

中国人民银行文件

银发〔2006〕123号

中国人民银行关于进一步加强银行业 金融机构信息安全保障工作的指导意见

人民银行上海总部,各分行、营业管理部,各省会(首府)城市中心支行,各政策性银行、国有商业银行、股份制商业银行:

为进一步增强银行业金融机构信息安全保障能力,保障国家经济运行安全,维护社会稳定和客户权益,现就“十一五”期间银行业金融机构信息安全保障工作提出以下指导意见:

“十一五”期间,我国银行业金融机构信息安全保障工作的目标是:建立和完善与银行业金融机构信息化发展相适应的信息安全保障体系,满足银行业金融机构业务发展的安全性要求,保证信息系统和相关基础设施功能的正常发挥,有效防范、控制和化解信息技术风险,增强信息系统安全预警、应急处置和灾难恢复能力,保障数据安全,显著提高银行业金融机构业务持续运行保障水平。

“十一五”期间,我国银行业金融机构信息安全保障工作的主要任务是:加强组织领导,健全信息安全管理体制,建立跨部门、跨

行业协调机制；加强信息安全队伍建设，落实岗位职责制，推行信息安全管理持证上岗制度；保证信息安全建设资金的投入，不断完善信息安全基础设施建设；进一步加强信息安全制度和标准规范体系建设；加大信息安全监督检查力度；加快以密码技术应用为基础的网络信任体系建设；加强安全运行监控体系建设；大力开展信息安全风险评估，实施等级保护；加快灾难恢复系统建设，建立和完善信息安全应急响应和信息通报机制；广泛、深入开展信息安全宣传教育活动，增强全员安全意识。

一、建立健全信息安全保障组织体系

建立和完善统一的信息安全领导协调机构。建立由高层行领导负责、相关各部门负责人及内部专家组成的信息安全领导协调机构，理顺关系，增进部门间协同配合、优化资源配置、提高信息安全管理决策的效率和科学性，决策指挥信息安全重大事宜。明确办事机构，统一协调各部门的信息安全保障工作。

建立健全各级信息安全管理机构，分支机构应设立信息安全管理岗位。要充实信息安全管理人員，进一步明确信息安全管理部門、运营部門和应用部門的信息安全管理職責分工，科学制定安全规划，有效组织实施安全策略，加大安全监督检查工作力度，充分发挥纵向衔接、横向协调的组织保障作用。

二、加强信息安全队伍建设，完善用人机制与激励机制

重视和加强信息安全人才建设。选拔素质高、技能强、具有一定管理经验的人才从事信息安全工作。加大人才培养力度，实行信息安全管理岗位任职资格考试制度，根据人民银行组织制定的银行信息安全管理岗位任职资格培训标准和要求，3年内逐步实现持证上岗。

建立良好的用人机制和激励机制。从人才引进、培养的渐进

性和连续性上优化人员结构,形成梯队,重点加强数据中心高端系统运行人员技能的培养力度,不断增强自我运行操作能力与应急能力。合理配置和使用人力资源,人尽其才,合理流动,广开人才来源。建立业绩评价体系,奖惩分明,通过确保重要运行岗位人员的物质待遇等多种激励手段,稳定人才、留住人才。

三、进一步健全标准规范与制度体系,加大信息安全监督检查力度

加快标准规范和制度体系建设等基础工作步伐。统筹规划、突出重点,加紧研究制定和完善当前急需的相关标准规范,配合国家和行业监管部门,重点加强电子支付,信息产品与服务的测评、准入、认证等相关技术法规与标准。密切结合本单位信息化发展实际,借鉴国内外先进经验和做法,加紧建立和完善集中式数据中心运营规范和制度体系,加强信息安全各项规章制度建设,健全岗位责任制度,全面落实“让标准说话,按制度办事”的信息安全管理准则。

建立健全信息安全检查机制,加大监督检查工作力度。依据已确立的技术法规、标准与制度,定期开展信息安全检查工作,确保信息安全保障工作落到实处。建立责任通报制度,对检查中发现的违规行为,按规定处罚相关责任人,对检查中发现的安全问题和隐患,明确责任部门和责任人,限期整改。在开展合规性检查的同时,应综合运用检测工具,明确安全控制目标,加强深度的专项安全检查工作,保证检查工作的针对性、深入性和时效性。

四、建立与技术集约化相适应的集约化生产管理体系

集中模式下的数据中心应及时革新原有生产管理模式,通过体制创新,机制创新,优化资源配置,积累经验,增强技术储备,建立健全与技术集约化相适应的集约化管理体系。要实施流程化管

理,借鉴信息技术基础框架库(ITIL)等国际管理规范,建立标准统一的服务管理流程,严格过程控制和操作规程,完善内控机制。要建立有效的部门间协作机制,严格变更管理,杜绝生产变更的随意性;变更前要进行必要的风险评估,并做好应急准备;有停机风险的变更原则上放在业务低峰期进行。落实岗位责任制,杜绝混岗、代岗和一人多岗现象;要采取主动预防措施,加强日常巡检,定期进行重要设备的深度可用性检查,关键运行设备应从高可用性要求上升到高可靠性要求,合理确定淘汰预期;要实施自动化管理,加强系统及网络的安全审计,实现数据中心各项操作的有效稽核,提升操作控制力,减少人为误操作,实现管理制度的强制执行,集中监控运行状况,实现对数据中心生产运行全局性把握和有效指挥;要从信息系统立项规划伊始,有效提高信息系统安全保障水平,建立信息安全审查制度,在信息系统生命周期关键环节进行安全性专项审查,项目立项未通过安全性审查的不予立项,系统投产运行前未通过安全性测试的不得上线运行,不符合运行条件的系统,运行部门不予接受运行,全面落实信息安全“一票否决制”。

五、以密码技术应用为基础,加快网络信任体系建设

根据国家密码管理相关规定,合理运用密码技术和产品,规范和加强以身份认证、授权管理、跟踪审计等为主要内容的网络信任体系建设。对重要信息的传输、存储要采取一定强度的加密措施,规范和强化密钥管理。通过身份认证、访问控制、内容过滤、信息

预览已结束,完整报告链接和二维码如下:

https://www.yunbaogao.cn/report/index/report?reportId=11_731

