

Q/HRCB

江苏海安农村商业银行企业标准

Q/HRCB 001—2026

海安农商银行数据安全分级指南

Guidelines on Data Security Classification of Haian Rural Commercial Bank

2026-10-20 发布

2026-10-20 实施

江苏海安农村商业银行股份有限公司 发布

目 次

前 言 III

海安农商银行数据安全分级指南 1

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 分级目标与分级原则 2

 4.1 分级目标 2

 4.2 六大分级核心原则 2

 4.2.1 合法合规性原则 2

 4.2.2 可执行性原则 2

 4.2.3 时效性原则 2

 4.2.4 自主性原则 3

 4.2.5 差异性原则 3

 4.2.6 客观性原则 3

5 数据安全定级范围 3

 5.1 客户类数据 3

 5.2 业务类数据 3

 5.3 经营管理类数据 3

 5.4 监管类数据 3

 5.5 系统运行安全管理类数据 3

6 数据安全定级要素与安全影响评估 4

 6.1 核心定级双要素 4

 6.1.1 影响对象分类 4

 6.1.2 影响程度定义 4

 6.2 三属性独立评估要求 4

 6.2.1 保密性评估 4

 6.2.2 完整性评估 4

 6.2.3 可用性评估 4

 6.3 定级要素识别规则 4

7 五级数据安全分级判定标准 5

 7.1 核心数据（5级） 5

 7.2 重要数据（4级） 5

 7.3 敏感数据（3级） 5

 7.4 一般数据（2级） 5

 7.5 公开数据（1级） 6

8 数据安全定级全流程管理规范 6

 8.1 组织保障架构 6

 8.1.1 牵头管理部门 6

 8.1.2 业务归口部门 6

 8.2 配套制度保障清单 7

 8.3 五步标准化定级流程 7

 8.3.1 数据资产梳理 7

 8.3.2 数据安全定级准备 7

8.3.3 数据安全级别判定	7
8.3.4 数据安全级别审核	7
8.3.5 数据安全级别批准	7
8.4 强制重评定触发场景	7
9 重要数据识别与管控要求	7
9.1 识别依据	7
9.2 硬性要求	8
9.3 识别流程	8
9.4 专项管控规则	8
9.4.1 存储	8
9.4.2 访问	8
9.4.3 共享	8
9.4.4 销毁	8
10 数据安全级别变更管理	8
10.1 变更触发情形	8
10.2 变更调整规则	8
10.3 变更操作流程	8
10.4 变更示例详见附录 B	8
附 录 A	9
附 录 B	9
附 录 C	9
参 考 文 献	10

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。

本文件依据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》、JR/T 0197—2020《金融数据安全 数据安全分级指南》、GB/T 43697—2024《数据安全技术 数据分类分级规则》，以及国家金融监督管理总局《银行保险机构数据安全管理办法》（金规〔2024〕24号）等法律法规、行业标准和监管规定，结合江苏海安农村商业银行股份有限公司存贷款、普惠金融、绿色信贷、柜面运营、风控、监管报送等实际业务场景编制，用于规范全行金融数据分级管理工作。

本文件由江苏海安农村商业银行股份有限公司提出。

本文件由江苏海安农村商业银行股份有限公司归口。

本文件起草人：陈勇、吴智星、朱骞、刘飞。

海安农商银行数据安全分级指南

1 范围

本文件规定了海安农商银行金融数据安全分级的目标、基本原则、定级覆盖范围、定级核心要素、安全影响评估方法、五级分级判定规则、标准化定级流程、重要数据识别规则、数据级别变更机制。

本文件适用于本行总行各管理部门、所有支行、营业网点开展全量金融数据资产分级梳理、定级、运维管理工作；同时为本行第三方数据安全评估机构、外部审计单位开展数据合规检查、风险评估提供参考。

排除适用范围：涉及国家秘密的金融数据，遵照国家保密法律法规单独管理，不适用本标准；仅纸质未电子化原始业务档案，按照本行档案管理专项制度执行，不纳入本分级体系。

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 25069—2022 信息安全技术 术语

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融数据 financial data

在开展存款、贷款、绿色金融、支付结算、银行卡、代理保险、普惠小微、风控审计、行政办公、监管报送、第三方合作等全流程业务活动中采集、生成、存储、传输、共享、衍生加工的全部电子化数据；包含纸质单据扫描影像、系统运行日志、客户业务音视频、跨机构交互数据、统计衍生数据集。

3.2

个人金融信息 personal financial information

通过业务渠道采集、加工、存储的自然人身份、账户、交易、财产、借贷、生物识别、联系方式等信息。

3.3

保密性 confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[来源：GB/T 25069—2022]

3.4

完整性 integrity

保证资产准确和完整的特性。

[来源：GB/T 25069—2022]

3.5

可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[来源：GB/T 25069—2022]

3.6

影响对象 affected parties

数据保密性/完整性/可用性遭受破坏后，权益受损主体，分为五类：国家安全、公众权益、个人隐私、企业合法权益、本行利益。

3.7

影响程度 degree of impact

依据破坏后果轻重，划分为四级：严重损害、一般损害、轻微损害、无损害。

4 分级目标与分级原则**4.1 分级目标**

- a) 全面盘点全行全部数据资产，建立统一、可落地的五级数据安全分级体系，搭建覆盖数据全生命周期的差异化安全保护框架。
- b) 精准划分数据敏感层级，合理分配安全防护人力、技术、成本资源，降低数据泄露、篡改、不可用、违规共享类安全风险。
- c) 满足人民银行、国家金融监督管理总局、江苏省地方金融监管部门的数据合规监管要求，实现数据定级过程可复核、结果可审计、管控可追溯。
- d) 规范内外部数据共享、第三方机构数据合作的分级准入标准，在守住数据安全底线前提下，合规释放数据业务价值。
- e) 建立动态分级管理机制，实现数据内容、业务场景、监管要求变化后及时调整安全等级。

4.2 六大分级核心原则**4.2.1 合法合规性原则**

严格遵守国家法律法规及金融行业监管规定，将合规性要求贯穿数据定级全流程，确保定级工作的合法性与规范性，筑牢安全基石。

4.2.2 可执行性原则

定级规则贴合业务实际场景与技术落地条件，兼顾管理效率与操作便捷性，确保定级标准可理解、可落地、可执行，避免脱离实际的空泛要求。

4.2.3 时效性原则

数据安全等级具备动态有效期，根据业务发展、监管政策更新及内外部环境变化，及时复核和更新定级结果，保障有效性。

4.2.4 自主性原则

在遵循国家统一框架和监管要求的前提下，结合海安本地客户体量、本行区域金融职能、自身风险承受能力，细化适配本行定级细则。

4.2.5 差异性原则

针对不同业务线、数据类型和应用场景，避免“一刀切”式管理，区分数据的差异，实现数据的精细化、差异化定级与管控，合理分配安全资源，提升管理效能。

4.2.6 客观性原则

定级规则应基于客观数据与标准，定级过程需规范留痕，确保结果可复核、可检查，经得起内外部审计与监管验证，杜绝主观随意划分等级。

5 数据安全定级范围

本行需纳入分级管理的电子化金融数据包含五大类，涉密数据、纯纸质无电子化档案不适用本标准。

5.1 客户类数据

指与各种业务的客户对象相关的各类信息，按照客户主体区分可进一步分为个人客户、对公客户、同业客户等。包含个人客户、小微企业客户身份信息、联系方式、不动产、经营资质、证照影像。

5.2 业务类数据

指在提供金融产品或服务过程中产生的数据，包括但不限于账户、协议、交易、产品等信息。包含存款、贷款、绿色信贷、支付结算、银行卡、票据、代理保险、普惠涉农业务合约、流水、授信、放款、还款数据、业务合同、抵押权证、客户业务音视频、纸质凭证扫描件、尽职调查影像、担保、保险、政务平台、第三方支付对接交换业务、客户、风险数据。

5.3 经营管理类数据

指在履行职能与经营管理过程中采集、产生的数据，包括但不限于营销服务、风险管理、运营管理等信息。包含客户风险评级、授信审批、不良处置、反洗钱监测、信贷统计、绿色金融碳核算、客户标签画像、营销分析数据、员工人事、薪资、内控审计、行政公文、会议影音、多源数据汇总、建模、批量客户统计、跨条线融合衍生数据集。

5.4 监管类数据

指按照监管机构有关规定和要求上报的各类信息，以及监管机构为实现有效管理和风险管控等目的，向本行发送的包括评价、处罚、违规情况、统计数据、预警信息以及安全审计等信息。

5.5 系统运行安全管理类数据

指各类信息系统运行过程中产生的技术信息，包括但不限于：服务器日志、网络流量记录、系统性能监控数据、数据库运行状态信息、安全审计日志、访问控制记录、漏洞扫描报告等。

6 数据安全定级要素与安全影响评估

6.1 核心定级双要素

数据安全等级判定核心依据为数据三属性受损后的影响对象、影响程度，综合保密性、完整性、可用性三项风险评估结果综合判定。

6.1.1 影响对象分类

- a) 国家安全：一般指数据的安全性遭到破坏后，可能对政治安全、国家安全重点领域、国民经济命脉、社会稳定等造成影响。
- b) 公众权益：一般指数据的安全性遭到破坏后，可能对生产经营、教学科研、公共健康和安全、公共交通等社会秩序和公众的政治权利、人身自由、经济权益等造成影响。
- c) 个人隐私：一般指数据的安全性遭到破坏后，可能对个人金融信息主体的个人信息、私人活动、财产安全和合法权益等造成影响。
- d) 企业合法权益：一般指数据的安全性遭到破坏后，可能对本行以外的企业或其他组织的生产运营、声誉形象、公信力等造成影响。
- e) 本行利益：一般指数据的安全性遭到破坏后，可能对本行的日常经营、声誉形象、安全合规等方面造成影响。

6.1.2 影响程度定义

- a) 严重损害：危害国家安全、数万级客户信息批量泄露、监管重大行政处罚、全行核心业务全面中断、大范围群众金融权益受损；
- b) 一般损害：局部公共秩序受影响、批量客户信息泄露、监管常规处罚、关键业务局部停滞、企业较大经济损失；
- c) 轻微损害：少量客户信息泄露、网点/条线业务短时中断、个别客户投诉、小额经济损失；
- d) 无损害：数据公开不产生任何风险，不影响国家安全、公众、个人、企业权益。

6.2 三属性独立评估要求

定级前需分别开展保密性、完整性、可用性风险评估，再综合判定等级。

6.2.1 保密性评估

评估数据未经授权泄露、外传、窃取后果，重点核查客户鉴别信息、批量信贷汇总、重要数据泄露风险，对照监管法规判断违规程度。

6.2.2 完整性评估

评估数据被篡改、删除、伪造后，信贷审批、资金结算、监管报表失真带来资金损失、合规处罚风险，重点覆盖交易流水、授信额度、抵押资料。

6.2.3 可用性评估

评估数据无法访问、系统宕机、勒索加密导致柜面、线上信贷、支付业务中断对客户与本行造成的负面影响。

6.3 定级要素识别规则

- a) 三项安全属性风险等级不一致时，以最高损害等级作为定级基准；
- b) 三属性风险程度基本一致，优先以保密性评估结果确定安全级别；
- c) 数据覆盖客户越多、涉及资金规模越大、跨机构融合衍生数据，影响程度自动上调一档判定。

7 五级数据安全分级判定标准

本行依据JR/T 0197—2020《金融数据安全数据安全分级指南》确定五级数据安全分级框架，根据数据的重要性和敏感程度，以及数据安全性遭受破坏后的影响对象和所造成的影响程度，将数据安全级别从高到低分为核心数据（5级）、重要数据（4级）、敏感数据（3级）、一般数据（2级）、公开数据（1级）共五个安全级别，分级如下：

注：本标准五级体系与《银行保险机构数据安全管理办法》（金规〔2024〕24号）第十八条“核心数据、重要数据、一般数据”三级框架及GB/T 43697—2024“核心数据、重要数据、一般数据”分类衔接。

7.1 核心数据（5级）

核心数据是指对领域、群体、区域具有较高覆盖度或者达到较高精度、较大规模、一定深度的数据，一旦被非法使用或者共享，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益。包括但不限于：

- a) 宏观特征数据，反映不可更改或长时间保持稳定的经济特征、社会特征的数据；
- b) 海量信息汇聚得到的衍生特征数据，如汇聚后覆盖多省份的金融消费者真实交易信息；
- c) 监管部门认定的其他核心数据。

7.2 重要数据（4级）

重要数据是指特定领域、特定群体、特定区域或者达到一定精度和规模的数据，一旦被泄露、篡改、损毁或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。包括但不限于：

- a) 行业监管机构决策和执法过程中的数据，如行政机关、执法机关在履职或执法过程中收集和产生的不涉及国家秘密且未公开的受控数据；
- b) 关键信息基础设施网络安全缺陷信息，如网络设备、服务器、信息系统等有关漏洞信息；
- c) 客户的用户鉴别信息，如银行卡磁道数据、卡片验证码、账户各类密码、网络支付交易密码、用于用户鉴别的个人生物识别信息等；
- d) 个人健康生理信息；
- e) 监管部门认定的其他重要数据。

7.3 敏感数据（3级）

敏感数据是指一旦被泄露或者篡改、损毁，对经济运行、社会稳定、公共利益有一定影响，或者对组织自身或者公民个体造成重要影响的数据。包括但不限于：

- a) 以电子形式存储的符合保密制度中AAA级的商业秘密数据；
- b) 敏感客户数据：可识别特定个人身份或特定个人金融状况，及单位敏感信息，如个人证件信息、个人财产信息、单位及个人用户鉴别辅助信息、管理层数据、内幕信息等；
- c) 敏感账务交易类数据：用于金融产品与服务的关键信息，如账户余额、交易对手详细信息、能够直接定位到个人金融信息主体的交易信息等；
- d) 重要经营管理数据：营销服务类数据中的新产品研发数据，运营管理类数据中的安防管理类数据、合作单位联系人数据、客户相关音视频数据，风险管理类数据中的风险偏好数据、黑名单数据，技术管理类数据中的规划信息、开发信息及系统运维信息，综合管理类数据中的战略规划信息、财务信息以及员工档案薪酬信息等；
- e) 其他经组合可识别和反映上述信息的基础数据集或监管报送统计数据；
- f) 监管部门认定的其他敏感数据。

7.4 一般数据（2级）

一般数据是指用于一般业务使用的数据。数据的安全性遭到破坏后，对个人隐私或企业合法权益造成轻微影响，但不影响国家安全、公众权益。包括但不限于：

- a) 以电子形式存储的符合保密相关制度中AA级和A级的商业秘密数据；
- b) 一般客户数据，包括内部使用的个人金融信息，或不能识别特定个人身份，或与特定个人及单位敏感信息无关的数据，如教育、职业、资质、党政信息、公私关系、行为等数据，单位未公开的工商信息、财务信息、关系信息、行为信息等；
- c) 一般业务数据，包括账户基本信息、冻结信息、合约信息、各类业务信息，交易基本信息、清算记账信息等；
- d) 一般性经营管理数据，包括营销服务类数据中的渠道信息、营销信息、产品管理信息，运营管理类数据中的业务运维、客户服务、单证管理等信息，风险管理类数据中的风险缓释、识别、计量、监测等信息，技术管理类数据中的项目质量管理、测试信息、软件资源、运行日志等信息，综合管理类数据中的招聘信息、机构信息、行政信息、资产负债信息、内控合规信息等；
- e) 外部数据中除个人敏感、单位敏感数据以外的数据；
- f) 其他敏感级别以上、经匿名化处理后，对个人、组织、社会、国家不构成安全影响的数据。

7.5 公开数据（1级）

公开数据是指可被公开或可被公众获知、使用的数据，数据的安全性遭到破坏后，对个人隐私或企业合法权益不构成影响，且不影响国家安全、公众权益的数据，包括但不限于：

- a) 根据监管要求或在特定场景下对外披露的业务经营管理公开数据，包括销售渠道、市场营销、招聘、财务报告及法律法规要求公开的数据；
- b) 个人客户、对公客户、同业客户等在特定场景下主动要求公开的数据；
- c) 工商基本信息、失信惩戒信息、司法涉诉信息、公开网站、新闻等公开渠道可获取的数据；
- d) 其他法律法规要求公开的数据。

8 数据安全定级全流程管理规范

8.1 组织保障架构

8.1.1 牵头管理部门

科技信息部是本行数据资产管理、数据安全、研发管理的归口部门，具体职责：

- a) 统筹规划、组织和监督本行开展数据分类分级工作，完善数据分类分级管理体系，推动数据分类分级要求的有效落实；
- b) 结合江苏农村商业银行股份有限公司企业级数据标准，明确数据分类分级标准，开展全行业数据分类分级认定；
- c) 制定、发布和更新数据分类分级相关制度、流程和操作规程；
- d) 负责为数据分类分级实施提供科技保障和技术支持；
- e) 在数据安全管理体系中执行数据分类分级标准，并制定相应的数据安全保护策略；
- f) 负责在应用系统全生命周期管理中落实数据分类分级管理要求及相应的数据安全保护策略。

8.1.2 业务归口部门

各业务部门作为本业务领域的业务主管部门，应当按照“谁管业务、谁管业务数据、谁管数据安全”的原则，明确各业务领域的数据安全保护责任，落实数据安全保护管理中数据分类分级相关要求，具体职责如下：

- a) 负责审核归属本部门的业务数据项分类分级结果，关注数据使用影响变化，根据变化情况及时向科技信息部提交数据安全级别调整需求；

- b) 根据数据分类分级结果，落实数据分类分级保护要求，确保本部门数据处理活动符合数据全生命周期安全保护策略；
- c) 协同科技信息部开展数据分类分级工作。

8.2 配套制度保障清单

《海安农商银行数据分类分级操作规程》（海商行发〔2026〕147号）。

8.3 五步标准化定级流程

8.3.1 数据资产梳理

根据自身数据分类分级范围及定级频率的需求，通过技术手段或工具对数据进行盘点、梳理与分类，形成统一的数据资产清单，以数据标准和分类分级为基础明确数据保护对象。

8.3.2 数据安全定级准备

按照全行业统一数据标准，开展数据资产对标及分类。针对数据标准已覆盖的数据资产，应按照数据标准颗粒度开展数据定级工作；对于数据标准暂未覆盖或非结构化数据，可根据本行实际情况，按照文件类型、表、字段等颗粒度开展定级工作。

8.3.3 数据安全级别判定

参考《海安农商银行数据分类分级操作规程》的相关要求以及江苏农村商业银行股份有限公司企业级数据标准，对数据分类分级进行初定，数据标准中确定的安全级别作为最低安全级别的参考依据。综合考虑数据规模、数据时效性、数据形态（如是否经汇总、加工、统计、脱敏或匿名化处理等）等因素，对数据分类分级结果进行复核，调整形成数据分类分级结果清单。

8.3.4 数据安全级别审核

业务主管部门审核数据分类分级评定过程和结果，必要时重复以上操作，直至数据分类分级的划定与本机构数据安全保护目标一致。

8.3.5 数据安全级别批准

由科技信息部对数据分类分级结果进行最终审议批准。本行判定数据安全定级低于江苏农村商业银行股份有限公司数据安全级别认定结果的，应阐明理由并报备江苏农村商业银行股份有限公司数据资产部。

8.4 强制重评定触发场景

出现以下任一情况，完整重走全套定级流程：

- a) 新增业务系统、新增第三方数据对接接口；
- b) 原有数据覆盖客户、资金规模大幅扩张；
- c) 多源数据汇聚融合生成全新数据集；
- d) 国家、金融监管更新数据安全管控要求；
- e) 年度数据安全内审发现定级错误、分级管控漏洞。

9 重要数据识别与管控要求

9.1 识别依据

参考本标准附录 C《本行重要数据识别清单参考》，结合GB/T 43697重要数据识别因素动态更新。

9.2 硬性要求

所有认定为重要的数据，最低安全等级固定为4级，不得下调。

9.3 识别流程

各业务部门初筛→科技信息部复核认定，形成全行《重要数据静态清单》，每年更新。

9.4 专项管控规则

9.4.1 存储

独立加密数据库存储，双机异地备份，禁止导出至办公电脑、私人设备。

9.4.2 访问

双人复核审批，操作日志永久留存，关键操作可同步留存录像。

9.4.3 共享

除监管报送、依法合规情形外，严禁对外提供，并明确报送审批流程。内部跨条线调取重要数据，应履行审批流程，重要情形需行长专项书面审批，一般情形可授权分管行长审批。

9.4.4 销毁

纸质、电子介质统一由科技信息部物理销毁，留存销毁记录备查。

10 数据安全级别变更管理

10.1 变更触发情形

满足其一需启动变更流程：

- a) 数据内容发生变化，导致原有数据的安全分类分级不适用变化后的数据；
- b) 数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式发生变化，导致原有的分类分级不再适用；
- c) 因数据汇聚融合，导致原有数据分类分级不再适用融合后的数据；
- d) 因国家或行业主要部门要求，导致原定的数据分类分级不再适用；
- e) 需要对数据分类分级进行变更的其他情形。

10.2 变更调整规则

- a) 脱敏、去标识、删除敏感字段：安全级别可下调一档；
- b) 多源数据融合、批量汇总、扩大使用范围：安全级别上调一档。

10.3 变更操作流程

业务部门提交变更申请→科技信息部复核→更新分级清单与系统标签，全程留存变更审批档案。

10.4 变更示例详见附录 B

附 录 A
(资料性附录)
本行典型数据定级参考表

一级分类	二级子类	细分数据项	最低安全级别
个人客户数据	个人身份鉴别信息	银行卡密码、短信验证码、指纹虹膜	4
个人客户数据	个人基础信息	身份证、手机号、家庭住址	3
个人客户数据	个人职业/学历信息	工作单位、学历记录	2
小微企业数据	企业信贷档案	全套授信、抵押资料	3
小微企业数据	企业工商基础信息	统一社会信用代码、注册地址	2
业务数据	账户余额、单户流水	个人账户资金明细	3
业务数据	全行信贷宏观汇总	县域普惠信贷总量统计	4
风控数据	大额可疑交易批量汇总	全行反洗钱批量统计	4
内部管理	员工薪资档案	全员薪酬明细	3
内部管理	网点运营台账	日常柜面业务台账	2
公开信息	网点地址、产品宣传	官网对外公示材料	1

注：表格仅为最低安全级别，发生汇聚融合等场景需要按规则上调等级。

附 录 B
(资料性附录)
数据安全级别变更典型场景

场景 1：3 级单户客户信贷明细，脱敏去除身份证、手机号后，下调至 2 级；
 场景 2：达到本行客户总量一定比例的 3 级客户信贷数据汇总融合生成批量统计表，上调至 4 级；
 场景 3：2 级网点台账，批量汇总全行运营总表，上调至 3 级。

附 录 C
(资料性附录)
本行重要数据识别清单参考

县域涉农、普惠信贷宏观汇总统计数据；
 全行大额可疑交易批量汇总数据集；
 区域性系统性风险计量与监测模型；
 向人民银行报送的县域金融核心统计报表；
 全行不良资产批量汇总分析数据；
 跨机构批量客户信贷融合数据集；
 反洗钱大额交易全行汇总台账。

注：清单中部分数据满足条件应定为 5 级，其余不低于 4 级。

参 考 文 献

- [1] 全国人民代表大会常务委员会，《中华人民共和国网络安全法》，2016.
- [2] 全国人民代表大会常务委员会，《中华人民共和国数据安全法》，2021.
- [3] 全国人民代表大会常务委员会，《中华人民共和国个人信息保护法》，2021.
- [4] 国家金融监督管理总局，《银行保险机构数据安全管理办法》（金规〔2024〕24号），2024.
- [5] 中国银行保险监督管理委员会，《银行业金融机构数据治理指引》（银保监发〔2018〕22号），2018.