浅谈邮储银行信息系统风险管理体系构建

刘洪锋

随着业务种类和经营范围的拓展，邮储银行的信息系统日益复杂和庞大，系统风险也随之增加。针对邮储银行的现状，笔者认为应从以下五个方面加强信息系统风险管理，构建信息系统风险管理体系。

（一）信息系统治理

1.健全信息系统风险管理组织架构。邮储银行的信息系统风险管理工作应该包括决策、管理、执行和监督四级机构。邮储银行总行层面应成立科技风险管理委员会，作为决策机构。该委员会应由行长担任主任委员，主管副行长担任副主任委员，办公室、风险管理部、信息系统部、运行管理部等相关部门负责人为成员，其主要职责是负责审议信息系统战略、信息系统重大决策事项，并定期向董事会、行长办公会汇报信息系统风险管理工作；邮储银行总行和各分行的风险管理部负责信息系统风险工作的具体组织和管理工作，属于管理机构；各级信息系统部门负责制度的具体落实，属于执行机构；总行和各分行的内审部负责信息系统风险管理的监督工作，属于监督机构。

2.明确信息系统风险管理三道防线职能。根据银监会《商业银行信息科技风险管理指引》的有关规定，邮储银行信息系统风险管理体系的核心部分应由信息系统管理、信息系统风险管理、信息系统风险审计三道防线构成。

信息系统管理作为信息系统风险管理的第一道防线，是整个信息系统风险管理体系的基础。各级信息系统部门承担该项职能，具体负责落实信息系统风险管理策略以及信息系统管理制度等的各项要求，制定和实施具体的信息系统风险控制措施，传播信息系统风险管理理念，并加强与相关部门的沟通协调以便更好地进行系统应用研发、系统运行、信息安全管理等信息系统管理工作过程中的风险控制。

信息系统风险管理作为信息系统风险管理的第二道防线，是整个信息系统风险管理体系的核心。各级风险管理部门承担该项职能，按照风险评估、风险控制、运行监控、应急恢复这条主线开展具体工作。风险评估是指确定银行的信息系统风险管理需求及可接受的剩余风险；风险控制是指用具体的风险控制措施将风险减少到可接受的程度；运行监控是指对执行的控制措施进行监控跟踪，确保其能够持续地满足银行的风险管理需求，同时对残余风险可能引起的风险事件进行实时的监控；应急恢复是指对已经发生的信息风险事件和突发事件

因此财税[2012]75号文进一步明确，批发、零售纳税人享受免税政策后开具的普通发票不得作为计算抵扣进项税额的凭证。

结合上述案例可以看出，财税[2012]75号文在以下四种情况下没有增加税负。第一，面向终端最终消费者的销售，比如零售给个人，批发给单位食堂。第二，面向非增值税纳税人，例如销售给饭店，其效应同第一种。第三，销售对象是增值税免税的纳税人。比如，从事鲜活肉蛋产品批发、零售的纳税人将免税货物销售给仍然从事部分鲜活肉蛋产品批发、零售的纳税人，不会导致税负增加。第四，销售对象是增值税小规模纳税人，免税政策也会产生价格下降的效应。但如果从事部分鲜活肉蛋产品批发、零售的纳税人销售的下一道环节是增值税一般纳税人且购进货物需要进一步深加工出售的，则免税政策就导致了增值税抵扣链条的中断，可能会导致终端物价的上涨。很多肉制品深加工企业需要从商贸企业采购部分鲜活肉蛋产品，依据财税[2012]75号文规定，由于这些商贸企业免税，肉制品深加工企业购进的这些产品将无法抵扣增值税，其结果必然是加大肉制品深加工成本，导致熟肉制品（终端环节）价格上涨。

财税[2012]75号文执行中还有两个问题值得关注。一是增值税一般纳税人从农业生产者手中收购的农产品能否按13%的扣除率计算进项税抵扣？笔者认为是可以的。首先，财税[2012]75号文只是给予从事部分鲜活肉蛋产品批发、零售的纳税人免税，农业生产者不是批发、零售纳税人，与财税[2012]75号文规定无关。其次，《增值税暂行条例》明确规定，农业生产者销售自产农业产品免征增值税，增值税一般纳税人购进农产品按照农产品收购发票或者销售发票上注明的农产品买价和13%的扣除率计算的进项税额。二是增值税一般纳税人从农业合作社收购农产品的增值税进项税抵扣问题。《财政部 国家税务总局关于农民专业合作社有关税收政策的通知》（财税[2008]81号）对于对农民专业合作社销售本社成员生产的农业产品，视同农业生产者销售自产农业产品给与免征增值税政策。因此，在政策执行中宜将农民专业合作社视同从事农业产生而非批发、零售的纳税人，从而对增值税一般纳税人从农民专业合作社购进的免税农业产品，仍可按13%的扣除率计算抵扣增值税进项税额。 ■

（作者单位：国家税务总局税务干部学院
河南省鹿邑县财政局）

责任编辑 武献杰

以及重大灾难性事故进行快速响应和恢复，减少其对银行业务的负面影响，保证业务的持续性。

信息系统风险审计作为信息系统风险管理的第三道防线，是整个信息系统风险管理体系有效运作的保障，也是邮储银行内部风险控制的重要组成部分。银行内审部门承担该项职能，负责制定信息系统风险审计制度和流程，对信息系统风险管理的效果进行检查和评价，并监督其进行缺陷整改，以确保信息系统风险管理体系的良好运行和持续改进。开展信息系统风险审计，要求银行培养或引进具有专业胜任能力的信息系统风险审计人员。

（二）系统应用研发管理

1. 加强信息系统部门与业务部门的沟通合作，实现风险共担。邮储银行在研发新系统时，应该把业务部门纳入研发小组，全程参与软件需求编写、系统设计、开发测试、验收投产和系统推广等工作，使研发项目真正做到以业务为导向，避免由于系统规划不合理导致的信息孤岛或重复建设，降低项目风险。

2. 建立系统应用研发管理规范，防范系统性设计风险。邮储银行需要制定统一的系统应用研发管理规范，主要内容应包括系统总体设计、功能设计、系统详细设计、程序设计、编码阶段的管理要求、技术结构评审流程和要求。这一规范能够确保应用研发过程的规范性和合理性以及全行技术架构的同一性和科学性，有效防范系统性设计风险。

（三）系统运行管理

邮储银行应该始终坚持“安全第一”的管理理念，从系统运行监控、容量规划、变更管理等方面加强系统运行管理工作，降低系统运行风险。比如，建立操作管理流程，明确具体的操作规范并通过在系统中设置操作日志功能记录系统运行情况，及时跟踪、发现并解决系统运行中的问题；建立系统性能容量分析优化工作机制，制定信息系统容量规划，定期对性能容量进行分析和优化，避免因性能降低或容量不足影响业务服务水平。

（四）信息安全管理

1. 坚持制度防内，构建信息安全内控体系。邮储银行信息系统部门、风险管理部门、业务部门等职能部门应密切合作，共同制定信息安全管理制度，确保全行全员各行其职、各负其责，实现信息安全管理全覆盖。同时，还应通过例行检查和通报等形式，对可能出现的管理漏洞和执行不力等问题查缺补漏、调整优化，严格评估信息安全内控体系的完整性和实施的有效性。

2. 坚持技术防外，优化信息安全技术控制手段。邮储银行应积极优化信息安全技术控制手段，做好各类安全防护工具的使用管理，充分发挥安全防护工具的作用。比如加强网络系统的安全规范及访问控制，明确安全防护边界，保证网络系统的安全运行，减少网络中断或拥塞发生的机率，提高网络系统恢复能力。又如，在信息系统安全设计和安全管理过程中，使用国家及行内相关制度要求的加密技术和加密设备，制定并落实有效的密钥资源管理流程，保护信息及信息系统的安全。

（五）业务持续性管理

1. 加强基础设施建设，维护信息系统运行的连续性与安全性。目前，邮储银行已经按照银监会的要求建成了灾备中心，初步建立了全行统一的灾难恢复组织体系，并且经受了汶川地震和玉树地震等突发事件的考验。为了适应银行业务的快速发展，特别是数据大集中之后，还应继续加大基础设施建设投入，确实保证本地使用数据的安全性，对于一些对安全性、完整性、及时性要求相对较高的交易数据，应当利用实时热备份技术或者采用程序备份方式以满足业务处理等的数据需求；在网络灾备方面，如果网点尚不具备启用主网和辅网双路并行的条件，可以利用多个不同网络供应商为同一区域不同网点提供线路租用的方式，来降低突发故障风险造成的影响。

2. 完善突发事件的应急管理机制，注重应急演练，提高实战能力。目前，邮储银行已按照银监会的要求发布了一系列突发事件应急管理办法，初步建成了应急管理机制。在此基础上，邮储银行一方面应注意加强各类应急预案的定期培训、演练和更新，以提高实战能力；另一方面需要转换工作观念，把灾备工作由信息系统部门工作层面提升至全员参与、人人有责的全行工作层面，以保证灾备体系和业务连续运行方案的有效性和可操作性，切实提高风险防控能力和风险管理水平。■

（作者单位：石家庄邮电职业技术学院）

责任编辑　张璐怡