金融行业信息化风险研究

◎石兴

摘要：金融行业作为国家经济神经中枢，是信息数据密集的行业，高度依赖信息技术，业态环境已被深度改变。金融业在创新发展的同时，也在积聚信息化风险或引发新的风险。本文基于风险的一般性定义，在全面剖析信息化风险源、传导因子、传导载体及其脆弱性、触发事件、作用客体、传导基本路径和事件损失与影响的基础上，提出了最新的信息化风险定义，并对其分类、特征以及与他类风险的关系进行深入研究。对信息化风险的研究为全面加强信息化风险生命周期管理奠定了理论与实践基础。

关键词：信息化；风险；事件；作用；路径；分类；特征

中图分类号：F832　　**文献标识码：**A

一、风险相关定义简介

根据国际标准组织 ISO 发布的 ISO31000：2018《风险管理指南》，风险的标准定义是指不确定性对目标的影响。不确定性是指与事件及其后果，或与可能性的理解或知识相关信息的缺失或不完整的状态；目标包含财务、健康、安全、环境等方面，体现在不同的层次，例如，战略、组织范围、项目、产品和过程等；不确定性对目标带来的偏差可以是积极的，也可以是消极的。风险通常以潜在事件和后果或其组合来描述，也可定义为某一事件的发生导致未来结果出现收益或损失的不确定性。

魏华林（2012）认为风险有两种定义，一种定义强调了风险表现为不确定性，另一种定义则强调风险表现为损失的不确定性。若风险表现为不确定性，说明风险产生的后果可能包括损失、获利或是无损失也无获利，属于广义风险；若表现为损失的不确定性，则风险只能表现出损失，没有从风险中获利的可能性，属于狭义风险。从风险可保性角度讲，引致积极后果的风险是不可保的，故可保风险是指狭义风险。佩费尔（Peffer）认为，风险的不确定性是主观的，而概率是客观的，并认为风险是可测度的客观概率的大小。本文认为，风险是指在致灾因子、风险暴露的价值和抗风险

作者简介：石兴，北京师范大学理学博士，中国海事仲裁委仲裁员，英国特许保险学会高级会员，高级经济师，太平金融运营有限公司。

能力三因素综合作用下，可能造成人身伤亡、经济损失或责任风险等不利事件发生的不确定性。风险量化的手段之一是数学上某种可能性的测度。人们常常用概率论作为可能性测度来量化风险。忽略时间、空间和管理因素的情况下，风险量化用数学公式表示如下：

Risk = f(hazard,value@exposure,resistance)

风险的致灾因子通常可归纳为自然灾害、意外事故和外来原因，更多强调的是突发的、非主观因素的风险源。根据不同的风险定义，有不同角度的理解，也有一定的应用场景，不存在孰错孰对，但综合起来，为信息化风险及其传导机理研究提供了借鉴。

二、信息化风险定义研究

业内专家学者对信息化风险研究不多，其定义散见于相关监管文件之中。《商业银行信息科技风险管理指引》将信息科技风险定义为“信息科技在金融机构运用过程中，由于自然因素、人为因素、技术漏洞和管理缺陷产生的操作、法律和声誉等风险”。《保险机构信息化风险非现场监管报表及评价体系》将信息化风险定义为“信息化工作在合规管理、支持业务创新和业务运营过程中，由于管理流程及资源缺失或不足、自然因素、人为因素和技术漏洞产生的操作风险、法律风险和声誉风险等”。按照国际信息系统审计和控制协会（ISACA）的定义，信息化风险指由于使用或依赖信息、通信技术、运营技术、网络或物联网技术、电子数据和数字化通信手段等引发的业务或企业目标方面的损失、损坏、业务中断等不利影响的不确定性。

本文认为，为准确定义信息化风险，有必要对信息化风险的要素和传导机理进行全面剖析。

（一）风险源

风险源又称风险因子，包括以下一个或多个因素的共同作用：一是信息技术自身风险漏洞，例如，资产设备老化、新技术不稳定、资产设备性能缺陷和计算机病毒等。二是内部人员、外包人员技术专业技能认知缺陷导致的操作错误、技术漏洞、资产设备性能缺陷、管理不当等非故意行为以及故意行为。三是信息化治理与管理不善，包括信息化规划、立项决策、信息化采购及其决策、内部运行管理、信息安全管理等方面的过失。四是意外事故，例如，火灾、电力供应中断等。五是有组织的外部第三方无意或故意攻击。六是外部运行环境突变风险，例如，发生恐怖活动、自然灾害等。其中，前三项可以归类于内部因素，后三项大多为外部因素。

（二）传导因子

不是所有风险因子都有传导机理，例如，自然灾害、火灾等就没有传导机理。具有传导机理的传导因子也不一定就是致灾因子。如果该传导因子没有产生不利的影响或损失，它也仅仅是传导因子。只有传导因子利用传导载体（信息技术环境）的脆弱性，通过一定的传导机理，产生不利影响或损失，才是致灾因子。传导因子可做如下分类。

第一，外部人员攻击，指外部的黑客、牟利人员和恶意组织机构等第三方利用勒索软件、渗透测试工具、DDOS 攻击工具、网络钓鱼工具、社交工程等手段，突破信息技术环境的安全防护控制，在获得系统高级权限后，对应用系统、管理工具、基础架构、基础设施等实施破坏，窃取机密信息，通过敲诈勒索获利。还有一些外部人员利用信息系统漏洞，例如，身份校验机制的不完善等，冒充客户交易获利。

第二，内部人员恶意攻击，指内部人员利用可直接或间接接触机密信息的职务之便，在利益驱使下，利用信息技术环境漏洞，绕过信息技术内部控制手段，窃取机密信息，进行业务欺诈并从中获利。

第三，内部员工不当操作，此类不当操作是由于内部员工缺少必要的专业知识、风险意识不到位或者误操作所致，并无获利动机；而信息系统未设置正确的检测或恢复机制，内控流程复核和校验机制的可能缺失，将导致或增加操作差错、账务错误、数据丢失等损失发生的风险。这里也包括外包人员的不当操作。

第四，内部管理风险，主要表现为技术环境管理不善导致信息技术环境自身故障，包括设备老化、

技术缺陷或系统自身代码错误等问题。此类问题在日常维保、巡检等工作中难以被发现，一旦触发会导致信息系统服务不可用、功能失效等后果。

第五，技术自身缺陷，指因对专业技术的认知受限、技术固有等原因，信息技术存在一些难以避免的缺陷、漏洞和后门等风险。

（三）传导载体及其脆弱性

信息化风险的传导载体是内部信息技术或通过其传导的外部信息技术。信息化风险通常耦合于系统的建设、测试、上线、运行管理等操作环节之中，包括应用系统、数据架构、基础架构和基础设施，以及贯穿其中的信息技术管理活动等。

具体来看，应用系统方面的脆弱性包括系统输入控制缺陷、边界控制缺陷、处理控制缺陷、输出控制缺陷、授权控制缺陷、日志控制缺陷和系统设置缺陷等。数据架构方面的脆弱性包括数据质量缺陷和架构设计缺陷等。基础架构方面的脆弱性包括关键设备缺少、容量不足，虚拟化配置缺陷，网络分区不当，主、备中心应用和数据不一致等。管理流程方面的脆弱性主要包括治理架构不完整、职责分工不完善、制度设计不规范、需求设计和业务流程相脱节、版本管理混乱、开发和运维权限不分离、开发环境和生产环境不隔离、网络安全级别低、病毒库更新不及时、外包人员权限管理不当、外包商集中度过高、灾难恢复应急预案不完整、应急演练不全面等。

上述载体的种类及其脆弱性的深度和广度决定了载体被风险源所作用的可能性和严重性。一般而言，脆弱性越大，发生风险事件的概率就越高。例如，应用系统之间的耦合度决定了某一应用系统发生问题时对其他应用系统的影响程度；软件代码的安全性不足，可能更易受到内外部攻击；基础设施的使用年限越长，故障发生的概率就越大；未对系统账号权限的开启、变更与撤销进行有效审批，则内外部攻击者容易获取离职人员的用户权限进行访问和数据盗用等。

（四）作用的客体

信息化风险通过传导载体，作用于或合力作用于一个组织的分析决策、交易运营、信息安全、内部控制、基础设施和设备设施等承灾体（客体）。

（五）触发事件

不是所有信息化风险都会造成信息化故障触发事件；只有达到一定触发条件，使信息技术环境发生异常，信息安全受到严重威胁，不能提供信息化服务，并造成损失的情形，才成为信息化触发事件。信息化风险的要素与定义决定了触发事件有多种分类，从风险生成角度来看，可以分为以下五类。

一是内部事件，包括信息化管理不当、新技术选择与应用风险、专业人员技术能力所限和误操作、决策失误、员工可能的蓄意报复等。例如，因管理不当，导致建筑物安全性受到影响，基础设施与设备老化，意外事故导致的信息化事件、火灾或断水引起消防失效等意外事故。二是外部事件，包括黑客和第三方等故意行为、合作伙伴误操作、敌对国家的战争行为、竞争对手的有组织行为等。三是技术事件，包括技术性能缺陷、技术漏洞等，例如，货币政策、利诱产品上线销售等内外部政策传导导致信息系统瞬间容量不足，系统瘫痪或中断。四是运行环境事件，例如，停电、重大疫情与卫生医疗事件等。五是自然灾害事件，典型的有地震、台风和洪水等。

常见的信息化风险触发事件有网络攻击事件、信息破坏事件、信息内容安全事件、网络故障事件、服务器故障事件、软件系统故障事件、灾难性事件和其他事件等。触发事件根据响应等级可分为集团事件、子公司管理层响应的事件，有的触发事件不引起管理层的响应。

（六）传导的基本路径

根据前述的信息化风险传导载体及其脆弱性，信息化风险传导的基本路径有四个方面。

第一，应用系统，传导路径为功能损毁（服务于业务流程的各类应用系统功能损毁，流程环节中断）、功能失效（体现在系统控制功能，如复核、校验等的失效）和功能篡改（如客户评级标准调整、关键计算逻辑更改）等。

第二，数据资源，传导路径体现在数据损毁

（如数据不可读写、备份数据损坏等）、数据丢失（机密数据被窃取、数据库拖库[①]等）和数据篡改（数据格式及内容被篡改，非授权增删数据）等。

第三，基础设施，传导路径通常为实体破坏（机柜、服务器、存储设备等被破坏导致不能正常工作，甚至生产 / 灾备机房服务中断等）和功能失效（空调控温失效、UPS 监控失效、动环监测失灵等）。其风险源可能来自外部，也可能来自内部。

第四，管理流程，传导路径体现为能力难以胜任、流程效率低下、流程失效等，也可能会对业务流程带来不良影响。

信息化风险作用点及其程度不同，带来的影响差异较大。在基础设施、管理流程等领域传导作用，其影响可能是普遍性的，会带来整个数据中心的服务中断；信息技术开发运维团队的工作失效，可能会影响应用系统、数据架构的稳定性和安全性。

（七）影响与损失

信息化风险影响是指所发生的信息化风险触发事件通过相关流程或活动，给战略规划、经营管理目标、交易达成、运营管理、营业收入、品牌声誉以及法律责任等方面带来直接和间接的损失、不良影响或导致经营风险的扩大等。

1. 损失类型

一是业务欺诈方面，主要是入侵者采用虚构或者隐瞒信息等方法，骗取金融机构的信任，非法获利的情况。业务欺诈的表现形式有盗窃、欺诈、安全破坏等。二是营业收入方面，信息化风险事件会导致金融机构无法为客户提供服务，例如，信息系统中断、外部服务中断等导致业务中断，无法正常营业。三是经营利润方面，主要表现形式是相关容错风险所导致的风险模型、精算模型、资信或信用模型等方面出错，进而引入高风险客户或标的，造成业务质量不高，影响经营利润；此外，还可能导致准备金计提不准，影响财务真实性等。四是投资利润方面，金融机构都会持有以价值形态存在的资产，例如，因容错风险导致信贷模型、投资回报模型等发生差错，进而引入高风险客户导致信贷损失，乃至发生资产全损、减值或丢失、所有者权益丧失等，直接影响资产质量，影响投资利润。五是资产损坏方面，自然灾害或意外事故的发生会对信息化资产，包括软硬件、基础设施和设备等造成有形或无形的损失和毁坏。

2. 影响分析

评估信息化风险的影响需要从金融机构自负盈亏的企业性质以及其所承担的社会责任等角度出发。对国家整体利益而言，金融行业的相关数据资源关系到国计民生，如果泄露，会对国家、行业产生重大安全影响。对金融机构而言，信息化风险直接影响其经营管理、营业收入，产生重大品牌声誉风险；不严格遵守法规条例、监管规定，还会招致行政处罚、监管罚款、监管评级下调、法律赔偿、额外费用、民事问责乃至刑事问责。对员工而言，对信息化风险事件的处置、灾难恢复，可能会导致长时间加班，影响身心健康。对客户而言，信息化风险会导致运行质量和效率的下降，客户体验会受到明显影响，客户交易意愿及其选择因此可能发生改变；敏感数据泄露有可能会对客户产生人身安全等方面的影响，增加其时间成本，也可能包括金融资产损失。对合作伙伴而言，以保险业为例，信息化风险事件会对专兼职代理、经纪人、公估人等合作伙伴产生影响，主要表现在合作伙伴的业务选择、数据泄露等，进而导致客户流失，收入和利润减少。

据此，本文认为，普适性的信息化风险定义如下：一个组织在营运管理过程中，使用或依赖互联互通等信息科技时，因管理不善、专业技术能力所限、内外部故意和 / 或无意攻击源、自然灾害、意外事故、外部运营环境等因素所导致的技术缺陷或漏洞、设施与设备毁坏、管理与决策失误等，可能会引发与原定目标的不利偏差、不确定性和不安全性等。

① 拖库本来是数据库领域的术语，指从数据库中导出数据。现被用来指网站遭到入侵后，黑客窃取其数据库文件。拖库的主要防护手段是数据库加密。

三、信息化风险分类

前述的信息化风险源和触发事件涉及信息化风险的分类。事实上，有很多维度的分类，例如，作用对象、作用载体、攻击来源、攻击类型、管理功能、管理内容、管理目标等。这些分类方式都对信息化风险管理有一定的指导作用，但还存在一些问题，例如，大多分类方式侧重于从信息化风险的某一线索进行分类，并未统揽全局，其影响分析也难以将技术缺陷与后果（损失）合理挂钩，风险敏感度不高，对信息化风险管理的前瞻性和预测性不足，不利于风险管理及其流程的落实等。此外，风险分类之间存在互相交叉、较难清晰划分等问题。本文按照发生情景维度分类，将信息化风险分为以下三种。

第一，容灾风险。容灾风险是指由于信息科技基础设施、基础架构和/或其备份资源所提供的服务中断而带来的风险，主要包括楼宇级容灾风险和城市级容灾风险。容灾风险的成因包括地震、火灾、洪水、雷电等自然灾害，战争和恐怖袭击，以及断电、网络中断、备份资源故障等。

第二，容错风险。容错风险是指因信息化管理或者信息技术软硬件存在漏洞而出现的非预期故障风险，包括软件故障、硬件故障、人为操作失误和人为恶意破坏等。容错风险与容灾风险的最大区别在于，容错可以通过站点内的软硬件冗余、高可用设计、备份恢复、故障修复等措施来实现，而容灾必须通过灾备环境接管生产环境提供服务来实现。

第三，安全风险。信息安全风险指的是在信息化建设中，各类应用系统及其赖以运行的基础网络所处理的数据信息，由于其可能存在的软硬件缺陷、系统集成缺陷等，以及信息安全管理中潜在的薄弱环节，而导致的信息资产的机密性、可用性和完整性被破坏并带来损失的风险。信息安全风险内部也有较多分类，例如，按保护对象可分为数据安全风险和资产安全风险，按安全破坏的表现形式可分为本体安全风险和路径安全风险，按信息系统环境可分为物理环境安全风险、网络边界安全风险和人员安全风险。

以上分类是将技术风险与功能管理相结合的一种综合分类，与前述各种信息化风险分类既有联系又有区别。其主要的实践意义在于，一是厘清了风险来源、风险载体及其脆弱性、管理流程等元素之间的关系，使风险的识别不会遗漏，也互不重复；二是为风险的传导路径分析奠定了较好的逻辑分析基础；三是根据致灾因子，前文提及的各种分类项下的细分风险都能归于这一分类项下的容错风险、容灾风险或安全风险，且不存在分类之间的相互交叉；四是便于信息化风险管理及其流程的执行。因此，这一划分较为科学合理。当然这一分类的颗粒度较粗，需要根据致灾因子或近因原则[①]，准确细分信息化风险，以便在三大类项下合理归类。

四、信息化风险的主要特征

信息化风险特征要结合风险因子、传导载体、作用对象、风险类型和影响后果等因素来分析。金融行业信息化风险一般具有以下特点。

第一，正态分布特征明显。总体而言，信息化风险的特征呈正态分布，绝大多数信息化风险事件是常态化、可以承受的风险；小部分风险天天发生低频高损，随时随地修复；小部分事件则会使金融机构产生重大直接损失，乃至第三方法律责任、品牌信誉等间接损失。

第二，影响面广。信息化故障，尤其是信息系统失效会广泛影响到用户，网络环境下的信息系统会影响到更大范围的分支机构和用户；即使局部系统失效，影响面也会较大，因为金融行业涉及千家万户，影响面会较快扩大；如果是跨境金融业务，则有可能产生国际性影响。信息化风险具有无疆特征。

第三，隐蔽性强。对于一般的操作者和使用者而言，信息系统是一个“技术黑箱”，很多信息化风险在发生前是隐含在应用界面之下难以被发现的。一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、

① 对于单一原因造成的损失，单一原因即为近因；对于多种原因造成的损失，持续地起决定或有效作用的原因为近因。

干了什么不知道”，长期“潜伏”在里面。

第四，专业性强。信息化风险的要素及其定义说明信息化风险专业性较强。信息化风险的产生和防范都需要专业人士实施，这使得具体风险的预警、监测、控制和故障的解决等需要专业技术人员来实现。

第五，非标准性。信息化风险表现形式复杂多样，且分布于几乎所有的信息化工作、系统运行和业务流程之中。查找信息技术故障原因的程序和方法可能大同小异，但修复则针对性很强，都是一对一的，非标准性风险特征十分明显。

第六，成因复杂。信息化风险定义及其分类研究说明信息化风险的成因和传导路径较为复杂，既有信息技术自身的风险，也有人为的管理与技术能力不足风险，更有内部或外部攻击风险。尤其是内外部攻击者可通过多种手段，遍历多条破坏路径，获得信息技术环境的最高管理权限，窃取机密敏感信息。基于安全管理的“木桶原理”，只要任何一条破坏路径被打通，其他所有的安全管理手段都形同虚设。

第七，普遍绝对性。信息化已经渗透到社会的各个组织、各个行业，金融业对信息化的依赖性无处不在。信息化风险的定义说明只要信息技术作用于一个组织的营运管理过程就有可能产生信息化风险，既有信息技术内生的，也有内外部疏忽和攻击所致的，更有在网络环境下传导感染的。由于谋利性或恶意攻击是不会停止的，所以信息化风险会不断产生，具有普遍存在的绝对性，不可能杜绝。

第八，相互关联的动态性。数字化时代，信息安全可能牵一发而动全身，会影响到与其共享或关联的网信系统，影响业务运营与交易，因此，信息安全风险呈高度关联、相互依赖的特征，而并非孤立或封闭的。金融集团内相关信息技术共享，增加了交叉感染的可能性；同时，网络安全威胁的来源和攻击手段是不断变化的，不是静态的。

第九，“非工作”时空风险。传统的金融行业作业模式通常在工作时间、工作场所内完成。在数字化生态环境下，作业模式从 5 × 8 小时的工作时间，更多地转向非工作时间，升级为 7 × 24 小时不间断运营，特别是在节假日和重大活动期间，金融服务需求更加活跃，线上服务需求较线下现场服务的要求更加强烈。“非工作”时空风险表现在三个方面：一是服务资源配置不到位风险；二是线上服务稳定性风险；三是现场服务配套响应能力风险。

第十，攻击风险的低成本性。信息化风险的攻防双方处于完全不对称的地位，处于暗处的攻击可以用少量的人力、低廉的工具，长时间偷窥观察，以较低的支出攻破守方的防线。敏感信息、竞争信息等能给攻方带来不义收入的对象，往往成为其目标。国家政治、军事、经济和社会安全往往成为竞争性对手、竞争性国家和敌对组织的黑客攻击的目标。

综上，对比“风险”的定义，信息化风险有几点特殊之处。一是信息化风险源较为复杂多样；二是信息化风险源更多的是内外部主观人为因素，而风险以客观原因或自然灾害因素居多；三是信息化风险属于狭义风险，一般都会导致不利情景的发生，至多是发生了风险，但没有达到触发损失的条件；四是通过信息技术媒介作用于一个组织的经营管理活动，才会产生信息化风险，虽然没有轨迹，但有传导载体，有一定的形成机理，这也是信息化故障处理的基础；五是影响和结果较为复杂，计量难度显著增加；六是作用的客体主要是无形的经营管理活动，而非有形的固定资产或流动资产；七是专业性较强，非专业人士对信息化风险管理与处置往往束手无策。

五、信息化风险与他类风险

本文所称他类风险特指信用风险、市场风险、流动性风险、保险风险、账户利率风险、声誉风险、战略风险和操作风险等。信息化风险与上述风险之间有紧密的关联性。

（一）成因相互交织

在信息技术应用过程中一旦发生信息化风险事件，就会成为触发他类风险的因素。例如，由于信用风险模型设计和实施过程中存在版本错误或者代

表1 信息化风险与操作风险比较表

比较维度	操作风险	信息化风险
风险事件	内外部欺诈，就业政策和工作场所安全，客户、产品和业务活动，实物资产损坏，业务中断和系统异常，执行、交付或交割及流程管理等	容错风险、容灾风险和安全风险事件都是操作风险风险事件的一部分
风险因子	内部：人员、流程、信息系统等 外部：第三方、自然条件、技术、法律法规、社会舆论等	内部：人员、流程、信息系统等 外部：第三方、自然条件、技术、法律法规、社会舆论等
传导载体	业务和系统流程	业务和系统流程 信息技术环境 信息技术管理流程
损失后果	经济损失、非经济损失	经济损失、非经济损失
计量方法	有统一标准的计量方法，例如，基本指标法、标准法、高级计量法	业内有相关的计量方法，但在探索之中，尚未经监管部门认可

资料来源：作者根据公开资料整理

码缺陷，造成高风险客户引入带来信用违约风险；又如，由于信息系统故障导致运营中断，造成客户赔付延时引起投诉，带来法律和声誉风险；再如，由于系统之间接口传输数据不准确造成净值计算错误带来市场风险；等等。

与此相反，也有少部分风险是信息化风险的成因，例如，战略风险。当集团的发展战略没有达成或与目标产生较大偏差，信息化规划预算会与实际产生偏离，导致信息化风险的产生，乃至造成严重的决策浪费。此外，某些操作风险事件也是信息化风险的成因。例如，人为错误、工作程序有误、内部控制不当等都是信息化风险的主要成因。因此，信息化风险与他类风险有时互为因果。

（二）信息化风险与操作风险的关系

根据《巴塞尔新资本协议》，操作风险的基本定义是由于不完善或者有问题的内部程序、人员及系统或外部事件所造成损失的风险，表现为七种形式：内部欺诈、外部欺诈、雇佣合同及工作状况产生的风险事件、客户与产品及商业银行引起的风险事件、有形资产损失、经营中断和信息系统出错、涉及执行与交割及交易过程管理的风险事件。在这一定义下，操作风险可以被认为是一家金融机构所面临的所有风险中，除去信用风险、市场风险、战略风险及声誉风险等之外的其他风险的总和。所以信息化风险属于操作风险的范畴。表 1 列示了操作风险和信息化风险的相似性与不同点。

由表 1 可见，信息化风险与操作风险有较高的相似性。对于其区别，以下展开进一步分析。

第一，在管理工具方面，操作风险管理主要依托 KRI（关键风险指标）、RCSA（风险与控制自评估）和 LDC（损失数据库）三类管理工具进行风险识别和评估，使用关键风险指标对风险水平进行持续监测，使用损失数据库对风险损失进行持续跟踪和分析，结合这些工具的输出进行风险计量。信息化风险管理同样可以借鉴这三类工具进行风险识别、评估、监测和计量，但由于信息化风险的技术特征及其与业务流程的高度耦合性，需要在每类业务流程形成普适性的业务规范和标准化管理基础上才能实现其应用。

第二，在管理方法方面，操作风险管理以梳理业务流程为基础，分析流程中可能面临的风险点，进行固有风险评估，识别对应内部控制措施的有效性，进而判断剩余风险是否在可接受的范围之内。信息化风险管理既要关注业务流程中的信息科技风险，也要将信息化治理、信息化流程所存在的控制缺陷等纳入统一识别和评估的范畴，并充分评估其对业务运营和管理活动的影响，因此，管理的复杂性明显高于操作风险。

第三，在损失计量方面，操作风险可以将损失与业务条线的资金敞口、收入、利润等因素建立直接的关系，一般可用货币来计量。而信息化风险会产生修复成本、人工成本、业务减少、声誉及合规等多方面的损失，部分可以用货币计量，部分则不行，计量也较为复杂，需要进一步探索计量方法。

信息化风险虽然属于操作风险，但从其重要性角度讲，几乎占操作风险管理的全部。因为信息化风险与合规渗透于金融机构经营管理的方方面面，贯穿于全面风险管理的始终。

（三）信息化风险计量方法较他类风险复杂

信用风险、市场风险、流动性风险、账户利率风险等损失计量均有较为成熟的模型和方法。例如，信用风险预期损失为违约概率、违约损失率及违约风险暴露三者相乘得到，市场风险以风险价值（Value at Risk）进行计量。信息化风险的计量与其完全不同，但可借鉴利用操作风险相关计量模型和工具。由于信息化风险通常需要通过传导造成损失，而且损失可能是多方面的，在分析和计量上均有一定的难度。以业务运营系统中断为例，既需要考虑受影响的软硬件设备恢复成本、执行手工替代程序的成本，也要计算被影响客户的经济和非经济损失，更要考虑信息化故障所带来的客户流失、业务收入减少等损失，还可能还涉及监管处罚相关的损失等。

六、结语

由于网络的开放性和计算机系统的不完善性带来了许多病毒、漏洞，乃至被人趁隙攻击，信息化风险管理面临严峻的挑战。

金融行业是信息数据密集的行业，高度依赖信息技术，业态环境已被深度改变；信息化已经成为日常运营的操作平台，管理决策的重要支持，创新发展的重要载体，获客能力的先发优势和风险管理的智能工具。如因信息化风险事件导致系统中断，会局部影响或系统性严重影响其业务连续性运营、经营管理和市场竞争能力，进而可能会影响客户的交易意愿选择与个人隐私，乃至国计民生的数据安全和社会安全稳定。

对信息化风险的研究是信息化风险管理、信息安全管理的基础，只有厘清了信息化风险本义，完整了解其传导机理、分类与特征，才能开展全面信息化风险生命周期管理，及时采取防范和处置措施，降低信息化风险故障概率，妥善解决信息化故障事件，确保信息系统安全平稳运行，这对防范化解金融机构重大风险具有重要意义。

参考文献：

[1] 巴塞尔银行监管委员会、国际证监会组织和国际保险监督官组织联合论坛．金融集团监管原则 [S].2012

[2] 国际标准化委员会．风险管理指南 [S].2018

[3] 国际信息系统审计和控制协会（ISACA）．信息及相关技术控制目标 [R].2013

[4] 石兴．巨灾风险可保性与巨灾保险研究 [M]. 北京：中国金融出版社，2010

[5] 魏华林、林宝清．保险学原理 [M]. 北京：高等教育出版社，2012

[6] 阎庆民等．银行业金融机构信息科技风险监管研究 [M]. 北京：中国金融出版社，2013

[7] 中国银行业监督管理委员会．商业银行信息科技风险管理指引 [S].2009

（责任编辑：冯天真）