

研究报告

2020 年第 62 期

2020.12.25

执笔人：王可 陈垣桥

邮箱：

wangke.csjr@icbc.com.cn

yuanqiao.chen@icbc.com.cn

美国银行业科技风险管理中行业规范的应用

摘要：

- 大量新兴技术与银行业务的深度融合对银行的科技风险管理提出了新的挑战。美国的信息科技标准组织在长期的实践中制定了大量专业、前沿和全面的行业标准和规范性文件，成为科技风险监管中重要的参考依据。行业规范与法律法规相结合的监管模式有助于强化银行的科技风险管理，维护金融系统的稳定运行。

关键词：

- 科技风险 标准组织 行业规范 金融稳定

重要声明：本报告中的原始数据来源于官方统计机构和市场研究机构已公开的资料，但不保证所载信息的准确性和完整性。本报告不代表研究人员所在机构的观点和意见，不构成对阅读者的任何投资建议。本报告（含标识和宣传语）的版权为中国工商银行现代金融研究院所有，仅供内部参阅，未经作者书面许可，任何机构和个人不得以任何形式翻版、复制、刊登、上网、引用或向其他人分发。

随着移动互联网、大数据、云计算和人工智能等新兴技术与商业银行业务创新深度融合，商业银行的数字化转型深入推进，信息科技风险的管理成为全球银行业面临的重要课题。与初创型金融企业和互联网金融公司不同，作为整个金融系统中的核心，商业银行的稳健性直接影响到整个社会金融经济体系的稳定运行。因此，商业银行在信息科技应用领域具有更低的风险偏好，需要更为规范和严格的管理措施。美国的信息科技起步较早，为规范信息科技的应用和运行，ISACA和NIST等标准组织在长期的实践中制定了大量的行业标准和规范性文件，成为商业银行科技风险管理的重要依据。本文总结了美国银行业在信息科技风险管理中所涉及的标准组织制定的规范性文件特征和应用方式，为我国商业银行完善信息科技的管理体系提供借鉴。

一、商业银行科技风险的特征

信息科技通过与行业场景深度融合，推动商业银行加速向数字化、智能化、生态化的发展，而信息科技的应用也给商业银行带来了新的风险和挑战。与传统的信用风险、操作风险和市场风险相比，科技风险具有以下显著的特征：首先，银行在应用信息科技的过程中，涉及计算机、通讯、系统和软件开发等大量的底层技术，也会使用大量的外部科技供应商提供的产品和服务，因此科技风险具有较高的复杂性；其次，目前全球主要经济体的商业银行基本实现了数字化，各项业务的正常运行均建立在信息技术的基础上，决定了科技风险将



会直接影响到各业务条线，对银行业务的影响具有综合性；第三，科技风险发生时，既有可能导致银行的核心业务中断遭受巨大损失，也有可能仅仅造成移动端 APP 短暂的登录时间延长，风险损失极为分散。巴塞尔协议 III 中将科技风险纳入操作风险的管理框架，由于科技风险的特征与传统的操作风险存在较大差异，近年来巴塞尔委员会开始对科技风险制定针对性的监管要求。

二、我国银行科技风险管理框架

当前我国商业银行进行科技风险管理的核心指导文件是 2009 年颁布的《商业银行信息科技风险管理指引》（下文中简称《指引》）。

《指引》共分为十一个章节，对商业银行的信息科技治理、风险管理、信息安全、信息系统开发测试和维护、信息科技运行、业务连续性外包和内外部审计等方面进行了规范。《指引》与美国 FFIEC 制定的 IT 检查手册和欧洲监管文件中的要求基本保持一致，标志着我国银行业信息科技风险管理正向国际规范靠拢。此外，银行在信息科技应用过程中还需要遵守涉及不同领域的法律规范，主要包括《电子银行业务管理办法》《银行业金融机构重要信息系统投产及变更管理办法》《商业银行内部控制指引》《网上银行系统信息安全通用规范》等。

三、美国银行业科技风险管理标准组织与行业规范

美国信息科技产业的起步较早，由于科技风险的管理专业性要求，在长期的信息科技应用和管理过程中，美国成立了专门的研究机

构和行业协会等标准组织，集中讨论和制定科技管理的原则、流程等规范。随着对信息科技的依赖程度不断加深，商业银行也被纳入上述规范的管理对象，并以此为标准完善科技风险管理体系。美国银行业科技风险管理中涉及的主要标准组织和行业规范性文件主要包括：

（一）ISACA 的 COBIT 框架

COBIT (Control Objectives for Information and related Technology, 信息及相关技术的控制目标) 是 ISACA (Information Systems Audit and Control Association, 信息系统审计和控制协会) 指定的面向过程的信息系统审计和评价的标准框架。ISACA 是全球范围内信息科技治理、风险管理以及标准制定的权威组织，目前会员接近 10 万人。在 ISACA 的主导下，COBIT 整合了包括 ISO、ITIL、TOGAF 等多个框架和标准，主要关注信息科技的价值和风险管理，同时兼顾了信息安全和商业模式，是全球公认的、权威的信息技术管理和控制的标准。

（二）NIST 的网络安全框架

NIST (National Institute of Standards and Technology, 美国国家标准与技术研究院) 是美国商务部下属的研究机构，主要从事纳米技术、工程学、信息技术、中子和材料学等方面的研究。NIST 具有雄厚的科研实力，在多个领域制定了计量准则和技术标准，也是美国重要的产品质量标准的制定者。2014 年，NIST 在美国总统行政



命令的要求下制订了《减少关键基础设施网络风险的框架》，用于保护商业机密、隐私和公民自由，增强国家关键基础设施的安全性和可靠性，维持一个鼓励高效、创新和经济繁荣的网络环境，具有明确的国家利益和安全导向。目前，该框架已经被广泛应用于美国的通信、计算机等关键基础设施领域的安全风险管控。

（三）FAIR 风险分析框架

如何对风险因素及其影响进行归类和分析是信息科技风险管理中的一大难点，FAIR (Factor Analysis of Information Risk, 信息风险因素分析)通过解构影响信息风险发生的频率和预期损失的因素为测度信息科技风险提供了一个量化分析框架，在 ISO/IEC 27000 系列等信息安全管理规范中得到了广泛的应用。FAIR 主要关注网络安全风险可能导致的企业数据泄露、声誉损失等内容。

四、标准组织和行业规范的优势与应用

与传统的银行监管法律法规相比，由研究机构 and 行业组织制定的标准文件和行业规范具有以下显著的特征：第一是专业性，研究机构 and 行业组织中有大量的信息科技相关从业人员，在信息科技的低层技术、应用场景和风险特征等领域具备大量的知识储备和经验积累，能够在复杂的业务链条中定位关键的风险因素；第二是前沿性，信息科技的高速发展对风险管理造成了巨大的挑战，研究人员和从业者是对技术最为敏感的人群，能够及时将技术的更新和应用带来的潜在风险

纳入管理框架,相比于法律法规繁琐的制定和修改流程,NIST 于 2014 年制定了网络安全框架,COBIT 标准已经更新到 2019 年版本,FAIR 等框架也在随着技术进步不断更新,充分反映了行业规范的前沿性;第三是全面性,标准组织指定的行业规范性文件覆盖了信息科技应用和风险管理的各个环节,不仅规定了信息科技的治理机制、管理层责任、审计方式等内容,还提供了大量的低层技术应用标准、风险评估方法、数据管理方式等领域的操作规范,能够为商业银行提供全面、可执行的信息科技风险管理框架。

目前,美国在银行业的科技风险监管中,广泛使用了各标准组织制定的规范性文件。联邦金融机构监察委员会(Federal Financial Institutions Examination Council, FFIEC¹)制定的 IT 检查手册(IT Exam Handbook)是美国信息科技风险监管的核心文件,在制定过程中参考了大量 COBIT 的标准,FFIEC 还会追踪技术进步和行业规范不断更新手册中的内容。为了应对日趋复杂的网络威胁,FFIEC 还结合了 NIST 的网络安全标准和 FAIR 的风险分析框架制订了专门的网络安全评估工具 CAT (Cybersecurity Assessment Tool),为金融机构评估网络安全的稳健性提供了一个可重复、可测度的方法,由 OCC (Office of Comptroller of Currency, 货币监理署)负责监督和检查银行的具体执行情况。此外,COBIT 也是银行的内外部审计中

¹ FFIEC 由美联储(FRB),联邦存款保险公司(FDIC),联邦信用管理委员会(NCUA),货币监管局(OCC),以及联邦消费者金融保护局(CFPB)等成员组成。



制定信息科技领域的审计标准的核心参考文件。由此可见，美国的标准组织制定的行业规范与法律法规形成了相互促进和补充的关系，行业规范中被验证的成熟的规定和标准成为科技风险监管中重要的参考依据。

五、美国银行业科技风险管理对我国的借鉴意义

商业银行信息科技系统的安全是我国金融稳定的重要组成部分，构建完善的科技风险管理体系是预防金融风险的重要保障。近年来，信息科技风险事件的频繁发生引发了社会各界对银行科技风险管理的密切关注，如何有效地预防、控制和管理科技风险，成为监管层和银行面临的重要议题。科技风险的特殊性决定了商业银行需要构建具有针对性的风险管理框架，对信息科技的底层技术、系统开发、数据管理以及业务领域的应用进行全面的科技风险管理。美国科技风险管理的实践为我国商业银行科技风险管理提供了宝贵的经验：建立由专业的研究人员和从业者组成的标准组织并制定行业规范，与监管要求和法律法规形成相互促进和补充，能够为商业银行在信息科技的应用和管理提供专业、前沿和完善的参考标准，有助于完善银行科技风险管理体系，降低科技风险对商业银行和金融系统造成的冲击，维护我国的经济金融体系的稳定运行。