防范信息系统风险 提升保险监管效能

陈静 郭迪春

保险信息系统存在五大风险

从普查情况来看，保险信息系统存在五大风险问题。

1.基础条件相对简陋，存在系统运行中断风险。从信息系统普查看，各公司信息系统建设基本能够满足安全运行的需要，但还存在一些突出问题。一是机房较为简陋。部分分支机构机房供电系统不完善，没有配备 UPS 或 UPS 功率过小，一旦出现电路故障，系统将无法运行；有些机构机房防火防漏措施不到位，没有监控报警系统，个别甚至没有经过消防部门验收。二是网络较为脆弱。部分机构网络接入管理混乱，存在未经总公司批准、没有任何安全防护措施下私自接入本地，或是使用无线网卡上网的情况；部分三级机构没有备份线路，没有部署防病毒软件。三是维护力量相对不足。大部分省分公司只有 1 名专职 IT 人员，在机构不断扩张、业务不断发展的情况下，系统运维压力不断增大。

2.系统管理比较薄弱，存在经营违规的风险。目前，保险分支机构在系统管理上还存在许多漏洞或不足。一是系统管理权责不清。部分机构的信息技术部门划归办公室或业管部负责，没有明确的岗位职责分工，导致内控执行力减弱，管理出现“两张皮”现象。二是重要功能管理不严。有的机构利用赔案注销权集中注销赔案；少数机构擅自更改重要科目的会计处理方法；部分机构隐瞒应收保费账龄信息，在系统中调节坏账准备金的比例系数；还有的机构利用单证管理系统与核心业务系统没有对接，进行撕单埋单、违规批退等。三是数据管理权限下放存在管理失控风险。数据省级集中的公司，由于总公司对系统日志的审计流于形式，没有实际执行，信息技术人员可能通过技术手段来核销应收保费、违规批单退费、虚列手续费等。

3.系统功能不规范，存在数据失真风险。保险公司分支机构使用的信息系统存在以下问题。一是重要系统对接不规范。普查发现大部分公司财务业务系统对接不及时，制约了财务数据的时效性；部分公司的系统间对接科目没有锁定，允许分支机构以手工凭证方式干预对接结果。二是系统功能不适应。部分公司系统的指标定义在系统中没有及时调整，造成数据无法准确录入。如普查发现一家公司信息系统将农信社代理的小额借款人意外伤害保险保费归属为团险直销，但手续费归属在银邮代理渠道；部分公司系统各指标之间缺少逻辑比对功能，造成相关联的统计口径出现不匹配，如某寿险公司出现过意外险手续费远远大于相应保费的情况。三是新老系统切换脱节。如个别公司分支机构部分险种仍然沿用老系统，且数据存放在本地，无法与总公司系统进行对接，容易滋生违规操作。

4.信息安全保障不到位，存在信息安全风险。常见的问题包括：一是安全保障手段欠缺。保险分支机构层面广泛使用 VPN 连接方式，但没有采用身份认证机制对用户进行安全认证管理；部分机构连接了银行、行业协会等外部网络，但未部署有效的入侵检测设备，使公司业务系统暴露在互联网之上。二是制度执行力不强。部分三级机构没有按照公司统一规定制定相应的系统运维办法，不能严格执行各项信息安全制度，存在内外网混接、IP 地址乱用、不按规定安装防病毒软件、账户口令管理不严等问题。三是安全培训教育不到位。分支机构负责人出于保费规模压力和费用紧张的考虑，应急演练走形式，信息安全教育培训工作几乎空白。

5.信息化监管相对落后，存在监管“逆向选择”风险。相对于国际保险监管，我国保险信息化监管仍然相对滞后：一是监管信息系统共享能力不足。我国虽然已经建立了“三网一库”，积累了一定的信息资源，但现有监管信息系统的发展缺乏统一的规划，系统建设各自为政，技术手段和监管指标缺乏统一标准，无法有效地实现系统的集成和资源的共享。二是对公司信息系统监管乏力。目前相关信息系统监管法律法规不完善，技术手段有限，监管人员的信息化监管经验不足，对信息系统无法进行有效监管。三是现有的监管

信息系统智能分析功能相对有限。在现场检查中主要依靠手工翻阅凭证发现违规线索，非现场监管依靠自行设定一些报表要求保险公司手工报送，进行数据分析。信息不对称，监管决策往往依靠经验，易出现监管“逆向选择”。

保险信息系统风险产生的原因

对系统风险认识和防范不到位。一是有认识、有行动但措施不当。部分公司认识到信息系统存在一定的风险，制定了许多管理办法，召开了多次信息安全会议，但没有监督执行，没有相关考核，风险依然存在。二是有认识、无行动、无措施。部分公司出于保费规模压力和费用紧张的考虑，无暇顾及信息系统的风险管理。三是无认识、无行动、无措施。部分分支机构领导认为数据大集中后，信息系统已经不存在风险了，没有采取任何措施加强系统风险管理。

系统功能不规范使内控存在漏洞。如有的公司业务已覆盖到乡镇，但信息化建设跟不上业务发展的需要，保单赔案等重要资料不能及时审核、及时出单，客服理赔服务不能及时跟上。又如有的公司单证管理系统没有和核心信息系统实时对接，单证管理存在潜在风险。再如有的公司意外险信息没有纳入核心业务系统管理，需要代理机构将保单信息手工录入，使撕单埋单、违规批退等行为形成可能。

内控体系不合理引发数据失真。有些公司对保费等目标进行考核时，不要求分险种分渠道核算、共同费用也不要求进行分摊。分支机构基层工作人员录入保单资料时就可能随意选择险种类别、销售渠道录入，对专属费用、共同费用随意进行分摊，造成财务业务数据失真。此外，对基层工作人员的培训不到位、绩效考核的不科学，也使维护数据真实性工作失去了约束和激励机制。

制度不完善使信息化监管相对滞后。近几年监管部门陆续出台了一些信息化管理制度，但由于对公司信息化监管起步晚、投入不足、缺乏统一的保险机构信息化监管标准，如保险机构信息化工作指引、保险机构信息系统安全管理办法等制度尚未出台，监管制度对实际监管工作的指导仍有所欠缺，监督检查有待加强。

违规成本与收益不对称诱发违规。信息系统违规涉及数量和金额往往较大，而且具有较强的隐蔽性，监管部门和总公司由于技术能力、监管制度、关注重点等方面因素，难以及时准确查处分支机构对信息系统进行的违规操作。违规行为得不到与收益相应罚责，就会使违规者得到额外的丰厚利益。久而久之，就会使利用系统漏洞违规的行为演化成一种惯例或行业“潜规则”。

防范和化解保险信息系统风险的对策

1.做好保险信息化监管的总体规划。制定科学完善的保险信息化监管总体规划，明确今后一段时期信息化监管的发展目标、基本原则、建设项目和经费预算，通盘考虑，有序推进。加强保险信息化监管方面的立法研究，将保险信息化监管纳入保险监管的整体框架。

2.尽快完善信息系统监管制度体系。大力推进保险机构信息系统标准化建设，尽快出台保险机构信息系统监管工作指引，推动保险公司加强内控制度执行力，提高信息系统建设的能力和水平；尽快出台保险机构信息系统安全管理办法、保险信息化内控管理机制等。

3.建立保险信息系统风险评级体系。借鉴国际金融监管经验，结合我国保险行业的特点和现状，从影响信息系统正常运行的物理条件、技术、组织和管理等方面，研究保险信息系统风险评级指标体系，依据

等级保护的思想和适度安全的原则，确定各指标的权重。信息系统风险评级结果可作为分类监管的依据之一。

4.着力提高信息系统风险监管能力。整合行业内部资源，深入分析全行业的信息化建设，广泛吸取其中的成功经验，提高行业的技术基础。鼓励各地开展区域性保险信息化监管探索，在坚持数据大集中的总体原则下，积极鼓励各地开展各项信息化监管试点。开发和完善监管信息系统，改善用户界面，提高系统的易用性和资源共享能力。

5.加大信息系统风险监管检查力度。加强信息监管检查力度，完善长效监管机制，形成定期的现场检查和专项调研。加强对保险机构财务数据、业务数据的真实性监督检查，督促公司完善核心信息系统无缝链接，防范“三假”、撕单埋单、鸳鸯单、虚列应收、违规套费等违规行为，化解公司治理和经营风险。

6.引导行业加大信息化建设要投入。坚持信息系统建设与信息安全建设的协调同步发展，引导公司加大信息建设人力、物力、财力的投入，合理配置好资源，提升保险机构信息系统管理水平。通过信息化建设促进保险电子商务等新型业务发展，深化信息技术应用，降低经营成本，促进经营现代化和管理精细化，提高数据管理和数据挖掘能力，为科学管理决策提供支撑。

7.加强从业人员合规教育与培训。将高管人员、信息技术人员、操作人员的合规教育作为一项长期性、制度性工作来抓，使保险公司从业人员深刻认识到数据真实性、准确性的重要性和数据造假的法律责任，增强依法合规经营意识，打造一支依法合规、素质全面、精通业务的人才队伍。