银行业金融机构信息系统风险管理指引

第一章　总　则

第一条　为有效防范银行业金融机构运用信息系统进行业务处理、经营管理和内部控制过程中产生的风险，促进我国银行业安全、持续、稳健运行，根据《中华人民共和国银行业监督管理法》、国家信息安全相关要求和信息系统管理的有关法律法规，制定本指引。

第二条　本指引适用于银行业金融机构。

本指引所称银行业金融机构，是指在中华人民共和国境内设立的商业银行、城市信用合作社、农村合作银行、农村信用合作社等吸收公众存款的金融机构以及政策性银行。

在中华人民共和国境内设立的金融资产管理公司、信托投资公司、财务公司、金融租赁公司、汽车金融公司以及经中国银行业监

督管理委员会（以下简称银监会）及其派出机构批准设立的其他金融机构，适用本指引规定。

第三条 本指引所称信息系统，是指银行业金融机构运用现代信息、通信技术集成的处理业务、经营管理和内部控制的系统。

第四条 本指引所称信息系统风险，是指信息系统在规划、研发、建设、运行、维护、监控及退出过程中由于技术和管理缺陷产生的操作、法律和声誉等风险。

第五条 信息系统风险管理的目标是通过建立有效的机制，实现对信息系统风险的识别、计量、评价、预警和控制，推动银行业金融机构业务创新，提高信息化水平，增强核心竞争力和可持续发展能力。

第二章 机构职责

第六条 银行业金融机构应建立有效的信息系统风险管理架构，完善内部组织结构和工作机制，防范和控制信息系统风险。

第七条 银行业金融机构应认真履行下列信息系统管理职责：

（一）贯彻执行国家有关信息系统管理的法律、法规和技术标准，落实银监会相关监管要求；

（二）建立有效的信息安全保障体系和内部控制规程，明确信息系统风险管理岗位责任制度，并监督落实；

（三）负责组织对本机构信息系统风险进行检查、评估、分析，及时向本机构专门委员会和银监会及其派出机构报送相关的管理信息；

（四）及时向银监会及其派出机构报告本机构发生的重大信息系统事故或突发事件，并按有关预案快速响应；

（五）每年经董事会或其他决策机构审查后向银监会及其派出机构报送信息系统风险管理的年度报告；

（六）做好本机构信息系统审计工作；

（七）配合银监会及其派出机构做好信息系统风险监督检查工作，并按照监管意见进行整改；

（八）组织本机构信息系统从业人员进行信息系统有关的业务、技术和安全培训；

（九）开展与信息系统风险管理相关的其他工作。

第八条　银行业金融机构的董事会或其他决策机构负责信息系统的战略规划、重大项目和风险监督管理；信息科技管理委员会、风险管理委员会或其他负责风险监督的专业委员会应制定信息系统总体策略，统筹信息系统项目建设，定期评估、报告本机构信息系统风险状况，为决策层提供建议，采取相应的风险控制措施。

第九条 银行业金融机构法定代表人或主要负责人是本机构信息系统风险管理责任人。

第十条 银行业金融机构应设立信息科技部门，统一负责本机构信息系统的规划、研发、建设、运行、维护和监控，提供日常科技服务和运行技术支持；建立或明确专门信息系统风险管理部门，建立、健全信息系统风险管理规章、制度，并协助业务部门及信息科技部门严格执行，提供相关的监管信息；设立审计部门或专门审计岗位，建立健全信息系统风险审计制度，配备适量的合格人员进行信息系统风险审计。

第十一条 银行业金融机构从事与信息系统相关工作的人员应符合以下要求：

（一）具备良好的职业道德，掌握履行信息系统相关岗位职责所需的专业知识和技能；

（二）未经岗前培训或培训不合格者不得上岗；经考核不适宜的工作人员，应及时进行调整。

第十二条 银行业金融机构应加强信息系统风险管理的专业队伍建设，建立人才激励机制，适应信息技术的发展。

第十三条 银行业金融机构应依据有关法律法规及时和规范地披露信息系统风险状况。

第三章 总体风险控制

第十四条 总体风险是指信息系统在策略、制度、机房、软件、硬件、网络、数据、文档等方面影响全局或共有的风险。

第十五条 银行业金融机构应根据信息系统总体规划，制定明确、持续的风险管理策略，按照信息系统的敏感程度对各个集成要素进行分析和评估，并实施有效控制。

第十六条 银行业金融机构应采取措施防范自然灾害、运行环境变化等产生的安全威胁，防止各类突发事故和恶意攻击。

第十七条 银行业金融机构应建立健全信息系统相关的规章制度、技术规范、操作规程等；明确与信息系统相关人员的职责权限，建立制约机制，实行最小授权。

第十八条 在境外设立的我国银行业金融机构或在境内设立的境外银行业金融机构，应防范由于境内外信息系统监管制度差异等造成的跨境风险。

第十九条 银行业金融机构应严格执行国家信息安全相关标准，参照有关国际准则，积极推进信息安全标准化，实行信息安全等级保护。

第二十条 银行业金融机构应加强对信息系统的评估和测试，及时进行修补和更新，以保证信息系统的安全性、完整性。

第二十一条 银行业金融机构信息系统数据中心机房应符合国家有关计算机场地、环境、供配电等技术标准。全国性数据中心至少应达到国家 A 类机房标准，省域数据中心至少应达到国家 B 类机房标准，省域以下数据中心至少应达到 C 类机房标准。数据中心机房应实行严格的门禁管理措施，未经授权不得进入。

第二十二条 银行业金融机构应重视知识产权保护，使用正版软件，加强软件版本管理，优先使用具有中国自主知识产权的软、硬件产品；积极研发具有自主知识产权的信息系统和相关金融产品，并采取有效措施保护本机构信息化成果。

第二十三条 银行业金融机构与信息系统相关的电子设备的选型、购置、登记、保养、维修、报废等应严格执行相关规程，选用的设备应经过技术论证，测试性能应符合国家有关标准。信息系统所用的服务器等关键设备应具有较高的可靠性、充足的容量和一定的容错特性，并配置适当的备品备件。

第二十四条 信息系统的网络应参照相关的标准和规范设计、建设；网络设备应兼备技术先进性和产品成熟性；网络设备和线路应有冗余备份；严格线路租用合同管理，按照业务和交易流量要求保证传输带宽；建立完善的网管中心，监测和管理通信线路及网络设备，保障网络安全稳定运行。

第二十五条 银行业金融机构应加强网络安全管理。生产网络与开发测试网络、业务网络与办公网络、内部网络与外部网络应实施隔离；加强无线网、互联网接入边界控制；使用内容过滤、身份

认证、防火墙、病毒防范、入侵检测、漏洞扫描、数据加密等技术手段，有效降低外部攻击、信息泄漏等风险。

第二十六条 银行业金融机构应加强信息系统加密机、密钥、密码、加解密程序等安全要素的管理，使用符合国家安全标准的密码设备，完善安全要素生成、领取、使用、修改、保管和销毁等环节管理制度。密钥、密码应定期更改。

第二十七条 银行业金融机构应加强数据采集、存贮、传输、使用、备份、恢复、抽检、清理、销毁等环节的有效管理，不得脱离系统采集加工、传输、存取数据；优化系统和数据库安全设置，严格按授权使用系统和数据库，采用适当的数据加密技术以保护敏感数据的传输和存取，保证数据的完整性、保密性。

第二十八条 银行业金融机构应对信息系统配置参数实施严格的安全与保密管理，防止非法生成、变更、泄漏、丢失与破坏。根据敏感程度和用途，确定存取权限、方式和授权使用范围，严格审批和登记手续。

第二十九条 银行业金融机构应制定信息系统应急预案，并定期演练、评审和修订。省域以下数据中心至少实现数据备份异地保存，省域数据中心至少实现异地数据实时备份，全国性数据中心实现异地灾备。

第三十条 银行业金融机构应加强对技术文档资料和重要数据的备份管理；技术文档资料和重要数据应保留副本并异地存放，按规定年限保存，调用时应严格授权。信息系统的技术文档资料包括：系统环境说明文件、源程序以及系统研发、运行、维护过程中形成的各类技术资料。重要数据包括：交易数据、账务数据、客户数据，以及产生的报表数据等。

第三十一条 银行业金融机构在信息系统可能影响客户服务时，应以适当方式告知客户。

第四章 研发风险控制

第三十二条 研发风险是指信息系统在研发过程中组织、规划、需求、分析、设计、编程、测试和投产等环节产生的风险。

第三十三条 银行业金融机构信息系统研发前应成立项目工作小组，重大项目还应成立项目领导小组，并指定负责人。项目领导小组负责项目的组织、协调、检查、监督工作。项目工作小组由业务人员、技术人员和管理人员组成，具体负责整个项目的开发工作。

第三十四条 项目工作小组人员应具备与项目要求相适应的业务经验与专业技术知识，小组负责人需具备组织领导能力,保证信息系统研发质量和进度。

第三十五条 银行业金融机构业务部门根据本机构业务发展战略，在充分进行市场调查、产品效益分析的基础上制定信息系统研发项目可行性报告。

第三十六条 银行业金融机构业务部门编写项目需求说明书，提出风险控制要求，信息科技部门根据项目需求编制项目功能说明书。

第三十七条 银行业金融机构信息科技部门依据项目功能说明书分别编写项目总体技术框架、项目设计说明书，设计和编码应符合项目功能说明书的要求。

第三十八条 银行业金融机构应建立独立的测试环境，以保证测试的完整性和准确性。测试至少应包括功能测试、安全性测试、压力测试、验收测试、适应性测试。测试不得直接使用生产数据。

第三十九条 银行业金融机构信息科技部门应根据测试结果修补系统的功能和缺陷，提高系统的整体质量。

第四十条 银行业金融机构业务人员、技术人员应根据职责范围分别编写操作说明书、技术应急方案、业务连续性计划、投产计划、应急回退计划，并进行演练。

第四十一条 开发过程中所涉及的各种文档资料应经相关部门、人员的签字确认并归档保存。

第四十二条 项目验收应出具由相关负责人签字的项目验收报告，验收不合格不得投产使用。

第五章 运行维护风险控制

第四十三条 运行维护风险是指信息系统在运行与维护过程中操作管理、变更管理、机房管理和事件管理等环节产生的风险。

第四十四条 银行业金融机构信息系统运行与维护应实行职责分离，运行人员应实行专职，不得由其他人员兼任。运行人员应按操作规程巡检和操作。维护人员应按授权和维护规程要求对生产状态的软硬件、数据进行维护，除应急外，其他维护应在非工作时间进行。

第四十五条 银行业金融机构信息系统的运行应符合以下要求：

（一）制定详细的运行值班操作表，包括规定巡检时间，操作范围、内容、办法、命令以及负责人员等信息；

（二）提供常见和简便的操作菜单或命令，如信息系统的启动或停止、运行日志的查询等；

（三）提供机房环境、设备使用、网络运行、系统运行等监控信息；

（四）记录运行值班过程中所有现象、操作过程等信息。

第四十六条 银行业金融机构信息系统的维护应符合以下要求：

（一）除对信息系统设备和系统环境的维护外，对软件或数据的维护必须通过特定的应用程序进行，添加、删除和修改数据应通过柜员终端，不得对数据库进行直接操作；

（二）具备各种详细的日志信息，包括交易日志和审计日志等，以便维护和审计；

（三）提供维护的统计和报表打印功能。

第四十七条 银行业金融机构信息系统的变更应符合以下要求：

（一）制订严密的变更处理流程，明确变更控制中各岗位的职责，并遵循流程实施控制和管理；变更前应明确应急和回退方案，无授权不得进行变更操作；

（二）根据变更需求、变更方案、变更内容核实清单等相关文档审核变更的正确性、安全性和合法性；

（三）应采用软件工具精确判断变更的真实位置和内容，形成变更内容核实清单，实现真实、有效、全面的检验；

（四）软件版本变更后应保留初始版本和所有历史版本，保留所有历史的变更内容核实清单。

第四十八条 银行业金融机构在信息系统投产后一定时期内，应组织对系统的后评价，并根据评价及时对系统功能进行调整和优化。

第四十九条 银行业金融机构应对机房环境设施实行日常巡检，明确信息系统及机房环境设施出现故障时的应急处理流程和预案，有实时交易服务的数据中心应实行24小时值班。

第五十条 银行业金融机构应实行事件报告制度，发生信息系统造成重大经济、声誉损失和重大影响事件，应即时上报并处理，必要时启动应急处理预案。

第六章 外包风险控制

第五十一条 外包风险是指银行业金融机构将信息系统的规划、研发、建设、运行、维护、监控等委托给业务合作伙伴或外部技术供应商时形成的风险。

第五十二条 银行业金融机构在进行信息系统外包时，应根据风险控制和实际需要，合理确定外包的原则和范围，认真分析和评估外包存在的潜在风险，建立健全有关规章制度，制定相应的风险防范措施。

第五十三条　银行业金融机构应建立健全外包承包方评估机制，充分审查、评估承包方的经营状况、财务实力、诚信历史、安全资质、技术服务能力和实际风险控制与责任承担水平，并进行必要的尽职调查。评估工作可委托经国家相应监管部门认定资质，具有相关专业经验的独立机构完成。

第五十四条　银行业金融机构应当与承包方签订书面合同，明确双方的权利、义务，并规定承包方在安全、保密、知识产权方面的义务和责任。

第五十五条　银行业金融机构应充分认识外包服务对信息系统风险控制的直接和间接影响，并将其纳入总体安全策略和风险控制之中。

第五十六条　银行业金融机构应建立完整的信息系统外包风险评估与监测程序，审慎管理外包产生的风险，提高本机构对外包管理的能力。

第五十七条　银行业金融机构的信息系统外包风险管理应当符合风险管理标准和策略，并应建立针对外包风险的应急计划。

第五十八条 银行业金融机构应与外包承包方建立有效的联络、沟通和信息交流机制，并制定在意外情况下能够实现承包方的顺利变更，保证外包服务不间断的应急预案。

第五十九条 银行业金融机构将敏感的信息系统，以及其他涉及国家秘密、商业秘密和客户隐私数据的管理与传递等内容进行外包时，应遵守国家有关法律法规，符合银监会的有关规定，经过董事会或其他决策机构批准，并在实施外包前报银监会及其派出机构和法律法规规定需要报告的机构备案。

第七章 审 计

第六十条 银行业金融机构内设审计部门负责本机构信息系统审计，也可聘请经国家相应监管部门认定资质的中介机构进行信息系统外部审计。

第六十一条 信息系统风险审计应包括：总体风险审计、系统审阅和专项风险审计。

第六十二条 总体风险审计是指对本机构所有信息系统共有的公共部分进行审计，实施总体风险控制。根据信息系统的总体风险状况确定审计频率，但至少每 3 年审计一次。

第六十三条 信息系统的系统审阅是指对研发、运行及退出的全过程进行审计，分投产前与投产后的审阅。

第六十四条 投产前的系统审阅是指审计人员采用非现场形式，对信息项目开发过程中所提交的有关文档资料进行审阅，指出其中存在的风险，了解是否具有相应的控制措施，并提出评价和建议的过程。信息系统投产前的系统审阅应关注信息系统的安全控制、权限设置、正确性、连贯性、完整性、可审计性和及时性等内容。

投产前的系统审阅重点：

（一）被外界成功攻破的可能性；

（二）在内部安全控制方面的设计漏洞与缺陷；

（三）项目开发管理方面的问题；

（四）效率与效能；

（五）功能、设计和工作流程是否符合法律、法规和内部控制方面的规定并有连续兼容性；

（六）其他需重点审阅的内容。

第六十五条 投产前的系统审阅文档资料包括：

（一）项目可行性报告；

（二）项目需求说明书；

（三）项目功能说明书（包括业务与技术方面存在的风险及控制办法）；

（四）项目总体技术框架；

（五）项目设计说明书；

（六）项目实施计划；

（七）与第三方签订的外包协议；

（八）测试计划及验收报告；

（九）投产计划；

（十）项目开发例会的会议记录；

（十一）操作手册；

（十二）其他需审阅的文档资料。

对于所含内容较多的文档资料，应对关键交易的数据处理流程、交易接口和其他重要的安全事项进行审阅。

第六十六条 投产后的系统审阅是指在信息系统投入生产一段时间后进行的审计，旨在评估对信息系统各项风险的控制是否恰当，能否实现预定的设计目标。投产后的系统审阅应在信息系统投入生产半年后进行，审计报告应对被审计的信息系统提出改进或增加风险控制、能否继续生产等内容的审计建议。

第六十七条 信息系统专项风险审计是指对被审计单位发生信息安全事故进行的调查、分析和评估，或原有信息系统进行重大结构调整的审计，或审计部门认为需要对信息系统某项专题进行审计。

第六十八条 银行业金融机构信息系统风险审计也可以由银监会及其派出机构依据法律、法规和规章，委托并授权有法定资质的中介评估机构进行。

第六十九条 中介机构根据银监会或其派出机构委托或授权对银行业金融机构进行审计时，应出示委托授权书，并依照委托授权书上规定的委托和授权范围进行审计。

第七十条 中介机构根据授权出具的审计报告经银监会及其派出机构审阅确定后具有法律效力，被审计金融机构应对该审计报告在法定时间内提出整改意见，并按审计报告中提出的建议进行及时整改。

第七十一条 中介机构应严格执行法律法规，保守被审计单位的商业秘密和风险信息。审计过程中所有涉及资料的调阅应有交接手续，并不得带离现场或进行修改、复制。

第八章 附 则

第七十二条 本指引由中国银行业监督管理委员会负责解释、修订。

第七十三条 本指引自颁布之日起施行。