

中国人民银行关于加强 银行数据集中安全工作的指导意见

(2002-9-10)

(注意：本文内容来源于中国人民银行网站，由 ChinaCISSP 摘录整理，仅供参考。摘录者不保证内容的完全正确，关键应用应从正式渠道获得该规范文本。)

银发〔2002〕260号

人民银行各分行、营业管理部、省会(首府)城市中心支行，各政策性银行、国有独资商业银行、股份制商业银行：

为加强对银行数据集中工作的指导，防范相关技术风险和管理风险，现就银行实施数据集中的安全工作提出以下意见：

一、数据集中是我国银行信息化发展的重大举措，对于我国银行实现集约化管理，提高银行的市场适应能力，降低银行经营风险具有重要意义，但对计算机信息系统的可靠性和安全性也提出了更高的要求。各银行必须高度重视对数据集中安全工作的领导，建立健全计算机安全管理组织，落实计算机安全责任制。各银行计算机安全管理委员会(领导小组)主任委员(组长)为数据集中安全工作的第一责任人。

二、加强制度建设，建立与数据集中模式相适应的各项管理制度和内控机制。没有配套管理制度的数据中心和内控机制不完善的业务系统不能投入生产运行。

三、加强数据中心管理人员和技术人员的安全培训，提高全员的安全防范意识。要建立系统管理员、网络管理员、软件开发人员和安全管理人員持证上岗制度；要定期对业务操作人员进行业务操作考核。

四、各银行应高度重视数据集中总体技术设计的合理性和安全性。数据集中体系结构的合理性直接关系到银行信息系统的整体安全，体系结构的选择要有利于降低技术风险和管理风险。总体技术方案必须经过充分的论证。各银行在实施数据集中前要将总体技术方案和论证意见报中国人民银行备案。

五、做好适应数据集中模式的网络建设与改造工作，提高通信网络可用性。网络可靠率(指年无故障运行时间与总运行时间比值)要不低于 99.995%，连续故障时间小于 2 小时。要提高网络的抗攻击能力，严格控制银行网络与国际互联网的连接出口数量，对外联出口要实施严格的安全监控。要充分考慮銀行間以及銀行與清算(結算)機構間的互連、互通和安全要求，加強銀行間數據交換的安全控制，保障銀行與非銀行組織之間的数据交换安全。

六、数据中心是集中模式下银行信息系统技术风险和管理风险最集中的部位。要加强数据中心建设，完善运行安全管理，保障数据中心和业务数据的安全。数据中

心建设要遵循国家有关机房建设和管理的规定,达到国家有关防震、防磁、防洪、防火、防雷、防辐射的安全标准;要落实分区制度,运行、开发、维护、培训、生活和业务操作区域要严格分离。数据中心要建立除本银行和监管银行以外的第三方访问的安全控制制度;要

认真落实双路供电要求,不间断电源要能保障 4 小时供电,要保障备份发电机的有效性。空调、消防系统既要满足运行要求,也要充分考虑工作人员健康和安全撤离的需要;监控和报警系统要达到公安部有关标准。要保障数据处理中心周边环境安全,远离加油站、化工厂等各类危险建筑和重要军事目标。要做好数据中心的主机系统、操作系统、数据库系统的安全设计,充分考虑系统备份或系统冗余。主机系统和数据库系统的操作日志至少保留 6 个月,账务更改记录应保存 3 年。

七、要建立数据强制备份制度,数据完全备份的时间间隔不超过一个工作日,数据完全备份介质的循环周期不能小于 7 天。要定期对备份数据的有效性进行检查,检查时间间隔不超过 30 天,每次抽检数据量不低于 10%。备份数据要实行异地保存。

八、建立强制维护制度和工作人员强制休假制度。强制维护内容包括系统维护、软件维护、数据维护、环境维护。操作人员休假期间,其管理的操作账户应办理移交或注销手续。

九、新建系统投入运营前要做好第三方(业主和开发承建单位之外)测试和验收工作。测试内容至少包括数据一致性测试、系统可用性测试、数据完整性测试、系统综合压力测试和系统健壮性测试等,并建立相应的测试档案,未经第三方测试的新建系统不能通过验收,不得投入生产运行。新建应用系统投入生产运行前应进行不少于 1 个月的模拟运行和不少于 3 个月的试运行。

十、数据集中期间新旧系统的切换工作对银行业务的连续性影响重大。要高度重视数据集中前后新旧系统的切换工作,制定详细的切换方案和应急方案,并在模拟系统试验成功后方可实施,以确保业务系统平稳过渡。系统切换工作要尽量选择对银行客户影响较小的时间段进行。系统切换时间超过一个工作日,需至少提前 5 个工作日发布提示公告,并提供应急服务途径。

十一、为保障银行业务的连续性,确保银行稳健运行,实施数据集中的银行必须建立相应的灾难备份中心。数据集中初期的灾难备份必须能支持信息通过通讯网络从生产中心到备份中心的电子传送。数据集中两年内必须实现备份中心与生产中心相互镜像,支持双向恢复,保证数据一致性。

十二、灾难备份中心的建设可采取自建或联合共建等方式,也可以利用本银行外其他企业(组织)提供的灾难备份服务。向银行提供灾难备份服务的企业(组织)需获得中国人民银行的资质认可。

十三、要制订业务连续性计划,保障业务连续性及其有效性。业务连续性计划应报中国人民银行备案。业务连续性计划要定期演练,每年至少演练一次。

二〇〇二年八月二十六日