ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0199—2020

金融科技创新安全通用规范

Security general specification for FinTech innovation

2020－10－21 发布　　2020－10－21 实施

中国人民银行　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。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国人民银行科技司、中国人民银行南京分行、中国人民银行营业管理部、中国人民银行深圳市中心支行、中国支付清算协会、中国互联网金融协会、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行有限公司、中国金融电子化公司、北京银联金卡科技有限公司、北京中金国盛认证有限公司、北京金融科技产业联盟、交通银行股份有限公司、中国人寿财产保险股份有限公司、中信银行股份有限公司、中国民生银行股份有限公司、招商银行股份有限公司、广发银行股份有限公司、上海浦东发展银行股份有限公司、渤海银行股份有限公司、中国银联股份有限公司、上海银行股份有限公司、成都银行股份有限公司、重庆银行股份有限公司、苏州银行股份有限公司、杭州银行股份有限公司、重庆农村商业银行股份有限公司、上海华瑞银行股份有限公司、深圳前海微众银行股份有限公司、浙江网商银行股份有限公司、四川新网银行股份有限公司、传化支付有限公司、百行征信有限公司、工银科技有限公司、建信金融科技有限公司、兴业数字金融服务（上海）股份有限公司、华为软件技术有限公司、腾讯云计算（北京）有限责任公司、京东数字科技控股股份有限公司、度小满（重庆)科技有限公司、中金金融认证中心有限公司。

本文件主要起草人：李伟、潘润红、李兴锋、张宏基、但孝磊、丁华明、李健、渠韶光、于园、汤沁瑾、孙维挺、黄梦达、侯晓晨、贾铮、刘力慷、李博文、孙茂增、黄本涛、赵计博、周钰博、祁永、吴奕、徐激、孙昊、朱永红、马懿、钱卫星、刘炀、罗瑞、王若虹、李烨、吴峰、赵永、马杰、杨涛、白云飞、陈庆来、韩毅、李大栩、任雯雯、张德玮、傅杰、张奕华、朱一鸣、孙涵、杜霞、顾爱霞、何韬、佘科、李微羽、徐建芳、卢华玮、陈勤伟、李斌、黄超、李秀生、张勇钢、郭胜基、丁君之、何方竹、李洋、杜明灯、黄淼、范义鹏、吴同亮、孙越。

金融科技创新安全通用规范

1 范围

本文件规定了金融科技创新的基本安全要求，包括交易安全、服务质量、业务连续性、算法安全、架构安全、数据安全、网络安全、内控管理等。

本文件适用于从事金融服务创新的持牌金融机构，也适用于从事相关业务系统、算力存储、算法模型等科技产品研发的科技公司以及安全评估机构等。

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 20988 信息安全技术 信息系统灾难恢复规范

GB/T 22240 信息安全技术 网络安全等级保护定级指南

JR/T 0044 银行业信息系统灾难恢复管理规范

JR/T 0071 金融行业信息系统信息安全等级保护实施指引

JR/T 0118—2015 金融电子认证规范

JR/T 0166 云计算技术金融应用规范 技术架构

JR/T 0167 云计算技术金融应用规范 安全技术要求

JR/T 0168 云计算技术金融应用规范 容灾

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0193—2020 区块链技术金融应用 评估规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融科技创新应用 fintech innovation

在符合现行法律法规、部门规章、规范性文件等要求前提下，在尚不具备管理细则的领域，利用新技术设计、面向金融用户的产品或服务。

3.2

金融科技创新机构 fintech innovation institution

从事金融服务创新的持牌金融机构及从事相关业务系统、算力存储、算法模型等科技产品研发的科技公司。

3.3

个人金融信息 personal financial information

金融科技创新机构通过提供金融服务或科技产品等方式获取、加工和保存的个人信息。

注1：本文件中的个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

注2：改写JR/T 0171—2020，定义3.2。

3.4

业务连续性 business continuity

在中断事件发生后，组织在预先确定的可接受的水平上连续交付产品或提供服务的能力。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

APP：客户端应用软件（Application Software）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）

IP：网际互连协议（Internet Protocol）

LQA：可接受的最低质量(Lowest Quality Acceptable)

QoS：服务质量（Quality of Service）

RPO：恢复点目标（Recovery Point Objective）

RTO：恢复时间目标（Recovery Time Objective）

SDK：软件开发工具包（Software Development Kit）

UPS：不间断电源（Uninterruptible Power System）

Web：全球广域网（World Wide Web）

5 交易安全

5.1 交易验证

a) 交易验证可以组合选用下列3类要素：
   ——仅客户本人知悉的要素；
   ——仅客户持有并特有的，不可复制或者不可重复利用的要素；
   ——客户本人生物特征要素。

b) 交易验证要素的使用，应满足以下要求：
   ——应确保采用的要素相互独立，即部分要素的损坏或者泄露不应导致其他要素损坏或者泄露；
   ——应严格限制使用初始交易密码并提示客户及时修改，建立交易密码复杂度校验机制，避免交易密码过于简单（如“111111”、“123456”等）或与个人金融信息（如出生日期、证件号码、手机号码等）相似度过高；
   ——采用数字证书、电子签名作为认证要素的，数字证书及生成电子签名的过程应符合相关法律法规、JR/T 0118—2015 等有关规定，确保数字证书的唯一性、完整性及交易的抗抵赖性；

——采用一次性密码作为验证要素的，应切实防范一次性密码获取端与交易指令发起端为相同物理设备而带来的风险，并将一次性密码有效期严格限制在最短的必要时间内；
——采用客户本人生物特征作为验证要素的，应符合国家、金融行业标准和相关信息安全管理要求，防止被非法存储、复制或重放；
——应采取交易验证强度与交易额度相匹配的技术措施，提高交易的安全性；
——应经过客户确认并进行交易验证，交易验证宜同时采用上述3类要素中的两类要素，不足2类的应采取相应的风险补偿措施。

5.2 交易确认

交易确认应满足以下要求：

a) 应采取有效措施，确保客户在执行交易指令前可对交易内容、交易金额等交易信息进行确认，并在交易指令完成后展现交易信息或及时将结果通知客户。
b) 应确保交易信息的真实性、完整性、可追溯性以及在交易全流程中的一致性，不得篡改或者隐匿交易信息。
c) 应采用静态密码、动态口令、数字证书等可靠的技术手段实现本人主动确认，保障用户的知情权、财产安全权等合法权益。

5.3 交易监控

5.3.1 交易监控系统建立

金融科技创新机构应建立有效的交易监控系统，满足以下要求：

a) 应建立交易监控系统，能够甄别并预警潜在风险的交易，并生成风险监控报告。
b) 应根据交易的风险特征建立风险交易模型，有效监测可疑交易，对可疑交易建立报告、复核、查结机制。
c) 应采用大数据分析、客户行为建模等手段，建立交易风险监控模型和系统，对异常交易进行及时预警，并采取调查核实、风险提示、延迟结算等处理措施。
d) 应通过交易行为分析、机器学习等不断优化风险评估模型，提高欺诈交易拦截成功率，降低误判率，切实提升交易安全防护能力。

5.3.2 交易风险识别

金融科技创新机构应支持欺诈风险和合规风险的识别。

a) 欺诈风险指不法分子利用虚假申请、伪造或变造、盗用账户等手段盗取交易资金的风险，是非用户本人意愿发起的交易，或者不法分子勾结用户通过虚构交易等方式造成金融机构资金、权益等方面损失的风险，包括但不限于：
——非面欺诈，指欺诈分子窃取或骗取账号、PIN、有效期、短信验证码及其他关键身份验证信息后，通过邮购/电购、互联网、手机等非面对面渠道进行欺诈冒用；
——账户盗用，指欺诈分子冒充真实账户所有人的身份，通过修改账单地址、虚假挂失等一系列手段获取重制账户信息进行的欺诈交易；
——伪冒申请，指使用虚假身份或冒用他人身份开立账户完成欺诈交易；
——商户合谋，指特约商户在受理交易时，违规操作、蓄意进行欺诈交易或纵容、包庇、协助账户所有人开展欺诈交易的行为；
——营销欺诈，指不法分子利用营销主办方的营销漏洞，与商家勾结、虚构交易，骗取营销活动主办机构的营销费用，获得不正当收益。

b) 合规风险指虽然是用户本人意愿发起的交易，但该交易行为违反国家法律法规和监管要求，属于禁止的或不当的交易行为，包括但不限于：

——洗钱风险，指将通过各种手段掩饰违法所得，隐瞒违法来源，使其在形式上合法化，常见于毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪、金融诈骗犯罪等各类违法犯罪过程；

——电信诈骗，指不法分子通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人本人给不法分子汇款、转账、购物或代付等的犯罪行为，从而给受害人造成资金和权益方面的损失；

——非法集资，指单位或者个人未依照法定程序经有关部门批准，以发行股票、债券、彩票、投资基金证券或者其他债权凭证的方式向社会公众筹集资金，并承诺在一定期限内以货币、实物以及其他方式向出资人还本付息或给予回报的行为；

——移机切机，指交易终端出现了不正当的位置移动，以及被非法接入其他收单机构，发生与注册登记信息不符的行为。

5.3.3 交易风险处置

金融科技创新机构应建立交易风险处置机制。交易风险处置是在风险决策结束后进行的评估反馈、风险核查、关联排查、案件协查和损失处置的相关后续活动。风险处置的结果旨在完善现有风险防控的策略、风险信息处理的内容与交易风险评估的能力，实现风险防控流程的闭环反馈优化。

a) 风险核查指基于风险评估和决策输出的结果，对于已识别存有风险的业务进行调查，分析原因与风险特征，以确认当时的决策是否准确恰当，包括但不限于以下方式开展：

——对于拦截阻断的交易：

- 应配套后续调查流程完善防控手段；
- 宜与业务方进行确认，判断拦截阻断的准确性；
- 经调查拦截无误的，相关信息可纳入黑灰名单和负面样本，作为后续优化事中监测依据；
- 经调查拦截不准确的，宜恢复交易权限，及时调整事中监测策略。

——对于挂起确认和提示预警的交易：

- 应配套调查处置流程，并借鉴简化后续类似情况下的处理流程；
- 可事后统计分析存在的可疑点，集中与业务方沟通确认，回溯挂起确认和提示预警的必要性与准确性，并判断下一次类似条件的业务风险处理方式。

b) 关联排查指对于存有风险的业务相关元素，基于潜在关系进行关联分析，以挖掘是否存在同类风险或衍生风险，弥补事中监测决策可能未识别的潜在风险敞口，关联排查包括但不限于以下方式开展：

——应对存在风险交易的同账户关联交易进行分析。

——应对存在信息泄露风险的用户在一段时间内有交易的账户进行分析。

——宜对存在虚假申请风险的账户关联的设备信息进行分析。

——宜对存在风险交易的账户或者所属用户的位置信息进行分析。

——宜对存在风险交易的手机号码进行分析，包括验证手机号码、注册手机号码等。

c) 案件协查主要是指配合公安、司法机关开展的风险案件协查，包括但不限于以下方式开展：

——应对公安、司法机关提供必要的交易明细。

——应对公安、司法机关提供必要的用户开户获批的相关信息。

——应根据公安、司法机关的指令冻结账户和资金。

——宜对公安、司法机关提供已采集的交易信息、账户信息以外的风险案件行为特征，例如

IP、MAC 等。

d) 损失处置主要指对于明确产生的风险损失，通过快速挽损、风险责任认定，将风险化解、转移或者赔偿的处置方式，并控制后续风险损失敞口，可采取的主要方法包括但不限于：
——延迟结算：采取结算资金延迟到账方式挽回损失。
——货物拦截：针对互联网渠道实物类商品销售付款与收货存在较长时间的特性，在风险识别后及时控制在途货物，采取退款措施，控制风险损失敞口。
——追偿结算：通过事后损失追偿，转移化解已有风险损失。
——限制功能：针对识别的具有高风险特征的交易行为，对相关资金账户、商户终端采取限制交易权限措施。
——关闭通道：关闭交易通道，防范新增损失。
——保险赔付：通过事先投保、事后理赔方式，分散化解风险损失。
——法律诉讼：通过提起法律诉讼方式，解决风险责任认定和损失处置争端，转移化解风险损失。

6 服务质量

金融科技创新机构应建立有效的服务质量管理机制，满足以下要求：

a) 应建立服务质量管理规范，包括 QoS 预测、QoS 建立、QoS 监控、QoS 维护等过程管理。
b) 应通过对创新应用的业务功能、预期用户数、服务地域、服务时间等特性进行充分分析，从服务可用性、吞吐量、时间延迟等方面预测 QoS。
c) 应以满足用户或相关方的业务期望为基础，根据具体资源情况建立 QoS 目标，设置可接受最低质量（LQA）极限。
d) 应对通信线路、网络设备、主机设备、应用软件的运行情况进行 QoS 监控，检查服务可用性、吞吐量、时间延迟等是否满足 QoS 目标，对系统的服务水平低于 LQA 时进行预警。
e) 应在可接受的级别上为满足 QoS 进行资源分配。

7 业务连续性

7.1 业务影响分析

金融科技创新机构应根据业务连续性目标和业务发展规划，对金融科技产品及其服务模式进行详细的业务影响分析，满足以下要求：

a) 应根据当前的业务场景，使用恰当的分析方法，对所面临的威胁和当前体系的脆弱性进行深入剖析，评估各类风险发生的概率和可能导致的损失。
b) 应对风险可能造成的业务影响进行研判。
c) 应根据监管要求、业务性质、业务服务范围、数据集中程度、业务时间敏感性、功能关联性等要素进行业务功能分析，并在此基础上评估业务中断可能造成的影响，确定灾难恢复目标及恢复优先级。

7.2 业务连续性管理

金融科技创新机构应采取有效的业务连续性管理措施，满足以下要求：

a) 应制定业务连续性策略及计划。
b) 应从应用和数据等技术方面确保业务连续性，避免单点故障。

c） 应将业务连续性管理整合到组织的流程和架构中，明确指定相关部门负责业务连续性的管理。
d） 应制定员工在业务连续性方面的培训计划和考核标准。
e） 应定期或在业务系统发生显著变化时，测试并更新业务连续性计划与过程，以确保其持续有效。
f） 应至少每年组织 1 次业务连续性专项内部审计或委托第三方进行的审计，并形成包括审计意见、改进计划和改进结果的审计报告。
g） 使用的科技产品应至少支持容灾能力 3 级要求，容灾等级划分及关键指标要求参见附录。

7.3 业务连续性资源配置

金融科技创新机构应采取有效的业务连续性资源配置措施，满足以下要求：
a） 应避免机房采用的多路市电输入均来自于同 1 个变电站，应对 UPS 等重要设备的报警日志进行及时审核和处理。
b） 应提供冗余通信线路，并选择与主用通信线路不同的电信运营商和不同的物理路径。
c） 核心层、汇聚层的设备和重要的接入层设备均应双机热备或多机集群，例如，核心交换机、服务器群接入交换机、重要业务管理终端接入交换机、核心路由器、防火墙、均衡负载器、带宽管理器及其他相关重要设备。
d） Web 服务器、中间件服务器、前置服务器、数据库服务器等关键数据处理系统均应双机热备或多机集群，并设置磁盘冗余阵列或分布式多副本存储技术，以避免单一部件故障影响设备运行的风险。
e） 应梳理并维护关键的设备部件、备件清单，采取有效的措施防止因单个设备部件出现故障，导致冗余设备无法正常启用或切换的风险。

7.4 备份与恢复管理

金融科技创新机构应采取有效的备份与恢复管理措施，满足以下要求：
a） 应根据系统的业务影响性分析结果，制定不同数据的备份策略，并实施应用级备份，以保证灾难发生时，能尽快恢复业务运营。
b） 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存，明确规定备份数据的保存期，做好备份数据的销毁申请、审查和登记工作。
c） 应定期执行恢复程序，检查并测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份恢复。
d） 应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果，以满足灾难恢复策略的要求。
e） 应在统一的灾难恢复策略下建立完善的系统灾难恢复体系，开展灾难恢复需求分析、策略及计划制定、灾备系统建设及演练等工作，并根据实际情况对其进行分析和改进，确保各环节的正确性以及灾难恢复体系的有效性。
f） 同城数据备份中心应保证可以接管所有核心业务的运行，与生产中心直线距离应满足 JR/T 0071 相关安全技术要求。
g） 异地数据备份中心与生产中心直线距离应满足 JR/T 0071 相关安全技术要求。
h） 应实时监控生产中心和灾备中心的业务应用可用性和性能状态，并具备告警功能。
i） 应能够有效监控灾备切换过程和同步状态。

7.5 应急预案及演练

金融科技创新机构应建立有效的业务连续性应急预案及演练机制，满足以下要求：
a） 应建立业务连续性预案程序，预案应包括应急和系统灾难恢复两部分，具体要求如下：

——应急部分包括但不限于灾难场景和范围定义、应急的管理机构和决策机制、应急响应的流程、工具和工作制度等内容；

——系统灾难恢复部分包括但不限于灾难恢复的范围和目标、灾难恢复的总体规程、各系统恢复的切换步骤、操作手册和业务功能恢复验证测试方法等内容。

b) 应建立应急预案演练制度，定期开展应急演练培训，定期组织有业务部门参与的桌面演练和生产系统实战演练，定期对双机热备系统进行切换演练，备份系统与生产系统的切换要至少每年演练 1 次。针对 DDoS、数据窃取泄露等重要安全威胁，定期开展有相关单位、部门参与的联合演练。

c) 应急和灾难恢复流程应避免数据泄露的风险。

8 算法安全

8.1 算法设计

算法设计应满足以下要求：

a) 应正确定义目标函数，避免目标函数错误导致决策偏离预期甚至出现伤害性结果。

b) 应避免算法目标函数运算成本过高，确保算法目标函数运算的占用资源不会使整体运行效率明显降低。

c) 算法表达能力应充分，避免算法在实际使用时面对不同于训练阶段的全新情况产生错误的结果。

d) 应避免应用于金融业务中的算法存在因设计者和开发者的主观选择造成的偏见决策结果。

e) 应避免应用于金融业务中的算法存在因客观训练数据造成的偏见决策结果。

f) 应根据不同业务场景需要设计对应的算法或者模型。

8.2 算法可解释性

算法可解释性应满足以下要求：

a) 特征变量若从业务出发，其定义应满足相关业务逻辑和规则。

b) 特征分布应符合人的常识和业务规则，尽量避免特征变量的值是异常数据点。

c) 应明确记录特征选择的业务逻辑和算法依据。

d) 应能够标识代表性样本或非代表性样本，并对其进行相关说明。

e) 在模型构建过程中，应根据具体业务场景和具体算法，至少定义 1 项具体的指标来度量可解释性。

f) 应避免科技产品中的算法存在非公开性、算法复杂性造成的决策结果不可解释的问题。

g) 应通过代码注释等方式提高算法的可读性。

8.3 算法可追溯性

算法可追溯性应满足以下要求：

a) 应记录训练数据获取时间、训练数据量、数据存储介质标识。

b) 应对使用的训练数据有完整签名或校验码。

c) 应保存建模过程中建模脚本及参数迭代的相关记录。

d) 应对建模过程的操作者进行标识，记录建模的起止时间戳和迭代次数。

e) 应记录算法模型部署的操作者，标识部署时间及相关结果。

f) 应保存算法模型部署的相关脚本。

8.4 算法攻击防范

算法攻击防范应满足以下要求：

a) 应加强算法关于训练数据、模型的传输、存储等方面的安全管理，防范训练数据、模型被窃取。
b) 应保障算法训练步骤安全，防范训练过程被窃取导致训练信息泄露，进而恶意构建相似模型。
c) 算法模型应具有辨识度，如模型添加水印等，通过合适途径辨别恶意伪构模型。
d) 应确保训练数据来源可信、可靠，避免采集到标签错误等恶意药饵数据。
e) 应确保训练数据分布合理，防止药饵攻击数据点混入，造成模型倾斜等错误状况。
f) 在满足用户需求的前提下，算法模型输出的反馈信息应遵循最小够用的原则，避免泄露信息过多造成逆向攻击。
g) 应通过限制攻击者对人工智能算法测试频率，避免恶意探测获取人工智能算法信息，逆向构建恶意模型。

9 架构安全

9.1 云计算架构

金融科技创新机构使用的云计算架构应符合JR/T 0166、JR/T 0167、JR/T 0168等的相关要求。

9.2 区块链架构

金融科技创新机构使用的区块链架构应符合JR/T 0193—2020的相关要求。

10 数据安全

10.1 数据质量

金融科技创新机构应建立有效的数据质量管理措施，满足以下要求：

a) 应对数据进行分类管理，明确不同数据之间的关系和依赖性，制定数据质量管理目标。
b) 应明确数据质量管理部门和机制，定义数据质量管理的角色和职责，建立数据质量管理办法。
c) 应研发数据质量相关技术，支撑数据质量管理和数据质量提升。
d) 应识别数据生命周期各个阶段的数据质量关键因素，构建数据质量评估框架，包括但不限于数据的准确性、完整性、一致性、可访问性、及时性、相关性和可信度等。
e) 应采用定性评估、定量评估或综合评估等方法，评估和持续优化数据质量。

10.2 个人金融信息保护

10.2.1 全生命周期防护

金融科技创新机构应从个人金融信息采集、传输、存储、使用、删除、销毁等方面建立全生命周期防护措施，符合JR/T 0171—2020的相关要求。

10.2.2 安全管理

金融科技创新机构应从安全策略、访问控制、监测评估、事件处理等方面建立个人金融信息安全管理措施，符合JR/T 0171—2020的相关要求。

11 网络安全

11.1 基本安全要求

金融科技创新机构应按照GB/T 22240进行定级，并满足JR/T 0071中对应等级的要求。

11.2 物联网安全要求

11.2.1 感知终端安全

感知终端安全应考虑物理安全、接入安全、通信安全、设备安全等内容，满足以下要求：

a) 应在防盗窃防破坏、防水防潮、防极端温度、防震防灾等方面满足部署的要求。
b) 应在接入网络中具有唯一网络身份标识。
c) 应设置网络访问控制策略，限制对感知终端的网络访问。
d) 应具有并启用通信完整性校验机制，实现数据传输的完整性保护。
e) 应具有通信延时和中断的处理机制。
f) 应能控制数据的本地或远程访问。
g) 具有操作系统的感知终端应能控制操作系统用户的访问权限。
h) 具有操作系统的感知终端应能为操作系统事件生成审计记录，审计记录应包括日期、事件、操作用户、操作类型等信息。
i) 具有操作系统的感知终端应仅安装经授权的软件。
j) 具有操作系统的感知终端应按照策略进行软件补丁更新和升级，且保证所更新的数据来源合法和完整。
k) 感知终端在传输其所采集的数据时，应对数据新鲜性做出标识。
l) 感知终端应为其采集的数据生成完整性证据（如校验码、消息摘要、数字签名等）。
m) 应能自检出已定义的设备故障并进行告警，确保设备未受故障影响部分的功能正常。

11.2.2 感知层网关安全

感知层网关安全应考虑设备安全、入侵防范、运维管理等内容，满足以下要求：

a) 应具备基本的防火、防潮、防水等的措施。
b) 应能够对感知终端进行鉴别。
c) 应保证密钥存储和交换安全。
d) 应支持访问控制表（ACL）等访问控制策略，防止资源被非法访问和非法使用。
e) 应对感知层网关中存储的重要数据进行保护，避免非授权的访问。
f) 应具备对传输数据完整性校验机制，实现隐私数据、重要业务数据等重要数据的传输完整性保护（如：校验码、消息摘要、数字签名等）。
g) 应能控制感知层网关用户的访问权限，并避免权限的扩散。
h) 应提供安全措施对感知层网关进行远程配置。
i) 身份鉴别失败时，应记录用户的身份和所使用的访问设备的标识。
j) 协议转换失败时，应记录转换数据包的来源和时间。

11.3 安全防护要求

11.3.1 仿冒钓鱼

金融科技创新机构应采取有效的仿冒钓鱼防护措施，满足以下要求：

a) APP 安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。

b) APP 应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。
c) 客户端代码应使用代码加壳、代码混淆、检测调试器等手段对 APP 进行安全保护。
d) 应采取渠道监控等措施对仿冒客户端程序进行监测。
e) 网站应具有防网络钓鱼的安全提示功能，例如显示客户预留信息、客户自定义个性化界面等。
f) 应具备钓鱼攻击监测能力，例如增加客户端提交的页面来源地址信息的校验、设置转账白名单等。
g) 应采取防钓鱼网站控件、钓鱼网站监控工具、钓鱼网站发现服务等技术措施，建立钓鱼网站案件报告及快速关闭钓鱼网站的处置机制。

11.3.2 安全漏洞管理

金融科技创新机构应采取有效的安全漏洞管理措施，满足以下要求：
a) 应考虑功能逻辑设计的合理性，避免逻辑漏洞。
b) 应避免调用存在安全漏洞的函数、组件。
c) 应进行开源系统或组件的安全评估，及时进行漏洞修复和加固处理。
d) 应在设计和开发阶段避免网站、客户端、SDK、API 等存在常见漏洞，包括但不限于：
——穷举尝试漏洞：
- 采取限制错误登录次数、设置图形验证码等方式防止穷举登陆尝试；
- 图形验证码应随机产生，采取图片底纹干扰、颜色变换、设置非连续性及旋转图片字体、变异字体显示样式、交互式认证等有效方式，防止验证码被自动识别；
- 应具有使用时间限制并仅能使用 1 次；
- 应由服务器生成，客户端源文件中不应包含验证码文本。

——重放漏洞：采取有效措施防范重放攻击，例如，在登录交互过程提交的认证数据中增加服务器生成的随机信息成分。
——注入漏洞：
- 服务器应用程序应对客户提交的所有表单、参数进行有效的合法性判断和非法字符过滤，防止攻击者恶意构造语句实施注入攻击；
- 不应仅在客户端以脚本形式对客户的输入进行合法性判断和特殊字符过滤；
- 数据库应尽量使用存储过程或参数化查询，并严格定义数据库用户的角色和权限。

——跨站脚本漏洞：应通过严格限制客户端可提交的数据类型、对提交数据进行有效性检查、设置响应头防护参数、对输出信息进行编码等措施防范跨站脚本注入攻击。
——文件上传下载漏洞：对文件的上传和下载进行访问控制，避免攻击者执行恶意文件或发起未授权访问。
——缓冲区溢出漏洞：应使用安全的函数、方法，防止程序代码对缓冲区的错误利用。
——非法提权漏洞：应检查用户与访问资源的权限关系，防止用户访问非本人的资源。
——逆向工程漏洞：应采取措施防范逆向分析导致关键业务逻辑泄露。
e) 应在金融科技创新应用上线前进行源代码安全审计、渗透测试，及时处理安全漏洞，有效控制安全风险。
f) 应对金融科技创新应用进行定期及变更时的漏洞扫描，及时修补发现的系统安全漏洞。
g) 应建立紧急补丁（应急方案）的开发、发布流程，以备必要时提供紧急补丁或应急方案进行处理，以修补重要安全漏洞。

11.3.3 网络攻击防护

金融科技创新机构应采取有效的网络攻击防护措施，满足以下要求：

a) 应对客户端软件、网站、API 和 SDK 的常见网络攻击，包括但不限于穷举登录尝试、重放攻击、注入攻击、跨站脚本攻击、文件上传下载攻击、非法提权、逆向工程等，进行监测、识别和阻断。
b) 宜针对设备、IP、账号等建立关联关系，利用社群发现、风险传播等方式精准防御团伙欺诈行为。
c) 宜基于用户行为频率、属性聚集等特征，针对批量或高频登录等异常行为，例如异常登录、注册、邀请好友、提现下单，利用 IP 地址、终端设备标识等信息进行综合识别，及时采取附加验证、拒绝请求等手段降低安全隐患。

11.3.4 安全事件处理

金融科技创新机构应建立有效的安全事件处理机制，满足以下要求：
a) 对于重大信息安全事件，相关人员应注意保护事件现场，采取必要的控制措施。
b) 应定期对本机构及同业发生的信息安全事件及风险进行深入研判、分析，评估现有控制措施的脆弱性，及时整改发现的问题。

12 内控管理

12.1 技术管理

a) 金融科技创新机构在新技术选型时，应满足以下要求：
——应有效研判新技术在金融业务的应用价值，正确进行新技术选型；
——应审慎选择新技术，进行新技术应用风险评估，避免过度采用未成熟的新技术；
——应对技术复杂性与金融业务复杂性进行关联分析，提高缺陷及时识别的能力。
b) 金融科技创新机构在新技术研发时，应满足以下要求：
——应建立第三方技术、组件或产品的管理清单，明确记录提供方、版本等信息；
——应跟踪第三方技术、组件或产品的更新情况，及时甄别版本变化带来的影响；
——应与第三方技术、组件或产品的供应商明确安全责任，建立有效的风险联动机制。
c) 金融科技创新机构在新技术应用时，应满足以下要求：
——应结合当前的法规政策、标准规范、应用模式、服务产品、信息系统支撑等方面，结合自身工作基础，说明金融科技创新应用的必要性、可行性；
——应对金融科技创新应用的具体目标、预期效果提出可量化的指标；
——应明确金融科技创新应用的业务功能、服务对象、预期用户规模和应用模式，说明金融科技应用采用的主要技术；
——应监控金融科技创新应用运行的状态、资源耗用情况、异常报警情况等；
——应在监控管理、日志管理等方面提供相应的功能，保障新技术应用过程可回溯、可监控、可审计；
——应制定可行有效的新技术回退、中止方案。

12.2 风险控制

金融科技创新机构应采取有效的风险控制措施，满足以下要求：
a) 应采用科学的风险管理技术和方法，充分识别和评估金融科技创新应用面临的风险，对各类主要风险进行持续监控。
b) 应做好新技术金融应用风险防范，建立健全试错容错机制，完善风险拨备资金、保险计划、应

急处置等风险补偿措施，具体要求如下：

——应根据新技术与业务融合的潜在风险，制定风险拨备资金管理要求；

——应根据新技术与业务融合的潜在风险，完善保险计划；

——应具备先行赔付、保险补偿等保护金融消费者合法权益的具体措施；

——应根据新技术与业务融合的潜在风险，完善应急处置措施；

——应具备重大突发事件应急处置机制。

c) 应建立健全客户投诉处理机制，制定金融科技创新应用的投诉处理工作流程，定期汇总分析投诉反映事项，查找问题，有效改进服务和管理。

12.3 内控保障

金融科技创新机构应建立有效的内部控制保障机制，满足以下要求：

a) 应建立健全内部控制制度体系，为金融科技创新应用制定全面、系统、规范的管理制度和业务流程，并定期进行评估。

b) 应明确金融科技创新应用的工作组织机制，明确工作负责人。金融科技创新应用由多个机构共同开发、运营时，应指定牵头负责单位，建立工作协调机制、联合运营机制、问题协同处理机制等控制措施。

c) 应定期开展金融科技创新应用内部审计。

d) 应当建立内部控制问题整改机制，明确整改责任部门，规范整改工作流程，确保整改措施落实到位。

附　录
（规范性附录）
容灾等级划分及关键指标要求

1　容灾影响范围分级

应符合 GB/T 20988、JR/T 0044、GB/T 22240 的相关要求，按照系统发生故障或瘫痪的影响范围、危害程度等对容灾能力要求进行划分。

结合金融领域特性，将系统发生故障的影响范围分为 4 个层级：

a）　内部辅助管理：未对金融机构经济效益、社会声誉产生直接影响的内部管理事项。

b）　内部运营管理：对金融机构经济效益、社会声誉产生直接影响的内部管理事项。

c）　公民、法人和其他组织的金融权益，包括：

——公民、法人和其他组织的财产安全权、知情权、公平交易权、依法求偿权、信息安全权；

——其他影响公民、法人和其他组织的金融权益的事项。

d）　国家金融稳定、金融秩序，包括：

——国家对外活动中的经济金融利益；

——国家金融政策的制定与执行；

——国家金融风险的防范；

——国家金融管理活动；

——多数关键金融机构、金融市场及其基础设施的稳定运行；

——其他影响国家金融稳定、金融秩序的事项。

2　容灾能力等级划分

结合金融领域特性，根据金融机构系统发生故障的危害程度，将容灾能力等级划分为6级。如表1所示：

表 1　应用于金融领域的系统容灾能力等级要求划分

影响范围	危害程度		
	较小影响	一般影响	严重影响
内部辅助管理	第 1 级	第 2 级	第 3 级
内部运营管理	第 2 级	第 3 级	第 4 级
公民、法人和其他组织的金融权益	第 3 级	第 4 级	第 5 级
国家金融稳定、金融秩序	第 4 级	第 5 级	第 6 级

金融机构系统发生故障的危害程度可划分为以下 3 类：

a）　较小影响，指的是工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题、较低的财产损失等。

b）　一般影响，指的是工作职能受到一般影响，业务能力显著下降且影响主要功能执行，引发一般的法律问题、较高的财产损失等。

c） 严重影响，指的是工作职能受到严重影响或丧失行使能力，业务能力严重下降或功能无法执行，出现严重的法律问题等。

3 容灾关键指标

结合金融领域特性，应用于金融领域的系统各等级RTO、RPO、可用性等关键指标要求见表2所示。

表 2 应用于金融领域的系统容灾能力等级关键指标要求

容灾等级	RTO	RPO	可用性
3 级	≦24 小时	≦24 小时	每年非计划服务中断时间不超过 4 天，系统可用性至少达到 99%。
4 级	≦4 小时	≦1 小时	每年非计划服务中断时间不超过 10 小时，系统可用性至少达到 99.9%。
5 级	≦30 分钟	≈0	每年非计划服务中断时间不超过 1 小时，系统可用性至少达到 99.99%。
6 级	≦2 分钟	0	每年非计划服务中断时间不超过 5 分钟，系统可用性至少达到 99.999%。

参 考 文 献

[1] GB/T 18903-2002/ISO/IEC 13236:1998 信息技术 服务质量：框架

[2] GB/T 20984-2007 信息安全技术 信息安全风险评估规范

[3] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

[4] GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

[5] GB/T 30146-2013/ISO 22301:2012 公共安全 业务连续性管理体系 要求

[6] JR/T 0068—2020 网上银行信息系统安全通用规范

[7] JR/T 0092—2019 移动金融客户端应用软件安全管理规范

[8] JR/T 0185—2020 商业银行应用程序接口安全管理规范

[9] 中国人民银行.中国人民银行关于印发《金融科技（FinTech）发展规划（2019—2021年）》 的通知（银发〔2019〕209号），2019年08月19日

[10] 中国人民银行 中国银行保险监督管理委员会 中国证券监督管理委员会 国家外汇管理局关于规范金融机构资产管理业务的指导意见（银发〔2018〕106号），2018年04月27日

[11] 条码支付安全技术规范（试行）（银办发〔2017〕242号文印发），2017年12月22日

[12] 中国人民银行. 中国人民银行关于进一步加强银行卡风险管理的通知（银发〔2016〕170号），2016年06月13日

[13] 中国人民银行.中国人民银行关于改进个人银行账户服务加强账户管理的通知（银发〔2015〕392号），2015年12月25日

[14] 中国人民银行. 中国人民银行办公厅关于强化银行卡磁条交易安全管理的通知（银办发〔2017〕120号）， 2017年05月31日

[15] 非银行支付机构网络支付业务管理办法（中国人民银行公告〔2015〕第43号公布），2015年12月28日

[16] 人脸识别线下支付行业自律公约（试行）（中支协发〔2020〕30号文印发）

[17] 人工智能安全白皮书（2018年）（中国信息通信研究院安全研究所，2018年9月）

[18] 中华人民共和国电子签名法