KPMG

cutting through complexity

网络安全变革及对中国银行业的影响

安全可控监管政策解读与分析

毕马威企业咨询

二零一五年

kpmg.com/cn

KPMG
cutting through complexity

报告概要

银监会最近颁布了有关应用安全可控技术及网络安全的39号文及317号文，昭示着国内银行业信息化建设的思路将发生重大转变，监管机构的后续举措必将对银行业信息化工作带来深远影响。未来，在政策的引导及监管监督下，银行机构、技术厂商、研究机构、行业联盟、服务机构等相关利益方，需要及时调整工作方向，以策满足合规要求。

监管要求：

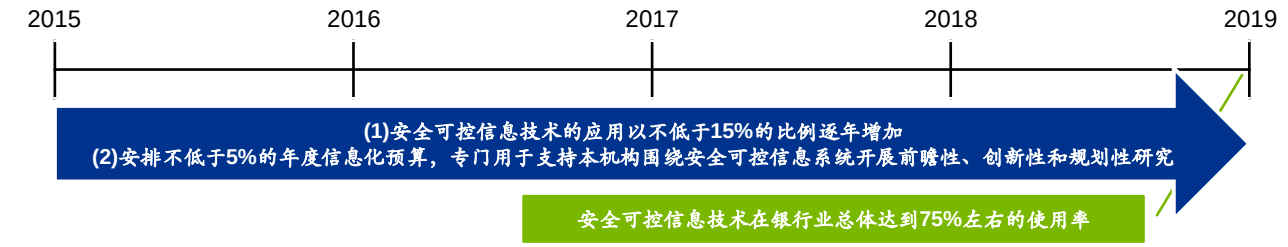
- 到2019年末，境内银行机构的安全可控信息技术使用率达到75%的“红线目标”将成为监管机构监督工作的方向；
- 2015年至2019年，监管机构的相关指导意见及要求将进一步细化，相应的可控评价标准、保障举措、考核及监督体系将逐步健全，以策指导银行机构遵照执行；
- 监管机构鼓励银行金融机构自主创新，加强经验总结和知识积累，以策银行机构推动行业安全可控技术能力的提升。

银行机构：

在监管要求的影响下，银行机构的战略规划、管理体系、治理结构、人员建设、信息化投资结构、创新机制、绩效体系、系统建设、信息化采购等，均需进行调整及优化，以策推动监管要求的有效执行。银行业金融机构将在以下管理领域重点关注安全可控相关内容：

- 治理体系：亟需组建应用可控技术及网络安全信息化响应组织，管理层及各职能条线均需委派代表参与。该组织的常设部门需牵头组织可控技术工作规划及计划，以及配套管理方向；
- 基础环境建设：对大型机的需求将进一步下降，基础环境中的网络设备、存储设备、安全设备等产品的核心组件可控率将逐年提升，银行机构对其研究力度及熟知程度将进一步提升；
- 配套体系：结合监管机构的要求，风险管理、信息安全管理等银行管理体系将受到直接影响，包括风险容忍度的调整、风险评估的专业度、风险监控指标的调整、信息安全技术标准的优化等等。

时间表：



KPMG
cutting through complexity

网络安全变革及对中国银行业的影响

监管政策解读与分析

目录

KPMG
cutting through complexity

应用安全可控政策出台背景

1 当前环境分析

社会对互联网金融、大数据、云计算等新兴热点的关注，很大程度上改变了组织的业务发展形式，也改变了民众的行为习惯。进而，组织及个人的隐私数据面临主动、被动泄露的风险也日趋明显。

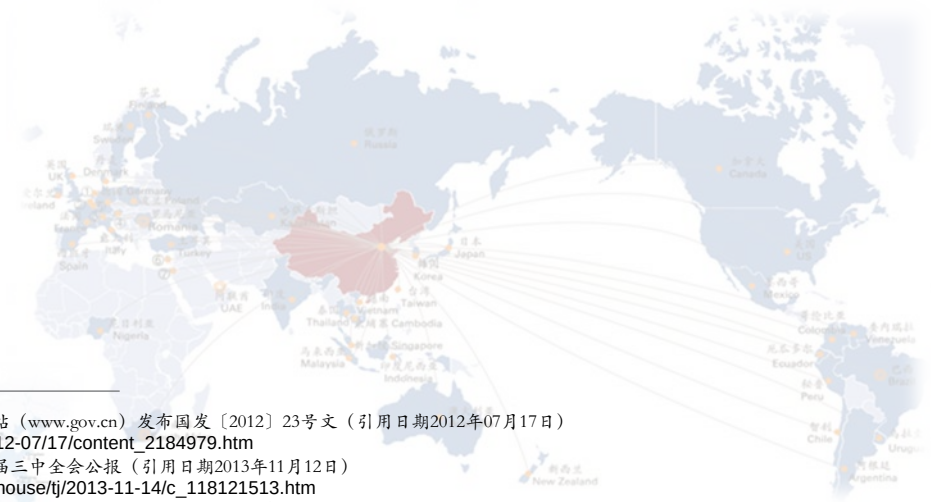
基于此，网络安全已成为关系国计民生的重要影响要素之一，中国政府更将其提升至国家战略高度。近年，伴随国家自上而下的导向推动，政府及行业监管机构颁布了不同的政策，要求提升行业安全可控水平，将其纳入信息化建设进程，以策降低组织的信息技术风险。

中国战略部署

面临国际国内新兴技术快速发展及严峻的信息安全形势，中国政府逐步将网络安全提升到国家战略高度：

- 2012年7月，国务院发布《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》[①]，**将信息安全发展提升到与信息化发展同等的地位**；
- 2013年11月，中央国家安全委员会成立，习近平任主席，**将信息安全确立为国家战略**[②]，昭示捍卫国家信息安全的意志；
- 2014年2月，**中央网络安全和信息化领导小组**成立[③]，习近平主席担任组长。

银监会也相继发布了《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）和《银行业应用安全可控信息技术推进指南（2014-2015年度）》（银监发[2014]317号）两份与安全可控技术发展相关的政策文件。毕马威旨在通过阐明其中的关键要点来对这些政策进行解读与分析，并为银行业提供行动建议。



1.源引自：中央政府门户网站（www.gov.cn）发布国发〔2012〕23号文（引用日期2012年07月17日）
http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm
2.源引自：中国共产党十八届三中全会公报（引用日期2013年11月12日）
http://news.xinhuanet.com/house/tj/2013-11-14/c_118121513.htm
3.源引自：新华网（www.news.cn）时政《中央网络安全和信息化领导小组成立》（引用日期2014年02月27日）
http://news.xinhuanet.com/info/2014-02/28/c_133148759.htm

KPMG
cutting through complexity

银行业应用安全可控政策概要

1 当前环境分析

- **国家政府**关注信息安全战略，中央国家安全委员会和中央网络安全和信息化领导小组的成立都显示着我国政府已经将信息技术安全可控和网络安全提升到国家战略高度。
- **监管机构**响应政府的安全策略，颁布了相关指导意见和推进指南，旨在加强信息技术安全可控领域的政策指导，明确责任方职责和关键工作时点。
- **银行业金融机构**应根据银监会的相关要求，制定信息技术安全可控部署战略，需重点关注信息技术的安全可控和自主创新。
- **信息技术企业**面临技术、产品和服务安全可控变革的机遇与挑战，国内厂商在技术上不断完善和创新，以促进产业环境变革；部分主流厂商长期占据主导地位的市场格局也将受到挑战，如何实施技术开放、证明技术和产品安全可控将成为各厂商的关注重点。

应用安全可控目标:

- 信息技术安全可控，重要信息系统自主可控
- 应用研究工作落实
- 掌握核心技术
- 维护信息安全
- 降低成本

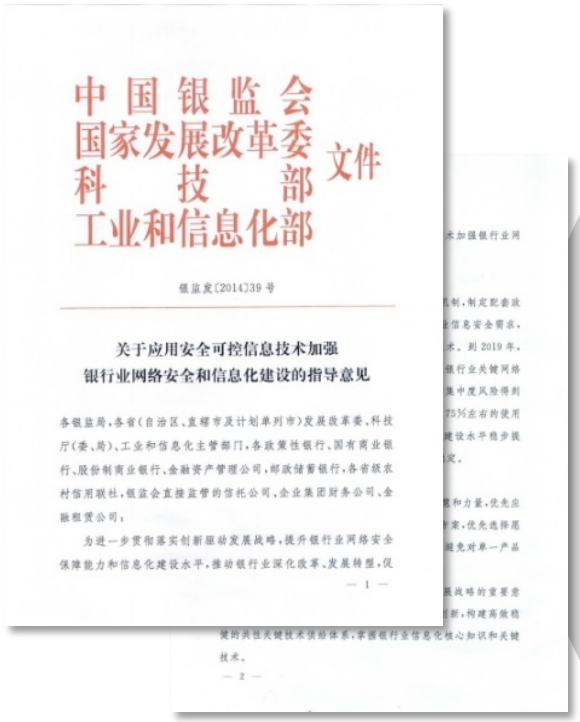
我国银行业监管机构针对当前的应用安全现状颁布了一系列监管指引文件

2014/09	2014/12	2015/01	2015/02
发布《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）**	发布《关于印发银行业应用安全可控信息技术推进指南(2014-2015 年度)》**（银监发[2014]317号）**	发布《关于开展2014年度银行业信息技术情况调研的通知》**（银监发[2015]100号）**	关于《银行业应用安全可控信息技术推进指南（2014－2015年度）》**（银监发[2014]317号）的相关说明**
指导意见	年度计划	调研检查	补充说明
• 安全可控长效机制 • 安全可控系统架构 • 开发与合作 • 自主创新	• 安全可控目标、任务、工作措施 • 信息技术资产分类和安全可控指标 • 安全可控评价标准和机制 • 监管保障措施	• 技术安全可控调研表 • 自评调研流程	• 源代码备案研究说明 • 供应商软件知识产权说明 • 安全可控产品国别说明

KPMG
cutting through complexity

银监发[2014]39号文概要

2 政策解读和毕马威的理解


中国银监会
国家发展改革委
科技部
工业和信息化部 文件

银监发〔2014〕39号

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

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，邮政储蓄银行，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

— 1 —

39号文概要

《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，以下简称《指导意见》)：

- 银监会、国家发展改革委员会、科技部、工业和信息化部联合发布；
- 提出总体目标，作为促进国产信息技术落地银行业的中长期政策和规划，提出2019年银行业应用安全可控信息技术总体比率达到75%的目标；
- 指导意见更为关注创新生态体系建设，银行不但要“自主可控”，而且要推动整个创新生态体系的发展，使银行和产业建立产业联盟，共同推进。

KPMG
cutting through complexity

银监发[2014]39号文概要

2 政策解读和毕马威的理解

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，大力推广使用安全可控的信息技术。至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，更好的保护消费者权益，维护经济社会安全稳定。

安全可控信息技术

即能够满足银行业信息安全需求，且**技术风险**、**外包风险**和**供应链风险**可控的信息技术。

对银行业机构的任务要求

- 完善信息科技治理机制；
- 优化信息系统架构；
- 优先应用安全可控信息技术；
- 积极推动信息技术自主创新；
- 积极参与安全可控信息技术研发；
- 加强知识产权保护与标准规范建设。

两个量化指标

- 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；
- 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。

KPMG
cutting through complexity

银监发[2014]39号文解读

2 政策解读和毕马威的理解

银监发[2014]39号文对于银行业安全可控信息技术的说明：

- 满足信息安全需求
- 技术风险可控
- 外包风险可控
- 供应链风险可控

《指导意见》要求银行业金融机构实现一个满足，三个风险可控

《指导意见》中明确阐述银行业需建立应用安全可控的长效机制，制定配套政策，搭建推进平台，以满足银行业的信息安全需求，并实现技术、外包、供应链领域的风险可控。

信息安全需求

银行业金融机构的信息安全管理，是全面信息科技风险管理的重要组成部分，相关信息安全管理要求参见银监会2009年颁布的《商业银行信息科技风险管理指引》，指引从人员的安全意识、管理职能、安全策略、访问控制、安全域、系统安全、加密、终端安全、以及信息的生命周期管理等九个方面对于银行业信息安全提出了详细的要求。

技术风险

银行业金融机构信息资产相关的固有风险和操作风险。银行业信息技术资产分类涵盖信息技术硬件、软件、服务类资产，包括10大类和68小类，类别目录参见《 关于印发银行业应用安全可控信息技术推进指南(2014-2015 年度)》附表。

银行业金融机构 – 对其所使用的信息技术、产品或服务具有技术风险的识别、监测和控制能力。

信息技术企业 –充分保障银行业金融机构识别技术风险的权利，并为识别和控制风险提供充分的知识、技能和工具支持。

外包风险

即由于信息科技外包而产生的科技能力丧失、业务中断、信息泄露等风险，信息科技外包类型包括（不限于）服务类外包和人员类外包。银行业金融机构和信息技术企业应依据银监发[2013] 5号《 银行业金融机构信息科技外包风险监管指引 》的相关要求实施充分的外包风险管控，对于非驻场集中式外包信息技术企业，还需依据银监发[2014]187号《 关于加强银行业金融机构信息科技非驻场集中式外包风险管理的通知》开展外包监管评估工作。

供应链风险

即由于技术、产品或服务供应渠道中断、知识产权限制而造成银行业金融机构无法获得必要的维修、支持、升级等服务，进而导致系统运行中断的风险。银行业金融机构需加强核心技术、产品和服务的供应链管理，积极主动使用安全可控、正版许可的信息技术。

KPMG
cutting through complexity

银监办发[2014]317号文概要

2 政策解读和毕马威的理解

《推进指南》要求建立银行业信息技术资产分类目录和安全可控指标管理体系

317号文概要

《银行业应用安全可控信息技术推进指南(2014—2015年度)》（银监办发〔2014〕317号，以下简称《推进指南》）：

- 银监会、工业和信息化部联合编制；
- 年度安全可控工作《推进指南》，对于“安全可控”进行了界定，对2015年的具体工作目标和要求进行了细化；
- 强调了**应用和研究**两个应用安全可控领域的建设，不仅要求银行业机构加强信息技术安全可控，也提出了应用可控安全领域的研究要求。

银行业信息技术资产分类和安全可控指标
到2019年末安全可控信息技术使用率达到75%

信息资产分类	信息技术资产分类由类别代码、名称、说明等要素构成，分为两个层次，共计10大类68小类，银监会对每类资产设定了不同的自主可控要求。
安全可控指标	银行业金融机构应渐进式地实现应用安全可控，具体工作要求如下： **1) 先关注新增应用，后着眼已有应用** 2015年安全可控指标的应用任务主要关注于“新增安全可控设备”；同时在39号文《指导意见》中则提出逐年不低于15%比例增加的年度可控指标要求。 **2) 先考虑成熟产品，后考虑自主创新** 2015年，安全可控技术相对成熟的网络设备、存储、中低端服务器优先级较高，而对于操作系统、大/小型机和数据库等领域，银行业需着重于探索尝试的研究任务，未来银行业信息架构上需逐步减少对高端服务器的依赖，如使用开源的X86应用集群替代高端服务器。
安全可控要求	关注信息技术、产品和服务的开放性、适用面和透明度； 信息技术厂商需逐步实施核心技术开放和产品开源，实现知识产权共享；对于各外资厂商，可以通过在国内成立合资公司，或者设立研发和技术中心等方式，提供及时的服务，确保国内金融机构未来能够迅速解决存在的潜在安全问题。

KPMG
cutting through complexity

银监办发[2014]317号文解读

银监办发[2009]437号文对于银行业重要信息系统的定义进行了说明，即：

- 支撑重要业务；
- 其信息安全和服务质量关系公民、法人和其他组织的权益，或关系社会秩序、公共利益乃至国家安全的信息系统。

重要信息系统主要包括：

- 面向客户的信息系统；
- 涉及账务处理且实时性要求较高的业务处理类、渠道类和涉及客户风险管理等业务的管理类信息系统；
- 支撑系统运行的机房和网络等基础设施。

银行业金融机构实施架构转型的实质是从改变其集中式架构中核心业务过度依赖闭源大型机设备的局面。闭源大型机设备的开放性较差，相关“基础软件”包括操作系统，中间件，数据库软件程序的源代码未实现共享，这些“排他性”的内嵌软件，出现问题很难快速解决，阻碍信息技术安全可控。

银行业实现信息技术安全可控，需要解决技术层面涉及的稳定性、性能、安全和风险控制等一系列的问题，无法一蹴而就，监管机构在架构转型方面循序渐进的推进，在一段时期内，我国的银行业金融机构将会出现集中式和分布式架构共存的系统运行模式。

银监会要求银行业金融机构建立信息技术应用安全可控能力自评机制

基于[2015]100号文《关于开展2014年度银行业信息技术情况调研的通知》，各机构针对自身安全可控工作的应用任务和研究任务执行情况进行成熟度自评，并开展年度安全可控指标数据收集和分析工作。自评范围包括信息系统设备总数，厂商性质及厂商国别等，并需提交自评结果与银监会。

KPMG
cutting through complexity

[2014]317号文相关说明解读

2 政策解读和毕马威的理解


中国银行业监督管理委员会
CHINA BANKING REGULATORY COMMISSION
树立监管权威 提高监管有效性
当前位置：中国银行业监督管理委员会 > 政务信息 > 公告通知

发布时间：2015-02-12 文章来源：信科部 文章类型：原创

关于《银行业应用安全可控信息技术推进指南（2014—2015年度）》
（银监办发〔2014〕317号）
的相关说明

2014年银监会会同工信部发布了《银行业应用安全可控信息技术推进指南（2014—2015年度）》（银监办发〔2014〕317号），现就有关事项进一步说明如下：

一、源代码备案具体工作还在研究中，备案方式和流程将在充分听取各方意见后实施。

二、在银行业范畴以内，关于随机软件拥有自主知识产权，现阶段只要求供应商提供软件的知识产权证明或合法来源证明。

三、相关要求不存在国别差别。

《[2014]317号文相关说明》补充说明了源代码备案和随机软件自主知识产权的管理要求，并澄清相关信息安全可控要求并不涉及国别差别

- 对于自主可控技术涉及的源代码备案要求，包括大型机设备相关的“基础软件”包括操作系统、中间件、数据库软件，银监会的补充说明表明可控要求存在比较大的协商空间，第三方备案的方式及操作细则尚存在不确定性；
- 监管机构放松了针对软件自主知识产权的要求，对于随机软件供应商只要提供软件合法的来源证明或知识产权证明即可，因此非国产产品亦可纳入银行业机构的安全可控应用软件的范畴；
- 明确强调我国银行业机构在选择安全自主可控技术时，产品国别并非必要考虑要素。对于各信息技术厂商来说，如果愿意开放核心信息技术，加强各相关方的合作沟通，参与产业创新联盟的技术和经验共享，仍可以被视为安全可控供应商。

KPMG
cutting through complexity

联系我们

银行业金融机构将需要进行IT 资产分析来认识当前的基础技术架构和与监管机构要求的差距，从而评估安全可控信息技术的应用对企业的影响。银行需要制定2015年至2019年的实施规划，并且修订管理架构来解决其信息系统与政策要求的差距。在毕马威中国，我們拥有网络与系统安全的专业服务团队来协助客户处理相关事宜。

北京

陈金峰
合伙人，管理咨询

电话：+8610 8508 5413
电邮：benson.tran@kpmg.com

刘逸明
合伙人，管理咨询

电话：+8610 8508 7094
电邮：kevin.liu@kpmg.com

上海

刘建刚
合伙人，管理咨询

电话：+8621 2212 3626
电邮：reynold.jg.liu@kpmg.com

张令琪
总监，管理咨询

电话：+8621 2212 3637
电邮：richard.zhang@kpmg.com

香港

石浩然
合伙人，管理咨询

电话：+852 2143 8799
电邮：henry.shek@kpmg.com

深圳

梁安超
合伙人，管理咨询

电话：+86 755 2547 3338
电话：kelvin.oc.leung@kpmg.com

KPMG

cutting through complexity