Deloitte.

德勤

# 冲破暗流

## 影响金融服务业的技术相关系统性风险因素

因我不同
成就不凡
始于1845

# 目录

# 内容摘要和主要成果

## 影响金融服务业技术相关系统性风险因素的六大要点

此前，世界经济论坛（WEF）携手德勤开展了有关技术如何加剧和降低金融服务业系统性风险的研究。在上一份报告《冰山之下：技术带来的系统性风险和持续的创新需求》中，我们总结了技术引发的各类系统性风险。

随着全球经济进入动荡时期，技术的重要性日益凸显。社交媒体和数字银行可能对近期银行业危机起了推波助澜的作用，加剧了金融服务业在抵御系统性冲击时的不确定性。生成式人工智能技术的进步，引发了人们对金融体系易受错误信息影响的质疑。在持续不断的地缘政治冲突下，金融机构已日渐成为网络战争的攻击目标。[1]

这些趋势促使我们将目光聚焦于技术相关系统性风险背后的行业和区域性影响。为识别相关风险及其应对措施，我们咨询了全球100多位金融服务业及技术领域的专家，并据此编制了本份报告《冲破暗流：影响金融服务业技术相关系统性风险的行业和区域性因素以及相关应对措施》。本文为此报告的内容摘要。[2]

# 专家访谈的六大要点

## 1

**金融服务业技术相关风险或将蔓延至各子行业和地区，并因产品开发和销售环节分离而产生系统性风险。**

不断扩张的金融基础设施、信贷发放及市场情报搜集使得行业分散化现象日益加剧。

金融基础设施因受监管金融服务实体提供的“即服务 (as-a-service)”模式而变得分散。风险监督部门与金融产品开发和销售部门相互分离，缺乏全面监管的风险亦随之增加。例如，银行通过银行即服务产品将现有基础设施扩展到非金融机构参与者，并与平台和应用程序接口 (API) 提供商合作以进入嵌入式金融领域。

技术平台提供商与非金融企业合作，旨在取代传统金融信贷产品并收集更多第一手数据。这增加了信贷违约风险的盲点，并将信贷产品的开发和销售分散到多个非金融实体。例如，“先买后付”等短期销售点产品使得零售商能够获取客户消费数据并向其提供贷款，而不受传统银行的直接风险及合规监管。

市场情报已分散到轻度监管实体中。此类情报被直接输入至能够做出实时财务决策的人工智能模型中，这可能会放大数据欺骗工具对金融市场和客户信任的影响 (例如深度伪造)。例如，投资机构正在通过不受监管的数据代理商来获取零售商和其他公司的市场情报。

## 2

**金融服务业的某些新近参与者无意中强调了短期的竞争优势，而忽视了长期运营韧性和透明度。**

金融服务业的许多新近参与者专注于为客户提供即时且可负担的金融产品。一味追求极速放款，对长期风险 (例如长期过度借贷和个人数据保护) 的管控将变得形同虚设。

个人金融业务越来越多地分散至非传统金融机构 (而非少数传统金融机构)，例如通过线上交易平台进行投资、从技术平台获取贷款以及借助应用程序编制预算。随着这一趋势逐渐成为主流，有义务或有能力保护客户免受财务损失或网络安全事件影响的私营实体将越来越少。

## 3 地缘政治和区域性因素瞬息万变，金融机构难以针对网络安全、劳动力短缺和环境威胁制定与时俱进的应对措施。

针对金融机构及其核心服务提供商的网络攻击愈加受到地缘政治驱动，且日趋复杂和频繁。鉴于金融机构的客群和供应商网络风险评估存在局限性，不断升级的网络攻击或对金融机构造成威胁。

由于区域内技术人才紧缺、邻近行业竞争加剧，某些金融机构可能缺乏关键运维（如灾难恢复解决方案）、客户数据保护及业务连续性管理等技术人才。

在获取用于评估客户受气候变化影响所需数据时，金融机构也受到局限。这可能导致对企业还款能力和保费支付能力的预测不够准确，进而造成对投资者所购买资产的风险评估出现误差。

## 4 行业和区域性差异为传统金融机构和金融科技公司带来机遇，有助于推广加强金融系统稳定性的增信产品和服务。

传统金融机构和金融科技公司可为客户提供覆盖所有金融交易的个人财务管理服务，同时保证便捷实惠的购物体验，以此填补市场空白。相关应用包括数字钱包产品和财务数据聚合服务。传统金融机构在拓展业务范围方面具有独特优势，其作为客户可信赖的合作伙伴，可以参与到与客户有多种金融交易的细分市场和邻近行业中去。

责任险产品可以保护客户免受数据泄露或未经授权活动的影响，例如防范客户的银行账户数据在第三方供应商托管的商户网站的泄露风险。

除已有的金融和媒体渠道，金融机构和金融科技公司还可在金融服务相关内容中嵌入身份验证和数字凭证服务，以保护客户免受虚假信息和数据欺骗工具的侵害。

**5** **公共和私营部门可携手打破信息孤岛，以准确识别生态系统层面的技术相关风险。**

正如本调查上份报告《冰山之下：技术带来的系统性风险和持续的创新需求》所述，网络规模是衡量金融生态系统参与者系统重要性的相关指标。监管机构和金融机构可以通过打破信息孤岛来应对生态系统中的风险。例如，监管机构可以通过开放银行平台和交易数据共享把握区域信贷风险的发展趋势，分析相关数据还可以了解不同监管措施对金融活动的影响。

为识别生态系统层面的技术相关风险，金融机构和监管机构应当厘清云基础设施、替代数据和API堆栈提供商之间的关系。这将为实施智能监控解决方案创造条件，从而预判对第三方供应商财务健康和安全防御的威胁，以便采取主动行动。

**6** **金融服务业参与者应当提高预测分析能力，以应对未来的地缘政治和区域不确定性，增强运营韧性。**

地缘政治和区域不确定性对运营韧性提出了新要求。在进行情景建模和制定韧性战略时，金融机构应权衡可能危及重要客户和服务提供商的情况，更新风险评估的方法，并在为金融产品定价时考虑区域性风险。

此外，金融机构应就行业韧性、全球共享基础设施韧性、响应模式以及地缘政治相关网络攻击带来的区域风险开展情景测试，还应在区域层面分析国际实验及其成果，以确定遏制攻击导致的系统性影响所需的公共资金支持和缓冲措施。

## 制定应对举措

归根结底，金融机构能否缓解技术相关系统性风险主要取决于其是否了解自身所面临的行业和区域风险。本报告将从银行及资本市场、支付行业、保险和投资管理行业视角来阐述行业风险，并按网络安全、技术人才和气候风险维度来分析区域风险。如您对相关内容有任何疑问或欲了解更多信息，请与我们联系。

# 行业视角

某些风险源自于金融服务业的特定子行业，但却有可能转化为系统性风险。本节将列举每个子行业存在的两种风险及其应对措施。

# 资本市场

## 风险1：利用合成媒体操纵市场

**可能出现的问题？**

合成媒体（例如深度伪造语音钓鱼和社交僵尸网络）可能传播虚假信息，对资本市场造成负面影响。这种风险正在增加，原因在于：

- 深度伪造工具、开源库和生成式人工智能的易用性降低了合成媒体的制作成本
- 央行行长、银行首席执行官和其他知名人士的图像和视频数量不断增加，提高了恶意合成媒体的精细度和欺骗性
- 重要机构使用社交媒体与公众沟通，提高了公众对这些平台的信任度

如果有人利用人工智能生成一段政府官员宣布大幅降低利率的视频，然后将视频发布到社交媒体上，则有可能引发系统性风险。

**哪些行业和区域因素会加剧风险？**

- 高度依赖另类媒体的社群
- 降低合成媒体制作成本的科技公司
- 基于高速实时数据传输的高频交易算法

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 加强对合成媒体的管控 | • 减少合成媒体变现的机会<br>• 通过众包对社交媒体进行事实核查 |
| 加强内容认证和提升媒体素养 | • 在社交媒体上传内容中嵌入数字内容凭证<br>• 使用人工智能事实核查插件 |

## 风险2：加密货币交易所危机扩散

**可能出现的问题？**

加密资产生态系统崩溃可能波及传统资本市场。这种风险正在增加，原因在于：

- 高杠杆交易的大众化可能会威胁交易所经营流动性
- 杠杆交易量和资本储备数据的透明度有限，可能造成投资者存款损失
- 区块链底层技术的伪匿名设计可能会增加信用评估的难度
- 为便于交易，交易所可能针对托管和借贷产品制定相互冲突的激励措施

如果一家大型加密货币交易所无法满足客户的提款需求并停止处理新的提款申请，引起投资者恐慌和其他加密货币交易所挤兑，则有可能引发系统性风险。

**哪些行业和区域因素会加剧风险？**

- 加密资产监管分散且不一致
- 去中心化加密货币交易所数量增加
- 去中心化金融应用互联互通

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 保护投资者存款 | • 限制使用客户存款用于高风险活动<br>• 设立共享准备金，帮助财务状况良好的交易所应对流动性问题 |
| 控制投资者参与杠杆交易的渠道 | • 利用公开的区块链交易数据进行信用评估 |
| 提高交易所偿付能力指标的透明度 | • 将第三方审计机构出具的准备金证明作为强制要求 |

*如欲进一步了解技术对银行行业系统性风险的影响以及相关案例，请参阅报告第24-35页。*

# 投资管理

## 风险1：社交媒体助长投机，引发市场波动

**可能出现的问题？**

随着个人投资者活动和投机行为在社交媒体平台的曝光率上升，模因股 (meme-stock) 投资等策略引发的市场波动可能会产生系统性影响。这种风险正在增加，原因在于：

- 复杂投资产品交易 (通过线上交易平台) 的大众化可能放大新手参与投机交易的影响
- 个人投资者将社交媒体平台视为可信市场数据来源，可能陷入助长投机和偏见的信息茧房
- 网上传播并吸引年轻一代散户投资者关注的模因股存在不可预测性，加大了投资机构更新风险模型的难度，个人投资者亦难以做出明智的投资决策

如果关于低估值股票的谣言在社交媒体传播，并通过另类媒体鼓动个人投资者从众购买，那么这种风险可能转化为系统性风险。

**哪些行业和区域因素会加剧风险？**

- 鼓励高风险交易行为的线上交易平台
- 社交媒体在各社群的渗透率
- 利用社交媒体抬高公司股价的投资者

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 防止投资者参与投机交易 | • 在线上交易平台开展金融素养教育<br>• 通过社交媒体提高个人投资者的参与度 |
| 增进机构投资者对领先模因股指标的了解 | • 设立交易所交易基金和指数，帮助投资者追踪模因股<br>• 利用机器学习算法帮助机构投资者发现模因股暴涨的预警信号 |

## 风险2：传感器数据泄露，投资者受到操纵

**可能出现的问题？**

越来越多的投资机构使用传感器生成数据来辅助决策，这扩大了恶意破坏和操纵市场数据的攻击面。这种风险正在增加，原因在于：

- 网络犯罪分子利用开源渠道快速共享恶意软件源代码，并加快对联网设备发动新型攻击的速度
- 高速5G网络帮助投资管理机构即时获取实时传感器生成数据
- 物联网的多个端点扩大了攻击面，加大了全面安全监控的难度
- 单个传感器受到恶意软件攻击时，所有联网设备均会受到影响

如果某种全球性商品的共享传感器遭到破坏（通过操纵或伪造数据），导致投资机构和对冲基金做出错误的交易决策，那么这种风险可能转化为系统性风险。

**哪些行业和区域因素会加剧风险？**

- 服务提供商使用非专有组件将设备连接到5G网络
- 传感器制造商的整合
- 数据代理行业未受到监管

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 提高来自传感器的数据质量 | • 建立联网设备全球认证和标记机制<br>• 强制要求替代数据供应商开展尽职调查 |
| 遏制恶意软件在传感器网络中的传播 | • 通过熵服务提供商保护传感器生成数据<br>• 利用扩展威胁响应技术跨设备整合数据 |

*如欲进一步了解技术对投资管理行业系统性风险的影响以及相关案例，请参阅报告第36-47页。*

# 支付行业

## 风险1：“先买后付”（BNPL）债务的累积和证券化

### 可能出现的问题？

销售点融资易于获取，加之承销规则不够完善，可能会导致过度借贷，并通过债务证券化影响金融系统。这种风险正在增加，原因在于：

- 薄弱的借贷审核为冲动购物和债务累积创造了机会
- 针对BNPL债务的报告要求有限，降低了客户总体债务状况的透明度
- BNPL债务证券化可能对整个金融系统造成负面影响
- 保护客户和增加销售额的措施相互冲突，可能会加速债务积累

如果发生经济衰退，影响客户还款能力，而BNPL债务量又处于相当高的水平，且大部分已被证券化为次级借款人债务，那么这种风险可能转化为系统性风险。

### 哪些行业和区域因素会加剧风险？

- 提供BNPL贷款的大型科技公司
- 提供BNPL融资的辖区缺乏相关法规
- 金融知识普及率低

### 行业应对措施

| 目标 | 应对措施 |
| --- | --- |
| 防止客户过度借贷 | • 设置保障机制，防止过度借贷和误导性广告<br>• 制定BNPL提供商行为准则 |
| 提高客户支付能力的透明度 | • 增强BNPL提供商之间的数据共享<br>• 将BNPL数据纳入征信机构报告 |

## 风险2：去中心化央行数字货币架构存在安全漏洞

**可能出现的问题？**

基于分布式账本技术 (DLT) 的央行数字货币 (CBDC) 扩大了恶意行为者的攻击面。这种风险正在增加，原因在于：

- 黑客可以通过DLT网络参与者发动攻击
- DLT支持平台的漏洞或故障可能导致系统瘫痪
- 边信道攻击 (side channel attack, SCA) 可以入侵用户钱包并窃取资金

如果某国对他国CBDC支付网络发动分布式拒绝服务攻击，导致关键服务中断，那么这种风险可能转化为系统性风险。

**哪些行业和区域因素会加剧风险？**

- 复杂的CBDC网络架构
- 与其他网络的互操作性
- 数量众多的参与机构

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 用户保护和数据隐私 | • 保护终端用户的数字钱包 |
| 强大的访问控制和网络安全 | • 建立CBDC分级分类账系统<br>• 使用抗量子算法保护CBDC系统 |
| 跨境安全标准化 | • 实现CBDC安全协议标准化 |

*如欲进一步了解技术对银行行业系统性风险的影响以及相关案例，请参阅报告第48-59页。*

# 银行业

## 风险1：银行即服务产品存在风险敞口

**可能出现的问题？**

银行即服务 (BaaS) 对API的依赖性日益增强，导致出现可能给银行带来风险的漏洞。这种风险正在增加，原因在于：

- 客户的敏感数据和资金可能遭受网络钓鱼和网络攻击
- 有漏洞的API可能为黑客入侵银行系统开后门
- BaaS提供商违反数据隐私规则可能会使合作银行面临声誉风险

如果恶意行为者对BaaS提供商发动分布式拒绝服务攻击，导致客户无法登录账户或进行交易，那么这种风险可能转化为系统性风险。

**哪些行业和区域因素会加剧风险？**

- 复杂的BaaS技术栈
- 有限的冗余措施
- 缺乏输入验证，使攻击者能够通过API将恶意代码上传至银行系统中

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 提高BaaS平台和API连接的安全性 | • 使用输入验证协议<br>• 采取网络分段和访问控制措施 |
| 针对BaaS合作伙伴进行严格审查 | • 改进针对BaaS提供商的尽职调查 |
| 推动银行向BaaS合作伙伴传递经验知识 | • 助力BaaS和其他金融科技提供商提升风险管理和合规能力 |

## 风险2：稳定币的稳定机制不完善

**可能出现的问题？**

稳定币是一种与法定货币、黄金等储备资产挂钩的数字货币，但未获得央行支持，这增加了挤兑的可能性。这种风险正在增加，原因在于：

- 治理和监管漏洞可能导致非法活动长期存在，从而对金融系统的完整性造成威胁
- 用于铸造和管理稳定币的新技术存在安全风险
- 存款保险等稳定机制的缺失增加了挤兑的风险

如果一家大型稳定币发行商未能及时满足客户的大额提款需求，从而引发挤兑并最终导致稳定币崩盘，那么这种风险可能转化为系统性风险。

**哪些行业和区域因素会加剧风险？**

- 监管环境不成熟
- 资本管制严格，可能促使个人将资产存放在全球稳定币中
- 系统不安全，内部流程管理不善

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 稳定币规范和监督 | • 要求稳定币发行商执行反洗钱和尽职调查流程 |
| 投资者和客户保护 | • 将稳定币纳入保险覆盖范围<br>• 实施负责任营销规则，开展客户教育 |
| 资本储备透明度 | • 针对稳定币发行商的储备资产定期进行审计和压力测试 |

*如欲进一步了解技术对银行行业系统性风险的影响以及相关案例，请参阅报告第60-70页。*

# 保险业

## 风险1：指数保险智能合约存在漏洞

**可能出现的问题？**

由于智能合约可以自动执行，因此任何编程缺陷或安全漏洞都可能造成巨大的保险损失。这种风险正在增加，原因在于：

- 智能合约可能会因区块链网络中的编码错误而受到破坏
- 智能合约的不可变性使得及时解决错误变得更加困难
- 依赖可能被操纵的外部数据来源会使智能合约面临风险
- 不断变化的监管和法律环境导致智能合约的执行充满不确定性

如果第三方数据泄露导致多家保险公司基于智能合约进行错误赔付，那么这种风险可能转化为系统性风险。

**哪些行业和区域因素会放大风险？**

- 有关数字合约的法律和监管标准不明确
- 技术基础设施不完善
- 对于智能合约的运作了解有限

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 网络和运营韧性 | • 审核智能合约源代码<br>• 采用最佳实践并使用安全的编程语言 |
| 稳健治理 | • 完善智能合约治理机制 |
| 监管和法律覆盖 | • 将智能合约纳入现有监管和法律框架 |

## 风险2：灾难性网络攻击的防护缺口不断扩大

**可能出现的问题？**

随着保险公司开始限制其风险敞口，金融机构从大规模网络攻击中恢复的能力可能正在减弱。这种风险正在增加，原因在于：

- 网络战战术越来越多地被用于加剧国家之间的地缘政治紧张局势
- 生成式人工智能降低了网络犯罪门槛（例如使用ChatGPT生成恶意软件）
- 利用国家资金可以发起影响巨大的复杂攻击
- 预测和抵御大规模网络攻击的能力有限，导致网络保险的可负担性降低

如果一家保险公司承保的多家银行或关键第三方服务提供商因网络攻击而瘫痪，那么这种风险可能转化为系统性风险。

**哪些行业和区域因素会放大风险？**

- 庞大的第三方服务提供商网络
- 有限的网络安全诊断数据
- 缺乏政府间跨境协调

**行业应对措施**

| 目标 | 应对措施 |
| --- | --- |
| 寻求替代资金来源以应对日益增长的网络风险 | • 通过保险连接证券在私募市场集资 |
| 开展公私合作以预防或吸收网络攻击相关损失 | • 针对网络承保风险和财务韧性进行压力测试<br>• 建立资源中心，提供网络安全工具和服务 |
| 获取有关网络攻击相关损失的情报 | • 量化网络风险相关损失，以衡量投资组合面临的网络威胁 |

# 区域性风险因素

某些系统性风险贯穿于整个金融系统，这些风险可能具有区域依赖性或者存在区域性差异。本节将列举三种区域性风险以及公共和私营部门正在探索的应对措施。

# 网络安全

## 有何风险?

地缘政治紧张局势的加剧、攻击面的扩大以及黑客工具的进步导致某些地区的网络安全威胁激增。

**影响风险的区域性因素有哪些?**

- 技术能力和资源的可用性
- 监管和法律环境的成熟度
- 区域合作水平
- 对外部市场基础设施的依赖程度

**区域应对措施**

| 应对措施 | 实例 |
| --- | --- |
| 协调网络安全计划和法律 | 欧盟《数字运营韧性法案》旨在改善运营韧性管理，包括网络安全和事件报告 |
| 提高网络安全工具和技术的可用性 | Snort和OpenVPN等开源软件以及AWS安全中心和谷歌云安全指挥中心等平台可以提供具有成本效益的基本网络安全服务 |
| 公私合作进行事件响应 | 在加拿大金融行业韧性小组的领导下，加拿大银行正在与私营部门合作应对系统性运营事件 |
| 提升跨境网络安全能力 | 澳大利亚网络安全中心为印太地区国家提供培训 |

*如欲进一步了解网络安全相关技术相关系统性风险受到的区域性影响以及相关案例，请参阅报告第84-86页。*

# 技术人才

## 有何风险?

在劳动力短缺加剧和技术依赖性增强的背景下，各地区的行业参与者都在努力寻找推动创新甚至维持核心运营所需的人才。

**影响风险的区域性因素有哪些?**

- 经济和社会因素
- 移民政策
- 创新和技术中心的建立
- 教育和培训计划的可用性

**区域应对措施**

| 应对措施 | 实例 |
| --- | --- |
| 与学术界开展合作 | 摩根大通的 “Tech for Social Good” 计划旨在通过为年轻人提供教育、指导和编程学习机会来弥合技术能力差距 |
| 员工技能重塑 | 汇丰银行 (马来西亚) 创建了Digital Black Belt Development Program，旨在帮助员工获得数据分析、机器学习和自动化方面的数字技能 |
| 使用无代码和低代码平台 | 安盛集团通过低代码平台OutSystems在三个月内实现了理赔处理系统的现代化，大幅减少了联络中心的接话量 |
| 建立技术中心 | 加拿大蒙特利尔银行正在北美地区建立技术中心 |

*如欲进一步了解技术人才相关技术相关系统性风险受到的区域性影响以及相关案例，请参阅报告第87-89页。*

# 气候变化

## 有何风险?

在各国承诺于未来三十年内实现净零排放的背景下，金融机构在获取为气候变化对客户的影响定价所需的数据方面却面临限制。

**影响风险的区域性因素有哪些?**

- 流入私募市场的资本份额透明度降低
- 遥感技术的可负担性和人才库的可利用性
- 高碳排放经济体和转型风险
- 净零排放目标

**区域应对措施**

| 应对措施 | 实例 |
| --- | --- |
| 实施中小企业气候中心计划 | 中小企业气候中心可以帮助小型企业衡量碳足迹并挖掘新的融资机会 |
| 发布气候相关统计指标 | 欧洲央行发布了实验性和分析性指标，旨在说明气候相关风险对金融行业的影响 |
| 建立全球公私数据存储库 | 正在开发的Net-Zero Data Public Utility旨在成为可验证过渡数据的可信存储库 |
| 基于复杂气候模型获取本地洞察和区域预测 | Climate Risk and Resilience Portal是一种新的公开可用工具，揭示了未来气候情景对美国城镇的影响 |

*如欲进一步了解气候变化相关技术相关系统性风险受到的区域性影响以及相关案例，请参阅报告第90-92页。*

# 结语

随着越来越多的金融机构在不断接受数字化创新，可能威胁金融系统稳定性的风险也随之而来。某些风险可能源自单一行业，某些风险可能为特定领域独有。无论哪种情况，若不妥善管理，这些风险都可能扩散并转化为系统性风险。

金融服务业应当如何缓解源自传统金融体系之外的技术相关风险？

- 私营部门组织可以加强其在客户财务决策过程中作为可信赖合作伙伴的作用，并推动不同利益相关者参与风险评估
- 公共部门组织可以利用现有技术建立共享风险库，并向客户普及媒体和金融知识
- 私营和公共部门组织可以合作针对响应和恢复能力进行压力测试，同时加强应对系统性冲击的缓冲措施

技术相关风险动态多变。这意味着，金融机构需要不断进行知识交流以及开展跨辖区和跨行业实验，才能有效并持续不断地应对所面临的风险因素。

本文为德勤与WEF联合发布的报告《冲破暗流：影响金融服务技术相关系统性风险的行业和区域性因素以及相关应对措施》(Pushing through undercurrents: Sectoral and regional forces influencing technology-driven systemic risk, and resulting mitigation opportunities) 核心要点概述。如欲了解更多信息，请参阅报告原文，欢迎来邮垂询和分享见解。

# 中国联系人

**方烨**
**德勤中国金融服务业**
**风险咨询主管合伙人**
电话：+86 21 6141 1569
电子邮件：yefang@deloitte.com.cn

**吴洁**
**德勤中国金融服务业**
**风险与合规服务主管合伙人**
电话：+86 21 6141 2237
电子邮件：kwu@deloitte.com.cn

报告原名*Pushing through undercurrents: Sectoral and regional forces that influence technology-driven systemic risk in financial services*，为德勤与世界经济论坛共同编制的研究报告*Pushing Through Undercurrents: Sectoral and regional forces influencing technology-driven systemic risk, and resulting mitigation opportunities*的内容摘要，德勤中国金融服务业风险咨询服务团队对报告摘要进行了翻译。

特别感谢Ayesha Madan、John Okoronkwo (报告作者) 、Gayatri Suresh Kumar以及Hwan Kim (项目顾问) 对本报告的支持和贡献。

## 尾注

1. For more on the information in this paragraph, please see Beneath the surface: Technology-driven systemic risks and the continued need for innovation, World Economic Forum and Deloitte, 2021, https://www.weforum.org/reports/beneath-the-surface-technology-driven-systemic-risks-and-the-continued-need-for-innovation/

2. For more on the information in this summary report, please see Pushing through undercurrents: Sectoral and regional forces influencing technology-driven systemic risk, and resulting mitigation opportunities, World Economic Forum and Deloitte, 2023, https://www.weforum.org/reports/pushing-through-undercurrents-sectoral-and-regional-forces-influencing-technology-driven-systemic-risk-and-resulting-mitigation-opportunities/

3. 92. Fanti, Giulia et al., "Missing Key: The challenge of cybersecurity and central bank digital currency," Atlantic Council, 15 June 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/


关于德勤

德勤中国是一家立足本土、连接全球的综合性专业服务机构，由德勤中国的合伙人共同拥有，始终服务于中国改革开放和经济建设的前沿。我们的办公室遍布中国31个城市，现有超过2万名专业人才，向客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务与商务咨询等全球领先的一站式专业服务。

我们诚信为本，坚守质量，勇于创新，以卓越的专业能力、丰富的行业洞察和智慧的技术解决方案，助力各行各业的客户与合作伙伴把握机遇，应对挑战，实现世界一流的高质量发展目标。

德勤品牌始于1845年，其中文名称“德勤”于1978年起用，寓意“敬德修业，业精于勤”。德勤全球专业网络的成员机构遍布150多个国家或地区，以“因我不同，成就不凡”为宗旨，为资本市场增强公众信任，为客户转型升级赋能，为人才激活迎接未来的能力，为更繁荣的经济、更公平的社会和可持续的世界开拓前行。

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构（统称为“德勤组织”）。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为承担责任，而对相互的行为不承担任何法律责任。德勤有限公司并不向客户提供服务。请参阅www.deloitte.com/cn/about了解更多信息。

德勤亚太有限公司（一家担保责任有限公司，是境外设立有限责任公司的其中一种形式，成员以其所担保的金额为限对公司承担责任）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100个城市提供专业服务，包括奥克兰、曼谷、北京、班加罗尔、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、孟买、新德里、大阪、首尔、上海、新加坡、悉尼、台北和东京。

本通讯中所含内容乃一般性信息，任何德勤有限公司、其全球成员所网络或它们的关联机构并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。

我们并未对本通讯所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。


Designed by CoRe Creative Services. RITM1581645

这是环保纸印刷品