中国银行业监督管理委员会办公厅文件

银监办发〔2010〕114号

中国银监会办公厅关于印发《商业银行数据中心监管指引》的通知

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：

为加强商业银行数据中心风险管理，保障数据中心安全、可靠、稳定运行，加强灾难恢复管理，提高业务连续性水平，现将《商业银行数据中心监管指引》印发给你们，请遵照执行。

请各银监局将本通知转发至辖内相关银行业金融机构。

中国银行业监督管理委员会办公厅

二〇一〇年四月十六日

商业银行数据中心监管指引

第一章 总 则

第一条 为加强商业银行数据中心风险管理，保障数据中心安全、可靠、稳定运行，提高商业银行业务连续性水平，根据《中华人民共和国银行业监督管理法》及《中华人民共和国商业银行法》制定本指引。

第二条 在中华人民共和国境内设立的国有商业银行、股份制商业银行、邮政储蓄银行、城市商业银行、省级农村信用联合社、外商独资银行、中外合资银行适用本指引。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指引执行。

第三条 以下术语适用于本指引：

(一) 本指引所称数据中心包括生产中心和灾难备份中心(以下简称灾备中心)。

(二) 本指引所称生产中心是指商业银行对全行业务、客户和管理等重要信息进行集中存储、处理和维护，具备专用场所，为业务运营及管理提供信息科技支撑服务的组织。

(三) 本指引所称灾备中心是指商业银行为保障其业务连续

性，在生产中心故障、停顿或瘫痪后，能够接替生产中心运行，具备专用场所，进行数据处理和支持重要业务持续运行的组织。

（四）本指引所称灾备中心同城模式是指灾备中心与生产中心位于同一地理区域，一般距离数十公里，可防范火灾、建筑物破坏、电力或通信系统中断等事件。灾备中心异地模式是指灾备中心与生产中心处于不同地理区域，一般距离在数百公里以上，不会同时面临同类区域性灾难风险，如地震、台风和洪水等。

（五）本指引所称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、涉及账务处理且时效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 《信息安全技术 信息系统灾难恢复规范》（GB/T 20988－2007）中的条款通过本指引的引用而成为本指引的条款。

第二章 设立与变更

第五条 商业银行应于取得金融许可证后两年内，设立生产中心；生产中心设立后两年内，设立灾备中心。

第六条 商业银行数据中心应配置满足业务运营与管理要求的场地、基础设施、网络、信息系统和人员，并具备支持业务不间断

服务的能力。

第七条 总资产规模一千亿元人民币以上且跨省设立分支机构的法人商业银行，及省级农村信用联合社应设立异地模式灾备中心，重要信息系统灾难恢复能力应达到《信息安全技术 信息系统灾难恢复规范》中定义的灾难恢复等级第5级(含)以上；其他法人商业银行应设立同城模式灾备中心并实现数据异地备份，重要信息系统灾难恢复能力应达到《信息安全技术 信息系统灾难恢复规范》中定义的灾难恢复等级第4级(含)以上。

第八条 商业银行应就数据中心设立，数据中心服务范围、服务职能和场所变更，以及其他对数据中心持续运行具有较大影响的重大变更事项向中国银监会或其派出机构报告。

第九条 商业银行应在数据中心规划筹建阶段，以及在数据中心正式运营前至少20个工作日，向中国银监会或其派出机构报告。

第十条 商业银行变更数据中心场所时应至少提前2个月，其他重大变更应至少提前10个工作日向中国银监会或其派出机构报告。

第三章 风险管理

第十一条 商业银行信息科技风险管理部门应制定数据中心风险管理策略、风险识别和评估流程，定期开展风险评估工作，对

风险进行分级管理，持续监督风险管理状况，及时预警，将风险控制在可接受水平。

第十二条 商业银行信息科技部门应指导、监督和协调数据中心明确信息系统运营维护管理策略，建立运营维护管理制度、标准和流程，落实信息科技风险管理措施。

第十三条 商业银行数据中心应建立健全各项管理与内控制度，从技术和管理等方面实施风险控制措施。

第十四条 商业银行数据中心应设立专门管理岗位，监督、检查数据中心各项规范、制度、标准和流程的执行情况以及风险管理状况。

第十五条 商业银行应根据业务影响分析所识别出风险的可能性和损失程度，决定是否购买商业保险以应对不同类型的灾难，并定期检查其保险策略及范围。投保资产清单应保存于安全场所，以便索赔时使用。

第十六条 商业银行内部审计部门应至少每三年进行一次数据中心内部审计。

第十七条 商业银行在采取有效信息安全控制措施的前提下，可聘请合格的外部审计机构定期对数据中心进行审计。

第十八条 商业银行数据中心应根据内、外部审计意见，及时制定整改计划并实施整改。

第四章　运行环境管理

第十九条　商业银行进行数据中心选址时，应进行全面的风险评估，综合考虑地理位置、环境、设施等各种因素对数据中心安全运营的潜在影响，规避选址不当风险，避免数据中心选址过度集中。

第二十条　数据中心选址应满足但不限于以下要求：

（一）生产中心与灾备中心的场所应保持合理距离，避免同时遭受同类风险。

（二）应选址于电力供给可靠，交通、通信便捷地区；远离水灾和火灾隐患区域；远离易燃、易爆场所等危险区域；远离强振源和强噪声源，避开强电磁场干扰；应避免选址于地震、地质灾害高发区域。

第二十一条　数据中心基础设施建设应以满足重要信息系统运行高可用性和高可靠性要求、保障业务连续性为目标，应满足但不限于以下要求：

（一）建筑物结构，如层高、承重、抗震等，应满足专用机房建设要求。

（二）应根据使用要求划分功能区域，各功能区域原则上相对独立。

（三）应配备不间断电源、应急发电设施等以满足信息技术设备连续运行的要求。

（四）通信线路、供电、机房专用空调等基础设施应具备冗余能力，进行冗余配置，消除单点隐患。

（五）机房区域应采用气体消防和自动消防预警系统，内部通道设置、装饰材料等应满足消防要求，并通过消防验收。

（六）应采取防雷接地、防磁、防水、防盗、防鼠虫害等保护措施。

（七）应采用环保节能技术，降低能耗，提高效率。

第二十二条 数据中心安防与基础设施保障应满足但不限于以下要求：

（一）各功能区域应根据使用功能划分安全控制级别，不同级别区域采用独立的出入控制设备，并集中监控，各区域出入口及重要位置应采用视频监控，监控记录保存时间应满足事件分析、监督审计的需要。

（二）应具备机房环境监控系统，对基础设施设备、机房环境状况、安防系统状况进行7×24小时实时监测，监测记录保存时间应满足故障诊断、事后审计的需要。

（三）每年至少开展一次针对基础设施的安全评估，对基础设施的可用性和可靠性、运维管理流程以及人员的安全意识等方面进行检查，及时发现安全隐患并落实整改。

第二十三条 数据中心应采用两家或多家通信运营商线路互为备份。互为备份的通信线路不得经过同一路由节点。

第五章　运营维护管理

第二十四条　商业银行应建立满足业务发展要求的数据中心运营维护管理体系，根据业务需求定义运营维护服务内容，制定服务标准和评价方法，建立运营维护管理持续改进机制。

第二十五条　数据中心应建立满足信息科技服务要求的运营管理组织架构。设立生产调度、信息安全、操作运行维护、质量合规管理等职能相关的部门或岗位，明确岗位和职责，配备专职人员，提供岗位专业技能培训，确保关键岗位职责分离，通过职责分工和岗位制约降低数据中心操作风险。

第二十六条　数据中心应建立信息科技运行维护服务管理流程，提高整体运行效率和服务水平，包括：

（一）应建立事件和问题管理机制。明确事件管理流程，定义事件类别、事件分级响应要求和事件升级、上报规则，及时受理、响应、审批和交付服务请求，保障生产服务质量，尽可能降低对业务影响；建立服务台负责受理、跟踪、解答各类运营问题；建立问题根源分析及跟踪解决机制，查明运营事件产生的根本原因，避免事件再次发生。

（二）应建立变更管理流程，减少或防止变更对信息科技服务的影响。根据变更对业务影响大小进行变更分级，对变更影响、变更风险、资源需求和变更批准进行控制和管理；变更方案应包括应急及回退措施，并经过充分测试和验证；建立变更管理联动机制，

当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性；应尽量减少紧急变更。

（三）应建立配置管理流程，统一管理、及时更新数据中心基础设施和重要信息系统配置信息，支持变更风险评估、变更实施、故障事件排查、问题根源分析等服务管理流程。

（四）应对重要信息系统和通信网络的容量和性能需求进行前瞻性规划，分析、调整和优化容量和性能，满足业务发展要求。

（五）应统一调度各项运维任务，协调和解决各项运维任务冲突，妥善记录和保存运维任务调度过程。

（六）应制定验收交接标准及流程，规范重要信息系统投产验收管理。加强版本控制，防范因软件版本、操作文档等不一致产生的风险。

（七）应根据商业银行总体风险控制策略及应急管理要求，从基础设施、网络、信息系统等不同方面分别制定应急预案，并及时修订应急预案，定期进行演练，保证其有效性。

（八）应集中监控重要信息系统和通信网络运行状态。采用监控管理工具，实时监控重要信息系统和通信网络的运行状况，通过监测、采集、分析和调优，提升生产系统运行的可靠性、稳定性和可用性。监控记录应满足故障定位、诊断及事后审计等要求。

第二十七条 数据中心应建立信息安全管理规范，保证重要信息的机密性、完整性和可用性，包括：

（一）应设立专门的信息安全管理部门或岗位，制定安全管理

制度和实施计划，定期对信息安全策略、制度和流程的执行情况进行检查和报告。

（二）应建立和落实人员安全管理制度，明确信息安全管理职责；通过安全教育与培训，提高人员的安全意识和技能；建立重要岗位人员备份制度和监督制约机制。

（三）应加强信息资产管理，识别信息资产并建立责任制，根据信息资产重要性实施分类控制和分级保护，防范信息资产生成、使用和处置过程中的风险。

（四）应建立和落实物理环境安全管理制度，明确安全区域、规范区域访问管理，减少未授权访问所造成的风险。

（五）应建立操作安全管理制度，制定操作规程文档，规范信息系统监控、日常维护和批处理操作等过程。

（六）应建立数据安全管理制度，规范数据的产生、获取、存储、传输、分发、备份、恢复和清理的管理，以及存储介质的台帐、转储、抽检、报废和销毁的管理，保证数据的保密、真实、完整和可用。

（七）应建立网络通信与访问安全策略，隔离不同网络功能区域，采取与其安全级别对应的预防、监测等控制措施，防范对网络的未授权访问，保证网络通信安全。

（八）应建立基础设施和重要信息的授权访问机制，制定访问控制流程，保留访问记录，防止未授权访问。

第六章　灾难恢复管理

第二十八条　商业银行应将灾难恢复管理纳入业务连续性管理框架，建立灾难恢复管理组织架构，明确灾难恢复管理机制和流程。

第二十九条　商业银行应统筹规划灾难恢复工作，定期进行风险评估和业务影响分析，确定灾难恢复目标和恢复等级，明确灾难恢复策略、预案并及时更新。

第三十条　商业银行灾难恢复预案应包括但不限于以下内容：灾难恢复指挥小组和工作小组人员组成及联系方式、汇报路线和沟通协调机制、灾难恢复资源分配、基础设施与信息系统的恢复优先次序、灾难恢复与回切流程及时效性要求、对外沟通机制、最终用户操作指导及第三方技术支持和应急响应服务等内容。

第三十一条　商业银行应为灾难恢复提供充分的资源保障，包括基础设施、网络通信、运维及技术支持人力资源、技术培训等。

第三十二条　商业银行应建立与服务提供商、电力部门、公安部门、当地政府和新闻媒体等单位的外部协作机制，保证灾难恢复时能及时获取外部支持。

第三十三条　商业银行应建立灾难恢复有效性测试验证机制，测试验证应定期或在重大变更后进行，内容应包含业务功能的恢复验证。

第三十四条　商业银行应每年至少进行一次重要信息系统专

项灾备切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，以真实业务接管为目标，验证灾备系统有效接管生产系统及安全回切的能力。

第三十五条 商业银行进行全面灾备切换和真实业务接管演练前应向中国银监会或其派出机构报告，并在演练结束后报送演练总结。

第三十六条 商业银行因灾难事件启动灾难恢复或将灾备中心回切至生产中心后，应及时向中国银监会或其派出机构报告，报告内容包括但不限于：灾难事件发生时间、影响范围和程度，事件起因、应急处置措施、灾难恢复实施情况和结果、回切方案。

第七章 外包管理

第三十七条 商业银行董事会对外包负最终管理责任，应推动和完善外包风险管理体系建设，确保商业银行有效应对外包风险。

第三十八条 商业银行应根据信息科技战略规划制定数据中心外包策略；应制定数据中心服务外包管理制度、流程，建立全面的风险控制机制。

第三十九条 商业银行应确定外包服务所涉及的信息资产的关键性和敏感程度，审慎确定数据中心外包服务范围。

第四十条 商业银行应充分识别、分析、评估数据中心外包风

险，包括信息安全风险、服务中断风险、系统失控风险以及声誉风险、战略风险等，形成风险评估报告并报董事会和高管层审核。

第四十一条 实施数据中心服务外包时，商业银行的管理责任不得外包。

第四十二条 数据中心服务外包一般包括：

（一）基础设施类：外包服务商向商业银行提供数据中心机房、配套设施或运行设备的服务。

（二）运营维护类：外包服务商向商业银行提供数据中心信息系统或基础设施的日常运行、维护等服务。

第四十三条 商业银行在选择数据中心外包服务商时，应充分审查、评估外包服务商的资质、专业能力和服务方案，对外包服务商进行风险评估，考查其服务能力是否足以承担相应的责任。评估包括：外包服务商的企业信誉及财务稳定性，外包服务商的信息安全和信息科技服务管理体系，银行业服务经验等。提供数据中心基础设施外包服务的服务商，其运行环境应符合商业银行要求，并具有完备的安全管理规范。

第四十四条 商业银行应与数据中心外包服务商签订书面合同，在合同中明确重要事项，包括但不限于双方的权利和义务、外包服务水平、服务的可靠性、服务的可用性、信息安全控制、服务持续性计划、审计、合规性要求、违约赔偿等。

第四十五条 商业银行应要求外包服务商购买商业保险以保证其有足够的赔偿能力，并告知保险覆盖范围。

第四十六条 商业银行应加强对数据中心外包服务活动的安全管理，包括但不限于：

（一）商业银行应将数据中心外包服务安全管理纳入数据中心的整体安全策略，保障业务、管理和客户敏感数据信息安全。

（二）商业银行应按照“必需知道”和“最小授权”原则，严格控制外包服务商信息访问的权限，要求外包服务商不得对外泄露所接触的商业银行信息。

（三）商业银行应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。

（四）商业银行应要求外包服务商遵守商业银行有关信息科技风险管理制度和流程。

（五）商业银行应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告。

（六）商业银行应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。

第四十七条 商业银行应禁止外包服务商转包并严格控制分包，保证外包服务水平。

第四十八条 商业银行应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。

第四十九条 商业银行应建立外包服务考核、评价机制，定期对外包服务活动和外包服务商的服务能力进行审核和评估，确保获得持续、稳定的外包服务。

第五十条 商业银行在实施数据中心整体服务外包以及涉及影响业务、管理和客户敏感数据信息安全的外包前，应向中国银监会或其派出机构报告。

第五十一条 商业银行应在外包服务协议条款中明确商业银行和监管机构有权对协议范围内的服务活动进行监督检查，包括外包商的服务职能、责任、系统和设施等内容。

第八章 监督管理

第五十二条 中国银监会及其派出机构可依法对商业银行的数据中心实施非现场监管及现场检查。现场检查原则上每三年一次。

第五十三条 针对商业银行数据中心设立、变更、运营过程存在的风险，中国银监会或其派出机构可向商业银行提示风险并提出整改意见。商业银行应及时整改并反馈结果。

第九章 附则

第五十四条 本指引由中国银监会负责解释、修订。

第五十五条 本指引自公布之日起执行。

附件:《商业银行数据中心监管指引》报告材料目录和格式要求

附件

《商业银行数据中心监管指引》报告材料目录和格式要求

一、数据中心规划报告材料目录

（一）数据中心建设规划报告，包括：

1. 立项报告和可行性分析报告，包括建设背景、建设目标、风险评估、效益分析、成本投入等。

2. 基础设施规划方案，包括选址、建筑物结构、功能区域划分、监控、防雷接地及消防等配套设施、机房等级等。

3. 信息系统建设规划方案，包括功能与技术方案规划、人员配置计划、系统服务的区域和业务范围等。灾备中心还需提供灾难恢复目标、灾难恢复等级、灾备技术方案规划及风险评估报告等。

（二）区域环境及基础设施风险评估说明，包括风险识别，风险分析和风险控制策略等。

（三）建设及运营模式说明，包括技术支持及运行维护体系等。如采用外包，需提供外包的服务内容和外包风险评估报告；

（四）组织架构规划。包括拟设立的部门与岗位职责、计划采用的人员数量等。

（五）建设及投入运营的时间进度计划和财务预算（基础设施

建设和运维管理费用等)。

(六) 中国银监会或其派出机构要求提供的其它文件和资料。

二、数据中心设立报告材料目录

(一) 由商业银行法定代表人签署的数据中心投产审批文件,包括数据中心上线申请,数据中心上线审批报告等。

(二) 基础设施情况,包括地址、建筑物结构、功能区域划分、监控、防雷接地及消防等配套设施验收报告、机房及附属设施验收报告等。

(三) 信息系统情况,包括系统架构、系统名称、系统服务的区域和业务范围、数据备份方案、灾备技术方案等。

(四) 运营模式说明,包括技术支持及运行维护体系等。如采用外包需说明主要外包管理情况,包括主要外包项目名称、外包内容(业务类型及范围等)、外包商基本情况、外包合同(包括安全保密条款、知识产权保护条款)、外包服务水平协议和外包风险评估报告等。

(五) 组织架构,包括部门设置与岗位职责、人员配备、主要负责人名单等。

(六) 管理制度和规范清单及相关说明,包括运行管理流程、安全管理制度、应急管理制度和规范(含应急恢复策略、信息系统备份和恢复方案、应急管理流程及预案、应急演练及培训计划等)、灾难恢复预案。

(七) 中国银监会或其派出机构要求提供的其它文件和资料。

三、数据中心重大变更报告材料目录

（一）变更说明，包括变更原因、目的、内容、时间和影响范围等。

（二）变更方案，包括变更准备、变更计划和步骤、变更应急和回退措施。

（三）风险评估报告，包括风险分析，控制措施、变更有效性评估。

（四）中国银监会或其派出机构要求提供的其它文件和资料。

四、报告材料格式要求

数据中心规划、设立及重大变更报告材料应向中国银监会或其派出机构报送纸质材料和电子文档。

主题词：数据中心　监管　通知

内部发送：信息中心、法规部、银行一部、银行二部、银行三部、银行四部、非银部、合作部、创新监管部　（共印135份）

联 系 人：付　林　　联系电话：66279134　　校　对：付　林

中国银行业监督管理委员会办公厅　　二〇一〇年四月二十日印发