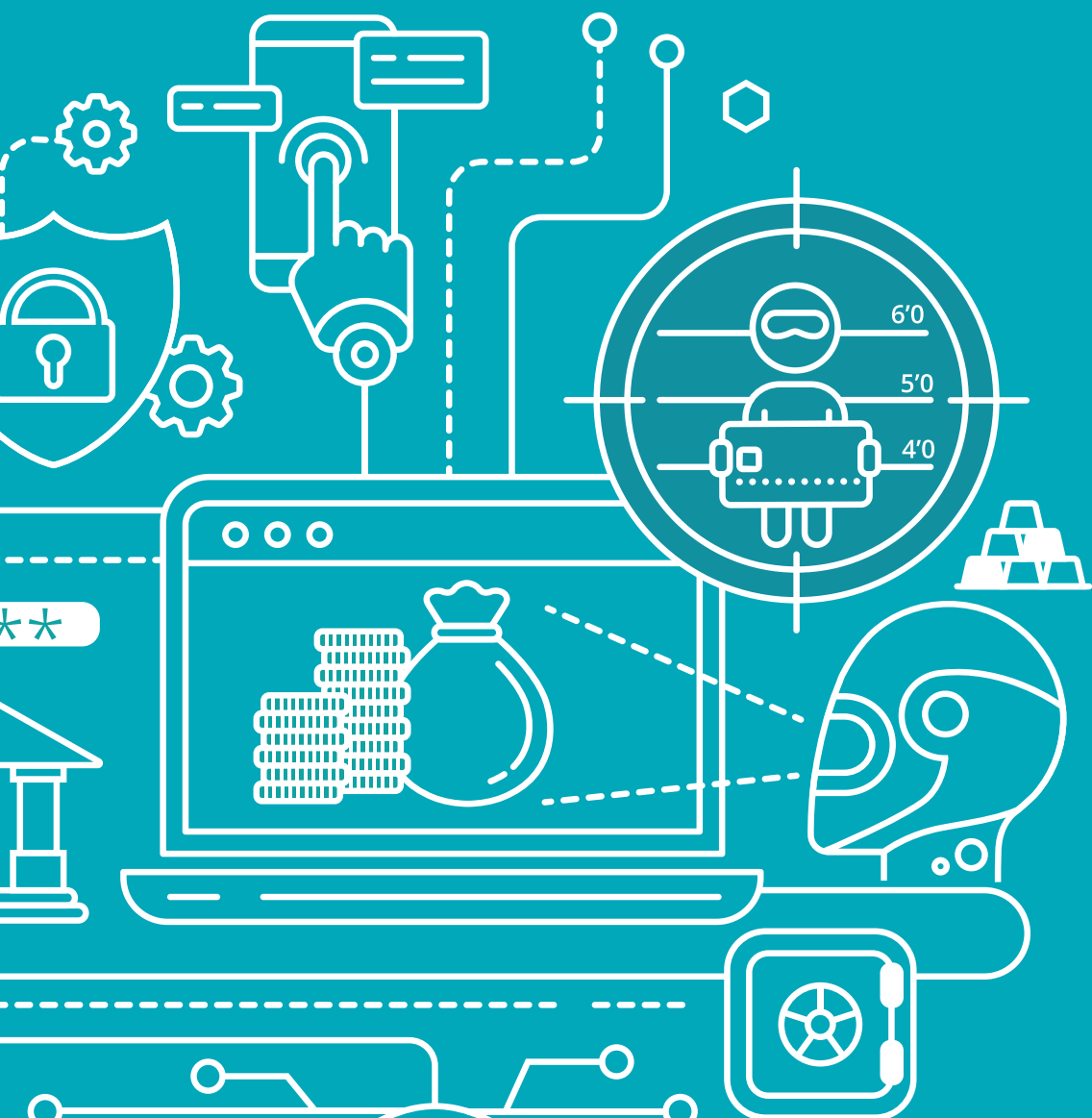




科技助力金融犯罪管理转型

因我不同  
成就不凡  
始于1845



# 目录

|              |    |
|--------------|----|
| 引言           | 1  |
| 近期发展情况概述     | 3  |
| 科技应用助力打击金融犯罪 | 15 |
| 科技解决方案案例研究精选 | 19 |
| 案例研究重要启示     | 29 |
| 科技管理贯穿客户生命周期 | 33 |
| 前景展望         | 38 |
| 结论           | 41 |
| 术语表          | 43 |
| 联系人          | 45 |
| 尾注           | 47 |

# 引言

尽管在检测、预防和威慑能力方面已经投入大量资金，金融犯罪仍有可能造成数万亿美元的损失，也是金融服务行业和社会目前面临的主要风险之一。

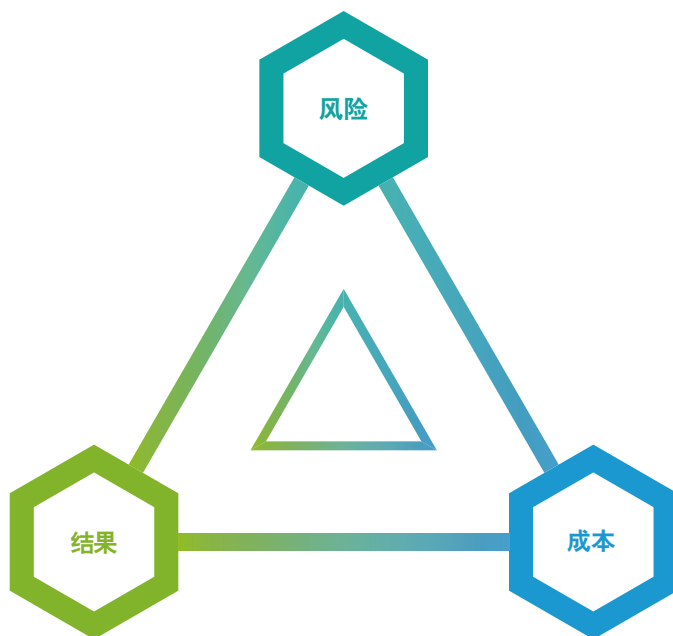
犯罪分子在运用科技实施金融犯罪方面变得更加熟练，他们可以发现和利用金融系统中的漏洞，并且借助新型支付平台和加密货币等新兴技术进行愈发难以被检测和追踪的复杂、多层交易。

与此同时，洗钱和恐怖融资活动继续威胁社会秩序，阻碍全球应对重大社会和道德问题，例如环境危害以及人口、野生动物和毒品贩卖。

然而，科技不仅可以用于犯罪。数字化趋势因新冠疫情而加速发展，并且正在改变金融犯罪的类型以及执法机构和受监管实体检测金融犯罪的方式。例如，传统现金指标和纸质文档验证控制在数字化交易中的重要性逐渐降低。

在这种背景下，金融机构一直致力于提高其金融犯罪管理能力。然而，尽管金融机构已经投入大量时间和资金应对金融犯罪风险，但是监管机构的重大执法行动以及金融犯罪方面的重大丑闻表明，其依然任重道远。

因此，金融机构需要重新思考科技应用，从而实现风险、结果和成本的有效平衡。



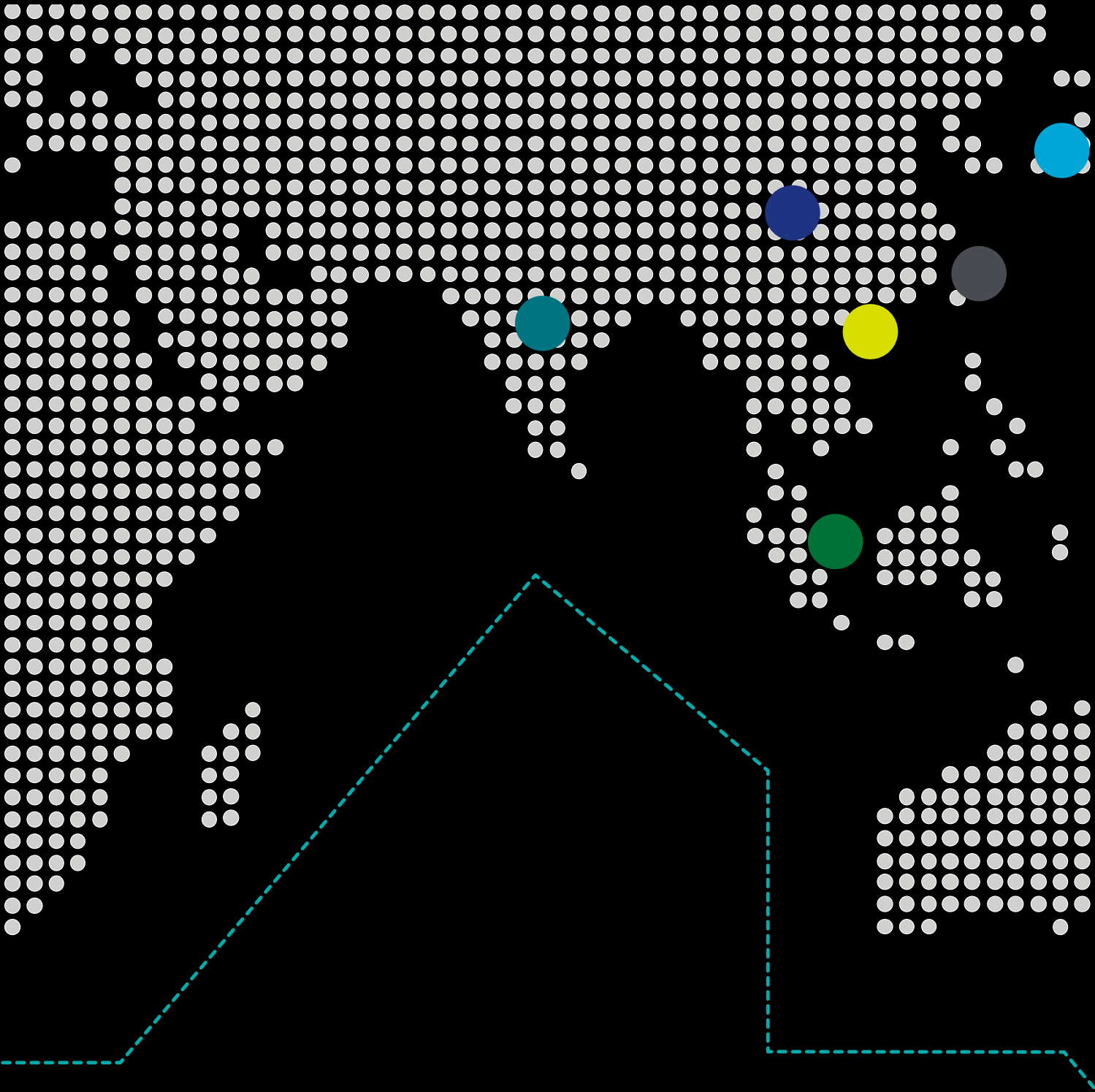
为了解科技在打击金融犯罪方面的最大优势，金融机构需要在客户生命周期中积极应用科技解决方案。

然而，不同金融机构所处的科技应用阶段以及对于科技应用的需求和预算有所不同且差异较大，尤其是科技解决方案通常需要完整和准确的数据并且在很大程度上依赖于其与现有系统能否有效集成。

此外，在选择科技解决方案时，尖端解决方案（使用未经测试的最新技术）与成熟解决方案（具有优异表现记录）在安全性和可信度方面存在矛盾。因此，在对解决方案增加投资之前，金融机构通常需要从“监管科技”<sup>[1]</sup>的概念验证入手。此外，金融机通常需要在现有流程中“同步运行”创新解决方案，并且向组织内部和监管机构证明此等解决方案的有效性。但这将会引发成本问题，因此金融机需要致力于投资中长期变革。

本报告探讨了金融机如何利用科技打击金融犯罪，从而提升业务效益、改善成果质量并在长期内提高效率和降低成本。此外，本报告列举了亚太地区的五个案例，旨在提供关于如何利用科技预防和发现金融犯罪的行业实践和洞察。

<sup>[1]</sup> “监管科技”是指旨在改进现有流程以满足监管要求和期望（尤其是金融犯罪相关法律、法规和条例）的科技解决方案。



# 近期发展情况概述





司法管辖区：澳大利亚



关键法规更新

继澳大利亚两家大型银行因违反反洗钱和反恐融资法律而被处以创纪录的罚款之后，澳大利亚监管机构——澳大利亚交易报告和分析中心 (AUSTRAC) ——在继续关注澳大利亚金融服务和支付领域参与者如何管理金融犯罪风险方面获得动力和政治支持。

因此，AUSTRAC针对澳大利亚金融行业的主要参与者以及支付领域的跨国企业和新兴参与者开展了详细审查，审查结果强调了金融犯罪风险管理方面的许多系统性问题。

此外，澳大利亚政府和AUSTRAC等监管机构在继续推进金融犯罪风险和风险管理改革议程方面一直面临压力。因此，澳大利亚为应对全行业审查出台了一系列改革措施，例如皇家委员会金融服务行业不当行为调查以及金融行动特别工作组 (FATF) 互评估建议，包括：

- **银行高管问责制度 (BEAR)** 的适用范围扩大到其他金融服务公司，这将导致金融服务公司和其他实体 (例如财富管理公司和支付服务提供商) 需要履行与行为、文化和风险管理 (包括金融犯罪风险管理) 相关的更多职责和端到端产品责任。适用范围扩大之后，BEAR制度将会更名为**财务问责制度 (FAR)**。<sup>1</sup>



- 2020年12月通过《2020年反洗钱和反恐融资及其他立法修正案 (Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2020)》(简称《修正案》),《修正案》将会落实2015年FATF报告中的建议,并变更澳大利亚反洗钱/反恐融资框架中与客户识别程序、代理银行关系、犯罪举报、信息获取和跨境资金流动相关的关键要素。相关变更已于2021年6月18日生效。<sup>2</sup>
- 审慎监管机构——澳大利亚审慎监管局 (APRA) ——更新风险管理 (《CPS 220风险管理审慎标准 (Prudential Standard CPS 220 Risk Management)》和《CPG 220风险管理审慎实践指南 (Prudential Practice Guide CPG 220 Risk Management)》, 2019年7月1日生效)<sup>3</sup> 和信息安全 (《CPS 234信息安全审慎标准 (Prudential

Standard CPS 234 Information Security)》, 2019年7月1日生效)<sup>4</sup>相关标准和指南。与此同时, APRA要求金融服务公司和董事会建立适当的报告机制, 以此提高其在遵守金融犯罪相关规定和管理风险方面的透明度。

除此之外, AUSTRAC还与众多行业和社区组织合作针对《反洗钱/反恐融资客户识别和验证规则 (AML/CTF Customer ID and Verification Rule)》<sup>5</sup> (2020年5月8日生效) 进行修订, 以此帮助逃离家庭暴力的澳大利亚人获得经济独立。根据该规则, 如果客户不能出示驾照或出生证明或提供不同地址, 银行和其他受监管实体可以采用其他方式验证客户身份。参阅AUSTRAC发布的更新指南获取关于报告主体如何应用该规则的更多信息。<sup>6</sup>



## 执法行动

2020年9月, AUSTRAC对澳大利亚某大型银行的反洗钱/反恐融资违规行为开出13亿澳元的创纪录罚单, 部分原因在于其未对儿童性剥削相关交易进行监测。AUSTRAC调查发现, 该行违反《2006年反洗钱和反恐融资法案 (Anti-Money Laundering and Counter-Terrorism Financing Act 2006)》(简称《反洗钱/反恐融资法案》) 的次数超过2,300万次, 导致澳大利亚金融系统长期暴露在风险之中。

2019年, 由于担忧持续存在, AUSTRAC下令为两家大型支付/技术公司任命外部审计师, 负责审查其遵守《反洗钱/反恐融资法案》规定的情况。

2019年, AUSTRAC还对两个报告主体未根据《反洗钱/反恐融资法案》规定报告国际资金转移情况的行为向其发出罚款和违规通知。



## 司法管辖区：新西兰

### 关键法规更新

2020年9月，新西兰反洗钱和反恐融资监管机构联合更新《增强版客户尽职调查指南 (Enhanced Customer Due Diligence Guideline)》<sup>7</sup>，以此帮助报告主体了解何时需要或者应当根据报告主体的反洗钱/反恐融资风险评估开展增强型客户尽职调查。

2020年3月，反洗钱/反恐融资监管机构发布与新冠疫情期间个人身份识别相关的紧急指南。该指南<sup>8</sup>概述了报告主体如何继续履行与客户尽职调查和账户监测相关的反洗钱/反恐融资义务，从而限制新冠疫情的扩散和传播以及客户交互。

2019年11月，新西兰反洗钱/反恐融资监管机构、内政部 (DIA)、金融市场管理局 (FMA) 和新西兰储备银行 (RBNZ) 联合更新并发布两份新的指导文件，其中概述了修订后的反洗钱/反恐融资监管框架<sup>9</sup> (说明三大反洗钱/反恐融资监管机构的职权范围) 以及《反洗钱/反恐融资法案》适用的地域范围。<sup>10</sup>

新西兰反洗钱/反恐融资法律<sup>11</sup> (2017年根据《2017年反洗钱和反恐融资法案修正案 (Anti-Money Laundering and Countering Financing of Terrorism Amendment Act 2017)》颁布) “第二阶段修订”已于2019年8月1日进入最后阶段。这意味着，自2019年8月1日起，新西兰竞赛委员会 (负责管理新西兰的所有竞赛和体育博彩) 必须将反洗钱/反恐融资措施落实到位。此外，如果某些操作标准适用，会计师、律师、房地产经纪以及高价值商品 (例如珠宝、贵金属、宝石、手表、汽车、游艇、艺术品或古董) 贸易企业都需要遵守《反洗钱/反恐融资法案》。



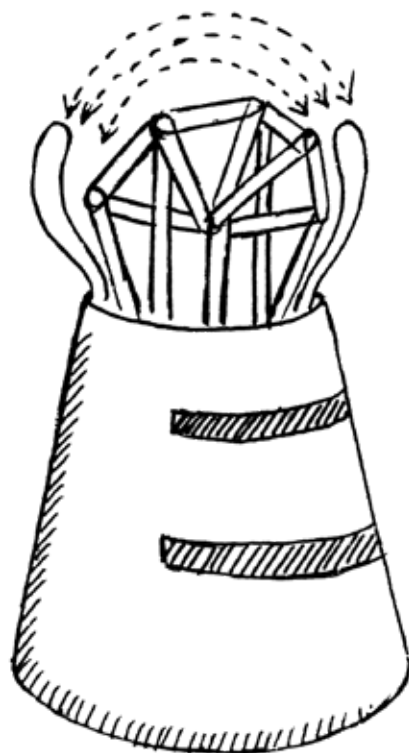
## 执法行动

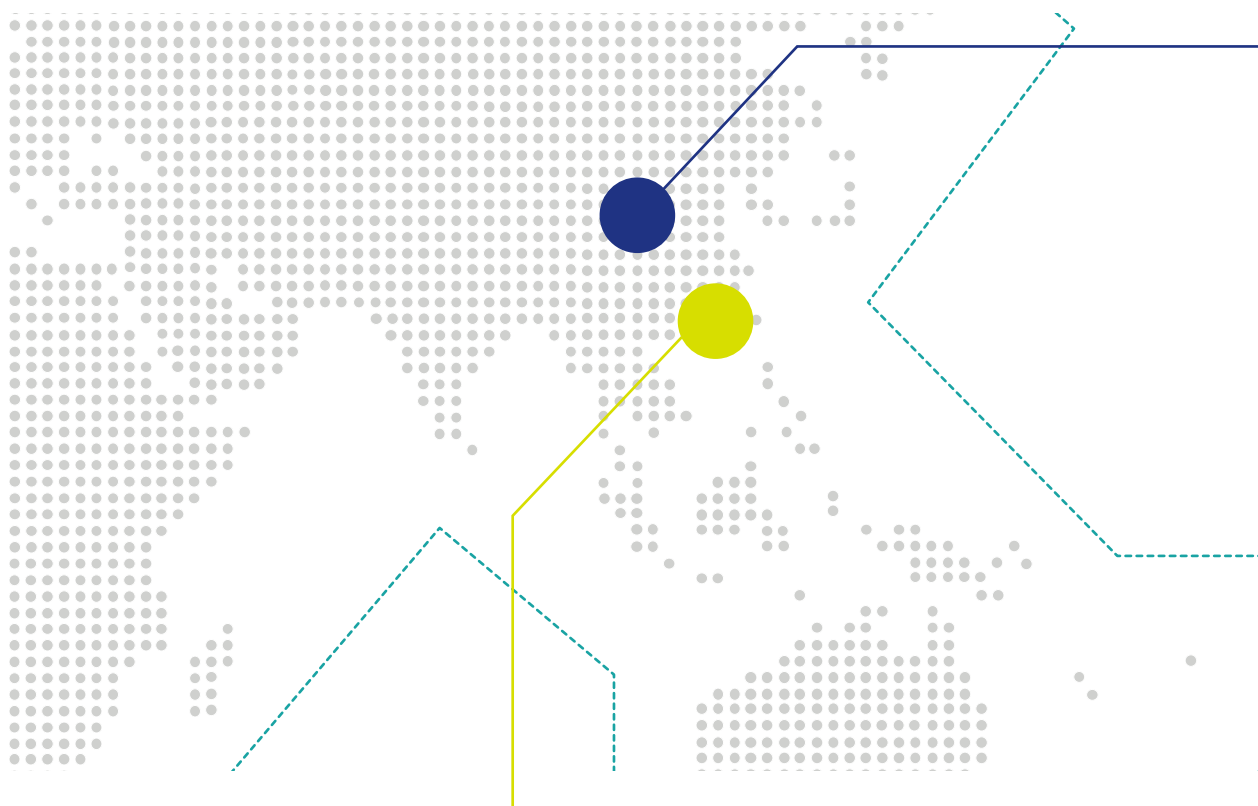
2020年7月, DIA对两家汇款业务公司在2014至2019年期间违反《2009年反洗钱和反恐融资法案 (2009 Anti-Money Laundering and Countering Financing of Terrorism Act) 》的行为处以超过750万新西兰元的罚款。违规行为包括不配合DIA的调查、试图误导DIA以及试图掩盖其中一家汇款业务公司作为报告主体的身份。

2019年8月, 新西兰警方在奥克兰展开重大反洗钱调查, 逮捕六人, 查获数百万资产。

2019年7月, DIA对新西兰某领先工作场所提供商内的七个报告主体违反《反洗钱/反恐融资法案》的行为向其发出正式警告, 违规行为包括未开展客户尽职调查和增强型尽职调查、未保存相关记录以及未制定、实施和维护现行风险评估和反洗钱/反恐融资计划。

2019年6月, DIA对新西兰某大型保险箱业务供应商未履行反洗钱/反恐融资义务的行为向其发出正式警告, 相关行为包括未开展客户尽职调查、未充分监测账户和交易、未保存相关记录以及未制定、实施和维护反洗钱/反恐融资计划。





## 司法管辖区：中国香港



### 关键法规更新

香港金融管理局 (HKMA) 继续致力于“推动反洗钱工作中的负责任创新”，<sup>12</sup>并且重点关注：

1. 确保新兴行业实现负责任发展，并为避免其被不良行为者利用制定充分的保障措施；
2. 及时更新相关要求，推动金融机构充分利用新技术提供的机会；

3. 根据HKMA的目标推进变革，“以便我们能够继续开展有效监管；在监管过程中，我们需要基于我们所监管部门发生的变革进行思考和采取行动”。

为支持“反洗钱工作中的负责任创新”，HKMA更新关键法律法规<sup>13, 14</sup>，旨在针对如何利用科技打击金融犯罪以及市场新进入者（例如储值支付工具提供商和虚拟银行）如何为管理金融犯罪风险制定充分的保障措施和建立完善的框架体系提供明确指引。



### 执法行动

香港证券及期货事务监察委员会 (SFC) 对几家金融机构的反洗钱违规行为（包括与反洗钱风险相关的内部控制问题）处以超过2,500万港元的罚款。



## 司法管辖区：中国大陆



### 关键法规更新

2021年1月，中国人民银行（PBOC）发布更新指南<sup>15</sup>，其中概述了受监管金融机构应当如何完成针对洗钱/恐怖融资风险的机构风险评估。根据该指南，受监管金融机构须在2021年12月31日前建立机构风险评估制度，并于2022年12月31日前完成首次机构风险评估。法人金融机构开展洗钱风险自评估应当遵循以下原则：

- 全面性原则
  - 覆盖本机构所有经营地域、客户群体、产品业务（含服务）、交易或交付渠道；
  - 覆盖境内外所有与洗钱风险管理相关的分支机构及总部有关部门；
  - 充分考虑各方面风险因素，贯穿决策、执行和监督的全部管理环节；

- 客观性原则；
- 匹配性原则；
- 灵活性原则。

2020年12月30日，PBOC公布《金融机构反洗钱和反恐怖融资监督管理办法（修订草案征求意见稿）》<sup>16</sup>，其中概述了在2019年完成FATF评估之后旨在全面改革中国反洗钱框架的拟议措施。在完成意见征集和审批流程之后，这些新措施将取代PBOC于2014年建立的反洗钱制度。该管理办法自2021年8月1日起施行。



### 执法行动

在过去几年中，反洗钱执法检查力度持续加大，处罚频率和处罚金额均有增加。据不完全统计，2019年，人民银行全系统共对1,744家义务机构开展反洗钱执法检查，针对违反反洗钱规定的行为依法予以处罚，罚款金额总计人民币2.15亿元，同比增长13.7%。依法处罚违规机构525家，罚款人民币2.02亿元；处罚违规个人838人，罚款人民币1,341

万元。2020年，人民银行对614家金融机构、支付机构等反洗钱义务机构展开了专项和综合执法检查，依法完成对537家反洗钱义务机构的行政处罚，处罚金额人民币5.26亿元；处罚违规个人1,000人，处罚金额人民币2,468万元。鉴于人民银行和其他政府机构对此问题十分重视，因此未来几年的检查和处罚力度预计将会继续增加。



## 司法管辖区：新加坡



### 关键法规更新

新加坡持续关注监管科技，并且已针对支付、数字银行和加密资产等不断发展的新兴金融服务领域出台相关法规。其中一项重要法规是《2020年支付服务法案 (Payment Services Act (2020))》(PSA)，<sup>17</sup>该法案于2020年1月1日生效并将支付服务提供商纳入监管范围。

在监管领域外，新加坡加密货币企业和初创企业协会 (ACCESS) 等新加坡金融科技<sup>[2]</sup>协会共同制定自愿行为准则<sup>18, 19</sup>，以将新加坡反洗钱/反恐融资法规的适用范围扩大到加密资产公司。



### 执法行动

新加坡金融管理局 (MAS) 对新加坡资产管理公司和信托公司违反反洗钱监管要求的行为 (包括与反洗钱/反恐融资风险相关的内部控制问题) 给予吊销执照的处罚。

除此之外，MAS还对未履行反洗钱/反恐融资义务的行为处以超过200万新加坡元的罚款，相关行为包括未执行适当的反洗钱/反恐融资政策和程序、未对反洗钱/反恐融资控制措施进行独立审计以及未核实财富来源或客户关系相关信息。

<sup>[2]</sup> “金融科技”是指旨在支持、改善和推进银行和金融服务的科技解决方案。



## 司法管辖区：日本



### 关键法规更新

日本金融厅 (JFSA) 公布关于部分修订《反洗钱和反恐融资措施指南 (Guidelines on Measures against Money Laundering and the Financing of Terrorism)》的意见征集结果，并且发布修订后的指南。<sup>20</sup>主要更新内容包括：

1. 鉴于恐怖主义威胁正在跨国界蔓延，为金融机构建立有效的控制环境至关重要；
2. 针对常见客户类型开展风险评估，酌情针对所有客户开展风险评估并且采取缓释措施；
3. 在进行境外汇款时注意进出口交易可能涉及转移犯罪收益以及买卖毒品和用于军事用途的货物。

JFSA还在考虑为本地银行打击洗钱活动开发联合系统，该系统将使用人工智能评估客户风险并且根据制裁清单进行审查。<sup>21</sup>

此外，JFSA宣布在转移加密资产时必须告知加密资产的来源地和目的地信息 (数据转移规则)，<sup>22</sup>并且要求日本虚拟和加密资产交易所协会 (JVCEA) 全面宣传配套系统。



### 执法行动

JFSA对某加密支付平台提供商的以下违规行为采取行政行动 (称为“业务整改命令”)，包括：

- 违反《报告收集命令 (The Order for Collection of Reports)》；
- 违反《犯罪收益转移防止法 (Act on Prevention of Transfer of Criminal Proceeds)》(2007年第22号法案) 第4条和第6条；
- 未根据《反洗钱和反恐融资措施指南》制定充分措施。

业务整改命令要求该公司向JFSA提交业务整改计划，并且建立反洗钱/反恐融资风险管理系统，确保交易确认和记录可在一小时内完成。



司法管辖区：中国台湾



关键法规更新

从“强化后续程序”转变为“常规后续程序”之后，台湾与香港、澳门、印度尼西亚和库克群岛属于相同监管类别，并且可以降低向亚太反洗钱组织 (APG) 提供报告的水平 and 频率。<sup>23</sup>

评级变化的关键在于台湾立法院针对《洗钱防制法 (Money Laundering Control Act) 》(MLCA) <sup>24</sup>进行的一系列修订——在2018年将“虚拟货币平台业务运营和货币交易”纳入监管范围，这为台湾建立虚拟银行许可框架以及在2020年下半年推出虚拟银行奠定了基础。<sup>25</sup>

近年来，台湾已采取措施全面改进反洗钱制度，因此2019年底其在关键区域监管机构 (APG) 中的排名有所提高。



执法行动

在过去几个月中，台湾金融监督管理委员会 (FSC) 已对某些本地银行的行为风险和内部欺诈行为处以超过7,200万新台币的罚款。





## 司法管辖区：印度



### 关键法规更新

随着科技应用日益广泛、支付产品不断推出以及非金融机构的数量持续增加，支付系统领域实现快速发展，印度储备银行 (RBI) 推出一系列变革以改进网络安全和金融犯罪监管框架，包括：

- 更新《数字支付安全控制主指令 (Master Direction on Digital Payments Security Controls)》<sup>26</sup> (2021年8月生效)。为受监管实体建立完善的治理结构以及实施数字支付产品和服务安全控制的通用最低标准提供指导。
- 在住房金融公司的监管权移交至RBI之后，将《客户尽职调查主指令 (Master Direction – Know Your Customer Direction)》<sup>27</sup> (2016年发布) 的适用范围扩大到所有住房金融公司 (2020年5月19日生效)。该主指令包括客户尽职调查、反洗钱和反恐融资相关指令，适用于受RBI监管的所有实体。根据2020年12月发布的修正案<sup>28</sup>，法人实体纳入适用范围，并且受监管实体需要将2021年4月1日或之后所开立法实体的客户尽职调查数据上传至中央KYC登记处。根据2021年5月10日发布的修正案<sup>29</sup>，RBI规定受监管实体在基于视频的客户识别流程的基础设施、程序、记录和数据管理方面必须遵守修订后的最低标准。此外，该修正案限制在（非面对面）线上客户尽职调查中使用基于密码的一次性验证。
- 2020年3月更新《支付聚合服务提供商和支付网关运营商监管指南 (Guidelines on Regulation of Payment Aggregators and Payment Gateways)》<sup>30</sup> (2020年4月1日生效)。该指南修改了“中介机构电子支付账户开立和运营以及支付结算指令”（最初属于第DPSS.CO.PD.No.1102/02.14.08/2009-10号通知 (2009年11月24日) 的一部分内容)。修订后的指南包括RBI针对反洗钱/反恐融资法规所含客户尽职调查要求、欺诈预防和风险管理框架以及信息技术系统、信息安全治理和数据安全要求相关安全建议的最新指导。
- 修订《2007年支付与结算系统法案 (Payment and Settlement Systems Act, 2007)》第30条和第31条的框架内容。修订后的框架<sup>31</sup> (2020年1月更新《2007年支付与结算系统法案》) 依然以决策过程的客观性和透明度为中心。



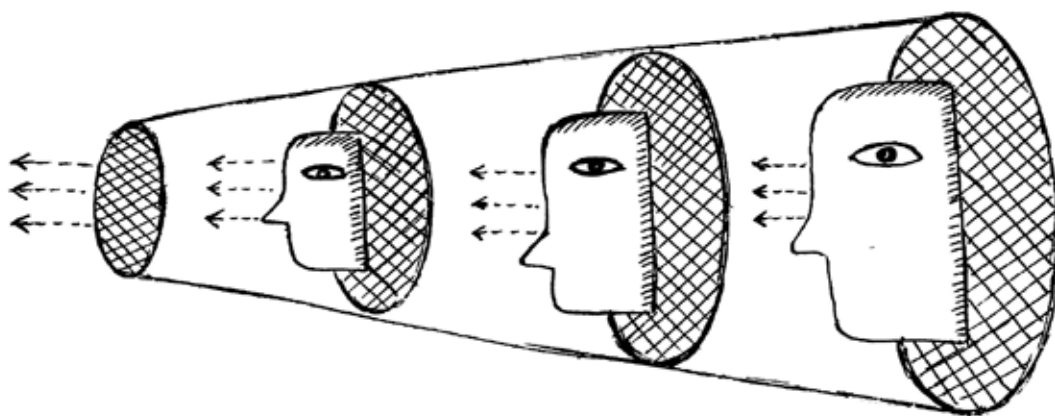
### 执法行动

在过去12-18个月中，RBI执法部门对几家银行和非银行金融机构违反反洗钱/反恐融资监管要求的行为处以超过2,300万印度卢比的罚款。

# 科技应用助力打击金融犯罪



我们将在本章阐述可以用于打击金融犯罪的现有和新兴关键技术。某些技术可能存在一定程度的重叠，或可相互补充并提高各自的效率。在某些情况下，金融机构可以利用监管科技解决方案组合改进金融犯罪风险管理流程，从而获得显著收益。





机器学习

机器学习属于人工智能范畴，可以持续改进模型，从而有效捕捉在规则导向型方法下几乎不可能有效编码的犯罪行为。通过不断接触数据点，机器“学会”理解数据中的模式或除预定义编码之外的任务，因此可对大型复杂数据集进行更加准确的预测分析。这主要得益于机器快速适应新威胁和新方法的能力。机器学习尤其适用于洗钱/恐怖融资交易监测，原因在于其可针对犯罪行为“做出判断”，从而提高风险评估准确性并且降低误报风险（向团队发出注意可疑不当行为的错误提醒）。



人工智能

人工智能可以模拟人类认知并且承担相对复杂的推理和决策任务。人工智能可以帮助实现业务流程自动化、检测犯罪行为模式、生成洞察并且通过日常沟通推动客户和员工参与。该项技术主要用于改进客户尽职调查流程（加快流程速度并且生成更加准确的反洗钱数据），从而助力金融机构开展全面风险评估。



自然语言处理

自然语言处理同样属于人工智能范畴，可以帮助系统识别和解读人类语言的含义。自然语言处理可以助力机器处理和“理解”大量非结构化数据，例如新闻文章、电子邮件和社交媒体文章。从反洗钱/反恐融资角度来看，机器能够阅读和编辑个人或组织相关信息、考虑信息背景并且针对该个人或组织是否可疑“做出判断”。因此，自然语言处理可以通过自动生成使用标准术语和语言的报告来支持可疑活动报告和可疑交易报告流程，从而帮助金融机构减轻管理负担并且确保采用一致方法。此外，自然语言处理可为金融机构识别政治敏感人物和被制裁人员提供更加可靠的筛查解决方案。



### 机器人流程自动化

机器人流程自动化利用逻辑和结构化输入实现此前人工业务流程的自动化。机器人流程自动化软件可以捕捉、解读和处理数据，从而执行移动文件夹和文件、将数据复制粘贴到不同系统以及填写表单等操作。由于机器人流程自动化具有重复性、常规性和规则导向性特点，因此许多人工金融犯罪风险管理流程均可受益于机器人流程自动化的应用，包括姓名筛查、交易监测和可疑活动报告/可疑交易报告。此外，机器人流程自动化可以推动需要进行“综合推理”的复杂任务实现自动化，因此其与机器学习和自然语言处理等人工智能技术相结合时所发挥的效果尤为突出。



### 大数据/数据分析

大数据分析利用先进的诊断方法消化各种来源的大量数据，包括结构化和非结构化数据集。鉴于全球每天都会产生大量信息，因此大数据分析需求已变得愈发重要。作为分析的一部分，机器可以识别存在洗钱或恐怖融资风险的消费者行为模式和关系。



### 云计算

云计算可以在数据访问、整合、扩充和处理方面发挥作用，从而帮助金融机构提高灵活性并且显著降低运营成本。监管科技解决方案通常以云技术为基础。从反洗钱角度来看，云计算可以在不影响数据可访问性或数据质量的情况下助力整合来自不同来源的大量数据，因此尤其适用于通过识别资产受益人等方式开展客户尽职调查分析。

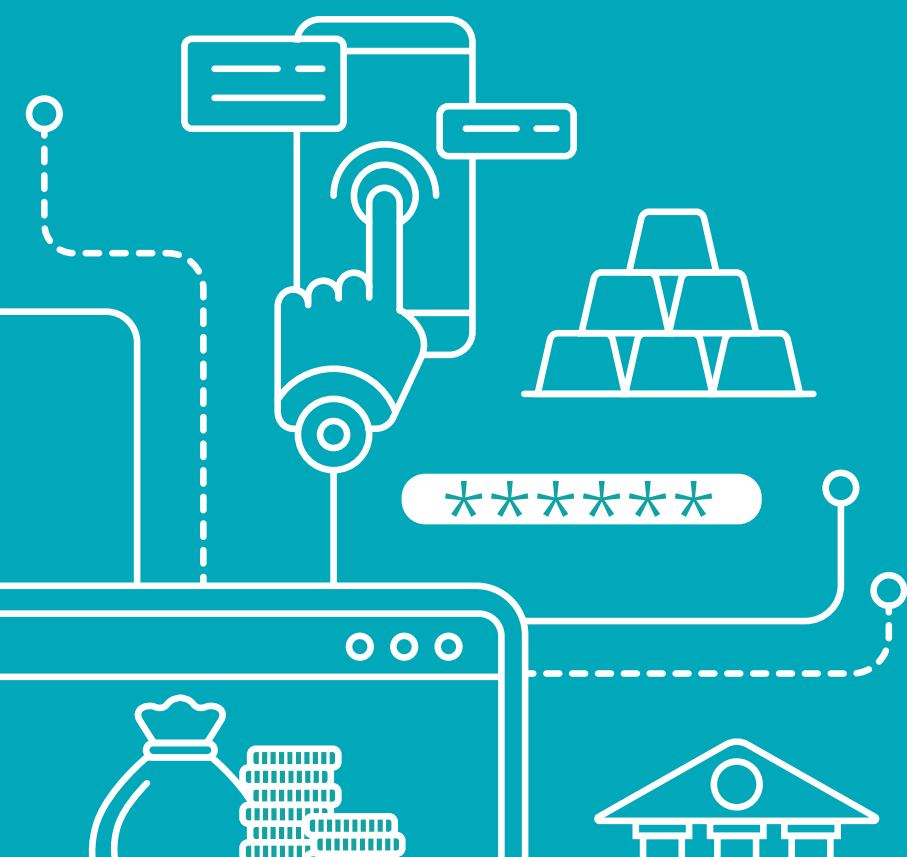


### 隐私增强技术

隐私增强技术可以帮助用户分析在安全环境中保存的数据，并且生成不泄露任何敏感信息的报告和分析结果。某些企业已经利用该项技术实现集团内部实体之间的信息共享，但是该项技术亦可显著提高在更广范围内进行信息共享的有效性。隐私增强技术可以改善金融机构（私人对私人）、金融机构与反洗钱/反恐融资监管机构（私人对公共）以及国家、国际和超国家层面监管制度（公共对公共）之间的信息共享，从而助力信息获取并且支持金融犯罪风险情报相关合作。

# 科技解决方案案例研究精选

我们将在本章介绍五个案例，以此说明如何利用监管科技解决方案改进金融犯罪风险管理计划。这些案例均为德勤曾提供支持的项目，旨在强调无论金融机构的规模、复杂程度、资源配置以及对于探索性解决方案的需求如何，科技应用均可创造价值。



## 案例一



案例一<sup>[3]</sup>是一家大型国际银行的香港子公司，业务遍及亚太地区多个司法管辖区，提供包括零售产品在内的广泛金融类服务。该行十多年来在反洗钱和反恐融资技术驱动型解决方案的开发和应用方面始终处于领先地位，是监管科技的早期采用者。本案例探讨了人工智能辅助机器学习和自然语言处理工具在该行姓名筛查流程中的应用，该流程旨在针对新客户开展尽职调查以及针对现有客户进行定期审查。



## 关键挑战

应用监管科技解决方案之前，该行的姓名筛查流程属于劳动密集型流程，需要300多名分析人员进行人工干预。随着观察名单和客户数量逐年增加，流程负担越来越重，因此造成运营成本上升以及出错风险增加。传统的规则导向型姓名筛查系统会产生大量告警（其中许多告警后来被认定为“误报”），导致过度紧张的分析人员难以彻底审查和清除告警，并且可能忽视关键数据点或无法完整或妥善记录调查信息。

该行力求大幅减少清除告警所需的人工干预，同时维持严格的控制标准。该行希望开发完全自动化的解决方案，不仅可为告警“打分”（基于潜在犯罪行为的可能性），而且可就升级或结束案件提出人工智能生成的合理建议。



## 解决方案

获得高管层的支持之后，该行组建多元化的跨职能团队，负责开发监管科技解决方案。团队包括金融犯罪、合规、风险和技术领域专家以及该行业务和产品运营部门代表。经过对可用技术和技术供应商的详细考量，该行决定与一家专门从事基于机器学习的反洗钱/反恐融资应用的第三方供应商合作开发解决方案。传统姓名筛查系统的告警数据（包括分析人员在审查过程中做出的决策）已被用于“训练”机器学习模型。这种“训练”重复多次之后，机器学习模型开始产生可喜成果并且进入内部概念验证阶段。

随着概念验证取得成功，人工智能可以在无需人工干预的情况下处理超过25%的告警，并为决策过程提供充分“依据”。在与第三方供应商开展合作一年之后，该行进入产出阶段，可为支持监管科技解决方案开发和重建内部系统和控制并且在某些复杂市场中开展全面测试。



人工智能



机器学习



自然语言处理



机器人流程自动化

<sup>[3]</sup>本案例刊载于香港金融管理局在2021年1月与德勤合作撰写的题为《反洗钱合规科技：案例研究与见解 (AML/CFT RegTech: Case Studies and Insights)》的报告中。



实施障碍

虽然该行在实施过程中并未遇到重大挫折，但是确实需要应对一些挑战。鉴于项目规模较大，该行无法在市场找到可以满足其所有标准的现成解决方案。因此，该行花费大量时间寻找合适的第三方供应商来共同开发解决方案，并且投入大量精力和资源进行模型开发和测试。

解决方案缺乏“追踪记录”以及现有系统较为复杂也导致该行需要花费大量时间更新内部系统和控制以及开展严格测试。从与第三方供应商合作到进入产出阶段，该行总共耗时约12个月完成项目。



战略影响

尽管实施过程十分漫长，但是该行采用的全面方法以及开展的严格测试已帮助内外部利益相关方（包括监管机构）建立信心。

基于机器学习的姓名筛查解决方案的主要优势在于其可显著提高调查效率，将需要人工干预的告警数量平均减少35%（在某些司法管辖区甚至达到50%）；同时亦可简化审查流程，让分析人员更加聚焦那些真正标记告警而需要审查的案例。



## 案例二



案例二是一家新加坡银行，其在亚洲拥有大量业务，提供包括银行、投资和资产管理在内的广泛服务。该行是监管科技的积极倡导者，一直致力于在亚洲地区培育金融科技初创企业并且助其实现加速发展。本案例探讨了在该行的端到端“反洗钱组件 (AMLS)”集成解决方案中如何利用机器人流程自动化、人工智能辅助机器学习和自然语言处理技术改进交易监测和姓名筛查告警流程。从启动阶段到“业务运行”阶段，该项目历时近三年时间。



## 关键挑战

该行在姓名筛查和交易监测方面拥有规则导向型反洗钱和反恐融资系统。与所有规则导向型系统一样，尽管该行已经采取优化措施，但是考虑到该行的交易量和交易速度，仍有大量“误报”情况出现。

该行希望利用创新和前瞻性提高效率 and 效益。这也可简化相关反洗钱流程以及借助人工智能、机器学习和机器人流程自动化技术关注重大风险提供机会。

该行合规团队和数据管理办公室与技术供应商的金融科技数据科学家密切合作，共同设计、开发、分析和部署该行反洗钱框架中的四大关键流程模块（客户尽职调查、交易监测、姓名筛查和付款筛查）。最终，该行针对交易监测和姓名筛查推出AMLS集成解决方案——结合有监督和无监督机器学习技术的端到端系统，可以提高可疑活动和高风险客户检测速度和准确性。

该行致力优化交易监测流程模块中的全新、未知可疑模式检测功能，同时确保姓名筛查流程模块能够处理更多复杂姓名组合，并且可以利用增强“推理”功能和附加客户信息标识符减少未确定告警的数量。新规范与先进机器学习技术的结合显著提高了标记告警的准确性。



## 解决方案

在对潜在选择进行战略评估之后，该行决定与一家新加坡监管科技公司合作开发可承载反洗钱技术、工具和系统的人工智能驱动单一集成平台。该行与技术供应商合作设计机器人流程自动化与机器学习技术结合的解决方案，旨在补充和改进该行的现有系统，并且共同开发监管科技模型风险管理和治理框架，以此支持技术风险管理、确保妥善使用技术并且验证已开发模型。

此外，该行还利用机器人流程自动化和自然语言处理技术自动生成可疑活动报告。对于每次告警，机器人流程自动化技术会从不同系统中提取客户信息和交易数据，然后使用自然语言处理技术生成的额外数据点以及客户资金流动的可视化图表充实此类数据。



人工智能



机器学习



自然语言处理



大数据/数据分析



机器人流程自动化



云计算

2018年,该行针对AMLS解决方案进行概念验证并且取得重要成果——交易监测流程方面,报警准确率提高5%,误报率下降40%;姓名筛查流程方面,针对个人的误报率下降60%,针对企业的误报率下降50%。

随着试点项目取得成功,该行于2019年进入“技术运行”阶段,并且开始在常规业务职能中部署模型。该行在此阶段继续进行模型测试和开发,促使交易监测流程误报率以及针对个人和企业的姓名筛查流程误报率进一步下降10%。

最后,在该行建立完善的治理框架和低价值告警管理框架并对其进行测试和验证之后,AMLS解决方案已于2020年10月进入“业务运行”阶段。



### 实施障碍

考虑到该行的愿景及其致力于开发优质、耐用和可扩展产品的承诺,该行投入大量时间(近三年)和资源进行工具开发、测试和验证。

在概念验证阶段,该行数据管理办公室开展了严格的内部验证,并且通过对试点项目及其方法的独立评估进一步证实了内部验证“符合要求”。评估内容包括与规则导向型监测流程进行详细比较以及针对机器学习模型和AMLS解决方案进行压力测试,以此确保二者能够处理各类反洗钱合规案件。

随后,该行数据管理办公室在“技术运行”阶段多次重复上述验证,并在进入“业务运行”阶段之前进行额外的独立评估和模型验证。

此外,该行还投入大量时间开发针对监管科技的人工智能和机器学习模型管理框架,以此指导治理和模型架构的关键环节,从而确保模型的准确性和稳定性。



### 战略影响

在实施人工智能和机器学习模型之后,该行的交易监测和姓名筛查告警管理效率有所提高。“业务运行”阶段结束之后,姓名筛查模型在“技术运行”阶段建立的预测边界内继续运行,因此“误报”结果显著减少。其他优势包括:

- 显著降低错误率(由于实现人工输入的自动化);
- 减少分析人员在输入信息、审查告警和生成报告方面所需的工时,并将工时重新分配给价值更高的工作;
- 改善合规性,提高可审计性;
- 规范交易监测流程。

该行计划通过向数据库中添加新的交易数据来继续优化AMLS机器学习算法,并且希望未来可在整个反洗钱框架中实施AMLS解决方案。

### 案例三



案例三是越南的一家大型贷款机构。该行现有的反洗钱、欺诈检测和交易监测流程均为规则导向型流程，并且与各业务线系统的集成程度不同。此外，规则本身可能存在较高的错误率，因为规则是由专业知识推导而来。因此，该行计划采用更加全面的集成解决方案，旨在利用机器学习和情景分析技术改进规则导向型监测。截至本报告发布时，该项目仍在进行中。



#### 关键挑战

目前，该行的反洗钱和欺诈检测控制框架正面临诸多挑战，并且控制环境中存在多个待改进领域。例如，员工可以绕过人工控制或未嵌入系统解决方案（即端到端视图）中的控制措施。此外，缺少数据和深度模型已经造成“误报”结果。



#### 解决方案

该项目分为两个阶段。第一阶段目前正在进行——开展差距分析，将该行的现有能力与反洗钱和欺诈风险方面的国际标准和实践进行比较，例如特雷德韦委员会赞助组织委员会（COSO）欺诈风险管理指南<sup>32</sup>以及《AS 8001-2008澳大利亚欺诈和腐败控制标准》<sup>33</sup>。该行将会根据差距分析结果制定第二阶段行动计划。

经过初步评估，该行目前正在考虑利用机器学习和情景分析技术支持规则导向型分析，同时完善反洗钱和欺诈检测平台。新平台将会采用可以根据该行需求进行定制的先进技术，以此帮助该行全面了解（实时和批量）所有交易和活动的欺诈风险检测情况。此外，具有精确测试参数的机器学习模型将会提供更加稳健的统计基础，以此应对错误率较高的风险。



#### 实施障碍

如今，该行正在致力于利用新技术推动创新。截至目前，该行未遇到明显的实施障碍，该项目仍在进行中。

项目时间表和预期资源需求将主要取决于差距分析结果（目前正在进行）。然而，该行在与不同系统供应商接触以开发最符合需求的解决方案时或将面临某些挑战。这项工作可能影响该行诸多部门，并且涉及众多内外部利益相关方。因此，该行正在准备采取综合治理和执行方法，以此确保该项目取得成功。



#### 战略影响

该行希望利用机器学习技术改进现有方法。其所实施的端到端解决方案将会提高欺诈检测效率和准确性并且降低人力成本。此外，此项解决方案应当全面了解金融活动和客户风险以便为决策制定提供依据，同时确保潜在洗钱行为检测和调查的透明度。



案例四



案例四是一家总部位于中国的全球领先银行，在几十家一级分支机构（即位于主要城市的分支机构）拥有近十几个业务部门。本案例展示了利用现有技术（包括建模、数据分析和可视化）针对洗钱和恐怖融资风险开展企业范围风险评估（EWRA）的可能性。该行结合使用前端可视化技术和后端服务器支持EWRA解决方案。



关键挑战

中国人民银行反洗钱局提出的特定监管期望推动该行开展监管科技项目。人民银行要求金融机构针对洗钱和恐怖融资风险开展EWAR/机构风险评估（IRA）（视机构规模而定），并且涵盖所有分支机构、子公司、客户、产品和服务。所有洗钱和恐怖融资风险必须纳入考虑范围，金融机构的决策流程和治理框架以及基础方法必须明确记录。此外，人民银行期望金融机构继续改进EWAR/IRA流程。

开展全面评估之后，该行发现原有数据和流程中存在许多缺口。虽然该行已经建立洗钱和恐怖融资风险检测流程，但并不清楚如何开展EWAR/IRA，包括哪些数据应当输入新系统以确保模型正常运行以及如何证明计算算法的科学合理性以获得监管机构的批准。该行不仅需要提高现有数据的数量和质量以增强其准确标记客户和交易的能力，同时需要开发在组织内部确定异常值以及剩余洗钱和恐怖融资风险的能力。此外，为充分满足人民银行的预期，该行希望EWRA解决方案能够支持方法和流程的持续改进。



解决方案

该行投入一年半时间开发可以用于开展EWAR的定制系统。总体解决方案由前端分析工具和后端服务器组成，前者可以提供单个组件和合并视图的可视化，后者可以支持数据存储和处理。此项解决方案依赖以多项因素为基础的风险指标和分析技术，包括客户所处行业、地理位置、产品、渠道、固有风险计算逻辑、控制有效性和剩余风险。

新系统可以通过向EWRA引擎不断输入数据来推动方法的持续改进——使用索引技术追踪数百个评估单位的迭代数据提取过程，同时保留变更记录并且利用数据的横向和纵向验证逐步提高数据准确性。此外，近乎实时的数据可用性和数据更新可以推动管理评估和响应快速完成。

EWAR解决方案可以帮助该行了解组织内部的洗钱和反恐融资风险并且提高风险管理效率和效益。此外，新系统可就分析和决策过程为用户提供完整准确的审计跟踪。



### 实施障碍

该项目规模庞大，涉及千余名参与者并且历时一年半时间完成。由于综合模型和引擎后端逻辑较为复杂，因此该行需要投入大量时间和精力帮助相关人员了解模型的细微差别，同时确保选择适当的参数和数据输入。在整个项目过程中，该行持续开展培训和宣传活动，主动发现上述问题并且采取相关补救措施，符合中国人民银行的期望。



### 战略影响

自2019年开始实施以来，EWAR解决方案已经帮助该行显著提高洗钱和恐怖融资风险评估效率和效益并且确保金融资源得到最合理的配置。该行目前能够针对上百个评估单位（一级分支机构的业务部门）开展EWAR。在已经收集上万个固有风险数据点和上万个控制措施有效性自我评估分数。随着推广工作取得成功，该行正在计划将EWAR解决方案的实施范围扩大到本地子公司以及海外子公司和分支机构。

由于对该项目兴趣较大，监管机构在整个开发和实施阶段不断了解项目情况并且提供相关意见。因此，该行仅需根据法人金融机构洗钱和恐怖融资风险自评估指引（银反洗发[2021]1号）对方法和系统做出较小限度的更新。

## 案例五



案例五[4]是一家大型外资银行的香港子公司，提供包括资产管理、财富管理和投资银行在内的众多服务。本案例探讨了一个为期两年的大型项目——利用云计算、数据分析和数据存储技术升级该行的金融犯罪数据基础设施。总体而言，该行采用监管科技解决方案已经超过五年，并且未来将会继续如此，力求实现技术基础设施的现代化和标准化。



## 关键挑战

该行的数据基础设施大多较为分散和孤立。反洗钱和反恐融资流程（例如负面新闻搜索、交易监测和姓名筛查）主要依赖来自众多系统的客户信息和交易数据。这就导致运营效率大幅降低，数据整合和数据质量出现问题，成本随着客户和交易量的增加而不断增长以及金融犯罪调查和报告方面的期望持续提高。此外，该行收到的特别和独立数据请求越来越多，需要大量人工处理。例如，特别报告团队通常需要两周或更长时间来为香港特别行政区联合财富情报组（JFIU）编制报告。

因此，该行开始整合、规范、改进反洗钱和反恐融资相关数据的收集和存储方式。该行希望确保分析人员能够直接访问数据，从而简化特别报告编制流程，提高数据提取效率。此外，该行计划利用合并数据集开发主动调查可疑客户群体的能力。



## 解决方案

该行决定重点关注数据收集、数据完整性和数据访问，以此全面升级数据基础设施。此项解决方案包括创建单一综合数据存储库。数据存储库可以汇集超过80亿个数据点并将其直接输入该行的反洗钱/反恐融资控制系统，同时为最终用户提供近乎实时的直接数据访问权限。该项目规模较大，总共历时两年时间完成。

监管科技解决方案可以帮助反洗钱/反恐融资和FIU分析团队有效编制特别报告，同时确保反洗钱/反恐融资专家能够从存储库中直接提取数据并且进行数据分析审查，即“纵览”工作。在此过程中，反洗钱/反恐融资专家将会根据FIU调查确定的风险模式开展数据分析，以此确定是否存在预示其他客户群体可能存在犯罪活动的类似模式。



大数据/数据分析



云计算

[4] 本案例刊载于香港金融管理局在2021年1月与德勤合作撰写的题为《反洗钱合规科技：案例研究与见解（AML/CFT RegTech: Case Studies and Insights）》的报告中。



### 实施障碍

该行面临的最大的挑战在于如何定位多个系统的数据并将其整合到综合数据存储库中。事实上，数据获取、清理和整合是两年开发周期中的最大驱动因素。



### 战略影响

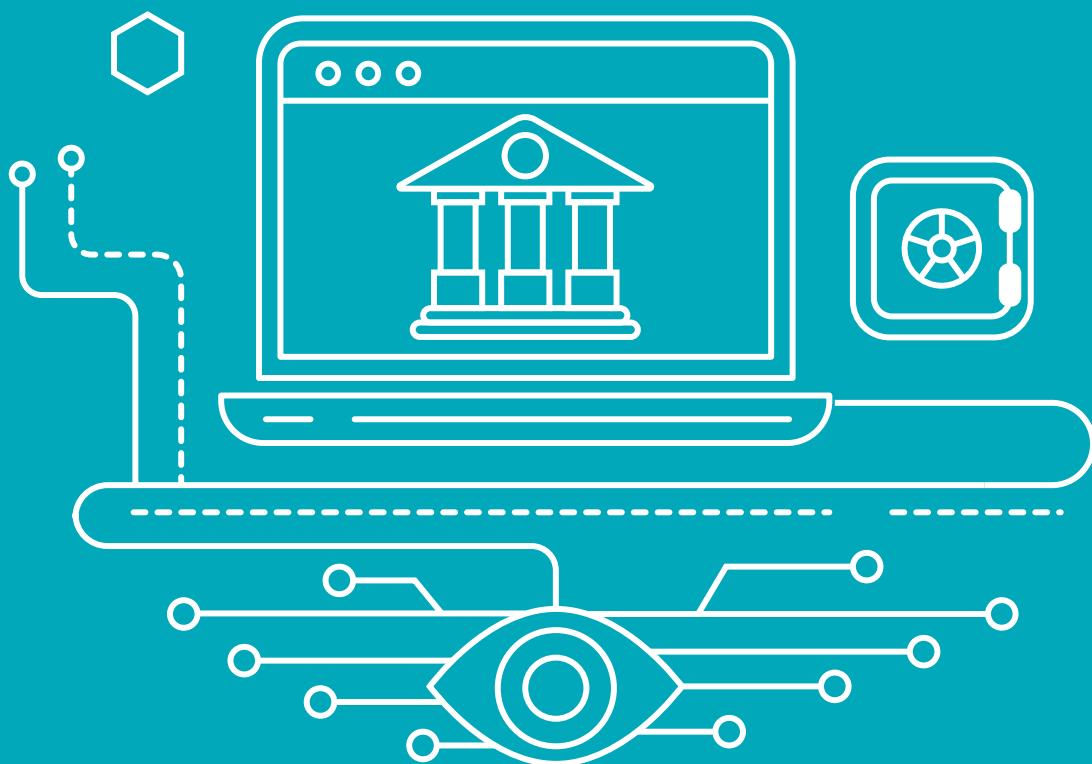
创建可以提供近乎实时的数据访问权限的单一综合数据存储库可以显著提高数据报告效率，并将编制特别报告所需的时间从几周缩短至几天。

此外，这将帮助分析人员开展具有前瞻性的详细数据分析，以此识别不同客户群体的潜在犯罪活动。例如，该行在存储库上线后开展了三次“纵览”工作，在存储库上线后的18个月内对客户和交易数据进行了十次详细审查。评估结果导致出现若干次需要向JFIU上报以及向执法部门提交可疑交易报告的情况。

该行的聚合数据存储功能也为开发更加先进的人工智能驱动技术奠定了坚实基础。例如，该行目前正在开发基于机器学习的新闻和姓名筛查应用以及网络分析工具，该行希望这将有助于评估客户实体之间的未披露或不明显关系，从而加强JFIU调查。

# 案例研究 重要启示

我们可以从案例研究以及我们在亚太地区支持金融机构采用监管科技解决方案的综合经验中收获重要启示。





评估数据质量和准备情况

在开发和实施监管科技工具的过程中，数据问题通常构成重大（甚至最大）挑战。金融机构不应低估识别、获取、处理、转换和解读数据所需的时间和精力。金融机构时常为数据质量问题所困扰，而数据完整性和数据有效性往往才是监管科技应用的主要阻碍。此外，监管科技解决方案有时需要不易获取的数据，因此金融机构需要投入大量时间和成本开展修复工作。

开始实施监管科技解决方案之前，金融机构必须全面了解相关数据要求和潜在数据障碍。“错进则错出”，金融机构必须确保数据的完整性、相关性和多样性，并且充分解决数据偏差问题。然而，金融机构不应追求完美数据，管理层则应了解并认识到监管科技应用过程中的局限性。

了解自身系统

对于许多金融机构而言，操作系统和数据质量问题密切相关。事实上，梳理现有系统和流程对于存在收购遗留问题的大型金融机构而言极具挑战。但是所有金融机构都需要了解其现有系统如何运作以及对于监管科技应用有何影响。在设计监管科技解决方案时，金融机构必须决定是否取代、集成亦或绕开现有系统。

这主要取决于项目规模以及金融机构的短期、中期和长期目标愿景。开展技术基础设施或系统变革或将为金融机构带来普遍利好，但是需要大量的前期成本、资源和时间投入。

确保合规性

了解所有市场在数据共享、数据本地化、数据处理和数据隐私相关监管要求方面的差异将成为金融机构开展项目的核心原则。相比专项部署计划，涉及多个司法辖区的大型项目将会更早面临相关挑战。

金融机构需要在扩大规模和/或扩展业务的过程中考虑其长期愿景，并且在满足适用监管要求的同时保持足够的灵活性和敏捷性。例如，管理层应当考虑开展定期审计和审查，以此识别非预期结果并采取相应行动。

建立完善的治理框架

金融机构必须明确从启动、实施到实施后审查流程中的监管科技解决方案管理和风险管理相关角色与职责。由于解决方案可能涉及众多利益相关方以及现有流程、系统和数据，因此适当的治理和支持对于成功实施解决方案至关重要。

严格的管理将确保金融机构充分了解其解决方案和相关模型，这对其与利益相关方（例如董事会或监管机构）接洽至关重要。最后，金融机构应当持续监测模型结果，确保模型始终在所需参数范围内运行并且符合要求，同时记录并储存模型变更相关信息，以备审计之用。

寻求利益相关方支持

在反洗钱/反恐融资监管科技解决方案的设计、测试和实施过程中，获得高管支持有助于建立可信度，避免孤岛现象并且确保项目方法和成果符合预期。

除此之外，金融机构亦需确保外部利益相关方（尤其是监管机构）了解并支持监管科技应用。与监管机构开展合作还可以带来其他收益，例如其可根据与其他金融机构和/或监管机构的对话得出宝贵见解。

与监管科技的早期采用者相比，这对处于技术转型初期的金融机构而言更具挑战。金融机构必须与内部利益相关方建立良好关系，使其充分了解组织的反洗钱/反恐融资流程和控制措施以及监管科技应用的潜在优势，从而推动内部利益相关方在与高管讨论反洗钱/反恐融资监管科技应用时成为监管科技的积极倡导者。

综上所述，金融机构必须设定明确愿景，并且在科技环境不断变化的情况下保持灵活性和敏捷性。

组建跨职能和跨区域的多元化团队

在实施监管科技解决方案时，金融机构必须组建跨职能和跨区域的多元化团队，其中包括金融犯罪、合规、风险和技术领域专家与数据科学家以及银行业务和运营部门代表。多元化团队可以提高项目效率（就时间和成本而言），确定潜在障碍并且采取补救措施，支持针对第三方供应商的全面评估，确保项目获得支持，同时识别向其他领域部署监管科技解决方案的交叉机遇。

此外，大型国际金融机构可以打造共享平台，推动与反洗钱/反恐融资监管科技应用相关的理念、知识和经验在不同企业与地区之间实现共享。

### 全面审查第三方供应商

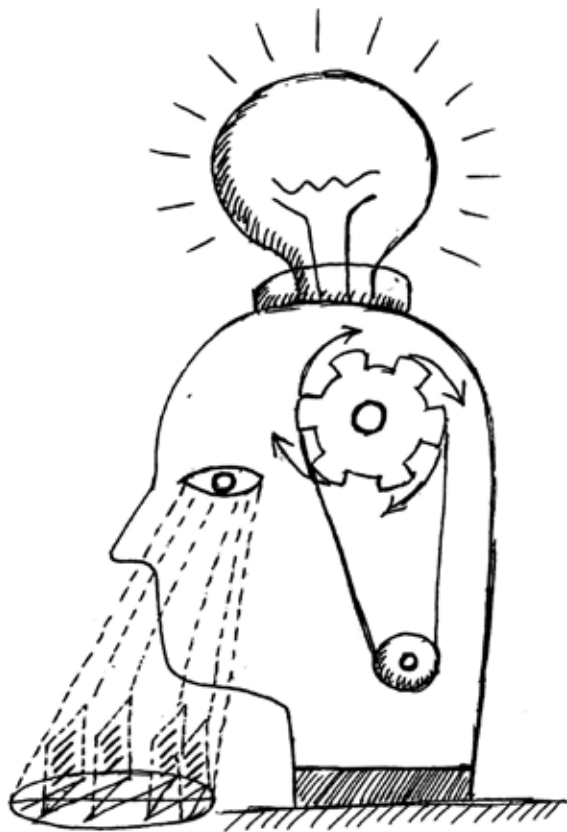
在开发监管科技解决方案时，合适的第三方供应商可以带来丰富的经验和技術知识，但这并非毫无风险。金融机构需要评估供应商的长期生存能力（特别是在需要供应商持续提供解决方案维护或更新服务的情况下），并且确定供应商的业务和产品规模与其系统和结构以及当前和预期项目规模是否适配。

与第三方供应商接洽或合作开发解决方案之前，金融机构还需要考虑知识产权所有权相关事宜，同时确保供应商根据不同司法管辖区的适用监管要求管理数据（必要时）。

### 提高知识水平

完成监管科技解决方案开发之后，金融机构必须确保其具备足够的专业知识，可以推进解决方案的有效应用和深入开发；并且拥有必要的专业资料，可就技术、功能、业务要求、结果、风险缓释方法、测试与保证以及灾难恢复进行解释说明。

此外，金融机构应当开展员工培训，帮助员工了解如何推动解决方案充分发挥作用，同时管理层也应充分了解解决方案，以便有效开展审查和质询工作。



# 科技管理 贯穿客户生命周期



## 科技应用贯穿客户生命周期

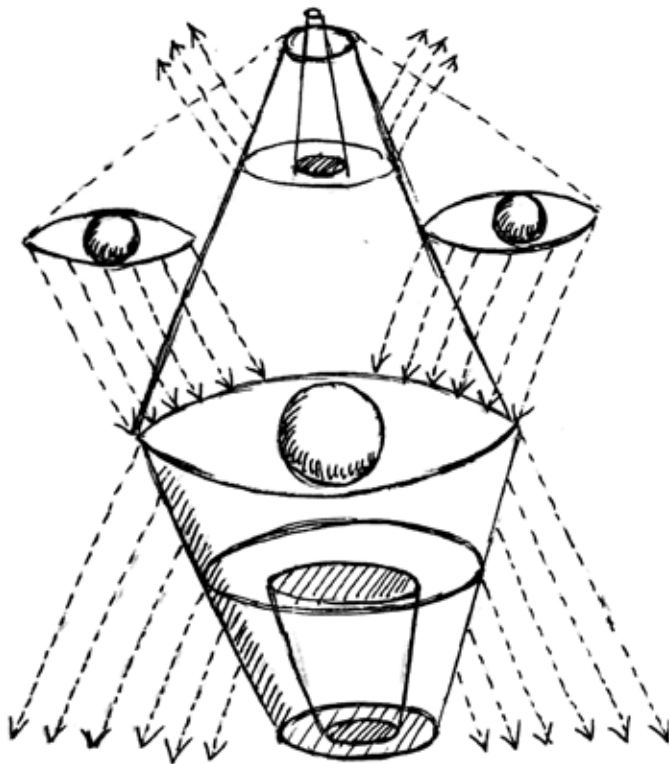
### 抓住创新机遇，利用科技全面打击金融犯罪

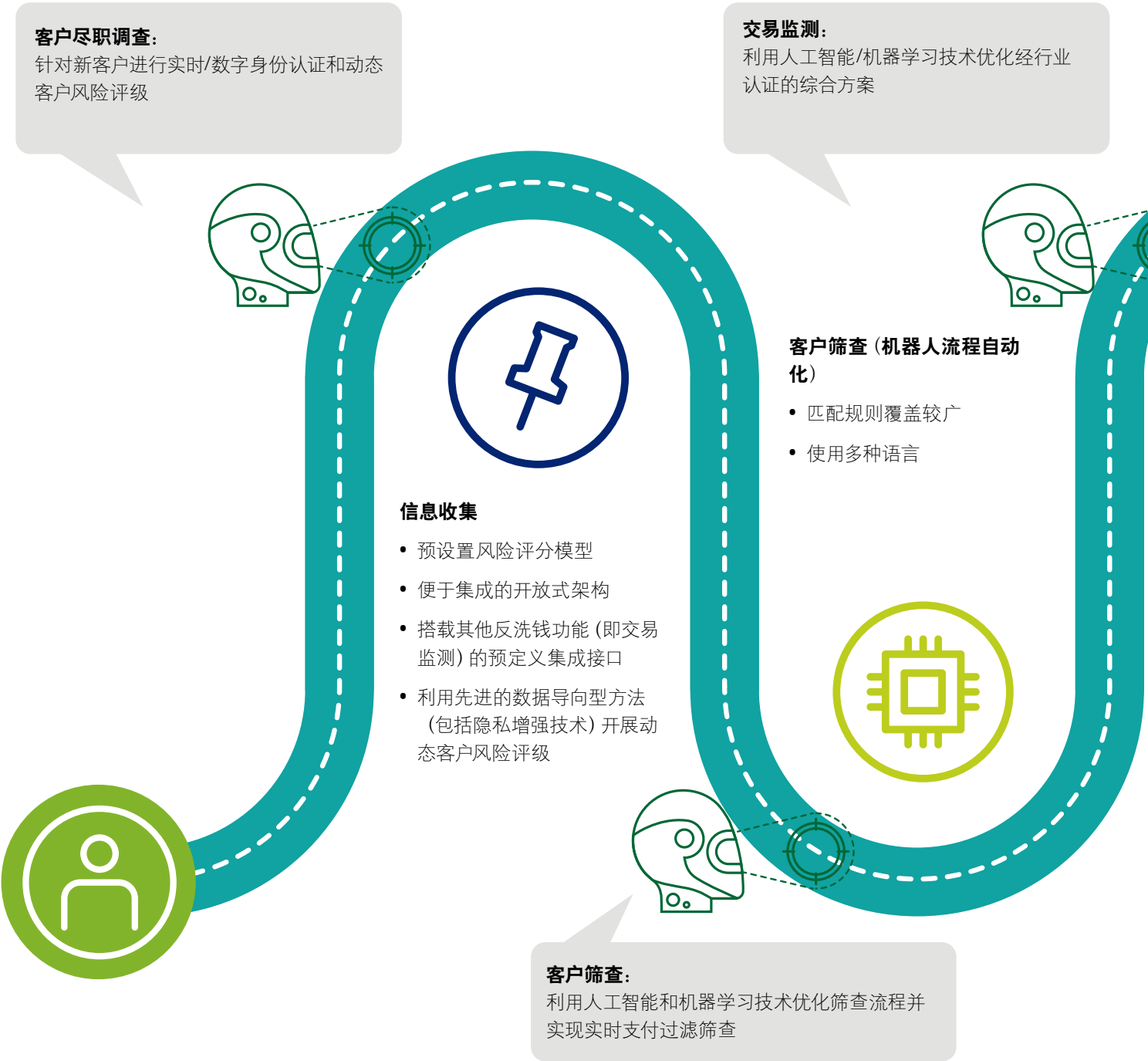
#### 新方法

为有效打击金融犯罪，金融机构应将科技应用贯穿整个客户生命周期。

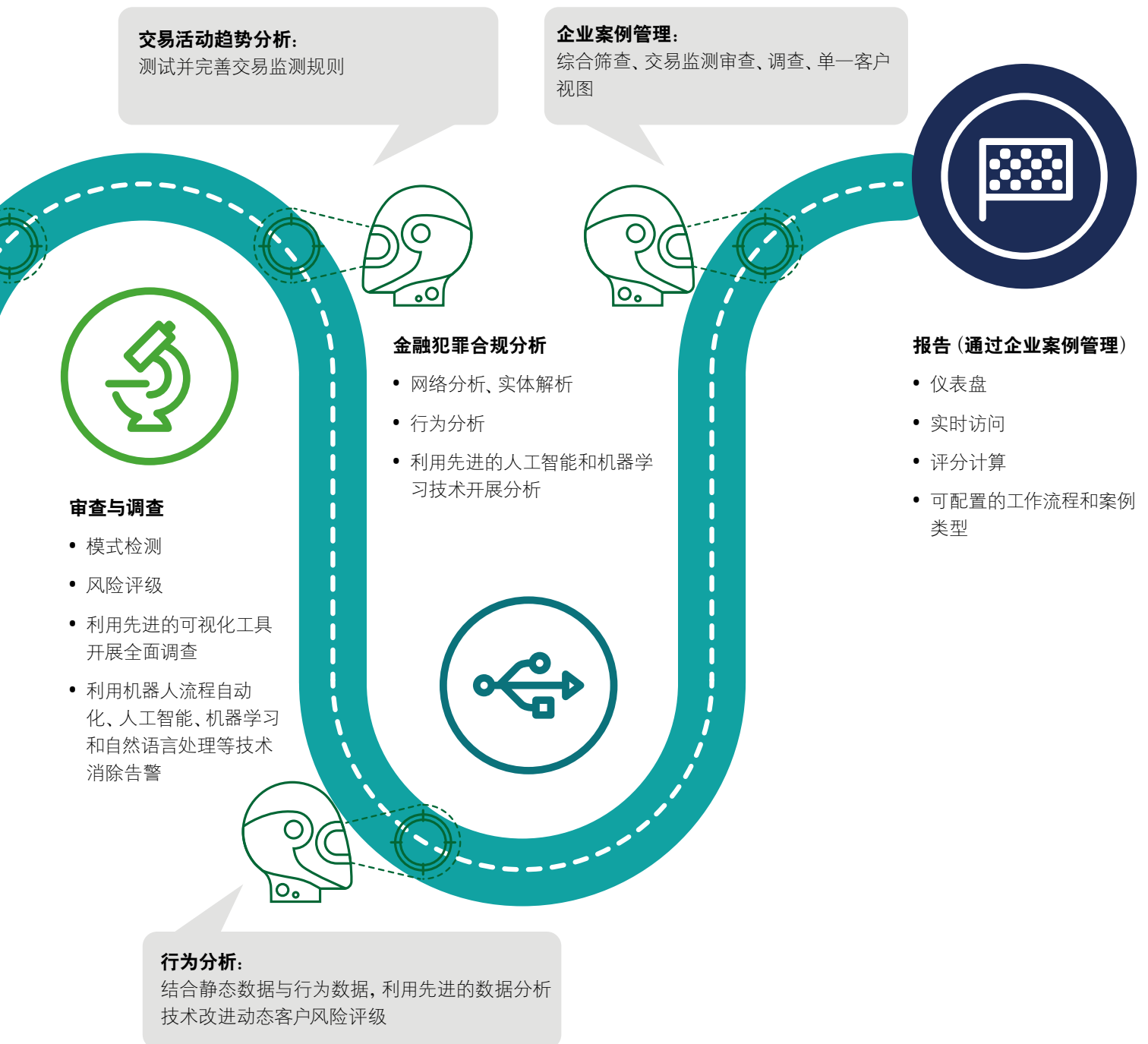
由于业务模式、基础设施和经费预算各不相同，金融机构不会采用相同技术，但是某些监管科技解决方案可以在结合使用时（例如人工智能和机器人流程自动化）以及在客户生命周期的特定环节中有效发挥作用。

云计算和大数据/数据分析等技术可以助力数据收集、整合和扩充，从而为客户生命周期各环节提供支持。此外，隐私增强技术等新兴技术或将显著提高金融机构的数据获取能力。











## 客户风险至关重要



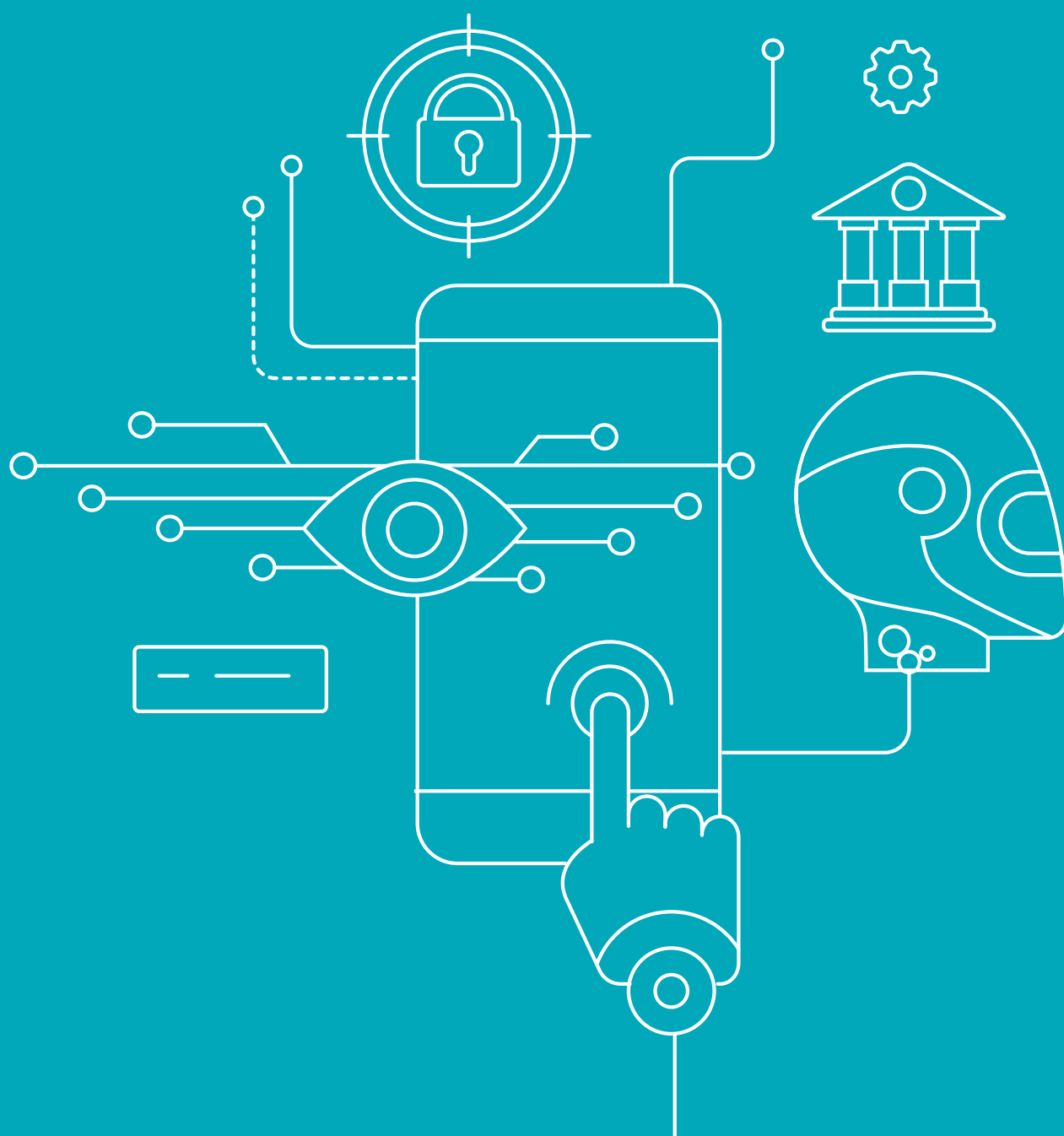
## 为全面管理金融犯罪风险奠定基础

部署科技解决方案  
下表旨在说明如何利用科技解决方案改进金融犯罪风险管理计划

| 案例  | 概述                           | 主要成果                                      | 技术类型   |
|-----|------------------------------|---|--|
| 案例一 | 改进姓名筛查流程                     | 需要人工干预的告警数量减少35%                          |       |
| 案例二 | 改进交易监测和姓名筛查告警流程，开发端到端“反洗钱套件” | 交易监测流程误报率下降50%，针对个人/企业的姓名筛查流程误报率下降70%/60% |    <br>  |
| 案例三 | 开展欺诈检测和交易监测流程转型              | 提高欺诈检测效率和准确性，降低人力成本                       |   |
| 案例四 | 开展企业范围风险评估                   | 收集20,000多个固有风险数据点和20,000多个控制自我评估分数        |    |
| 案例五 | 升级金融犯罪数据基础设施                 | 创建单一综合数据存储库，实现近乎实时的数据访问；显著缩短编制特别报告所需的时间   |     |



# 前景展望



## 01 开展全球合作与跨组织协作

洗钱和恐怖融资已形成全球产业链，犯罪分子在运用科技实施犯罪活动方面变得愈发熟练。因此，金融机构必须协同合作，提高信息透明度，确保针对数据和技术共享制定协调战略，同时严格管理数据隐私相关风险和法律法规。就此而言，科技进步或将助力实现上述目标，例如隐私增强技术可以确保用户在安全环境中分析数据，并且在不披露敏感信息的情况下提取数据。跨组织和跨区域的知识交流活动、论坛和委员会亦可支持行业共享成功实施监管科技解决方案所需的数据、工具和技术。信息共享可为行业提供更加全面的专业知识和情报，同时提高打击金融犯罪的效率和效益。在此方面，监管机构和国际组织可以发挥引导和推动作用。

## 02 积极预防新数字时代的金融犯罪

数字平台和数字银行的发展（在2020/2021年发展迅速）已使客户受益颇丰，但是加密货币、网上银行和电子支付等技术的匿名性和闪电般的交易速度也让犯罪分子有机可乘。通常情况下，当可疑交易被发现时，非法资金已经跨境转移，无法追回。但是先进的人工智能预测分析技术正使前瞻性犯罪预防变得更加可行。例如，情景分析和威胁建模可以帮助金融机构评估其反洗钱/反恐融资流程和系统中的薄弱环节，并且预先处理高风险问题。与此同时，技术还可用于行为分析，以此预测未来犯罪活动，帮助金融机构先发制人，始终走在犯罪分子之前。

## 03 关注客户生命周期

随着在科技应用方面变得愈发成熟，金融机构可开始全面审视并管理整个客户生命周期中的反洗钱/反恐融资风险。金融机构需要考虑如何在每个环节充分发挥技术优势，包括客户引导、数据收集与验证、客户数据管理、交易监测、调查以及报告。通过关注客户生命周期，金融机构不仅能够处理利于犯罪活动的潜在漏洞，还可确保无缝的客户体验。

隐私增强技术

### 帮助金融服务公司打击金融犯罪、保护客户信息

如何在保护客户信息与获取重要数据的需求之间取得平衡一直是金融犯罪与合规管理方面的主要难题。然而，新兴隐私增强技术可以帮助金融机构满足上述需求——在支持海量数据分析的同时保证个人可识别信息的安全性和加密性。例如，某领先隐私增强技术供应商与某著名金融机构技术供应商近期开展合作，在后者供应至澳大利亚市场的金融犯罪与合规管理产品组合中搭载隐私增强技术产品。

通过本次合作，金融机构可以获得隐私增强技术工具，帮助其在满足全球隐私和保密规定的同时安全共享敏感数据（例如交易数据）。此工具能够确保用户安全分享见解（跨机构和跨区域），并且保护潜在客户的个人可识别信息隐私。此外，这种轻松分享加密和去识别客户数据的能力也将有助于开展开放银行业务以及实现其他金融犯罪管理目标，如客户尽职调查、行为监测和协作金融犯罪调查，且不影响风险和监管合规管理。例如，通过加密查询流程可以在数秒内得出结果，从而帮助金融机构有效清除“误报”，识别金融犯罪。

其他应用

| 客户尽职调查   | 交易监测   | 调查  |
|--|--|---|
| 金融机构可在针对其考虑接洽的潜在个人或实体开展客户尽职调查时使用该项技术，以此深入了解客户，并在不受干扰的情况下完成身份验证，同时提升客户体验。 | 金融机构间的合作意味着金融机构可以获取更加广泛的客户信息，例如资金来源、相关账户和交易记录，从而显著降低交易监测误报率，提高客户洞察力。 | 广泛的信息共享简化了可疑事件报告的数据和证据收集流程。这有助于快速验证“误报”结果，消除调查流程中的死角盲区，同时在不侵犯调查对象隐私权的情况下帮助金融机构编制更加可靠和全面的报告。<br><br>跨机构协作可以帮助金融机构识别金融犯罪与合规管理流程中的盲点，从而降低相关风险。加强协同合作、信息共享和流程可见性有助于打造安全的金融犯罪合规环境。 |

# 结论

正如案例研究所示，虽然金融机构在打击金融犯罪方面采用的技术存在明显差异，但是所有金融机构均可利用监管科技解决方案提高金融犯罪风险识别和缓释的效率与效益。此外，在整个客户生命周期中全面应用监管科技解决方案有助于充分发挥其优势。

为实现投资回报最大化，金融机构需要确保其所采用的监管科技解决方案充分考虑到数据质量和访问权限、系统、流程和组织结构以及可用技术和技术供应商等因素。与此同时，金融机构可以组建跨职能和跨区域的多元化团队，并且寻求利益相关方的支持，这对取得成功至关重要。除此之外，金融机构应当健全治理框架，不断开展金融犯罪风险管理培训和监管科技解决方案开发活动，这对实现持续成功必不可少。

如欲保持运营韧性并且减少监管执法行动对财务和声誉造成损失的风险，金融机构必须采用新方法应对金融犯罪方面不断变化的挑战（例如金融服务行业的数字化以及愈发精通技术的犯罪分子等）。

综上所述，金融机构的高管层和董事会可以思考以下问题，以此深入了解其对监管科技的需求以及当前及预期的机会和战略目标。

- 监管机构对于利用技术进行风险管理和确保监管合规的满意程度如何？
- 监管重点是什么（特别是就近期的法规和检查/审查更新而言）？
- 当前与监管机构的关系如何？监管机构是否相信组织的金融犯罪管理能力？
- 组织采用何种技术架构？未来几年有何改革计划？
- 组织的金融犯罪风险状况如何？与整个行业的对比情况如何？市场中是否存在相关科技解决方案？
- 金融犯罪风险管理计划的有效性如何？金融犯罪风险管理计划中是否存在可识别的改进和发展机遇？

上述问题可以帮助金融机构评估如何实施监管科技解决方案才能获得最佳效果。此外，随着科技环境不断变化以及金融机构开始从单一平台解决方案转向更加灵活的多方法解决方案（即针对特定风险类型采用特定技术/方法），开发监管科技解决方案组合以支持现有金融犯罪风险管理计划的价值将会凸显。



# 术语表

|          |                  |
|----------|------------------|
| ECM      | 企业案例管理           |
| ACCESS   | 新加坡加密货币企业和初创企业协会 |
| AI       | 人工智能             |
| AML      | 反洗钱              |
| AMLS     | 反洗钱组件            |
| AP       | 亚太地区             |
| APG      | 亚太反洗钱组织          |
| APRA     | 澳大利亚审慎监管局        |
| AU       | 澳大利亚             |
| AUSTRAC  | 澳大利亚交易报告和分析中心    |
| BAU      | 常态化工作            |
| BEAR     | 银行高管问责制度         |
| CDD      | 客户尽职调查           |
| CFT      | 反恐融资             |
| CN       | 中国大陆             |
| CTF      | 反恐融资             |
| COSCO    | 特雷德韦委员会赞助组织委员会   |
| COVID-19 | 新冠疫情             |
| DIA      | 内政部              |
| EWRA     | 机构洗钱和恐怖融资风险评估    |
| FAR      | 财务问责制度           |
| FATF     | 金融行动特别工作组        |
| FI       | 金融机构             |
| FIU      | 联合财富情报组          |
| FMA      | 金融市场管理局          |
| FSC      | 金融监督管理委员会        |
| FSI      | 金融服务行业           |
| HK SAR   | 香港特别行政区          |

|              |                |
|--------------|----------------|
| <b>HKMA</b>  | 香港金融管理局        |
| <b>IRA</b>   | 机构风险评估         |
| <b>IT</b>    | 信息技术           |
| <b>JFSA</b>  | 日本金融厅          |
| <b>JVCEA</b> | 日本虚拟和加密资产交易所协会 |
| <b>KYC</b>   | 客户尽职调查         |
| <b>MAS</b>   | 新加坡金融管理局       |
| <b>MD</b>    | 主指令            |
| <b>ML</b>    | 洗钱             |
| <b>MLCA</b>  | 《洗钱防制法》        |
| <b>NLP</b>   | 自然语言处理         |
| <b>NZ</b>    | 新西兰            |
| <b>PBOC</b>  | 中国人民银行         |
| <b>PEP</b>   | 政治敏感人物         |
| <b>PET</b>   | 隐私增强技术         |
| <b>PSA</b>   | 《2020年支付服务法案》  |
| <b>PSS</b>   | 支付与结算系统        |
| <b>RBI</b>   | 印度储备银行         |
| <b>RBNZ</b>  | 新西兰储备银行        |
| <b>RE</b>    | 受监管实体          |
| <b>RPA</b>   | 机器人流程自动化       |
| <b>SFC</b>   | 香港证券及期货事务监察委员会 |
| <b>SG</b>    | 新加坡            |
| <b>SME</b>   | 行业专家           |
| <b>STR</b>   | 可疑交易报告         |
| <b>TF</b>    | 恐怖融资           |

# 联系人



## Akihiro Matsuyama

亚太地区监管策略中心主管  
金融服务业风险咨询合伙人

电话: +852 2852 1287

电子邮件: amatsuyama@deloitte.com.hk



## 黄毅城

亚太地区监管策略中心东南亚联席主管  
执行总监

东南亚监管策略主管

电话: +65 6800 2025

电子邮件: nawong@deloitte.com



## Mike Ritchie

亚太地区监管策略中心澳大利亚联席主管  
金融服务业风险咨询合伙人

电话: +612 9322 3219

电子邮件: miritchie@deloitte.com.au



## 何思明

亚太地区监管策略中心中国联席主管  
金融服务业风险咨询总监

电话: +852 2238 7892

电子邮件: jnamad@deloitte.com.hk



## Shiro Katsufuji

亚太地区监管策略中心日本联席主管  
金融服务业风险咨询总监

电话: +81 70 6473 7748

电子邮件: shiro.katsufuji@tohmatcu.co.jp

# 报告作者



## Nicola Sergeant

高级经理  
报告统筹

电子邮件: nicola.sergeant@tohmatcu.co.jp



## Siddharth Agarwala

高级咨询顾问  
撰稿人

电子邮件: siagarwala@deloitte.com



## Jaramie Nejal

高级经理  
撰稿人

电子邮件: jnejal@deloitte.com.au



# 中国联系人

## 吴卫军

德勤中国  
副主席  
金融服务业主管合伙人  
电话: +86 10 8512 5999  
电子邮件: davidwjwu@deloitte.com.cn

## 张丰裕

德勤中国  
财务咨询反洗钱中心合伙人  
电话: +86 10 8512 5353  
电子邮件: chrcheung@deloitte.com.cn

## 余培

德勤中国  
财务咨询反洗钱中心合伙人  
电话: +86 21 3313 8838  
电子邮件: jackiepyu@deloitte.com.cn

## 王璐

德勤中国  
财务咨询反洗钱中心总监  
电话: +86 10 8512 5706  
电子邮件: celwang@deloitte.com.cn

## 董聪

德勤中国  
财务咨询反洗钱中心总监  
电话: +86 10 8512 5692  
电子邮件: cdong@deloitte.com.cn

## 高岩梅

德勤中国  
财务咨询反洗钱中心总监  
电话: +86 21 3313 8960  
电子邮件: yagao@deloitte.com.cn

# 致谢

## Lisa Dobbin

合伙人  
澳大利亚

## Amanda Lui

合伙人  
澳大利亚

## Radish Singh

合伙人  
东南亚

## Marc Anley

合伙人  
东南亚

## Mark Woodley

合伙人  
东南亚

## 张丰裕

合伙人  
中国

## Thao Nguyễn Hoàng

高级经理  
东南亚

## 王璐

总监  
中国

## Sally Watson

高级分析师  
澳大利亚

# 尾注

1. The Treasury, Australian Government, "Consultation: Financial Accountability Regime (FAR)", 22 January 2020, <https://treasury.gov.au/consultation/c2020-24974>
2. Australian Government, "Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020", 17 December 2020, <https://www.legislation.gov.au/Details/C2020A00133>
3. Australian Prudential Regulation Authority, "Risk Management", 1 July 2019, <https://www.apra.gov.au/risk-management>
4. Australian Prudential Regulation Authority, "Prudential Standard CPS 234 Information Security", 1 July 2019, [https://www.apra.gov.au/sites/default/files/cps\\_234\\_july\\_2019\\_for\\_public\\_release.pdf](https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf)
5. Australian Transaction Reports and Analysis Centre, "New Rule will help Australians fleeing family and domestic violence gain financial independence", 28 May 2020, <https://www.austrac.gov.au/about-us/media-release/new-rule-will-help-australians-fleeing-family-and-domestic-violence-gain-financial-independence>
6. Australian Transaction Reports and Analysis Centre, "Identifying customers who don't have conventional forms of ID", Aug 2020, <https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/identifying-customers-who-dont-have-conventional-forms-id>
7. Financial Markets Authority & Reserve Bank of New Zealand, "Enhanced Customer Due Diligence Guidelines", September 2020, <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/guidance-and-publications/Enhanced%20Customer%20Due%20Diligence%20Guideline%202020.pdf>
8. Financial Markets Authority & Reserve Bank of New Zealand, "Guidance: Complying with AML/CFT verification requirements during COVID-19 Alert Levels", 26 March 2020, <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/AMLCFT-Supervisor-Guidance-COVID-19-Alert.pdf>
9. Financial Markets Authority, "AML/CFT Supervisory Framework", 22 November 2019, <https://www.fma.govt.nz/compliance/guidance-library/amlcft-supervisory-framework/>
10. Financial Markets Authority, "AML/CFT – territorial scope of the AML/CFT Act 2019", 22 November 2019 <https://www.fma.govt.nz/compliance/guidance-library/amlcft-territorial-scope-of-the-amlcft-act-2009/>
11. Ministry of Justice "Tackling money laundering and terrorist financing", 2019, <https://www.justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/>
12. Stewart McGlynn (Hong Kong Monetary Authority) "Moving the Needle: Improving Outcomes in Anti-Money Laundering", 26 September 2019, [https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/Speech\\_Stewart\\_McGlynn\\_201909.pdf](https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/Speech_Stewart_McGlynn_201909.pdf)
13. Hong Kong Monetary Authority, "Guideline on Anti-Money Laundering and Counter Financing of Terrorism", September 2020, [https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/svf/Guideline\\_on\\_AMLCFT\\_for\\_SVF\\_eng\\_Sep2020.pdf](https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/svf/Guideline_on_AMLCFT_for_SVF_eng_Sep2020.pdf)
14. The Hong Kong Association of Banks, "Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism", February 2021, [https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/FAQ\\_amlcft\\_feb\\_2021.pdf](https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/FAQ_amlcft_feb_2021.pdf)
15. The People's Bank of China Anti-Money Laundering Bureau, Regulations and Policies webpage, <http://www.pbc.gov.cn/fanxiqianju/135153/135173/index.html>
16. The People's Bank of China, "Measures for the Supervision and Administration of Anti-Money Laundering and Anti-terrorist Financing of Financial Institutions", 17 April 2021, [http://www.gov.cn/xinwen/2021-04/17/content\\_5600258.htm](http://www.gov.cn/xinwen/2021-04/17/content_5600258.htm)

17. Monetary Authority of Singapore, "Payment Services Act", 15 April 2019, <https://www.mas.gov.sg/regulation/acts/payment-services-act>
18. Association of Crypto Currency Enterprises and Start-ups Singapore, "Code of Practice" (for members), August 2019, <https://www.access.org.sg/products/code-of-practice-members>
19. Association of Crypto Currency Enterprises and Start-ups Singapore, "Code of Practice" (for non-members), August 2019, <https://www.access.org.sg/products/code-of-practice>
20. Japan Financial Services Agency, "Results on Public Comments on partial Revisions to the Guidelines on Measures against Money Laundering and the Financing of Terrorism", 11 December 2020, [https://www.fsa.go.jp/news/r2/202102\\_amlcft/202102amlcft.html](https://www.fsa.go.jp/news/r2/202102_amlcft/202102amlcft.html)
21. Japan Financial Services Agency, "Financial Services Agency considers system development jointly with regional banks", 31 October 2020, <https://www.nikkei.com/article/DGXMZO51644020R31C19A0EE9000/>
22. Japan Financial Services Agency, "Notification of Originator and Beneficiary Information Upon Crypto Asset Transfer (i.e. the travel rule)", 31 March 2021, <https://www.fsa.go.jp/news/r2/sonota/20210331.html>
23. Taiwan Business TOPICS, "Enhanced Anti-Money Laundering Controls Pay-off For Taiwan", 27 May 2020, <https://topics.amcham.com.tw/2020/05/antimoney-laundering-controls-pay-off/>
24. Taiwan Ministry of Justice, "Money Laundering Control Act", 7 November 2018, <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380131>
25. Fintech Hong Kong, "Taiwan's First Virtual Banks: The Progress So Far", 7 October 2020, <https://fintechnews.hk/13536/fintechtaiwan/taiwans-first-virtual-banks-the-progresses-so-far/>
26. Reserve Bank of India, "Master Direction on Digital Payment Security", 18 February 2021, <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF>
27. Reserve Bank of India, "Extending Master Direction – Know Your Customer (KYC) Direction, 2016 to Housing Finance Companies", 19 May 2020, <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11892>
28. Reserve Bank of India, "Amendment to Master Direction (MD) on KYC – Centralized KYC Registry – Roll out of Legal Entity Template & other changes", 18 December 2020, <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12008&Mode=0>
29. Reserve Bank of India, "Amendment to the Master Direction (MD) on KYC", 10 May 2021, <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=12089&Mode=0>
30. Reserve Bank of India, "Guidelines on Regulation of Payment Aggregators and Payment Gateways", 17 March 2020, <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11822>
31. Reserve Bank of India, "Framework for imposing monetary penalty on authorised payment system operators / banks under the Payment and Settlement Systems Act, 2007", 10 January 2020, <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11785>
32. Committee of Sponsoring Organizations of the Treadway Commission & Association of Certified Fraud Examiners, "Fraud Risk Management Guide", September 2016, <https://www.acfe.com/fraudrisktools/guide.aspx>
33. Standards Australia, "Fraud and Corruption Control Standards" (AS 8001-2008), 2008, <https://www.standards.org.au/standards-catalogue/sa-snz/other/qfr-017/as--8001-2008>

因我不同  
成就非凡

始于 1845

#### 关于德勤

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及遗漏承担责任，而对相互的行为及遗漏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](http://www.deloitte.com/cn/about) 了解更多信息。

德勤是全球领先的专业服务机构，为客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务及相关服务。德勤透过遍及全球逾150个国家与地区的成员所网络及关联机构（统称为“德勤组织”）为财富全球500强企业中约80%的企业提供专业服务。敬请访问[www.deloitte.com/cn/about](http://www.deloitte.com/cn/about)，了解德勤全球约330,000名专业人员致力成就非凡的更多信息。

德勤亚太有限公司（即一家担保有限公司）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座城市提供专业服务，包括奥克兰、曼谷、北京、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、大阪、首尔、上海、新加坡、悉尼、台北和东京。

德勤于1917年在上海设立办事处，德勤品牌由此进入中国。如今，德勤中国为中国本地和在华的跨国及高增长企业客户提供全面的审计及鉴证、管理咨询、财务咨询、风险咨询和税务服务。德勤中国持续致力为中国会计准则、税务制度及专业人才培养作出重要贡献。德勤中国是一家中国本土成立的专业服务机构，由德勤中国的合伙人所拥有。敬请访问 [www2.deloitte.com/cn/zh/social-media](http://www2.deloitte.com/cn/zh/social-media)，通过我们的社交媒体平台，了解德勤在中国市场成就非凡的更多信息。

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（统称为“德勤组织”）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。德勤有限公司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。

© 2021。欲了解更多信息，请联系德勤中国。  
Designed by CoRe Creative Services. RITM0793431



这是环保纸印刷品