中国银行业监督管理委员会

银监办发[2016]188 号

中国银监会办公厅关于加强非银行金融机构信息科技建设和管理的指导意见

各银监局，各金融资产管理公司，中国信托业保障基金公司、中国信托登记有限责任公司：

为促进信托公司和金融资产管理公司、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、货币经纪公司等非银行金融机构（以下简称非银机构）信息科技建设，提升信息化管理水平，有效防范信息科技风险，保障非银机构稳健经营和持续发展，现就加强非银机构信息科技建设和管理工作提出以下意见。

一、指导原则

（一）明确主体责任。非银机构作为金融机构独立法人应承担相应的信息科技管理职责，建立符合业务特点的信息科技战略和风险管理策略，根据业务发展和经营管理需要，确定信息科技发展目标和功能定位，合理利用外部资源，自主开展信息科技管理工作。

（二）科技支撑发展。科学配备信息科技资源，充分发挥信息科技对业务发展和转型的支撑和引领作用，顺应“互联网+”发展趋势，积极稳妥地探索和应用新兴技术，为改善系统、渠道、产品的灵活性和可扩展性提供支持。

（三）倡导合作共享。积极与其他银行业金融机构协同合作，加强资源开放共享，交流先进技术与成功管理经验，取长补短，提高非银机构信息科技建设和管理水平。

（四）严守风险底线。建立健全信息科技风险管理架构，加强基础设施建设、开发测试、运行维护、信息安全、业务连续性、外包等重点领域的信息科技风险防控，避免和减少重大信息科技事件发生。

二、建立有效的信息科技治理架构

（一）夯实信息科技治理基础。非银机构应明确董事会、高级管理层应履行的信息科技管理职责，保证资金、人力和技术等资源投入，满足信息科技建设和管理需要。董事会应承担信息科技风险管理的最终责任，未设立董事会的，由本机构经营决策层履行相关管理职责。规模较大且主要业务对信息科技依赖度较高的非银机构应设立信息总监（首席信息官），将其纳入高级管理人员，专职负责信息科技战略规划和管理，参与同信息科技运用有关的业务决策等工作。应建立跨部门工作协调机制，成立由高级管理层、信息科技部门和主要业务部门负责人组成的信息科技管理委员会，承担信息科技战略规划审议、推进重大项目决策等职责，提高管理决策的科学性和有效性。应厘清与本机构出资人的信息科技管理工作职责，加强工作规划、预算投入、项目建设等重大事项的自主决策，推动信息科技健康有序发展。

（二）加强信息科技专业队伍建设。非银机构应设立相对独立的信息科技管理职能部门，合理配备专业人员，明确岗位职责和分工安排，建立内部岗位制约机制，确保关键岗位人员数量充足。应重视人才培养，

为信息科技人员提供履职所需的技能培训，建立健全晋升及激励考核机制，提供专业人才发展空间，确保信息科技队伍稳定发展。

（三）建立信息科技风险管控机制。非银机构应将信息科技风险纳入全面风险管理体系，建立常态化的风险识别、监测和管控机制，每年对全部重要信息系统至少开展一次风险评估，及时发现风险并采取有效控制措施。应将信息科技审计纳入审计部门工作范畴，对信息科技内控机制的充分性和有效性开展内部审计，或聘请专业机构开展外部审计；针对重大信息科技事件或重大风险隐患开展必要的专项审计，至少每三年完成一次全面审计。审计部门应定期向董事会和高级管理层报告审计和跟踪审计情况，督促相关部门及时整改审计发现的问题。

三、科学规划，提升信息科技对业务的支撑能力

（一）科学制定信息科技战略规划。非银机构应结合自身业务特色和发展趋势，制定与业务战略规划相匹配并适度超前的信息科技战略规划，科学构建信息技术架构，包括企业级应用架构、技术架构和数据架构，建立与规划相配套的组织和资源保障机制，定期跟踪规划执行进度，评估执行效果，确保有效落地实施。

（二）提高信息科技建设质效。非银机构应加强经营分析和风险控制系统建设，逐步构建覆盖全部业务流程的管理信息系统，满足业务发展需要和全面风险管理要求，提高业务运营效率，支撑管理和决策。信息系统建设应具有一定前瞻性，既要考虑业务的复杂性和实时性，又要考虑灵活性和可扩展性，有效应对市场需求变化，引领业务发展和机构转型升级。积极应用云计算、大数据、移动互联等新兴技术，通过创新

服务方式，提高金融服务的安全性、便捷性，提升自身核心竞争力，创造业务价值。有条件的机构，可积极探索开展同业之间在技术合作、信息服务、资源共享等领域的协作实践。

（三）完善数据治理体系。非银机构应探索建立有效的数据治理组织架构，制定统一规范的数据标准和数据管理机制，理顺各系统之间的数据交互关系，不断提高数据质量，满足监管机构在监管数据采集、报送等方面的要求。深化数据应用，发挥数据治理在实现差异化服务和风险管理等方面的积极作用，提升数据治理效能。

四、加强基础设施建设，提升开发测试和运维管理水平

（一）加强数据中心基础设施建设。非银机构应结合业务发展需要和自身实际情况，科学选择数据中心（含中心机房）建设方式，实现数据中心的安全、高效与节能；为节约成本、提高专业化管理水平，规模较小的非银机构可考虑选择租用、托管、共享数据中心等建设方式，具有一定规模、信息科技基础较好、管理能力较强的非银机构可自建数据中心。数据中心选址应符合有关监管要求，在选址前应实施安全评估，充分考虑地理位置、环境、设施等各种因素影响，规避选址不当造成的风险。数据中心建筑物结构（如层高、承重、抗震等）应满足专用机房建设要求，电力供应、精密空调、网络通信线路等重要基础设施应具备冗余能力，机房应采取有效的防火、防雷、防水等保护措施。数据中心与其他机构（包括出资人）共用或托管至外包服务商的，应确保重要信息科技设备与其他机构的有效隔离，明确物理安全区域，严格控制物理访问权限。

（二）规范开发测试管理。非银机构应制定开发测试相关制度、标准、流程，规范管理自主开发或外包开发过程。安排专人负责项目管理，合理控制项目进度。重视需求分析，规范设计，兼顾业务功能与非业务功能需求。选取适当的开发测试方法，确保系统开发测试的完整性和有效性。明确安全开发规范，加强信息系统的安全设计、研发和测试。

（三）提升运行维护能力。非银机构应根据工作需要建立专业化的运行维护管理队伍，不断提高自主运维管理能力；科学划分运维岗位职责，杜绝关键岗位兼职兼岗。建立健全运维管理制度，明确事件管理、问题管理、配置管理、变更管理、发布管理等要求，编制运维操作手册，规范重要信息系统投产上线及重大变更操作。加强重要设备和设施定期巡检和维护，及时更新老化陈旧设备，全面做好软件正版化工作，健全软件产品和硬件设备缺陷管理机制，采取适当升级措施，确保系统服务的连续可用性。加强容量规划，以适应业务发展和交易量增长的需要。建设自动化运维手段，建立全面覆盖基础设施、网络、系统、应用等多领域、多层次的监控体系，妥善存储日志，有效防范和处置各类故障事件。

五、健全信息科技风险管理体系，加强重点领域风险防控

（一）加强信息安全管理。非银机构应配备专职信息安全管理人员，制定完善的安全管理制度，严格落实国家网络安全政策法规的有关要求，定期开展安全教育，提高员工信息安全意识。加强安全技术保障体系建设，采取有效的防病毒、防攻击、防篡改、防泄密、防抵赖等措施，提高系统抵御内外部攻击破坏的能力。严格配置网络访问控制策略，实现

开发、测试、生产、办公等不同网络安全域之间以及与出资人等外联单位、国际互联网之间的风险隔离。加强系统安全漏洞和补丁信息的监测、收集和评估，确保及时发现和处置重大安全隐患。开展应用系统安全检测，对官方网站等通过互联网提供服务的系统，在上线及重大投产变更前进行渗透测试，杜绝系统“带病”上线。对敏感数据实施分类分级管理，强化数据生命周期各阶段安全管理要求，严格控制生产系统访问权限，禁止未经授权查看、下载生产数据；采取符合要求的加密、脱敏等技术，提高数据存储、传输、测试的安全性。落实终端、移动存储介质安全控制措施，加强对非法外联等各类违规行为的监控、阻断和审计。

（二）重视业务连续性能力建设。非银机构应建立业务连续性管理组织架构，有效开展业务影响分析，识别各项重要业务，合理确定业务恢复时间目标（RTO）和业务恢复点目标（RPO）。加强业务连续性资源与能力建设，依据业务恢复目标，对重要信息系统采取高可用技术，制定并实施重要数据备份策略；规模较大、业务服务实时性要求高的非银机构，应建立或与其他机构共享灾备中心（含灾备机房），对重要信息系统和数据进行同城或异地备份，确保生产系统不可用时及时恢复重要业务。制定信息科技突发事件应急预案，对重要系统每年至少开展一次应急演练，加强业务与技术应急有效衔接，不断提高事件应急处置能力。

（三）严格控制外包风险。非银机构应识别和分析信息科技外包风险，制定外包策略，明确外包范围和责任边界，严守“安全管理责任不能外包、安全标准不能降低”的风险底线，建立与信息科技战略目标相适应的外包管理体系。加强对外包服务商的风险管理，对关键外包服务

商的技术实力、内控体系和管理能力定期开展风险评估，制定外包服务中断应急预案；重视关联外包管理，将与出资人之间的外包活动纳入关联外包管理，不得因关联关系而降低外包服务管理要求；识别具有机构集中度风险的外包服务商，加强持续监控和管理，积极采取风险分散措施，对外包合作项目进行必要的知识产权转移，有条件的机构应逐步提高自主研发能力，降低对外包服务商的依赖。严格外包合同管理，规范合同条款，明确外包服务商安全保密等各类责任与义务。

六、加强监管指导

（一）提高监管关注。各级监管机构应加强对非银机构的信息科技监管，按照属地原则，有序开展监管和指导工作。合理分配监管资源，加强内部监管联动，提高监管工作质效。积极跟踪非银机构信息科技发展动态，分析和研判风险态势，加强风险识别、评估和预警，及时开展风险提示，将风险管控关口前移。

（二）突出监管重点。各级监管机构应积极引导非银机构提高对信息化工作的重视程度，加强资源保障，不断提升专业化管理能力，有效支撑业务发展和创新。督促非银机构在信息化建设过程中，合法、规范地应用信息技术和信息产品，在开展同业、跨业交流与合作时严格遵守相关规定。积极运用非现场监管、现场检查等监管手段，及时发现非银机构存在的突出问题，开展专项整治，特别要加大重点风险领域的监管力度，严防重大风险隐患。

（三）强化责任追究。各级监管机构应强化对非银机构信息科技建设和管理的监管问责，对违反监管政策或监管要求落实不力的机构，要

追究相关责任，必要时依法采取行政处罚措施。督促指导非银机构严格落实事件报告制度，按照《商业银行业务连续性监管指引》有关要求，及时报送重要信息系统服务中断或重要数据损毁、丢失、篡改、泄露情况，妥善处置对本机构或客户利益造成较大损害的重大突发信息科技事件。

2016 年 12 月 26 日