495--关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见  
（银监发〔2014〕39号）

各银监局、各省（自治区、直辖市及计划单列市）发展改革委、科技厅（委、局）、工业和信息化主管部门、各政策性银行、国有商业银行、股份制商业银行、金融资产管理公司、储蓄银行、各省级农村信用联社，银监会直接监管的信托公司、企业集团财务公司、金融租赁公司：

为进一步贯彻落实创新驱动发展战略，提升银行业网络安全保障能力和信息化建设水平，推动银行业深化改革、发展转型，促进战略新兴产业发展，现就应用安全可控信息技术加强银行业网络安全和信息化建设提出以下指导意见。

**一、总体目标**

建立银行业应用安全可控信息技术的长效机制，制定配套政策，建立推进平台，大力推广使用能够满足银行业信息安全需求，技术风险、外包风险和供应链风险可控的信息技术。到2019年，掌握银行业信息化的核心知识和关键技术；实现银行业关键网络和信息基础设施的合理分布，关键设施和服务的集中度风险得到有效缓解；安全可控信息技术在银行业总体达到75％左右的使用率，银行业网络安全保障能力不断加强；信息化建设水平稳步提升，更好地保护消费者权益，维护经济社会安全稳定。

**二、指导原则**

（一）坚持开放合作。兼容并蓄，凝聚各方智慧和力量，优先应用开放性强、透明度高、适用面广的技术和解决方案，优先选择愿意在核心知识和关键技术领域进行合作的机构，避免对单一产品或技术的依赖。

（二）鼓励自主创新。充分认识创新驱动发展战略的重要意义，鼓励原始创新、集成创新和引进消化吸收再创新，构建高效稳健的共性关键技术供给体系，掌握银行业信息化核心知识和关键技术。

（三）发挥市场作用。加快建立高效的创新体系，激发各类创新主体的积极性，以银行业信息化需求培育和带动市场，以信息产业发展促进银行业发展转型，主动把握新兴技术发展机遇，推动银行业信息化创新发展，促进信息产业做大做强。

（四）加强协同合作。统筹规划，加强政、产、学、研协同合作，营造安全可控信息技术研究、发展和应用的良性互动环境，形成“需求拉动、产业推动、科研驱动”的良性循环。

**三、任务要求**

（一）完善信息科技治理机制。银行业金融机构应将提升网络安全保障能力和信息化建设能力纳入战略目标，将安全可控信息技术应用纳入战略规划；建立以安全可控、自主创新为导向的制度体系，明确目标、策略与职责分工；加强创新组织建设和人才培养，保障创新资源；有序推进整体架构自主设计、核心应用自主研发、核心知识自主掌握、关键技术自主应用等重点工作。

（二）优化信息系统架构。银行业金融机构要建立安全、可靠、高效、开放、弹性的信息系统总体架构，在架构规划和设计过程中应充分考虑安全可控；掌握关键技术的选择权，摆脱在关键信息和网络基础设施领域对单一技术和产品的依赖。从战略角度规划和建设业务连续性系统架构，应当至少有一种基于安全可控信息技术架构的数据级或应用级存储、备份、归档和容灾等一体化的业务连续性方案。

（三）优先应用安全可控信息技术。银行业金融机构应客观评估自身信息化需求和信息科技风险情况，开展差距分析，按年度制定应用推进计划；建立科学合理的信息技术和产品选型理念，选择与本单位信息化需求相匹配的技术与产品，避免一味求大求全。在涉及客户敏感数据的信息处理环节，应优先使用安全可靠、风险可控的信息技术和服务，当前重点在网络设备、存储、中低端服务器、信息安全、运维服务、文字处理软件等领域积极推进，在操作系统、数据库等领域要加大探索和尝试力度；从2015年起，各银行业金融机构对安全可控信息技术的应用以不低于15％的比例逐年增加，直至2019年达到不低于75％的总体占比（2014年应用的技术和产品可纳入2015年度计算）。

（四）积极推动信息技术自主创新。银行业金融机构应积极尝试应用安全可靠、自主创新的信息技术，通过应用提出改进需求，增强创新技术的适应性和健壮性；探索通过统一标准、统筹产品、联合攻关、试点示范等，加快自主创新信息技术应用磨合适配及系统性优化。在技术选型中，如存在安全可靠的自主创新产品和技术，应至少引入一家此类产品或技术进行选型和测试；对提供专用设备或集成解决方案的供应商，应要求其方案使用的硬件和软件至少能够各应用一项安全可靠的自主创新产品或技术。

（五）积极参与安全可控信息技术研发。银行业金融机构应加强与产业机构、大学和科研机构的合作，联合开展关键技术的研发和生产，围绕安全可控信息技术在银行业应用的关键问题，开展技术合作，实施技术转移，形成高质量、具有行业推广价值的科技成果；在核心应用基础架构、操作系统、数据库、中间件和银行业专用设备等领域加大研究力度，集中突破制约安全可控发展的关键技术。2015年起，银行业金融机构应安排不低于5％的年度信息化预算，专门用于支持本机构围绕安全可控信息系统开展前瞻性、创新性和规划性研究，支持本机构掌握信息化核心知识和技能。

（六）加强知识产权保护与标准规范建设。银行业金融机构应加强知识产权保护意识，对各项研究成果及时申请技术专利保护；应积极参与各类技术标准的研究和制定工作，推进安全可控信息技术的标准化、专利化。

**四、主要措施**

（一）建立银行业信息安全审查和风险评估制度。依据国家网络安全审查相关政策，建立与银行业信息安全需求相适应的配套政策，建立银行业网络安全审查标准，加强银行业专用信息技术和产品的安全检测；建立常态化的风险评估制度，建立信息技术在银行业应用过程中的风险识别、评估和控制机制，加强功能测试、性能测试和安全性测试；密切跟踪安全可控信息技术的应用情况，建立缺陷库和风险库，结合行业应用不断促进技术的完善。

（二）建立银行业安全可控信息技术落地推进平台。组建银行业安全可控信息技术创新战略联盟，创建技术实验室和国家工程实验室，研究挖掘银行业应用安全可控信息技术的机会和需求，协调银行业金融机构、信息技术企业、大学和研究机构等共同推进安全可控信息技术的研究和推广。

（三）组织开展银行业应用安全可控信息技术示范项目。结合国家信息安全专项、国家有关科技计划和国家财政支持的其他项目，组织开展安全可控信息技术在银行业的应用示范，组织推动银行业开展安全可控前瞻性研究；加强部门间协作，加强政策协同，加大力度支持银行业应用安全可控信息技术，以银行业应用不断完善安全可控信息技术，为安全可控信息技术创造市场空间。

（四）制定银行业应用安全可控信息技术推进指南。依托银行业安全可控信息技术创新战略联盟和技术实验室、国家工程实验室，分析银行业应用需求，解决共性问题，逐年制定推进指南，对推进领域、重点信息技术和产品以及推进方案予以细化。各级工业和信息化主管部门应做好适用技术、产品、服务及典型解决方案推介，推动需求对接。

（五）持续监督和评价。建立银行业金融机构应用安全可控信息技术工作情况的监督评价机制，通过安全可控信息技术应用率、重要系统自主掌控率、自主创新信息技术试用情况等指标评估安全可控能力成熟度；逐年对银行业金融机构应用安全可控信息技术情况进行考核，对纳入监管评级体系的机构，考核结果并入机构信息科技监管评级。

2014年9月3日