



中國互聯網金融協會
National Internet Finance Association of China

互联网金融从业机构
反洗钱和反恐怖融资风险管理
及内控框架指引手册

目录

第一章 概述.....	1
1.背景.....	1
2.应用.....	3
3.反洗钱监管体系	4
3.1 监管制度	4
3.2 反洗钱主管部门	5
3.3 国务院有关金融监督管理机构	6
3.4 中国反洗钱监测分析中心	6
3.5 自律管理	6
4.适用范围.....	7
4.1 机构范围	7
4.2 风险类别	8
5.政策概览.....	9
6.基本目标.....	10
7.基本原则.....	10
7.1 风险为本原则	10
7.2 全覆盖原则	10
7.3 独立性原则	11
7.4 匹配性原则	11
7.5 有效性原则	11

7.6 严格合规原则	11
7.7 勤勉尽责原则	12
8.文化建设.....	12
9.基本要素.....	13
第二章 管理架构	14
10.基本要求	14
11.反洗钱职责.....	14
11.1 职责权限.....	14
11.2 反洗钱岗位.....	14
11.3 人员管理.....	15
12.董事会职责	16
13.监事会职责	17
14.高级管理层职责	17
14.1 反洗钱负责人	18
14.2 反洗钱工作领导小组	19
15.内部组织架构	20
15.1 事业部制或类事业部制下的反洗钱风控.....	32
16.反洗钱管理部门（含次级的反洗钱管理部门、专业团队）职 责.....	21
17.业务部门	23
18.运营部门职责	25
19.内控审计部门职责	25

20.法务部门职责	26
21.人力资源部门职责	26
22.战略投资部门职责	26
23.技术部门职责	26
24.数据部门职责	27
25.政府关系（公共事务）部门职责	27
26.会计部门职责	27
27.分支机构和相关附属单位管理	28
28.金融控股公司（集团）管理	28
第三章 管理策略	29
29.策略管理	29
29.1 风险管理目标偏离	29
29.2 协同性	30
29.3 数据化	30
第四章 管理政策和程序	31
30.政策路径	31
31.主要内容	31
32.评估规则	32
32.1 评估方法	32
32.2 评估维度	33
33.数据信息源	33
34.评估频率	34

第五章 管理计划	36
35.总体要求	36
36.报告制度	36
37.应急计划	36
37.1 重大风险情况	37
37.2 重大风险	37
38.应对措施	39
第六章 信息系统与数据治理	40
39.基本要求	40
40.系统功能	40
41.系统建设	41
第七章 检查、绩效考核与奖励机制	42
42.内部审计	42
43.反洗钱合规检查	42
44.接受有权机关的监管、调查	43
45.绩效考核和奖惩机制	43
第八章 培训教育	45
46.培训	45
47.宣传	45
第九章 客户身份识别制度	46
48.基本要求	46
49.制度规范	46

第十章 大额交易和可疑交易报告制度	48
50.基本要求	48
51.监测分析策略	48
51.1 监测单位	48
51.2 监测范围	48
51.3 风险维度	49
51.4 合规性	49
52.大额交易	49
53.可疑交易	49
54.名单监测	50
55.后续风险控制措施	50
第十一章 身份资料和交易记录保存制度	52
56.基本要求	52
57.保存范围	52
58.保存标准	53
58.1 客户身份资料	53
58.2 交易记录保存	53
59.保存期限	53
60.保存方式	54
第十二章 保密制度	55
61.基本要求	55
62.保密范围	55

63.涉及跨境事项的保密要求	56
64.管理措施	56
第十三章 附则.....	58

第一章 概述

1.背景

1.1 反洗钱和反恐怖融资（以下如无特殊情形，统称反洗钱）是金融基础设施的重要组成部分，是从事金融业务的各类机构、人员的法定义务，是国际金融监管的惯例和普遍要求。

党中央、国务院高度重视反洗钱工作。《国务院办公厅关于完善反洗钱、反恐怖融资、反逃税监管体制机制的意见》指出：“反洗钱、反恐怖融资、反逃税监管体制机制是建设中国特色社会主义法治体系和现代金融监管体系的重要内容，是推进国家治理体系和治理能力现代化、维护经济社会安全稳定的重要保障，是参与全球治理、扩大金融业双向开放的重要手段。”

从事金融业务的各类机构、人员应当高度重视反洗钱工作，服从和配合监管部门，积极主动履行反洗钱法定义务。

1.2 互联网金融是传统金融机构与互联网企业（以下统称从业机构）利用互联网技术和信息通信技术实现资金融通、支付、投资和信息中介服务的新型金融业务模式。互联网与金融深度融合是大势所趋，将对金融产品、业务、组织和服务等方面产生更加深刻的影响。

互联网金融本质仍属于金融，没有改变金融风险隐蔽性、传染性、广泛性和突发性的特点。从业机构均应纳入金融反洗钱监管范围，同样执行金融反洗钱法律法规及其他监管规定、国际反洗钱标准、反洗钱行业规则。为切实履职，从业机构应建立健全反洗钱风险管理体系

及内控机制。

1.3 从业机构建立健全反洗钱风险管理体系、内控机制应符合监管政策、行业规则的要求。

互联网金融是新生事物和新兴业态，具有不同于其他金融业态的新特点，其所涉及的洗钱、恐怖融资风险同样具有新特征。相应地，从业机构应采用更有针对性的反洗钱方法和工具，需要更有针对性、指向性和专业性的制度安排。

中国人民银行会同银保监会、证监会发布了《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》（以下简称《管理办法》）。

《管理办法》要求中国互联网金融协会（以下简称互联网金融协会）协调各行业自律组织，根据风险防控需要和业务发展状况，组织从业机构制定或调整，报中国人民银行、国务院有关金融监督管理机构批准后公布施行反洗钱工作规则及相关业务、技术标准等行业规则。

在制度层面，反扩散融资等工作与反洗钱存在机制上的联系。从业机构可以建立一套反洗钱风险管理体系及内控机制，同时实现反洗钱、反恐怖融资、反逃税、反扩散融资、国际制裁合规等多项功能目标。

1.4 良好的反洗钱风险管理体系和内控机制对于从业机构具有特殊的重要性。互联网金融业态众多、模式各异、创新速度快，行业相关的洗钱和恐怖融资风险复杂多变，因此可能出现反洗钱监管政策和行业规则不能针对互联网金融行业反洗钱新问题、新风险，及时做出调整的情况。在此情形下，从业机构仍需要满足反洗钱监管制度和

监管政策所设定的风险管理目标、功能和要求。科学合理、运行有效的反洗钱风险管理体系和内控机制，能引导从业机构及其高级管理层、工作人员适时、适度地做出风险应对，主动管理风险，取得良好的效果。

2.应用

本指引是互联网金融协会为引导和协助从业机构采用风险为本方法，建立健全反洗钱风险管理体系和内控机制，而提供的指导意见。

本指引相关内容或直接来源于中国人民银行等反洗钱职能部门已发布的金融反洗钱监管制度政策、监管评价标准，或归纳总结了从业机构按照反洗钱监管要求开展反洗钱工作的一些最佳实践经验，并予以系统化、流程化。

本指引可为过去没有反洗钱工作经验、接受金融监管历史较短的一些从业机构，开展反洗钱工作提供基础性指引。已建立相关政策制度的从业机构可参照本指引内容，对现有反洗钱内控体系进行完善。

反洗钱知识经验不足的从业机构可直接按照本指引框架，结合自身情况在细化充实的基础上建立内部的政策、制度、流程；有较充足的反洗钱知识经验的从业机构可借鉴本指引的框架、思路或具体方法；已建立相关政策制度的从业机构可对照本指引内容，对照现有体系进行评估后完善。

除非另经必要程序，本指引暂不构成《管理办法》所称的行业规则，对互联网金融协会会员以外的从业机构无直接拘束力。但考虑到

互联网金融协会会员单位的行业代表性、互联网金融协会的反洗钱工作职能定位以及本指引的专业性、认可度，从业机构可能因按照低于本指引的要求开展反洗钱工作，而事实上没有采取行业公认的应有的反洗钱工作标准。如此，从业机构不符合勤勉尽责要求。

3.反洗钱监管体系

根据《管理办法》，互联网金融领域要建立监督管理与自律管理相结合的反洗钱监管机制，建立对全行业实质有效的框架性监管规则，同时明确由互联网金融协会协调其他行业自律组织制定行业规则，实现监管和自律管理的有效衔接。

3.1 主要监管制度

3.1.1 法律

《中华人民共和国反洗钱法》（中华人民共和国主席令第五十六号）

《中华人民共和国反恐怖主义法》（中华人民共和国主席令第三十六号）

3.1.2 部门规章

《金融机构反洗钱规定》（中国人民银行令〔2006〕第1号）

《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》（中国人民银行、银监会、证监会、保监会令〔2007〕第2号）

《金融机构大额交易和可疑交易报告管理办法》（中国人民银行

令〔2016〕第3号）

《涉及恐怖活动资产冻结管理办法》（中国人民银行令〔2014〕第1号）

《中国人民银行修改<金融机构大额交易和可疑交易报告管理办法>的决定》（中国人民银行令〔2018〕第2号）

3.1.3 规范性文件

《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》（银发〔2018〕230号）

《中国人民银行 工业和信息化部 公安部 财政部 工商部 法制办 银监会 证监会 保监会 国家互联网信息办公室关于促进互联网金融健康发展的指导意见》（银发〔2015〕221号）

《国务院办公厅关于印发互联网金融风险专项整治工作实施方案的通知》（国办发〔2016〕21号）

3.1.4 其他监管文件

《国务院办公厅关于完善反洗钱、反恐怖融资、反逃税监管体制机制的意见》（国办函〔2017〕84号）

《法人金融机构反洗钱分类评级管理办法（试行）》（银发〔2017〕1号）

《法人金融机构洗钱和恐怖融资风险管理指引（试行）》（银反洗发〔2018〕19号）

3.2 反洗钱主管部门

中国人民银行是国务院反洗钱行政主管部门，组织、协调全国的反洗钱工作，负责反洗钱的资金监测，制定或者会同国务院有关金融监督管理机构制定金融机构反洗钱规章，监督、检查金融机构履行反洗钱义务的情况，在职责范围内调查可疑交易活动，履行法律和国务院规定的有关反洗钱的其他职责。中国人民银行分支机构在中国人民银行的授权范围内，对金融机构履行反洗钱义务的情况进行监督、检查。

3.3 国务院有关金融监督管理机构

国务院有关金融监督管理机构参与制定所监督管理的金融机构反洗钱规章，对所监督管理的金融机构提出按照规定建立健全反洗钱内部控制制度的要求，履行法律和国务院规定的有关反洗钱的其他职责。

3.4 中国反洗钱监测分析中心

中国人民银行设立中国反洗钱监测分析中心，负责大额交易和可疑交易报告的接收、分析，并按照规定向中国人民银行报告分析结果，履行中国人民银行规定的其他职责。

3.5 自律管理

互联网金融协会按照中国人民银行、国务院有关金融监督管理机构关于从业机构履行反洗钱义务的规定，制定并发布各类从业机构执

行《管理办法》所适用的行业规则，配合中国人民银行及其分支机构开展线上和线下反洗钱相关工作，开展洗钱和恐怖融资风险评估，发布风险评估报告和风险提示信息，组织各类从业机构制定并实施反洗钱和反恐怖融资方面的自律公约。

其他行业自律组织按照中国人民银行、国务院有关金融监督管理机构的规定对从业机构提出建立健全反洗钱内控制度的要求，配合互联网金融协会推动从业机构之间的业务交流和信息共享。

4.适用范围

4.1 机构范围

在中华人民共和国境内经有权部门批准或者备案设立的，依法经营互联网金融业务的机构适用于本指引，具体包括：

4.1.1 开展互联网金融业务的金融机构：

（1）政策性银行、商业银行、农村合作银行、农村信用社、村镇银行；

（2）证券公司、期货公司、基金管理公司；

（3）保险公司、保险资产管理公司、保险专业代理公司、保险经纪公司；

（4）信托公司、金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司、贷款公司；

（5）中国人民银行确定并公布的应履行反洗钱义务的从事金融业务的其他机构。

4.1.2 开展互联网支付业务的非银行支付机构。

4.1.3 依法从事以下互联网金融业务的机构，包括但不限于：

- (1) 网络借贷；
- (2) 网络借贷信息中介；
- (3) 股权众筹融资；
- (4) 互联网基金销售；
- (5) 互联网保险；
- (6) 互联网信托；
- (7) 互联网消费金融；

(8) 中国人民银行会同国务院有关金融监督管理机构按照法律规定和监管政策确定、调整并公布的其他业务。

4.1.4 互联网金融协会会员单位。

4.2 风险类别

4.2.1 洗钱和恐怖融资风险(以下如无特殊情形,统称洗钱风险):
不法分子利用从业机构、工作人员及其提供的互联网金融服务或产品,进行洗钱、恐怖融资等违法犯罪活动,危害国家和人民的财产安全,破坏互联网金融管理秩序,同时给从业机构及工作人员带来持续经营能力、资金、声誉等方面损失的可能性。

4.2.2 反洗钱合规管理风险(以下如无特殊情形,统称合规风险):
从业机构及其工作人员因未按照反洗钱法律、行政法规、部门规章及其他规范性文件、经营规则、自律性组织的行业准则、行为守则和职

业操守的要求，履行反洗钱义务或者履行反洗钱义务缺乏必要的有效性，导致不能有效打击洗钱、恐怖融资等违法犯罪活动，受到监管部门处罚、自律组织惩戒或者公众舆论批评的可能性。

5.政策概览

从业机构及其工作人员，特别是董事会、高级管理层，要提高反洗钱意识，建立符合监管期望、与自身社会责任相适应、有利于增强持续经营能力的反洗钱风险管理体系和内控机制。

一应认识到反洗钱及相关联的反扩散融资、反逃税等工作的重要意义，主动预防洗钱、恐怖融资活动，配合有关部门打击各类违法犯罪行为，积极维护经济金融和社会稳定。

一应认识到自身在开展业务和经营管理过程中可能被违法犯罪活动利用，任何洗钱风险事件都可能进一步引发合规风险、声誉风险、法律风险等，进而削弱甚至根本性损害自身持续经营的基础。

一应认识到洗钱风险、合规风险与其他金融风险之间的关联性和传导性，将对洗钱风险和合规风险的管理（以下统称反洗钱风控）纳入全面风险管理框架、依托良好公司治理、置于董事会和高级管理层的管控之下十分必要。

一应认识到反洗钱工作对于董事、高级管理层和全体员工个人合规、职业发展的重要性，所有人员均应勤勉尽责，牢固树立合规意识和风险意识，积极主动工作和学习，不断提升自身的反洗钱风控能力。

一应认识到反洗钱资源稀缺是长期存在的问题，要按照风险为本

方法，合理配置资源，对本机构洗钱风险进行持续识别、审慎评估、有效控制及全程管理，均衡成本收益，有效防范洗钱风险。

6.基本目标

切实发挥从业机构作为国家反洗钱工作的第一道防线作用，自建反洗钱风控机制引导自身反洗钱履职，有效落实反洗钱监管要求、配合有权部门工作，通过自我发展、自我约束让监管放心、社会满意、客户信任，参与共建有利于行业创新发展的良好机制。

7.基本原则

7.1 风险为本原则

从业机构应定期或不定期评估洗钱风险和合规风险，根据风险评估的结果采取相应的反洗钱风控措施。

应在风险高的领域里采取强化的反洗钱风控措施，在风险低的领域里可以采取适度简化的反洗钱风控措施，不断提升反洗钱工作的有效性。

如出现超出自身风险控制能力的情形，从业机构不得与客户建立业务关系或进行交易，已经建立业务关系的，应中止交易并考虑提交可疑交易报告，必要时终止业务关系。

7.2 全覆盖原则

反洗钱风控机制至少应覆盖各项互联网金融业务活动、运营流程

及互联网金融业务合作渠道，贯穿决策、执行和监督全过程；至少应覆盖所有境内外附属单位、分支机构、部门条线、事业部及各层级人员岗位。

7.3 独立性原则

从业机构应从组织架构、制度、流程、人员安排、报告路线等方面确保反洗钱合规管理工作具有应有的独立性和履职充分性，并通过建立科学合理的报告渠道，在合规、风险管理条线与业务条线之间形成相互制衡的运行机制。

7.4 匹配性原则

反洗钱风控机制应当与风险状况相适应，并根据环境变化予以调整。从业机构在决策反洗钱资源投入前，应综合考虑所处行业的风险特征、管理模式、业务规模、产品复杂程度等因素，确保资源投入与所面临的风险状况相当，并根据情况变化及时调整。

7.5 有效性原则

从业机构应将反洗钱风控目标融入公司治理、经营管理、日常业务流程，提升反洗钱风控措施的针对性，确保结果符合预先设定的反洗钱风控目标。

7.6 严格合规原则

从业机构应严格执行反洗钱法律、规则和准则，包括但不限于各类适用于从业机构反洗钱工作的法律、行政法规、部门规章及其他规范性文件、反洗钱行业规则以及其他自律性组织的行业准则、行为守则和职业操守，并采取更有针对性、更严格、更有效的执行措施。

如无反洗钱法律、规则和准则可直接适用于某一种互联网金融新业务或新业态的，从业机构应参照具有类似风险特性的业务、业态所涉及的反洗钱法律、规则和准则所提出的反洗钱风控要求，遵循风险为本原则，设定实质有效的反洗钱风控措施。

从业机构制定或修改反洗钱制度后，应按照规定通过互联网金融反洗钱和反恐怖融资网络监测平台（以下简称网络监测平台）及时向中国人民银行报备。

7.7 勤勉尽责原则

从业机构及其工作人员应在发现、评估、了解、认识洗钱风险过程中，尽到与自身业务、职业、职责、知识、经验、能力等相当的合理注意义务，采取相适应的反洗钱措施有效管控风险。

8.文化建设

从业机构应当在集团或公司层面通过政策、制度、培训、教育、运营、考核、激励、惩戒等多种措施，推行积极的反洗钱合规文化和稳健的反洗钱风险文化，塑造契合自身情况的价值准则，组织和激励全员理解和履行反洗钱义务。

从业机构董事会、监事会、高级管理层应在反洗钱履职方面率先垂范，充分认识反洗钱的重要性，及时全面掌握洗钱和合规风险状况，给予部门和工作人员反洗钱履职充分的支持和激励，传导正确的反洗钱风控观念。

从业机构应确保员工不会因向高级管理层或反洗钱管理部门报告本机构及其工作人员的反洗钱违规行为、不当操作或疑似洗钱活动而遭受打击报复、歧视。

从业机构应确保境内外附属单位、分支机构、部门、事业部及各类人员反洗钱履职言行一致，积极传导反洗钱风控的重要意义。

从业机构应确保文化建设有相适应的制度、机制、技术、系统等为基础和保障。

9.基本要素

完整的反洗钱风险管理体系及内控机制具备以下基本要素：管理架构，管理策略，管理政策和程序，管理计划，信息系统与数据治理，检查、绩效考核和奖惩机制，培训教育，客户身份识别，大额交易和可疑交易报告，身份资料和交易记录保存，保密等。内容上应当涵盖反洗钱履职所涉及的各个方面。

第二章 管理架构

10.基本要求

从业机构应建立组织健全、结构完整、职责明确的反洗钱风控组织架构，明确职责分工，建立层次清晰、相互协调、有效配合的运行机制。

11.反洗钱职责

11.1 职责权限

从业机构应具体明确董事会、监事会、高级管理层及境内外附属单位、分支机构、部门、事业部的反洗钱职责。从业机构应在组织架构、管理流程等方面确保各部门及人员反洗钱履职的独立性，赋予其反洗钱履职所需的充足资源和权限，保证其能够及时获得履职所需数据信息。

从业机构的董事长等主要负责人应对本机构反洗钱工作的合规性和风险管理有效性负首要责任，董事、高级管理层在职责范围内对反洗钱工作的合规性和风险管理有效性承担首要责任。

11.2 反洗钱岗位

反洗钱岗位包括专职从事反洗钱工作的专业岗位和兼职承担反洗钱工作的兼职岗位。

按照职能，反洗钱岗位可包括：1. 合规管理类，负责反洗钱政策

制度建设、流程评审、监管汇报、内部合规检查、系统流程规划等。

2. 风险管理类，负责交易监测分析、业务审核、客户评级、风险评估、可疑线索排查、案件管理等。3. 合规科技类，负责风险监测分析工具建设、系统设计、工具研发创新。4. 操作运营类，负责执行反洗钱任务流程，完成相关操作。

反洗钱合规管理岗位职级不得低于本机构其他合规管理岗位职级，反洗钱风险管理岗位职级不得低于本机构其他风险管理岗位职级。

反洗钱工作任务外包必须符合反洗钱监管制度和行业规则的要求，并要求并确保外包方的工作符合反洗钱法律、规则和准则。

除风险极低的机构外，从业机构应配备专职反洗钱人员，不得以兼职人员替代专职人员，反洗钱管理部门兼职反洗钱人员占全部反洗钱工作人员的比例不得高于 80%。

对于风险高或者反洗钱监管部门、自律组织明确提出要求的高风险业务条线，从业机构应在该部门或业务条线配备专职反洗钱人员。从业机构在业务部门安排反洗钱岗位职责时，应注意避免因一人担任的多个岗位之间出现利益冲突、职能冲突。

11.3 人员管理

从业机构在聘用员工、任命或授权高级管理人员、选用洗钱风险管理人员、引入战略投资者、引入新的大股东或控股股东之前，应对相关人员是否涉及刑事犯罪、是否存在其他犯罪记录及过往履职经历

等情况进行充分的背景调查，评估可能存在的洗钱风险。对于存在风险的人员，从业机构应采取适当的管控措施，杜绝本机构被不法分子利用。

负责反洗钱合规管理或风险管理工作的高级管理人员应具备较强的履职能力和职业操守，具有五年以上合规或风险管理工作经历，或者具有所在行业十年以上工作经历。

反洗钱专职人员和兼职人员均应具备必要的履职能力和职业操守。除高管人员外，从业机构至少应配备一名有三年以上金融行业从业经历的反洗钱专职人员或兼职人员。

12.董事会职责

除依照《公司法》、反洗钱监管制度的规定外，可考虑由董事会履行以下反洗钱职责：

- （1）确定合规、风险管理基本政策；
- （2）确立洗钱风险管理文化建设目标；
- （3）审定合规、风险管理策略；
- （4）设定合规、风险管理偏好；
- （5）审批风险管理的基本政策和关键性程序；
- （6）督促高级管理人员履职；
- （7）定期审议反洗钱工作报告；
- （8）审批反洗钱重大事项；
- （9）及时了解重大洗钱风险事件及处理情况；

（10）其他相关职责。

下设风险、合规等专业委员会的董事会，应当将反洗钱工作纳入相关专业委员会的职责范围内。

未设立董事会的从业机构，由执行董事承担应由董事会履行的反洗钱职责。

13.监事会职责

除依照《公司法》、反洗钱监管制度的规定外，建议考虑由监事会承担合规、风险管理的监督责任，负责监督董事会和高级管理层反洗钱履职并督促其整改，对反洗钱风控提出建议和意见。

未设立监事会的从业机构，由监事承担应由监事会履行的反洗钱职责。

14.高级管理层职责

除依照《公司法》、反洗钱监管制度的规定外，可考虑由高级管理层履行以下反洗钱职责：

（1）组织开展合规、风险管理文化建设；

（2）建立并及时调整管理组织架构，明确反洗钱管理部门、业务部门及其他部门在洗钱风险管理中的职责分工和协调机制，为反洗钱管理部门履行职责配备充分和适当的人员，确保反洗钱管理部门的独立性；

（3）制定书面的合规、风险管理政策，组织开展反洗钱风险评

估，并根据风险评估结果以及法律、规则和准则的变化情况适时修订相关政策，报经董事会审议批准后传达给全体员工；

（4）贯彻执行合规、风险管理政策，审核批准反洗钱合规管理工作计划；

（5）定期向董事会报告反洗钱工作情况，及时向董事会及其下设委员会和监事会报告重大洗钱风险事件；

（6）组织反洗钱信息系统及相关数据治理工作；

（7）建立反洗钱绩效考核和奖惩机制，完善执行和问责机制，确保能及时对所发现违规问题、风险采取适当的纠正措施，追究责任人的相应责任；

（8）其他相关职责。

14.1 反洗钱负责人

从业机构应在公司和集团层面任命或授权一名高级管理层人员牵头负责反洗钱工作，作为反洗钱负责人。如风险管理和合规管理分属于不同的高级管理层人员负责的，从业机构可根据自身组织架构、风险偏好、管理策略，选择其中一人兼任。反洗钱工作任务重或合规、风险管理难度较大的从业机构，应考虑在首席风险官、首席合规官等职位之外，另设首席反洗钱官，并纳入高级管理人员。

反洗钱负责人应牵头组织协调反洗钱工作，督促、管理反洗钱管理部门执行反洗钱计划，联系、协调管理其他部门的高级管理人员，向高级管理层报告反洗钱情况。

反洗钱负责人不分管或不独立分管业务经营条线，有权直接向董事会报告反洗钱工作。任命或调整反洗钱负责人的，应当得到董事会批准。对于不符合监管要求和期望的反洗钱负责人，高级管理层应提请董事会予以调整。

任命或者调整上述高级管理人员，应当按照规定通过网络监测平台向中国人民银行备案。

14.2 反洗钱工作领导小组

14.2.1 职能和组成方式

反洗钱法律法规未见有关于反洗钱工作领导小组的规定，从业机构可酌情考虑是否成立反洗钱工作领导小组。反洗钱工作领导小组负责组织协调公司反洗钱工作，是日常反洗钱工作的决策机构，是高级管理层履行反洗钱职责的重要组织形式，建议由首席执行官或总经理任组长，反洗钱负责人和其他高管人员任副组长，各相关部门负责人为成员。

反洗钱工作领导小组并非法定的从业机构反洗钱内部组织形式，但因其契合我国金融监管文化和监管惯例，而易受到反洗钱监管部门的推介和赞赏。

14.2.2 职责建议

反洗钱工作领导小组职责建议如下：

（1）审定重要反洗钱工作计划、系统建设项目，并监督各部门落实；

(2) 研究规划反洗钱部门及人员设置, 研究解决反洗钱工作重要资源投入;

(3) 组织协调各部门参与反洗钱工作;

(4) 审查重要反洗钱制度、流程;

(5) 研究应对重大反洗钱风险事件;

(6) 对涉及反洗钱严重违规的部门、人员, 提出处理意见;

(7) 其他日常工作的重大决策。

14.2.3 运行

反洗钱工作领导小组的工作方式包括但不限于会议、现场督导、调研等。如本地区反洗钱监管部门将反洗钱工作领导小组履职情况纳入工作考核或风险评估范围, 从业机构则应考虑建立反洗钱工作领导小组相关组织制度, 细化工作流程和工作要求, 例如反洗钱工作领导小组每年至少召开 2 次工作会议。

15.内部组织架构

各附属单位、分支机构、部门和事业部的负责人应对本机构、本部门的反洗钱工作合规性和风险管理有效性负首要责任。

从业机构应根据附属单位、分支机构、部门和事业部的经营范围、业务规模、工作任务及风险状况的不同, 分别采取设立反洗钱管理部门、组建反洗钱专门工作团队、确定反洗钱专职岗位和明确反洗钱兼职岗位等措施, 确保组织措施到位, 由其在相应范围内牵头组织实施反洗钱工作。

反洗钱合规管理和反洗钱风险管理职能，既可同时归属于一个部门，又可以分属不同部门。从减少机构内部协调成本、便于沟通联系外部监管等角度考虑，最好能设立一个专门的反洗钱管理部门，由其牵头反洗钱合规管理和反洗钱风险管理工作，并在该部门内部设下一层级部门相应负责合规、风险管理等工作。

反洗钱合规管理职能应与内部审计职能分离，合规管理职能的履行情况应受到内部审计部门定期的独立评价。

15.1 事业部制或类事业部制下的反洗钱风控

现行反洗钱监管制度以法人监管、层级管理相结合为基础的，并没有考虑到很多从业机构采用的事业部、事业群等架构，这些从业机构在执行反洗钱法律、规则和准则过程中存在一定的不适应性。例如，一些机构出于合规、市场等方面的考虑，设立子公司、孙公司并以其名义取得某些金融业务许可、以其名义对外开展经营活动，但合规、风控等工作的实际承接主体及人员仍存在于上层架构或集团层面。

对于此种架构，反洗钱监管制度并未予以规范，也未予以确认或禁止。考虑到互联网金融业态快速迭代更新的特质，采用类似架构开展反洗钱风控的从业机构应注意处理以下问题：

（1）反洗钱监管部门对从业机构的建制及其部门、人员的独立性有专门规定，无法由上层实体或集团的部门、人员承担反洗钱工作职责时，从业机构应考虑增设专岗专人，优先满足合规要求。

（2）不违反反洗钱和其他金融监管相关的法律、规则和准则，

特别是要符合数据、业务相关防火墙制度、保密制度等强制性要求，人员在不同层级架构上履职不存在合规风险、道德风险、利益冲突。

（3）确保实际分配到各层架构的人员、技术及其他反洗钱资源应符合反洗钱监管的最低配置要求，能够满足各个架构实体同时并发反洗钱日常工作任务的运行要求。

（4）有清晰明确的授权问责机制。某一从业机构出现反洗钱违规行为或风险事件，外部监管部门一般不直接对反洗钱工作实际承接主体作出处罚决定，但从业机构内部仍应追究上层架构或集团中实际承担反洗钱职责的业务部门、反洗钱管理部门、其他部门及人员的合规责任。

（5）加强与监管部门的汇报沟通。从业机构可以按照实质重于形式的原则，将上层实体或集团层面实际承担相关反洗钱职责的部门、人员归于对应的被监管机构中，作为本机构反洗钱义务机构的部门、人员并完成相关向监管报备的程序。在此情形下，从业机构可在相关监管报告、报表中，对所报备或披露的信息做出备注。

16.反洗钱管理部门（含次级的反洗钱管理部门、专业团队）职责

从业机构应建立反洗钱管理部门或指定部门作为反洗钱管理部门，牵头开展反洗钱工作，推动落实各项反洗钱工作，可考虑由其履行以下职责：

（1）及时按照反洗钱监管制度和行业规则的要求，根据本机构

反洗钱工作实际，及时向高级管理层提出制定完善反洗钱风控政策的建议；

（2）贯彻落实反洗钱法律法规和监管要求，建立健全反洗钱内部控制制度及内部检查机制；

（3）制定并执行反洗钱风控计划，持续审核评价各项政策、规程的合规性和有效性，检查反洗钱工作制度的执行情况，对违规行为提出整改建议，督促各部门完善制度流程、提升工作有效性；

（4）提出建立健全反洗钱工作协调机制的建议，推动其他部门编制反洗钱风控制度，督促业务部门完善反洗钱工作相关流程；

（5）组织或协调各相关部门开展客户洗钱风险分类管理；

（6）组织落实交易监测和名单监控的相关要求，按照规定报告大额交易和可疑交易；

（7）负责与监管部门的日常反洗钱工作联系，牵头配合反洗钱监管，协调配合反洗钱行政调查；

（8）组织或协调相关部门开展反洗钱宣传和培训，推动建立健全反洗钱绩效考核和奖惩机制，推动建设完善反洗钱信息系统；

（9）其他相关职责。

17.业务部门职责

业务部门泛指面向个人和机构客户并承担建立维护客户关系、执行客户交易指令、管理客户资金账户、研发金融服务产品、发展维持金融机构合作关系等职责的各类部门，例如，2B 或 2C 的互联网金融

服务部门、产品部门、市场营销部门、商务发展部门等。实行事业部制的从业机构应将反洗钱职责进一步细化至下级的组织架构或子、孙公司。

业务部门应在业务范围内承担反洗钱直接责任，可考虑由其履行以下职责：

（1）识别、评估、监测本业务条线的洗钱风险，及时向反洗钱管理部门报告；

（2）建立相应的工作机制，将洗钱风险管理要求嵌入产品研发、流程设计、业务管理和具体操作；

（3）开展或配合开展客户身份识别和客户洗钱风险分类管理，采取针对性的风险应对措施；

（4）以业务（含产品、服务）的洗钱风险评估为基础，完善各项业务操作流程；

（5）完整并妥善保存客户身份资料及交易记录；

（6）开展或配合开展交易监测和名单监控，确保名单监控有效性，按照规定对相关资产和账户采取管控措施；

（7）配合反洗钱监管和反洗钱调查工作；

（8）组织或配合开展本业务条线反洗钱工作检查；

（9）开展本业务条线反洗钱宣传和培训；

（10）配合反洗钱管理部门开展其他反洗钱工作。

以上职责是对所有业务部门反洗钱职责的概括性描述，从业机构应注意区分不同业务条线的业务范围、职责、与客户之间沟通互动的

方式内容、相匹配的反洗钱能力等客观因素，进一步细化对应部门的反洗钱职责，以提升制度的可操作性。例如，对于渠道部门的反洗钱职责可强调其在评估反洗钱风险措施脆弱性方面的作用、推进与业务合作伙伴在双方反洗钱职责划分中的作用等；对于销售部门可强调其在采集、获取、评价客户身份信息等尽职调查信息资料方面，在日常可疑交易行为监控等方面的责任；对于产品部门，可强调其将洗钱风险管理要求通过产品研发、流程设计等工作进行落实的责任等。

18.运营部门职责

建议由运营部门及其相关作业中心负责客户信息资料审核，反洗钱监测分析数据制式化处理，制定或者督促业务部门制定将反洗钱风控要求嵌入业务流程的工作计划，确保处于本部门控制之下的流程符合反洗钱风控要求，对业务部门的反洗钱操作行为实施审核、跟踪、监督，及时提出改进反洗钱工作效率和有效性的工作方案。

19.内控审计部门职责

建议由内控审计部门负责管理审核各项反洗钱内部制度，推动反洗钱制度与机构内部其他制度之间的整合；对反洗钱监管制度、行业规则的执行情况、内控制度的执行及有效性、反洗钱风险管理情况进行独立、客观的审计评价。未设立内控审计部门的从业机构，应明确相关职责由承担审计职能的其他部门承担。

20.法务部门职责

建议由法务部门负责研究通过合同等法律工具落实反洗钱监管制度所提出的客户身份识别、可疑交易监测等要求，避免本机构因实施反洗钱合规流程而产生法律风险。

21.人力资源部门职责

建议由人力资源部门负责保障反洗钱工作所需的人力资源，合理配置洗钱风险管理职位、职级和人数，选用符合标准的人员，建立反洗钱绩效考核和奖惩机制，开展或配合开展反洗钱宣导和培训。

在聘用员工、任命高级管理层人员之前，人力资源部门应会同有关部门对其是否涉及刑事犯罪、是否存在其他犯罪记录及过往履职经历等情况进行充分的背景调查，评估其可能存在的反洗钱方面的风险后，决定是否录用或任命，如果风险较高或是无法控制风险但仍需要录用、任命的，应当提交高级管理层决定。

22.战略投资部门职责

建议由战略投资部门负责在引入战略投资者、新的大股东或控股股东之前，负责对拟引入投资者进行充分的背景调查，评估可能存在的洗钱风险，杜绝本机构被不法分子利用。

23.技术部门职责

建议由技术部门负责反洗钱相关系统的开发、日常维护及升级等

工作，为反洗钱工作提供必要的硬件设备和技术支持，根据相关数据安全 and 保密管理等监管要求，对客户、账户、交易信息及其他相关电子化信息进行保管和处理。

24.数据部门职责

建议由数据部门负责规划反洗钱相关数据治理工作，加强反洗钱工作所需数据资源保障，实施和优化反洗钱数据方案，及时提供监管部门、司法机关和行业自律组织所要求提供的反洗钱相关数据信息。

25.政府关系（公共事务）部门职责

建议由政府关系部门建立、维护、加强与中国人民银行、银保监会、证监会等监管部门及行业自律组织的工作联系，协助反洗钱管理部门传达和解读监管政策信息，向监管部门汇报本机构反洗钱工作情况和政策诉求，协调配合监管部门开展对本机构的检查、反洗钱调查等工作。

26.会计部门职责

建议由会计部门负责从会计操作、结算管理、账户管理等角度，参与大额交易与可疑交易的报告工作，参与客户洗钱风险识别工作，协助开展对子公司反洗钱工作的管理，协助有关部门对有关涉嫌洗钱的客户存款查询、冻结、扣划工作。

27.分支机构和相关附属单位管理

从业机构应加强对境内外分支机构和相关附属单位的管理监督，采取必要措施保证反洗钱合规、风控政策和程序在境内外分支机构和相关附属单位得到充分理解与有效执行，保持风险管理的一致性和有效性。

对于在境外设有分支机构或相关附属单位的从业机构，如果国内监管规定、行业规则的要求比所驻国家或地区的相关规定更为严格，但所驻国家或地区法律禁止或限制境外分支机构和相关附属单位实施的，从业机构应采取适当的其他措施予以应对，并向中国人民银行报告。如果经穷尽可能的手段仍无法有效控制风险的，从业机构应考虑在适当情况下关闭境外分支机构或相关附属单位。

28.金融控股公司（集团）管理

金融控股公司（集团）应当在集团层面实施统一的反洗钱风控政策，确保相关政策在全集团内涉及互联网金融业务的各子公司得到有效执行。金融控股公司（集团）应建立适用于集团层面的反洗钱风险评估体系，注重识别和应对跨市场、跨行业和跨机构的风险，防范洗钱风险在不同子公司间的传导。

除了执行集团层面统一的反洗钱风控政策外，金融控股公司（集团）应要求涉及互联网金融业务的各子公司结合自身的业务、产品特点，建立健全各自的反洗钱风控机制。

第三章 管理策略

29.策略管理

从业机构应当制定科学、清晰、可行的反洗钱风控策略，定期评估其有效性，并根据评估情况及时进行调整完善。

从业机构的反洗钱风控策略，应与本机构的风险偏好相适应，可分别针对反洗钱合规风险、洗钱风险等不同种类性质的风险，选择风险承担、风险规避、风险转移、风险转换、风险对冲、风险补偿和风险控制等策略。例如，反洗钱合规管理可选择风险规避策略，坚持底线思维，对董事、高级管理层和其他员工严重违规违法行为零容忍，守住不发生重要金融违法犯罪行为的底线，不能让互联网金融业务成为洗钱、恐怖融资等违法犯罪活动的通道。

反洗钱风控策略应可以通过员工培训教育、专门政策宣贯等形式，在机构内部充分传导，成为完善相关制度和工作机制，合理配置、统筹安排人员、资金、系统等反洗钱资源的基础。

29.1 风险管理目标偏离

从业机构在开展日常合规行为监测、反洗钱内部审计检查、风险评估、流程测试、绩效考核等工作后，应将各附属单位、分支机构、部门和事业部的反洗钱工作情况，与已确定的反洗钱风控策略进行对照。当发现有偏离策略或突破风险偏好目标的情况发生时，反洗钱管理部门应当分析或者会同相关部门分析原因，制定整改工作计划并组

织实施。

29.2 协同性

从业机构应当统筹考虑反洗钱因素，将反洗钱纳入全面风险管理体系，进行均衡管理。一旦出现反洗钱风控措施、要求低于其他种类风险管理一般水平的情况，监管部门和自律组织可能会认为该从业机构对反洗钱工作的重要性缺乏必要认识，风险管理策略失当。

从业机构应当积极开展普惠金融工作，根据本机构业务实际、客户的群体属性、洗钱风险评估结果和监管部门的要求，在有效管理洗钱风险的基础上，采取合理的客户身份识别措施，为社会不同群体提供差异化、有针对性的金融服务。

29.3 数据化

从业机构应当发挥互联网金融行业的技术优势，发展和创新风控工具，实现反洗钱风控的数据化，在保持基本政策稳定性的前提下，加快风控工具研发实施的速度。

第四章 管理政策和程序

30.政策路径

从业机构最初建立反洗钱风控政策和程序，可能主要是依照监管制度、行业规则或者参考同业机构的做法。但应该认识到，每家机构面临着不尽相同的风险状况和内部资源，更需要发展个性化的内部政策和程序。且按照中国人民银行反洗钱监管政策、国际反洗钱标准，从业机构应当在风险为本反洗钱方法框架下，自主建立健全反洗钱风控政策和程序。

从业机构应根据定期或不定期开展的风险评估结果，查找风险漏洞和薄弱环节，以此作为制定、调整和完善反洗钱风控策略、政策和程序的依据，合理配置反洗钱资源，采取有针对性的风控措施。

31.主要内容

反洗钱风控政策和程序，包括但不限于以下内容：

（1）基于风险为本的反洗钱方法建立的程序，包括针对不同种类风险的识别、评估、监测、控制或缓释的程序；

（2）反洗钱合规管理等内控制度，并在可能的情况下予以数据化和流程化；

（3）风险报告；

（4）应急计划；

（5）信息保密和信息共享。

32.评估规则

本指引所体现的评估规则，旨在方法论层面上为从业机构提供借鉴，并非要求从业机构必须采用本指引所推荐的具体方法、模型。从业机构应在不低于反洗钱监管规定的基础上，参考本指引的方法，发展自身的风险评估规则，并积极发挥互联网金融行业在技术方面的优势，创新出更有效的评估方法。

32.1 评估方法

从业机构应充分发挥自身技术和数据资源优势，探索建立定性与定量相结合的风险评估体系。从业机构在政策层面不需要具体确定各类风险评估具体方法，但应明确建立评估体系所涉及的一些基本规则。例如，风险评估体系应具有必要的可解释性，评估流程应具有可稽核性或可追溯性。

在其他条件不变的情况下，固有风险越高，脆弱性越强，风险评级越高；而控制措施越有效，控制效果越好，风险评级可下调。

固有洗钱风险 洗钱控制风险	低 [0-1]	中低 (1-2]	中 (2-3]	中高 (3-4]	高 (4-5]
弱 [0-1]	中	中高	高	高	高
较弱 (1-2]	中低	中	中高	高	高
可接受 (2-3]	低	中低	中	中高	高
较强 (3-4]	低	低	中低	中	中高
强 (4-5]	低	低	低	中低	中

从业机构应根据反洗钱工作形势变化，或是理论、工具创新的情况，定期对已建立的风险评估体系进行审查，不断改进完善。

从业机构应将风险评估结果运用到调整经营策略、发布风险提示、完善制度流程、增强资源投入、加强账户管理和交易监测、强化名单监控、严格内部检查和审计等工作环节中去。

32.2 评估维度

基本维度包括客户、产品（业务）、地域、行业（职业）等，并在此基础上通过公式、模型，得到评分或评级。

33.数据信息源

从业机构应当根据风险评估需要，统筹确定各类信息的来源，包括但不限于以下来源：

（1）金融行动特别工作组（FATF）、亚太反洗钱组织（APG）、欧亚反洗钱与反恐融资组织（EAG）、巴塞尔银行监管委员会（BIS）、

国际证券监管委员会组织（IOSCO）、国际保险监督官协会（IAIS）等国际组织、国家和行业的风险评估报告、研究成果、形势分析、工作数据等；

（2）国家相关部门通报的上游犯罪形势、案例或监管信息；

（3）中国人民银行、银保监会、证监会、外汇局等金融监管部门发布的洗钱风险提示和业务风险提示，互联网金融协会及其他自律组织发布的风险提示、研究报告、风险评估报告；

（4）在与客户建立业务关系时和业务关系存续期间，客户披露的信息、客户经理或其他人员的工作记录、保存的交易记录、委托其他金融机构或第三方对客户进行尽职调查工作所获取的合法信息；

（5）内部管理或业务流程中获取的信息，包括内部审计结果。

34.评估频率

从业机构应对每一类被评估对象的某一种风险的风险评估频率作出细化安排，一般情况下，其已获得风险评级越高的评估对象的评估频率相对更高。

出现以下情形时，从业机构应当及时开展洗钱风险评估：

（1）因工作需要，对单项业务（含产品、服务）或特定客户进行评估；

（2）反洗钱监管政策发生重大变化；

（3）出现重要风险事件或突发情况；

（4）拓展新的销售或展业渠道、开发新产品或对现有产品使用

新技术、拓展新的业务领域；

（5）设立新的境外机构；

（6）开展重大收购和投资。

对产品（业务）的洗钱风险评估结果，会运用到其他的风险评估过程中去，在反洗钱风险管理框架里具有一定的基础性，从业机构可考虑建立有关产品（业务）反洗钱风险评估方法及结论的清单。

第五章 管理计划

35.总体要求

从业机构应按年度制定反洗钱工作计划，明确各附属单位、分支机构、部门和事业部的反洗钱风控工作目标、措施和要求，并由反洗钱管理部门牵头组织实施。

从业机构应在每年一季度内完成计划制定工作，报高级管理层批准后实施，并在下一年一季度内完成上一年度的计划执行工作报告（反洗钱工作报告），向高级管理层及董事会报告。

36.报告制度

从业机构应建立反洗钱风险及合规工作报告制度。对于反洗钱风险评估情况、风险事件、风险异动等情况，境内外分支机构、相关附属单位应当及时向总部反洗钱管理部门报告，各部门、事业部应及时向本机构的反洗钱管理部门报告。对于反洗钱风险评估情况、合规管理工作情况、反洗钱工作计划制定执行情况、风险事件、风险异动等情况，反洗钱管理部门应及时向董事会和高级管理层报告。

37.应急计划

从业机构应明确应急计划制度，针对反洗钱工作可能遇到的洗钱、恐怖融资、制裁合规等风险，提出有针对性的应对措施，并据此对董事会、高级管理层及各附属单位、分支机构、部门和事业部的风

险应对行为作出指引。

从业机构应根据自身战略、业务、技术的迭代更新情况，对应急计划进行及时更新、演练或测试，确保能够及时应对和处理紧急或危机情况。

37.1 重大风险情况

应急计划应至少针对以下的重大风险情况，并可进一步细化出每一类风险情况中不同等级的细分风险：

（1）涉及本机构及其分支机构、附属单位的重大反洗钱、恐怖融资事件。

（2）涉及本机构股东、受益所有人、实际控制人、高级管理层的重大反洗钱、恐怖融资事件。

（3）涉及本机构及其分支机构、附属单位的反洗钱重大违规行为。

（4）涉及本机构及其分支机构、附属单位的重大反洗钱负面新闻报道。

（5）涉及本机构股东、受益所有人、实际控制人、高级管理层的重大反洗钱负面新闻报道。

（6）境内外反洗钱监管要求的重要调整。

（7）其他能出现的重大风险情况。

37.2 重大风险

从业机构反洗钱工作如果涉及以下情形的，可考虑将其列入“重大”风险、行为或事件：

（1）影响本机构或者子公司申请、取得、续展金融业务经营许可或登记备案的；

（2）影响高管人员申请、取得、保持任职资格的；

（3）导致本机构或工作人员依法被追究刑事责任的；

（4）导致本机构或工作人员被司法机关依法采取强制措施的；

（5）导致本机构被处以责令停业整顿或者吊销其经营许可证，工作人员被处以取消其任职资格、禁止其从事有关金融行业工作等重罚的；

（6）引发群体事件的；

（7）出现重要业务合作渠道中断、金融市场参与资格受限等情形，而无法正常提供互联网金融服务的；

（8）直接或间接导致各类监管评级、信用评级被降级；

（9）重大资金或资产损失；

（10）涉及权威媒体报道的重大洗钱、恐怖融资事件；

（11）发现或有合理理由怀疑客户涉及洗钱、恐怖融资等活动，且资金金额特别巨大或资产价值特别巨大，或是属于重要敏感事项的；

（12）涉及跨境洗钱、恐怖融资案件，且数额较大或社会影响较大的；

（13）可能导致境外监管部门调查或处罚的；

(14) 重大泄密事件;

(15) 其他可能导致本机构或工作人员遭受重大损失的。

38.应对措施

从业机构应针对不同种类、不同级别的风险事件，迅速成立风险应对小组，召集相关部门形成风险应对方案，第一时间向董事会进行报告。风险事件的风险级别越高，应对小组牵头负责人的层级应越高，以确保有足够的资源调度能力。

第六章 信息系统与数据治理

39.基本要求

从业机构应建立完善的、功能齐全的反洗钱系统或模块，有效支持反洗钱工作开展，并定期或不定期对反洗钱系统或模块进行评估，根据评估结果不断优化完善。

反洗钱相关信息系统应具有必要的数据整合能力，采集覆盖所有业务（含产品、服务）和客户的信息，及时、准确、完整采集和记录洗钱风险管理所需信息。

信息系统应尽可能支持反洗钱履职，减少人工成本，提升反洗钱工作效能。

40.系统功能

从业机构应加强数据治理，建立健全数据质量控制机制，积累真实、准确、连续、完整的内外部数据，用于洗钱风险识别、评估、监测和报告。反洗钱数据的存储和使用应符合数据安全标准、满足保密管理要求。

反洗钱信息系统及相关系统包括但不限于以下主要功能，以支持洗钱风险管理的需要：

（1）支持洗钱风险评估，包括业务洗钱风险评估和客户洗钱风险分类管理；

（2）支持客户身份识别、客户身份资料及交易记录等反洗钱信

息的登记、保存、查询和使用；

- (3) 支持反洗钱交易监测和分析；
- (4) 支持大额交易和可疑交易报告；
- (5) 支持名单实时监控和回溯性调查；
- (6) 支持反洗钱监管和反洗钱调查。

41.系统建设

从业机构应建立与业务规模、风险状况等相匹配的信息科技基础设施。在保密原则基础上，从业机构平台应根据工作职责合理配置本机构各附属单位、分支机构、部门和事业部的信息系统使用权限，确保各级人员有效获取洗钱风险管理所需信息，明确工作程序，按照规定将客户身份信息和交易记录迅速、便捷、准确地提供给监管机构、执法机构等部门。从业机构平台反洗钱信息系统应统筹考虑保存范围、方式和期限，确保客户身份信息和交易记录完整准确。

从业机构不得违反规定设置信息壁垒，阻止或影响其他从业机构正常获取开展反洗钱工作所必需的信息和数据。

第七章 检查、绩效考核与奖励机制

42.内部审计

从业机构应将反洗钱纳入内部审计范围，检查和评价其合规性和有效性，确保本机构在评估风险的基础上，确定了适当的反洗钱风控措施并有效运行了相关流程。

审计范围、方法和频率应当与洗钱风险状况相适应，原则上应至少每两年开展一次。反洗钱内部审计可以是专项审计或与其他审计项目结合进行。

内部审计过程中发现反洗钱有关的工作标准或相关制度有缺陷或未被执行的，应提出整改意见及纠正建议。反洗钱内部审计报告应当提交董事会或其授权的专门委员会。董事会或其授权的专门委员会应当针对内部审计发现的问题，督促高级管理层及时采取整改措施。内部审计部门应当跟踪检查整改措施的实施情况，涉及重大问题的整改情况，应及时向董事会或其授权的专门委员会提交有关报告。

反洗钱内外部审计工作应当均衡。在发展初期，从业机构可能较缺乏内部审计资源，应有意识地多借助外部审计的力量发现问题、改进工作。

43.反洗钱合规检查

从业机构根据工作需要，定期或不定期安排对业务部门、分支机构、相关附属单位的反洗钱合规检查，督促被检查对象合规履职。

原则上应每年组织至少一次反洗钱检查，反洗钱检查可以是专项检查或与其他检查、评价项目结合进行。

44.接受有权机关的监管、调查

从业机构应接受中国人民银行及其分支机构依法开展的反洗钱现场检查、非现场监管和反洗钱调查，配合其他监管机构、有权机关依法开展的反洗钱监管、调查等工作，包括但不限于：

（1）按照中国人民银行及其分支机构的时限要求提供相关信息、数据和资料，对所提供的信息、数据和资料的真实性、准确性、完整性负责；

（2）不得拒绝、阻挠、逃避监督检查和反洗钱调查，不得谎报、隐匿、销毁相关信息、数据和资料；

（3）开展协查，及时、如实、完整对外提供调查的内容；

（4）冻结客户资产应严格按照法律要求执行，在未得到有权机关确认前不得轻易解除冻结措施。

从业机构可就上述事项指定高管人员和部门牵头负责，组织相关部门、人员参与。

45.绩效考核和奖惩机制

从业机构应建立反洗钱绩效考核和奖惩机制，将反洗钱工作评价纳入对每名员工的绩效考核标准中，根据不同部门、岗位实际承担的反洗钱工作任务，设定员工的绩效目标。人力资源部门在组织开展绩

效考核时，应听取或督促其他考核主体听取反洗钱管理、内部审计等部门的意见。

从业机构应定期对反洗钱工作成绩突出的机构和个人进行评选和表彰，并给予通报表彰、积分奖励或其他适当形式的表扬；设立反洗钱举报通道，鼓励员工对内部人员涉嫌洗钱或其他严重的反洗钱违规行为进行举报，对有功人员按照规定给予表彰奖励；对于发现重大可疑交易线索或防范、遏止相关犯罪行为的员工给予适当的奖励或表扬。

从业机构应对反洗钱违规问题，分级分类进行处理，对于未有效履行反洗钱职责的，应予以问责；对于因反洗钱违规而受到外部处罚惩戒或致使本机构受到外部处罚惩戒的，应进行处分；对于发现或应知反洗钱违规行为而隐瞒不报的，应从严处分。

第八章 培训教育

46.培训

从业机构应建立反洗钱培训制度，制定反洗钱培训计划，确保全体员工充分知晓反洗钱监管政策及其所承担的反洗钱义务，提高全员反洗钱意识和水平。

反洗钱培训应遵循“不同对象、不同方式、不同层次、不同内容”的原则，包括新员工的入职培训、管理人员和业务人员的持续培训、反洗钱岗位人员专业培训等，覆盖从董事会成员到基层员工的各层级人员。原则上，每名从业人员应每年至少接受一次与本岗位反洗钱工作职责相匹配的反洗钱培训教育。必要时，反洗钱培训应延伸至重要的业务合作伙伴、重要客户及其工作人员。

反映反洗钱培训工作的有关资料应及时归档、留存，完整反映培训开展情况，以便于监管部门的评估和考核。

47.宣传

从业机构应建立反洗钱宣传制度，通过向公众宣传反洗钱法规，逐步形成反洗钱宣传培训工作制度化、常态化、系统化，保证良好的金融秩序和社会风气，夯实反洗钱及反恐融资工作的社会基础。

第九章 客户身份识别制度

48.基本要求

从业机构应建立专门的客户身份识别制度，并采取必要的技术手段，将客户身份识别制度中的各项要求嵌入业务流程、操作规程中，确保以下基本要求得以实现：

- （1）勤勉尽责，了解客户；
- （2）了解客户的真实身份及其建立业务关系、进行交易的目的和意图；
- （3）了解非自然人客户的受益所有人情况，了解自然人客户的交易是否为本人操作和交易的实际受益人；
- （4）不得为身份不明或者拒绝身份查验的客户提供服务或者与其进行交易，不得为客户开立匿名账户或者假名账户；
- （5）不得与明显具有非法目的的客户建立业务关系。

49.制度规范

从业机构应建立制度或操作规程，具体落实以下要求：

- （1）客户身份识别工作的基本原则，包括风险为本、勤勉尽责、了解客户等；
- （2）基本客户管理政策，包括不予接纳的客户范围、拒绝客户交易的情形等；
- （3）客户身份措施及其规格要求，包括识别、核验身份的方式，

需采集的资料信息，留存资料等；

（4）在与客户建立业务关系或进行规定范围的特定交易时的客户身份识别措施；

（5）客户风险分类标准及客户风险分类程序；

（6）重新识别客户的要求；

（7）持续的客户身份识别措施；

（8）客户信息、身份资料的登记、采集、核验、留存、更新；

（9）对非自然人客户的受益所有人的客户身份识别措施；

（10）对外国政要、国际组织高级管理人员及其特定关系人的客户身份识别措施；

（11）对代理他人办理业务的人员的客户身份识别措施；

（12）与其他从业机构、金融机构等开展业务合作时的客户身份识别相关要求；

（13）其他特定高风险客户的强化客户身份识别措施；

（14）依托第三方开展客户身份识别的措施。

第十章 大额交易和可疑交易报告制度

50.基本要求

从业机构应制定专门的反洗钱监测分析方案，或是在已有的风险监测方案中针对洗钱、恐怖融资等风险的特殊性，增设专门的反洗钱内容。

反洗钱监测分析方案应针对线上交易的特点，丰富数据来源渠道和监测分析的维度，创新发展技术工具，深度挖掘数据，识别发现涉及洗钱、恐怖融资等违法犯罪活动的资金、交易和行为。

从业机构应定期或者在发生特定风险时，评估上述方案、系统的有效性，并及时予以完善。

51.监测分析策略

51.1 监测单位

监管要求以客户为基本单位开展的监测分析。这不仅是基本的合规要求，而且是一个理论和实践均证明很有效的策略，从业机构应予以遵循。

在采纳上述策略的基础上，从业机构可充分发挥互联网金融行业的数据和技术优势，同时并行一些经科学理论或者评估验证过有效的创新监测策略。

51.2 监测范围

建议从业机构尽可能广泛地确定监测分析的对象范围，对客户及其所有业务、交易及其过程，甚至不构成金融层面交易的客户行为也开展监测和分析。在可疑交易监测方面，无论交易是否实际发生，无论交易是否最终完成，无论交易实际涉及资金价值转移，都应纳入监测范围。

51.3 风险维度

交易监测标准包括并不限于客户的身份、行为，交易的资金来源、金额、频率、流向、性质等。

51.4 合规性

从业机构应除了按照规定及时、准确、完整向中国反洗钱监测分析中心提交大额交易和可疑交易报告外，还应注意监测分析流程自身的可稽核性和可解释性。

52.大额交易

从业机构应按照中国人民银行发布的大额交易判断标准、计算规则等，建立相应的大额交易监测系统、报告流程。

53.可疑交易

从业机构发现或者有合理理由怀疑客户及其行为、客户的资金或者其他资产、客户的交易或者试图进行的交易与洗钱、恐怖融资等犯罪活动相关的，不论所涉资金金额或者资产价值大小，应按本机构可

疑交易报告内部操作规程确认为可疑交易后，及时提交可疑交易报告。

54.名单监测

从业机构应对下列恐怖组织和恐怖活动人员名单开展实时监测，有合理理由怀疑客户或者其交易对手、资金或者其他资产与名单相关的，应立即提交可疑交易报告，并依法对相关资金或者其他资产采取冻结措施，涉恐名单包括但不限于：

（1）公安部等我国有权部门发布的恐怖活动组织及恐怖活动人员名单；

（2）联合国发布的且得到我国承认的制裁决议名单；

（3）其他国际组织、其他国家（地区）发布的且得到我国承认的反洗钱和反恐怖融资监控名单；

（4）中国人民银行要求关注的其他反洗钱和反恐怖融资监控名单；

（5）洗钱风险管理工作中发现的其他需要监测关注的组织或人员名单。

55.后续风险控制措施

从业机构在报送可疑交易报告后，应根据中国人民银行的相关规定采取相应的后续风险控制措施，包括对可疑交易所涉客户及交易开展持续监控、提升客户风险等级、限制客户交易、拒绝提供服务、终

止业务关系、向相关金融监管部门报告、向相关侦查机关报案等。从业机构应注意将这些加强措施与客户管理政策、业务流程管控、风险运营管理等工作有机整合，减少运行成本，确保工作实质有效。

第十一章 身份资料和交易记录保存制度

56.基本要求

从业机构应按照规定建立客户身份资料和交易记录保存制度，强化内部管理措施，更新技术手段，逐步完善相关信息系统，统筹考虑保存范围、方式和期限，确保客户身份信息和交易记录完整准确，确保能够完整重现每笔交易及相关工作可追溯。

从业机构应当通过妥善方式记录开展洗钱风险管理的工作过程，采取必要的管理措施和技术手段保存工作资料，保存方式应当保证洗钱风险管理人员获取相关信息的便捷性。

从业机构业务部门不得违反规定设置信息壁垒，阻止或影响反洗钱部门正常获取开展反洗钱工作所必需的信息和数据。从业机构应建立适当的授权机制，明确工作程序，按照规定将客户身份信息和交易记录迅速、便捷、准确地提供给监管机构、执法机构等部门。

57.保存范围

从业机构应保存的客户身份资料包括记载客户身份信息、资料以及反映从业机构开展客户身份识别工作情况的各种记录，确保能够完整重现每笔交易、能足以重现每项交易的全过程，保证客户身份资料和交易记录保存的真实性、完整性、安全性和合规性。

58.保存标准

58.1 客户身份资料

合规性。从业机构不仅应按照反洗钱监管制度、行业规则所明确的规格要求，采集并保存客户及其交易目的、性质等各方面的信息资料，而且应将执行其他各项金融监管制度、行业标准、内部业务规程过程中收集、验证、获取的客户身份背景信息资料一并保存。

有效性。互联网场景下，从业机构能够实际获得的有助于识别、了解客户及其交易目的、性质的数据更为丰富，应从提升反洗钱风险管理有效性出发，尽可能全面保存数据，为技术发展预留空间。

58.2 交易记录保存

合规性。可完整重现交易是判断交易记录保存工作是否合规的核心标准，但迄今为止的监管制度或国际标准均未对此作出细化。从业机构至少应完整保留反映业务关系建立过程、交易指令从发出到执行全程的数据信息及据此进行记账、会计处理而留下的数据。

有效性。鉴于互联网交易场景下，交易行为及过程均可数据化，从业机构可考虑在成本可控范围内将尽可能多地反映客户行为、交易过程。

59.保存期限

客户身份资料(自业务关系结束当年或者一次性交易记账当年计

起)和客户交易信息(自交易记账当年计起)至少保存五年。

如客户身份资料和交易记录涉及正在被反洗钱调查的可疑交易活动,且反洗钱调查工作在前款规定的最低保存期届满时仍未结束的,从业机构应将其保存至反洗钱调查工作结束,从业机构破产或者解散时,应将客户身份资料和交易记录移交监管机构指定的机构。

60.保存方式

从业机构应采取必要管理措施和技术措施,防止客户身份资料和交易记录的缺失、损毁,防止泄漏客户身份信息和交易信息。

第十二章 保密制度

61.基本要求

从业机构应按照《中华人民共和国反洗钱法》、《中华人民共和国国家安全法》、《中华人民共和国网络安全法》和有关保密规定，健全内部控制机制，严格保护反洗钱工作中获得的信息，非依法律规定，不得向任何单位和个人提供。

62.保密范围

1.从业机构对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息，应予以保密；非依法律规定，不得向任何单位和个人提供。

2.报告大额和可疑交易的情况以及涉嫌恐怖融资的可疑交易信息包括但不限于以下：账户信息，交易信息，机构内部调查分析原因、过程、结果以及向中国人民银行报送的材料等信息。

3.配合中国人民银行调查可疑交易活动及协助侦查机关洗钱案件侦查等有关反洗钱工作信息包括但不限于以下内容：客户的身份资料信息，账户信息，历史交易记录，可疑交易数据，调阅的文件和资料，调查通知书内容，调查目的，调查人，调查进度、过程、结果等有关信息。

4.反洗钱现场、非现场监管信息。中国人民银行在对从业机构反洗钱现场检查时调阅的客户资料、文件以及依法要求从业机构要求报

送的反洗钱工作等信息。

5.举报反洗钱违规的内容和行为。从业机构应设立反洗钱举报通道，鼓励员工对机构内部人员涉嫌洗钱或其他严重的反洗钱违规行为进行举报，并对举报内容进行保密。对有功人员按照规定给予表彰奖励，隐瞒不报者，一经查实应从严处罚。

6.反洗钱规定要求保密的其他材料。

63.涉及跨境事项的保密要求

从业机构应建立涉及跨境事项的保密保障措施。对于在开展跨境业务、应对跨境监管等过程中所涉的客户、账户和交易信息、可疑交易报告等信息，应严格控制跨境信息知悉范围和程度，建立完善的内部跨境信息传递体系、风险控制流程和授权审批机制。

境外有关部门因反洗钱和反恐怖融资需要要求其提供客户、账户、交易信息及其他相关信息的，从业机构应告知对方通过外交途径、司法协助途径或金融监管合作途径等提出请求，不得擅自提供。有关国内司法冻结、司法查询、可疑交易报告、行政机构反洗钱调查等信息不得对外提供。

64.管理措施

出于洗钱风险管理需要，从业机构应建立内部信息共享制度和程序，根据信息敏感度及其与洗钱风险管理的相关性确定信息共享的范围和程度，制定适当的信息共享机制，明确信息安全和保密要求，建

立健全信息共享保障措施，确保信息的及时、准确、完整传递。

对内或对外发送已标注密级的反洗钱文件和材料，从业机构应采取符合保密要求的纸质形式运转或通过符合行业标准的公文数据加密传输系统发送，严禁通过非保密渠道传发。从业机构要加强反洗钱信息的保密管理，确保反洗钱信息的制作、收发、传递、使用、复制、保存和销毁符合有关保密规定，防止失密、泄密事件发生。

境外清算代理行因反洗钱和反恐怖融资需要要求提供除汇款信息、单位客户注册信息等以外的客户身份信息、交易背景信息的，从业机构应当在获得客户授权同意后提供；客户不同意或未获得客户授权同意的，从业机构不得提供。

第十三章 附则

本指引由中国互联网金融协会负责编制、修订和监督实施，根据监管要求做不时更新或年度重审。

本指引自 2019 年 6 月 24 日起施行。