301--中国银监会办公厅关于印发  
《银行业金融机构重要信息系统投产及变更管理办法》的通知  
（银监办发〔2009〕437号）

各银监局，各政策性银行、国有商业银行、股份制商业银行，邮政储蓄银行，各省级农村信用联社：

为加强银行业金融机构重要信息系统投产及变更风险管理，保障银行业金融机构重要信息系统安全稳定运行，现将《银行业金融机构重要信息系统投产及变更管理办法》印发给你们，请遵照执行。请各银监局将本通知转发至辖内各银行业金融机构。

中国银行业监督管理委员会

二00九年十二月二十九日

**银行业金融机构重要信息系统投产及变更管理办法**

**第一章　总则**

**第一条**　为加强银行业金融机构重要信息系统投产及变更风险管理，根据《中华人民共和国银行业监督管理法》、《中华人民共和国商业银行法》制定本办法。

**第二条**　在中华人民共和国境内设立的政策性银行、国有商业银行、股份制商业银行、邮政储蓄银行、城市商业银行、农村商业银行、农村合作银行、农村信用社、城市信用社、外商独资银行、中外合资银行适用本办法。中国银行业监督管理委员会（以下简称中国银监会）监管的其他金融机构参照本办法执行。

**第三条**　本办法所称的重要信息系统是指支撑重要业务，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。包括面向客户、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，以及支撑系统运行的机房和网络等基础设施。

**第四条**　本办法所称的重要信息系统投产及变更主要指：

（一）重要信息系统投产。

（二）支撑重要信息系统运行的机房和网络基础设施投产。

（三）影响全辖或一个（含）以上分行系统服务、重要业务中断时间3小时（含）以上的重要信息系统以及支持其运行的基础设施变更，包括机房场地迁移、网络及核心业务系统应用架构变更、核心业务系统版本变更等。

（四）其他对银行重要业务运营及重要信息系统的可用性、完整性、安全性具有较大潜在影响的投产及变更。

**第二章　组织管理**

**第五条**　银行业金融机构应健全IT治理结构，落实重要信息系统投产及变更管理责任。

**第六条**　银行业金融机构高级管理层应统筹管理重要信息系统建设，听取重大项目投产或变更的风险评估汇报，对风险控制过程进行监督。

**第七条**　银行业金融机构信息科技部门应建立重要信息系统投产及变更管理机制、制度与流程，承担技术管理工作，协调业务、管理部门开展重要信息系统投产及变更工作，保障信息科技资源投入。

**第八条**　银行业金融机构业务、管理部门应配合信息科技部门开展投产及变更工作，开展业务影响分析，制定业务管理办法，组织用户测试，保证业务资源投入。

**第九条**　银行业金融机构内部审计部门应开展重要信息系统投产及变更审计工作，针对问题发现提出整改意见。

**第三章　风险评估**

**第十条**　银行业金融机构应充分识别、分析、评估重要信息系统投产及变更风险，包括系统功能缺陷、客户信息泄露、业务中断、交易缓慢或其他因素可能造成的操作风险、法律风险和声誉风险，并形成风险评估报告。

**第十一条**　银行业金融机构在采取有效信息安全控制措施的前提下，可委托外部专家或具备相应资质的外部专业机构进行重要信息系统投产及变更的风险评估工作。

**第十二条**　银行业金融机构董事会及高级管理层应审慎重大项目的风险评估报告。

**第十三条**　银行业金融机构应针对风险评估中发现的薄弱环节制定整改方案，明确整改时间。不具备整改条件的应采取风险缓释措施。

**第四章　投产及变更控制**

**第十四条**　银行业金融机构应统一组织协调重要信息系统投产及变更工作，制定年度投产及变更规则，编制实施计划和方案，确定实施策略和步骤，明确岗位职责，确保关键岗位职责分离。

**第十五条**　银行业金融机构应对重要信息系统投产及变更过程进行安全审查，采取风险控制措施，有效控制重要信息系统投产及变更风险。

**第十六条**　银行金融机构应建立重要信息系统投产及变更内容评审和审批、授权机制。

**第十七条**　银行业金融机构应按照对业务影响最小原则，采取与风险程度相适应的重要信息系统投产及变更策略。

**第十八条**　银行业金融机构应合理避开业务高峰期和敏感时段安排重要信息系统上线，应提前将重要信息系统投产及变更可能对服务的影响告知客户。

**第十九条**　银行业金融机构应建立充分、完整的测试体系，测试结果应经过信息科技部门和相关业务部门确认，并形成测试和验收报告，确保系统上线后的正常稳定运行以及系统功能与业务目标的一致性。

**第二十条**　银行业金融机构应建立与生产环境相隔离的测试环境，测试环境应模拟生产环境的真实情况。

**第二十一条**　银行业金融机构应建立完善的版本管理制度，制定严格的审批、控制和操作流程，保存完整的日志记录。拟投产及变更的重要信息系统应保证版本完整、准确、有效，遵从系统开发和运行管理制度规范。

**第二十二条**　银行业金融机构应加强重要信息系统投产及变更过程中的数据管理与质量控制；测试环境中使用的敏感生产数据应进行脱敏、变形处理；需要历史数据迁移的，应制定详细的数据迁移计划，并提前进行数据迁移测试和数据有效性、兼容性验证，确保迁移后数据的完整性、安全性和可用性。

**第二十三条**　银行业金融机构应制定重要信息系统投产及变更应急预案，制定系统回退和应急处置计划和流程，必要时应实施演练。

**第二十四条**　重要信息系统投产及变更过程中，银行业金融机构应严格执行上线实施方案，加强监督与复核，避免操作失误和非法操作。

**第二十五条**　银行业金融机构应加强重要信息系统投产及变更过程的风险监控和预警，各相关部门协同做好应急准备。

**第二十六条**　银行业金融机构应制定并落实系统运行管理规程、制度，制定、完善相关业务管理办法、操作规程，明确业务及运行管理职责，组织必要的培训，确保投产及变更实施后业务顺利开展。

**第二十七条**　银行业金融机构应在重要信息系统投产及变更实施后，组织业务部门、管理部门和信息科技部门对投产及变更的有效性进行验证。

**第二十八条**　银行业金融机构应在重要信息系统投产及变更实施后及时更新各项相关应急预案，并适时实施演练。

**第二十九条**　银行业金融机构应对重要信息系统投产及变更过程产生的各类文档资料进行管理，确保文档资料的完整性、及时性和有效性，并满足独立审计要求。

**第五章　投产及变更报告**

**第三十条**　银行业金融机构应就重要信息系统投产及变更事项向中国银监会或其派出机构报告。

**第三十一条**　银行业金融机构应在重要信息系统投产前至少20个工作日、变更前至少10个工作日向中国银监会或其派出机构报告，包括但不限于：

（一）总体说明：投产及变更目的、内容、计划起止时间、业务影响范围、联系人及联系方式等。

（二）重要信息系统基本信息，包括：系统名称、业务功能，操作系统、数据库、中间件情况，应用架构、技术架构、数据架构，生产主机备份方案、数据备份方案，运行管理等相关职能部门，是否纳入灾难恢复计划等。

（三）重要信息系统安全策略和措施，包括对账户、交易和客户敏感信息的安全控制措施等。

（四）涉及基础设施的，需提供基础设施基本信息，包括机房和网络方案。机房方案包括等级标准、地址、供配电系统、消防、空调、弱电系统、机房加固、机房空间规划，以及机房验收报告等；网络方案包括网络架构分区、核心网络备份情况，以及区域间、外联网、互联网边界安全措施与网络监控措施等。

（五）采取外包方式的，需提交外包服务机构情况、外包服务内容、外包风险评估报告等。

（六）投产及变更方案，包括投产及变更的组织结构与实施计划、操作步骤等。

（七）风险评估报告，应包括业务影响分析，技术风险分析与评估，控制措施的有效性，以及剩余风险等。

（八）应急预案，包括应急处置组织结构，应急场景，应急处置流程、步骤，应急联系方式与报告路线等，实施演练的应提交演练总结报告。

**第三十二条**　银行业金融机构应在重要信系统投产及变更实施后1个月内向中国银监会或其派出机构提交总结报告材料，内容包括但不限于：投产及变更方案执行情况、效果，问题发现和处理情况，后续改进措施等。如投产及变更失败，应详细说明失败原因。

**第三十三条**　银行业金融机构应按照属地监管原则提交报告材料，报送路线如下：

（一）银行业金融机构法人组织实施投产及变更的，由该法人机构统一向中国银监会或其派出机构提交报告材料。

（二）银行业金融机构分行组织实施投产及变更的，由分行向所在地中国银监会派出机构提交报告材料。

**第三十四条**　重要信息系统投产及变更如失败需要重新安排的，银行业金融机构应再次向中国银监会或其派出机构报告。

**第三十五条**　银行业金融机构数据中心机房设立、场所变更，应按照中国银监会有关数据中心管理规范报告。

**第六章　监督管理**

**第三十六条**　针对银行业金融机构重要信息系统投产及变更风险，中国银监会及其派出机构可以采取风险提示、约见谈话、监管质询等措施。

**第三十七条**　中国银监会及其派出机构可依法对银行业金融的重要信息系统投产及变更实施现场检查。

**第三十八条**　银行业金融机构违反本办法有关规定的，中国银监会及其派出机构将依法追究相关责任。

**第七章　附则**

**第三十九条**　本办法由中国银监会负责解释和修订。

**第四十条**　本办法自公布之日起执行。