ICS 03.060
CCS A 11

T

团 体 标 准

T/CEATEC XXX—2026

金融数据安全合规要求与应用指南

Guidelines on compliance requirements and application for financial data security

2026-X-XX 发布 2026-X-XX 实施

中国欧洲经济技术合作协会 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》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。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

本文件为首次编制。

金融数据安全合规要求与应用指南

1 范围

本文件规定了金融数据安全合规要求与应用的总则、图计算应用基本要求、数据应用要求、图计算应用流程、应用安全要求、应用效果评估。

本文件适用于金融机构及相关企业在开展反欺诈业务过程中，基于图计算技术进行风险识别、风险预警、欺诈拦截和模型优化的应用系统设计、建设、运维和评估。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 42929 互联网金融智能风险防控技术要求

JR/T 0068 网上银行系统信息安全通用规范

JR/T 0223 金融数据安全 数据生命周期安全规范

3 术语和定义

GB/T 42929界定的以及下列术语和定义适用于本文件。

3.1

金融安全 financial security

指金融体系有效防范各类风险，保障机构稳健运行、市场有序发展、资产安全可控，维护金融消费者权益，防范系统性风险。

3.2

反欺诈风控 anti-fraud risk control

金融机构通过技术、流程、模型等手段，识别、预警、拦截各类欺诈行为，防范资金、声誉及合规风险的管控活动。

3.3

图计算 graph computation

基于风控图结构，对节点和边进行算法处理的过程，包括关系挖掘、路径分析、风险传播和评分计算等。

4 总则

4.1 基本原则

4.1.1 合规性原则

系统建设和应用应符合国家法律法规、金融监管要求及行业规范，数据采集、处理和使用过程应合法合规。

4.1.2 安全性原则

图计算系统部署应符合GB/T 22239的要求，核心金融机构系统应达到三级及以上等级保护标准，核心信息应加密存储，系统应具备容错能力。

4.1.3 准确性原则

图计算模型和风险识别结果应具备较高的准确性和稳定性，避免因误判、漏判对业务造成不良影响。

4.1.4 实时性原则

风控图计算应具备准实时或实时处理能力，满足金融业务高频交易和快速响应的需求。

4.1.5 可扩展性原则

系统架构和模型体系应具备良好的扩展能力，支持业务规模增长和技术升级。

4.1.6 可解释性原则

风险识别结果应具备可追溯性和可解释性，为人工审核、监管检查和业务复核提供依据。

4.2 应用目标

反欺诈风控图计算应用应实现以下目标：

a）构建统一、规范的风控图谱体系，实现多源风险要素的关联整合；

b）提升复杂关联欺诈行为的识别与分析能力；

c）提高风险预警与处置效率，支撑业务实时风控需求；

d）降低误报和漏报风险，提升风控决策精准性；

e）保障系统稳定运行和持续服务能力，满足金融业务7×24小时运行需求；

f）支持模型与规则的持续迭代优化；

g）满足监管合规和审计要求。

5 图计算应用基本要求

5.1 应用环境要求

5.1.1 硬件环境要求

5.1.1.1 服务器

应选用符合金融级安全标准的服务器，支持分布式部署，CPU主频应不低于2.5GHz，内存应不低于128GB，能够支撑海量图数据存储和计算分析。

5.1.1.2 存储设备

应支持海量数据的分层存储（热数据、冷数据分离存储），具备数据备份、恢复功能及数据加密存储能力，数据备份恢复时间应不超过1小时。

5.1.1.3 网络设备

应部署高性能路由器、交换机、防火墙等网络设备，实现网络隔离和访问控制；带宽应满足实时数据传输和图计算分析需求，核心业务链路带宽应不低于10Gbps。

5.1.2 软件环境要求

5.1.2.1 操作系统

应选用安全稳定、适配金融场景的操作系统，定期更新补丁和安全加固。

5.1.2.2 数据库软件

应选用支持海量图结构数据存储和高效计算的图数据库，并定期维护更新。

5.1.2.3 安全软件

应部署防火墙、入侵检测系统、防病毒软件及数据加密软件，并定期更新安全软件病毒库、规则库。

5.2 核心组件适配要求

5.2.1 图计算引擎

图计算引擎适配要求如下：

a）应能够处理大规模节点和边的数据，支持节点排序、路径分析、社区检测和风险传播计算等核心算法；

b）应提供标准化接口，支持业务系统和应用层交互调用计算结果，接口响应时间应不超过200ms；

c）应能够与图数据库、高性能计算平台和数据处理模块高效集成，并行计算效率应不低于80%。

5.2.2 图数据库

图数据库适配要求如下：

a）应能够存储多类型节点和边，支持属性标签和权重信息；

b）应具备高效查询能力，单条查询响应时间不应超过100ms；

c）应具备数据安全、访问控制、备份和恢复功能，支持数据加密存储和操作日志审计。

5.3 风控系统对接要求

5.3.1 图计算应用应能够与现有风控系统、交易系统和业务决策系统对接，实现数据共享和风险信息传递。

5.3.2 图计算应用系统应提供标准化API接口，接口兼容性应符合JR/T 0068的要求。

5.3.3 对接过程中应保证数据安全、访问控制和业务连续性，数据传输应采用TLS 1.3加密方式，设置接口调用权限，避免数据泄露和非法访问。

6 数据应用要求

6.1 数据来源要求

6.1.1 反欺诈风控图计算应用所使用的数据来源应合法、合规，并符合国家有关法律法规及金融监管要求。

6.1.2 数据来源宜包括交易数据、账户数据、设备数据、行为数据、身份信息数据及外部风险数据等。

6.1.3 内部业务数据应来源于核心业务系统、支付系统、信贷系统及客户管理系统等。

6.1.4 外部数据应来源于合法授权的征信机构、行业共享平台及第三方数据服务机构，并应明确数据使用范围和期限。

6.1.5 数据采集过程应具备可追溯性，能够记录数据来源、采集时间及处理过程等关键信息。

6.2 数据质量要求

6.2.1 用于图计算分析的数据应满足完整性、准确性、及时性、一致性和可用性要求。

6.2.2 数据缺失率应控制在5%以内，关键业务字段缺失率不应超过1%。

6.2.3 数据重复率应低于2%，对于高频交易类数据，应采取去重和校验机制。

6.2.4 数据逻辑一致性错误率应低于0.5%，异常数据应及时识别和修正。

6.2.5 应建立数据质量监测机制，对异常数据进行定期检测、分析和处理。

6.3 数据处理要求

6.3.1 采集后的原始数据应经过清洗、标准化、脱敏、特征提取等处理，处理过程应符合JR/T 0223的要求。

6.3.2 数据关联处理应基于统一的身份标识规则，实现账户、设备、人员及交易行为之间的有效关联。

6.3.3 图结构构建前，应对节点和边进行属性补全和权重计算。

6.3.4 数据处理过程应支持自动化和批量化处理，并具备异常回滚和恢复能力。

6.4 数据存储与使用要求

6.4.1 图计算应用中的业务数据、关系数据及分析结果应分类存储，并实施分级管理。

6.4.2 数据存储系统应支持高可靠性和高可用性部署，数据可用率宜不低于99.9%。

6.4.3 重要业务数据和分析结果应进行定期备份，备份周期宜不超过24 h。

6.4.4 数据访问应实行权限控制机制，按照“最小授权原则”分配访问权限。

6.4.5 数据使用应符合用途限定原则，不应超出反欺诈风控应用范围进行二次利用。

6.4.6 数据使用过程应全程留痕，实现访问记录、操作记录和审计记录的可追溯管理。

6.4.7 用户基础数据、交易数据留存期限应不低于5年，风险决策数据留存期限应不低于3年，临时数据留存期限应不超过30天，到期数据应及时清理或脱敏处理。

7 图计算应用流程

7.1 数据采集

7.1.1 应根据反欺诈业务需求，统一规划数据采集范围和采集方式。
7.1.2 数据采集应覆盖交易行为、账户信息、设备信息、关系信息及历史风险记录等关键要素。
7.1.3 数据采集应纳入业务流程管理体系，明确采集责任主体和操作规范。
7.1.4 实时采集与批量采集应结合使用，保障业务运行的时效性和完整性。
7.1.5 数据采集过程应符合数据安全和合规管理要求。

7.2 数据处理

7.2.1 数据采集完成后，应按照第6章有关要求对数据进行统一处理。
7.2.2 数据处理环节应作为图计算应用的必要前置流程进行统一管理。
7.2.3 数据处理过程应形成标准化作业规范，并纳入系统自动化运行机制。
7.2.4 处理完成的数据应经校验确认后方可进入后续应用流程。
7.2.5 不符合数据应用要求的数据，应及时进行补充处理或重新采集。

7.3 图结构构建

7.3.1 应基于业务实体及其关联关系构建风险关联网络模型。
7.3.2 图结构构建应遵循统一建模规则，明确节点类型、关系类型及属性定义。
7.3.3 图结构应能够反映用户、账户、设备、交易等要素之间的实际关联特征。
7.3.4 图结构更新应支持周期性更新与增量更新相结合的方式，批量更新时间应不超过2小时，增量更新延迟应不超过500ms。
7.3.5 图结构构建过程应形成标准化管理文档。

7.4 图计算分析

7.4.1 图计算分析应围绕风险发现、关系挖掘和团伙识别等业务目标开展。
7.4.2 应根据业务场景选择适宜的图计算方法和分析策略。
7.4.3 图计算任务应纳入统一调度和监控管理体系，明确计算任务的执行时间、优先级和处理流程，实时监控计算任务的执行状态，及时处理计算异常。
7.4.4 异常计算结果应及时进行复核和校正，组织风控人员对异常结果进行人工审核，分析异常原因，优化计算算法和参数，提升计算分析的准确性。

7.5 风险预警

7.5.1 应基于图计算分析结果建立风险预警机制，明确预警指标、预警阈值和预警等级。
7.5.2 风险预警应按照统一标准进行分级管理，分为高、中、低三个预警等级。
7.5.3 预警信息应及时推送至相关业务系统和管理平台，推送延迟应不超过1分钟。
7.5.4 风险预警规则应定期评估和调整，每季度应至少开展1次预警规则评估。
7.5.5 预警记录应完整保存并具备可追溯性，留存期限不低于3年。

7.6 欺诈拦截

7.6.1 对识别出的高风险行为，应按照业务管理要求及时采取处置措施。
7.6.2 拦截措施应兼顾风险防控效果和客户服务体验。
7.6.3 拦截策略应支持自动化和人工干预相结合，高风险交易应自动拦截，中风险交易人工审核后决定是否拦截。
7.6.4 拦截过程应形成规范化操作记录，对误拦截事件应建立快速纠偏机制。

7.7 结果反馈

7.7.1 应建立风险处置结果反馈机制，反馈信息应在处置完成后1小时内回传至图计算应用系统。
7.7.2 反馈流程应明确责任主体和处理时限，一般反馈数据的处理时限不应超过24小时，重大风险反馈的处理时限不应超过2小时。
7.7.3 反馈数据应纳入统一管理体系，分类存储和分析，形成反馈报告，定期总结反馈结果，为后续应用优化提供参考。

7.8 模型优化

7.8.1 应基于业务反馈和运行效果对图模型进行持续优化，模型迭代周期应不超过7天，重大欺诈手段出现时应立即启动迭代。
7.8.2 模型优化应包括结构调整、参数优化和规则修订等内容。
7.8.3 优化过程应形成完整评估和验证机制，优化后的模型应通过测试验证后投入使用。
7.8.4 模型迭代过程应具备完整文档记录，记录迭代原因、优化内容、测试结果等信息，便于模型追溯和监管检查。

8 应用安全要求

8.1 安全管理制度要求

8.1.1 应建立图计算应用安全管理制度，明确安全管理目标、职责分工和工作流程。
8.1.2 应制定数据安全、系统运行、访问控制和应急处置等专项管理制度。
8.1.3 安全管理制度应定期评估和修订，每年应至少开展1次制度评估，适应业务发展和监管要求变化。

8.2 运行安全要求

8.2.1 应建立系统运行监测机制，对关键运行指标进行持续监控。
8.2.2 应定期开展运行风险排查，每月至少开展1次常规排查，每季度开展1次全面排查，及时发现和消除安全隐患。
8.2.3 关键业务环节应设置运行保障措施，防止单点故障影响业务连续性。
8.2.4 系统应具备故障自动切换能力，切换时间应不超过30秒。
8.2.4 系统运行状态异常时，应及时启动应急处置机制，组织技术人员排查故障，采取应急措施，恢复系统正常运行，同时记录故障原因、处置过程和处置结果，形成应急处置报告。

8.3 人员与操作安全要求

8.3.1 应对从事图计算应用开发、运维和分析工作的人员实施分类管理，明确不同岗位的职责和权限，建立岗位责任制，避免权限交叉和越权操作。
8.3.2 关键岗位人员应定期接受安全培训和合规教育，每年培训时长应不低于40学时，提升人员安全意识和合规意识，掌握安全操作技能。
8.3.3 应建立岗位轮换和权限复核机制，关键岗位人员每2年至少轮换1次，每季度开展1次权限复核，防范内部操作风险。
8.3.4 人员变动时，应及时完成权限调整和安全交接。

9 应用效果评估

9.1 评估指标

主要应用效果评估指标如下：
a）基于图计算识别的欺诈行为中，实际被确认的欺诈事件占比应不低于90%；
b）系统识别为高风险但经核实为正常业务的比例应不高于6%；
c）从风险触发到图计算分析并输出风险结果的响应时间应不高于200 ms；
d）图计算应用系统年度可用性应不低于99.5%；
e）基于业务反馈和评估结果的模型或规则更新周期应不超过3个月。

9.2 评估流程与方法

9.2.1 评估周期

每季度开展1次常规评估，每年开展1次全面评估，系统重大升级或新型欺诈手段出现后，额外开展专项评估。

9.2.2 评估方法

应用效果评估可采用以下方法：

a）历史样本验证法：利用已确认的历史欺诈样本和正常样本，对图计算识别效果进行验证；

b）对比评估法：将引入图计算前后的风控效果进行对比分析，评估应用改进效果；

c）在线监测评估法：对系统运行过程中的实时指标进行持续监测和统计分析；

d）人工复核评估法：结合人工审核结果，对图计算识别结论的合理性进行验证。