ICS 号 03.060
中国标准文献分类号 A11

团 体 标 准

T/HBPFS 007-2022

银行重点区域多维数据综合风险管控平台建设(技术)规范

Multi Dimensional Data Comprehensive Risk Control Platform For Key Regions Of The Bank Construction (technical) Specifications

2022-12-27 发布　　2022-12-27 实施

河北省金融学会　　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。

本文件由中国人民银行保定市中心支行和保定银行股份有限公司提出。

本文件由河北省金融学会归口。

本文件起草单位：中国人民银行保定市中心支行、保定银行股份有限公司、云侦通信技术（河北）有限公司。

本文件的主要起草人：林振英、陈龙、赵克芳、鲁佳棋、李海超、李佳璐、朱贺鹏 。

引 言

十三届全国人大常委会第三十六次会议通过《中华人民共和国反电信网络诈骗法》,法案要求电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者承担风险防控责任,建立反电信网络诈骗内部控制机制和安全责任制度,加强新业务涉诈风险安全评估。同时要求电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者应当对从业人员和用户开展反电信网络诈骗宣传,在有关业务活动中对防范电信网络诈骗作出提示,对非法买卖、出租、出借本人有关产品、服务被用于电信网络诈骗的法律责任作出警示。

本项目通过对银行重点部位及周边区域内手机信息与生物特征信息的采集与分析,无感获取手机国际移动用户标识码（IMSI）、11 位手机号码（MSISDN）、生物特征信息。依托获取到的通信数据、生物特征信息构建基于银行反欺诈、重大事件回溯机制、重点人员重点号码预警的风控数据模型，构建银行及周边区域活动用户图码信息档案，为银行业务安全准确交易提供图码联侦决策引擎,提高银行业务推广的精准性,提升银行的宣传服务的有效性。通过银警企合作机制加强银行自身安全防控、预警能力。

银行重点区域多维数据综合风险管控平台建设（技术）规范

1、 范围

本文件规定了银行重点区域多维数据综合风险管控平台的术语和缩略语定义、业务场景、基本要求、系统性能要求、安全性要求等内容。

本文件适用于河北省行政区域范围内各银行营业机构。

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。

YD/T 3615-2019 5G移动通信网核心网总体技术要求

YD/T3628-2019 5G移动通信网安全技术要求

3GPP TS 23.288 5G (Architecture enhancements for 5G System (5GS) to support network data analytics services) 系统支持网络数据分析业务的架构增强

3GPP TS 23.501 5G（System Architecture for the 5G System; Stage 2）系统架构

3GPP TS 23.502 5G（Procedures for the 5G System; Stage 2）系统流程

3GPP TS 23.503 5G（Policy and Charging Control Framework for the 5G System; Stage 2）策略和计费控制框架

3GPP TS 24.501 5G（Non-Access-Stratum（NAS）protocol for 5G System; Stage3）系统非接入层协议

3GPP TS 28.530（Management and orchestration; Concepts, use cases and requirements）管理和编排；概念；用例和需求

3GPP TS 28.531 （Management and orchestration; Provisioning;）管理和编排；服务开通

3GPP TS 28.532 （Management and orchestration;Generic management services;）管理和编排；通用管理服务

3GPP TS 28.541 管理和编排；5G 网络资源模型（Management and orchestration;5G Network Resource Model (NRM);Stage 2 and stage 3）

中华人民共和国反电信网络诈骗法

公安部《关于开展城市报警与监控技术系统建设的意见》

公安部《城市报警与监控建设技术指南》

公安部关于城市报警与监控系统的建设、管理、应用规范性文件（公安部科技信息化局汇编2009年3月）

（公通字[2019]3号）国家保密局关于印发《公安工作国家秘密范围的规定》的通知

（GB8566-88）《计算机软件开发规范》

（GB17859-1999）《计算机信息系统安全保护等级划分准则》

（GB/T17963-2000）《信息技术开放系统互连网络层安全协议》

（GB/T22239-2019)《信息安全技术—网络安全等级保护基本要求》

（GB/T28181-2011《安全防范视频监控联网系统信息传输、交换、控制技术要求》

（GB/T35273 - 2020 《信息安全技术 个人信息安全规范》）

（JR/T0171 - 2020 《个人金融信息保护技术规范》）

（TC260-PG-2022A 《个人信息跨境处理活动安全认证规范》）
（GA216.1－1999）《计算机信息系统安全产品部件第 1 部分：安全功能检测》
（GA/T70-2004）《安全防范工程费用预算编制办法》
（GA/T670-2006)《安全防范系统雷电浪涌防护技术要求》
（GA/T669-2008）《城市监控报警联网系统技术标准》
（GA/T669-2008）《城市监控报警联网系统系列标准》
（GA/T74-2017）《安全防范系统通用图形符号》

3、 术语和定义

下列术语和定义适用于本文件。

3.1 术语

3.1.1 国际移动用户识别码 IMSI

用于区分蜂窝网络中不同用户的、在所有蜂窝网络中不重复的识别码。手机将 IMSI 存储于一个 64 比特的字段发送给网络。

3.1.2 生物特征

泛指人像信息，声音信息，指纹信息等。

3.1.3 重点人员

指公安系统关注的涉恐人员、涉稳人员、重大刑事犯罪前科人员、涉毒人员、在逃人员、肇事肇祸精神病人、重点上访人员、失信人员等。

3.1.4 监测模型

通过多维数据融合分析平台，实现对银行周边区域用户业务智能化宣传（疫情防控宣传、反电信诈骗宣传、银行自身业务宣传等）。同时对银行周边区域实时人群流量统计分析，结合多维数据对各银行网点人流量数据汇总与分析，实时掌握人流量分布状态，为银行网点完善和优化提供数据支撑。

通过对银行周边及场所内部安装前端感知设备，对手机特征（IMSI/MSISDN）、人像进行结构化动态实时采集（7*24 小时）。构建多维数据融合预警分析平台，针对进入银行周边区域目标，实现身份的准确识别、触网告警、动态追踪和态势感知的功能。通过银警合作机制，实现手机终端数据、人像结构化数据、公安重点人员数据、银行防控数据的融合分析。建立多维异常行为监测模型，包括频繁异地取款预警、本地短期多网点取款预警、电信诈骗人员/号码预警、重点（失信、在逃、诈骗等）人员预警、人员异常聚集预警等，便于银行部门依托公安资源数据，加强自身防范能力和预警级别。同时为公安部门在电信诈骗和银行周边案件提供回溯、预警机制。

3.1.5 缩略语

下列缩略语适用于本文件。

编号	3GPP	第三代伙伴计划	3rd Generation Partnership Project
1	3DI	设备管理及采集数据驱动中间件	Devices Data Driver Interface
2	DDE	数据驱动引擎	Data Driver Engine
3	DPE	数据处理引擎	Data Process Engine
4	SAE	布控预警引擎	Surveillance and Alert Engine
5	DAE	Spark 数据分析引擎	Spark Data Analysis Engine
6	EFS	多维数据预警管控平台	electric-Fence System
7	DSE	数据同步引擎	Data Synchronize Engine
8	AMS	应用程序管理及配置子系统	Applications Management System
9	ICAS	图像识别引擎服务	Image Content Alalysis Service

4、 业务场景

4.1 银行自身业务宣传

根据银行自身业务需求，对进入银行区域及周边人员进行业务推广和宣传和相关提示，提升银行服务的精准性和有效性。

4.2 银行区域内案件信息回溯

针对银行场所治安类案件提供事后回溯追查机制，提升银行风险防控能力；针对银行重点阵地实时出现的重点人群触发警企合作机制；针对银行场所内发生的案件可以有效进行事后回溯。针对进入银行区域的人员，进行反诈、防疫等公益宣传。

5、 基本要求

5.1 标准化

采用标准化开发过程，应该按要求编写好十三种文档，文档编制要求具有针对性、精确性、清晰性、完整性、灵活性、可追溯性。

可行性分析报告：说明该软件开发项目的实现在技术上、经济上和社会因素上的可行性，评述为了合理地达到开发目标可供选择的各种可能实施方案，说明并论证所选定实施方案的理由。

项目开发计划：为软件项目实施方案制订出具体计划，应该包括各部分工作的负责人员、开发的进度、开发经费的预算、所需的硬件及软件资源等。

软件需求说明书（软件规格说明书）：对所开发软件的功能、性能、用户界面及运行环境等作出详细的说明。它是在用户与开发人员双方对软件需求取得共同理解并达成协议的条件下编写的，也是实施开发工作的基础。该说明书应给出数据逻辑和数据采集的各项要求，

为生成和维护系统数据文件做好准备。

概要设计说明书：该说明书是概要实际阶段的工作成果，它应说明功能分配、模块划分、程序的总体结构、输入输出以及接口设计、运行设计、数据结构设计和出错处理设计等，为详细设计提供基础。

详细设计说明书：着重描述每一模块是怎样实现的，包括实现算法、逻辑流程等。

用户操作手册：本手册详细描述软件的功能、性能和用户界面，使用户对如何使用该软件得到具体的了解，为操作人员提供该软件各种运行情况的有关知识，特别是操作方法的具体细节。

测试计划：为做好集成测试和验收测试，需为如何组织测试制订实施计划。计划应包括测试的内容、进度、条件、人员、测试用例的选取原则、测试结果允许的偏差范围等。

测试分析报告：测试工作完成以后，应提交测试计划执行情况的说明，对测试结果加以分析，并提出测试的结论意见。

开发进度月报：该月报系软件人员按月向管理部门提交的项目进展情况报告，报告应包括进度计划与实际执行情况的比较、阶段成果、遇到的问题和解决的办法以及下个月的打算等。

项目开发总结报告：软件项目开发完成以后，应与项目实施计划对照，总结实际执行的情况，如进度、成果、资源利用、成本和投入的人力，此外，还需对开发工作做出评价，总结出经验和教训。

软件维护手册：主要包括软件系统说明、程序模块说明、操作环境、支持软件的说明、维护过程的说明，便于软件的维护。

软件问题报告：指出软件问题的登记情况，如日期、发现人、状态、问题所属模块等，为软件修改提供准备文档。

软件修改报告：软件产品投入运行以后，发现了需对其进行修正、更改等问题，应将存在的问题、修改的考虑以及修改的影响作出详细的描述，提交审批。

5.2 组件化

组件化技术，对于开发团队来说，在提高开发效率和代码维护上是一个十分有利的工具。对于相同的业务流程来说，它可以让我们的组件在启用时，只需要添加组件的依赖就可以引入组件，而不用关心，由于依赖导致的错误。这让我们的精力可以更聚焦于具体的业务。而编码风格的统一，无论是在开发阶段，还是打包阶段，都能有效帮我们规避掉很多问题。

5.3 成熟性

系统应用软件采用已有的成熟技术成果进行开发构建，加快实施进度；通过相应协议和规范接口访问其他原有系统获取业务实现所需的基础数据，降低数据风险。

硬件组件采用标准组件、标准接口，方便备品备件更换维护。

5.4 易用性

易用性是指软件界面的亲和力和舒适度，让用户感到界面友好，符合实际应用中的使用习惯和知识能力，为此系统应提供明确而友好的错误提示；采用良好的人性化设计，容易输入出错的地方尽可能采用选择菜单和提示；采用规范的行业术语。

5.5 开放性

系统建设应遵循有关国家标准、网络设备选型时应确认既具有广泛的厂商与标准的支持又符合网络技术发展的主流趋势，并能获得良好的技术支持，同时在不同层面实现对外应用接口，提供第三方业务应用系统的调用。

5.6 可靠性

系统具备完善的错误检验功能和容错处理功能。提供完善的并发处理机制和服务器集群机制。整个系统平台在设计之初就充分考虑高并发和高吞吐量的处理性能要求，采用先进的技术和设计理念指导整个开发过程，确保系统后期正确稳定的运行。从终端到各移动应用平台能够满足可靠性要求，确保各产品无单点故障和数据完整性，发生故障时能够及时预警，并进行自动恢复或将故障进行隔离；平台能够提供有效的故障诊断及维护工具，具备数据错误记录和错误预警能力；具备较高的容错能力，在出错时具备自动恢复功能。

5.7 安全性

具有有效可信的安全保密处理机制，防止非法入侵和数据截取，并确保数据在访问和交换中的安全和保密性。系统的建设，必须符合安全性原则，加强信息安全防护，所有的软硬件，必须具备有效的认证、授权和审计机制，在数据分类的基础上，能够对关键操作、采集的数据进行重点防护，同时对外部攻击和滥用，具备一定的检测和防御能力。

6、 系统性能要求

6.1 可扩展性

系统设计采用开放性架构，满足系统的扩展性要求，包括对前端系统接入的适应扩展和对相关业务功能的适应扩展。对于系统与前端设备的数据交互接口、与银行相关系统的数据交换接口、平台与公安其他系统的服务调用接口等要采用统一接口标准、数据传输标准，质量控制规范，实现数据的安全交互和共享。

6.2 安全可靠性

系统提供高性能的应用服务，确保各项业务功能可靠、高效。同时确保系统的接入安全、应用安全和数据安全、传输安全，敏感数据进行机密传输，系统稳定可靠，保证 7 * 24 小时不间断服务。

6.3 数据存储及备份

提供高可用的数据服务，满足双机热备。同时提供自动灾备功能及故障恢复功能。故障恢复窗口小于 2 小时。

6.4 技术先进性

系统建设充分利用大数据、云计算等先进技术，对现有资源进行整合利用，进一步提升资源应用效益。同时，考虑系统功能的实用性，确保系统功能实用、界面美观、操作方便。此外，在满足用户当前需求的同时，充分考虑业务发展，保证具有前瞻性，能够适应一定范

围内的发展和变化，保证系统具有较旺盛的生命力。

6.5 安全日志审计

非法访问、数据违规操作自行通告并生成报告。

6.6 用户鉴权及设备接入鉴权

支持对用户和采集设备进行鉴权和管理。

6.7 并发接入能力

多数据源并发接入能力:支持多种不同类型数据源并发实时接入,多用户并发访问能力:支持多用户的并发访问和数据分析请求处理及实时响应，确保系统的可用性和稳定性。

系统对于采集设备数据处理的吞吐量每天不小于 1000 万条。数据分析请求响应时间（RT）不高于 15 秒。并发用户数不低于 100。

6.8 数据处理能力

具备海量数据的清洗能力、数据快速运算能力、数据实时处理能力。系统提供实时的数据接入、处理能力。要求数据处理能力不低于 1T/天。对于支持实时对接的动态数据，要求数据接入系统后可立即进行分析展示。

7、 安全性要求

7.1 数据采集加密

数据回传通道做到专网专通道，数据进行加密传输设备对采集到的 IMSI 号进行信源加密，缺省为 DES 加密算法，根据用户要求还可选择 AES 或 3DES 加密算法；加密后的数据与其它数据混合到同一条传输链路中传递到中心,在线路中采用常规手段进行监测很难获得真正的信息。通过对数据的封装加密，对各层数据的规范设计和处理保证数据的安全。

7.2 传输链路安全

同网之间采用 TCP、UDP 传输方式。不同网之间采用安全隔离文件交换系统， 典型应用如 FTP 文件传输方式。

7.3 分层分级部署

各网点，各银行独立部署设备，数据统一汇聚各地市分行级（含）以上机构，确保数据隔离，互不影响。

7.4 数据存储安全

限制能够直接登录到存储主机上的人员,用户操作人员应经用户身份认证后才能访问存储数据。从根本上禁止不受控制和审计的用户对数据进行直接操作。

用户操作人员经过身份认证读取存储数据时候，需要二次认证才可进行数据只读查看，且关键数据已经加密，需要特权秘钥查看。任何的登录，查看操作均会留下操作痕迹。

7.5 登录认证/审计

通过认证、加密、安全检测、权限分配、访问记录等一系列手段来构建数据的应用安全。

采用数字认证方式来确保用户的登录身份与其真实身份相符，对用户进行数据及功能权限控制。

操作人员应经用户身份认证后才能访问平台的相关应用功能，禁止不受控制和审计的用户登录。

登录后权限的不同，应用级别不同，进行重要信息查看，修改等操作需要进行特权密钥确认。

记录用户登录系统的信息，为日后的安全审计提供依据；系统资源安全管理，限制系统软硬件的安装、卸载，控制特定程序的运行，限制系统进入安全模式，控制文件的重命名和删除等操作；

对于密级较低网络数据源在数据融合做好网络边界防范，原则上使用单向网络通道进行数据接入。