施和新闻报道的重大事项；
- 向上级单位报告应急管理工作情况。

6.1.3 应急响应实施团队

应急响应实施团队，由履行数据安全职责的团队牵头，此外需要至少包含法务应急接口人、合规应急接口人、公关应急接口人、业务应急接口人。另外对于一些大型机构，不同业务部门可能配备有专门的数据安全官，也应纳入应急响应实施团队。主要职责包括：

- a) 贯彻执行应急响应领导小组的工作要求；
- b) 确定应急响应策略和等级；
- c) 制定和实施数据安全事件的具体应急处置工作；
- d) 对数据安全事件影响情况进行分析和评估；
- e) 收集分析对数据安全突发事件应急处置过程中的数据信息和日志；
- f) 向应急响应领导小组报告应急处置进展情况和事态发展情况；
- g) 督促相关部门进行数据安全事件处置的培训及预案的演练；
- h) 负责数据安全事件发生时的损失控制和损害评估。

6.1.4 技术保障团队

技术保障团队的主要职责包括：

- a) 为数据安全事件的处置工作提供基础技术与工具等保障；
- b) 实施数据安全事件的分析排查及溯源；
- c) 协助配合应急响应实施团队及时有效应对数据安全事件。

6.1.5 日常运行团队

日常运行团队的主要职责包括：

- a) 负责日常数据安全的监测工作；
- b) 负责数据备份与恢复的日常管理；
- c) 当数据安全事件发生时，及时报告应急响应实施团队，并协助处置；
- d) 配合支撑数据安全事件发生时的损失控制和损害评估。

6.1.6 应急响应专家团队

应急响应专家团队的主要职责包括：

- a) 对重大数据安全事件进行评估，提出启动应急响应级别的建议；
- b) 研究分析数据安全事件的相关情况及发展趋势，为应急响应提供咨询或提出建议；
- c) 分析数据安全事件原因及造成的危害，为应急响应提供技术支持。

6.2 制度流程

6.2.1 概述

金融数据安全事件应急响应和处置复杂度高，需要内外部多团队协同配合，建立一套完备的应急响应制度流程至关重要。制度流程至少包含数据安全事件应急管理制度、数据安全事件应急演练制度、数据安全风险处置管理指南、数据安全事件应急预案、数据安全事件分类分级标准。

应急响应制度应当明确应急响应目标、原则、范围及各事项管理要求，应与相关利益方就应急响应达成一致。在组织战略、业务流程、客户需求等发生重大变化时，应对应急响应制度进行评审和调整。

6.2.2 数据安全事件应急管理制度

数据安全事件应急管理制度用于定义应急处置全链路的总体要求和标准流程，主要内容包括但不限于：

- a) 数据安全事件应急管理的总体原则；
- b) 数据安全事件应急事件分类和分级定义；
- c) 数据安全事件应急管理组织机构及职责分工；
- d) 应急预案制定要求和应急演练机制要求；

- e) 应急响应处置机制，包括但不限于风险监测预警机制、应急响应及同步机制、应急处置及决策机制、对主管单位或部门报送机制、对媒体及用户信息披露机制；
- f) 数据安全事件复盘整改、定责追责机制。

6.2.3 数据安全事件应急演练制度

数据安全事件应急演练用于检验应急预案的合理性、实用性和可操作性，检验应急准备工作的完备性，锻炼及检验相关组织和团队的配合能力和应急处置能力，进一步完善联动机制，对相关人员进行数据安全宣传教育，提高全员风险防范意识。数据安全事件应急演练制度包括但不限于：

- a) 数据安全事件应急演练原则；
- b) 数据安全事件应急演练形式，如模拟演练、实操演练、专项演练、综合演练等，具体可参考GB/T 38645—2020中第6章描述；
- c) 数据安全事件应急演练规划，包括演练形式、频次、规模、时间、地点等；
- d) 数据安全事件应急演练组织架构策略，包括参与应急演练各团队的职责分工，以及按照事件等级、演练形式、演练规模等，调整不同的团队进行演练；
- e) 应急演练实施过程。

6.2.4 数据安全风险处置管理指南

数据安全风险处置管理指南是通过业务影响分析（BIA）、数据安全风险评估和个人信息保护影响评估，识别机构内金融数据面临的威胁，分析各种威胁发生的可能性，对高影响、高风险的数据安全威胁场景进行风险控制，并基于剩余风险水位，由高到低推进场景化应急预案建设。数据安全风险管理与处置指南主要包括：

- a) 数据安全风险排摸机制以及由此形成的数据安全风险矩阵；
- b) 数据安全风险定级标准；
- c) 数据安全风险处置流程；
- d) 数据安全风险处置时效要求；
- e) 数据安全风险通知对象、升级通知规则、延期处置情形等。

6.2.5 数据安全事件应急预案

6.2.5.1 场景化应急预案

为最大化提升应急效率，需要针对重点场景制定精细化预案。场景化应急预案主要内容包括但不限于：

- a) 具体风险场景、涉及的具体业务或产品、可能发生的数据安全事件的类别和级别；
- b) 应急响应组织及人员；
- c) 完整的应急流程，包括监测预警、分析研判、应急启动、应急处置、应急决策、应急结束、后续处置等环节；
- d) 应急流程中每个环节涉及的操作人、具体执行动作（包含但不限于涉及的工具、系统、模板、口径）、操作时效、输出结果、信息传递方式。

6.2.5.2 应急预案有效性评估

为了确保应急预案的有效性，应针对预案进行有效性评估，并制定优化策略。包括但不限于：

- a) 具体有效性评估流程及规范，应具备可实施性；
- b) 应制定评估要求，包括但不限于应急预案响应时间、业务场景的覆盖率，当应急预案未达到相关要求时，应及时予以优化改进；

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/335013123314011120>