中国银行保险监督管理委员会湖北监管局办公室

中国银保监会湖北监管局办公室关于转发《中国银保监会统信部关于银行业信息科技外包风险提示的函》

各银保监局分局、直管组，各银行业金融机构:

现将《中国银保监会统信部关于银行业信息科技外包风险提示的函》（银保监统信函〔2020〕68 号）转发给你们，并提出以下要求，请各机构高度重视，认真组织，一并抓好贯彻落实:

一是排查风险。各机构要对照《中国银监会关于印发银行业金融机构信息科技外包风险监管指引的通知》（银监发〔2013〕5 号）要求，由风险管理部门会同信息科技管理等部门对本单位的信息科技外包服务机构、项目和合同开展一次外包风险专项排查，并针对风险排查结果及时向管理层专题报告。

二是落实整改。各机构要根据外包风险排查结果，有针对性地制定整改方案和整改措施，狠抓落实，确保不留安全隐患，切实规范信息科技外包管理，防范信息科技外包风险，加强信息科技外包服务的监控与评估，杜绝信息科技外包风险事件的发

生。

三是强化管理。各机构要由风险管理部门牵头，“三道防线”共同参与，梳理落实信息科技外包风险管理主体责任，按照通知要求，定期开展重点外包项目（合同）、重点外包活动、重要外包商的风险评估工作。

四是组织培训。各机构要针对通报的案例，并结合本单位自查发现的问题，开展专题研究分析，挖掘风险成因和根源，并在此基础上组织“三道防线”等相关部门和人员开展专题学习，吸取经验教训。

请各银保监分局、直管组将本通知转发至辖内法人银行业金融机构并督促机构做好外包风险排查和整治。

2020年4月20日

（联系人：张　鹏　联系电话：027-85565217）

中国银行保险监督管理委员会统信部

内部　　银保监统信函〔2020〕68号

关于银行业信息科技外包风险提示的函

各银保监局，各政策性银行、大型银行、股份制银行，外资银行，金融资产管理公司办公室：

当前银行业金融机构在银行卡制作、软件开发、应用系统托管等方面大量采用外包模式，在近期风险监测以及银行业金融机构对系统托管外包服务开展的联合核查中发现，部分外包服务存在突出的风险隐患，托管应用系统（银行委托外包服务商进行开发并提供生产运行服务的应用系统）漏洞较多，可能对部分银行业金融机构系统安全运行产生较大影响。为警示风险，加强防范，现将有关风险提示如下。

一、主要风险

（一）制卡外包商通过互联网邮箱明文传输客户敏感信息

某制卡服务外包商使用境外办公邮箱和互联网邮箱，以明文方式向银行机构传输客户敏感信息；该外包商的互联网SFTP服务器存有十余家银行制卡信息、回盘数据、公钥文件等，服务器

缺乏必要的安全控制策略，存在用户弱口令漏洞，可能造成客户信息和制卡数据的批量泄露，给银行带来较大安全风险隐患。

（二）软件开发外包商网络安全管理不善，存在信息批量泄露风险

某软件开发外包商将企业产品的部分底层框架代码、数十家银行系统的项目需求、系统设计、数据库设计、配置文档、项目开发进度报告、测试案例和问题等资料，存放于一台互联网 SVN 服务器，但网络安全管理粗放，可轻易从互联网访问该服务器，数据涉及银行机构数量较多，系统性风险较大。

（三）托管的应用系统高危安全漏洞较多、数据安全风险高

某托管于外包商的互联网应用系统存在 Weblogic 远程命令执行漏洞，可直接获取目标应用服务器中的源代码、配置文件等敏感信息，利用配置文件中存放的数据库账号密码，可获取应用数据库中的客户敏感信息，可攻击托管银行机构的内部网络；某托管于外包商的个人网银系统存在跨站脚本、加密绕过、逻辑绕过等漏洞，可直接仿冒客户并对系统交易进行篡改；多款托管的 APP 存在源代码敏感信息泄露、可暴力破解用户名和密码、密码明文传输、XSS 漏洞等问题。以上漏洞暴露出外包商普遍对应用开发的安全管理不足，安全需求、安全设计重视不够，上线前缺乏安全测试或测试不充分等问题，系统上线后缺乏安全管理，风险隐患较大。

外包商在托管系统的数据提取、存储和传输环节管控不严，

仅通过电话确认提取需求、超范围提取数据、办公终端长期存储银行生产数据、将客户敏感信息发送银行员工私人邮箱等情况多有发生，数据安全风险敞口较大。

（四）托管外包服务安全运行存在风险

部分托管银行信息系统的外包商机房，生产区域、开发区域和互联网区域互联互通现象较为普遍，生产运行管理松散，网络安全管理粗放，托管系统可能成为攻击银行自有系统的跳板。核心路由器和重要的交换机设备单点部署，安全运行风险较高。

（五）托管系统灾备建设不足

多家系统托管外包商基础设施建设严重不足，诸多应用托管系统无灾备，难以保障系统持续服务能力。在已有灾备系统中，外包商托管系统的RTO和RPO，较银行系统的要求和标准差距过大，生产数据备份与恢复验证管理机制不健全，不能满足银行的业务连续性管理要求，存在数据恢复不完整或完全不能恢复的风险。

二、下一步工作要求

各银行业金融机构应进一步强化“服务外包、责任不外包”的风险意识，切实承担起风险管理的主体责任，做好以下工作。

一是针对以上部分风险，我会前期已进行风险处置，并向相关银保监局、银行机构进行了提示。请各银保监局及派出机构，督促辖内银行，建立风险问题台账，做好问题跟踪和督促整改。

二是各银行要举一反三，开展专项排查工作，要将有关风险

和监管要求向本行所有合作的外包服务商进行传导，重点加强外包服务中的数据安全、网络安全、系统安全和业务连续性管理，加大对重点外包商的监控和审计检查力度。

三是各银保监局在本年度信息科技监管评级工作中，要对辖内银行业金融机构外包服务中的数据安全、网络安全和运行安全风险进行重点核查，核查风险问题整改落实情况。对整改不力、外包风险较大的银行业金融机构，降低其评分，并要求其采取整改纠正措施。

请各银保监局将本通知转发至辖内银保监分局及银行业金融机构

银保监会统计信息与风险监测部

2020年4月10日