McKinsey & Company

麦肯锡中国银行业转型与创新系列白皮书

合规管理：金融严监管时代的制胜良方

2019年8月


Government
Budget

目录

前言

金融严监管时代已经到来。在2017年开启的金融市场乱象专项治理风暴中，监管机构的“三三四十”整顿波及千余家银行，开出的罚单高达数十亿元人民币，剑指各类违规业务。由于政府随即将“大力整治违法违规业务，进一步深化整治银行业市场乱象”纳入到2018年监管十大任务，金融合规监管的鼓声可谓是愈演愈烈。2018年全年，银保监会机关、原银监局及原银监分局，对银行业金融机构和从业人员共开出了超过3800张罚单，涵盖国有大行、股份制银行、城商行等各类机构，涉及贷款管理不当、票据业务违规、同业投资违规和理财销售违规等多个领域。2019年业已过半，严格合规监管的总基调丝毫未松懈，监管机构坚决治理乱象沉疴的决心不减。

监管高压下，五大重点风险领域成为各方关注焦点。2019年5月，银保监会发布了《关于开展“巩固乱象成果，促进合规建设”工作的通知》，明确要求银行机构持续推动五大重点领域的问题整治，包括股权与公司治理、宏观政策执行、信贷管理、影子银行和交叉金融业务风险以及重点风险处置。具体而言，同业业务违规、反洗钱和反恐怖融资、互联网金融风险等，已成为近期监管的重点和热点。

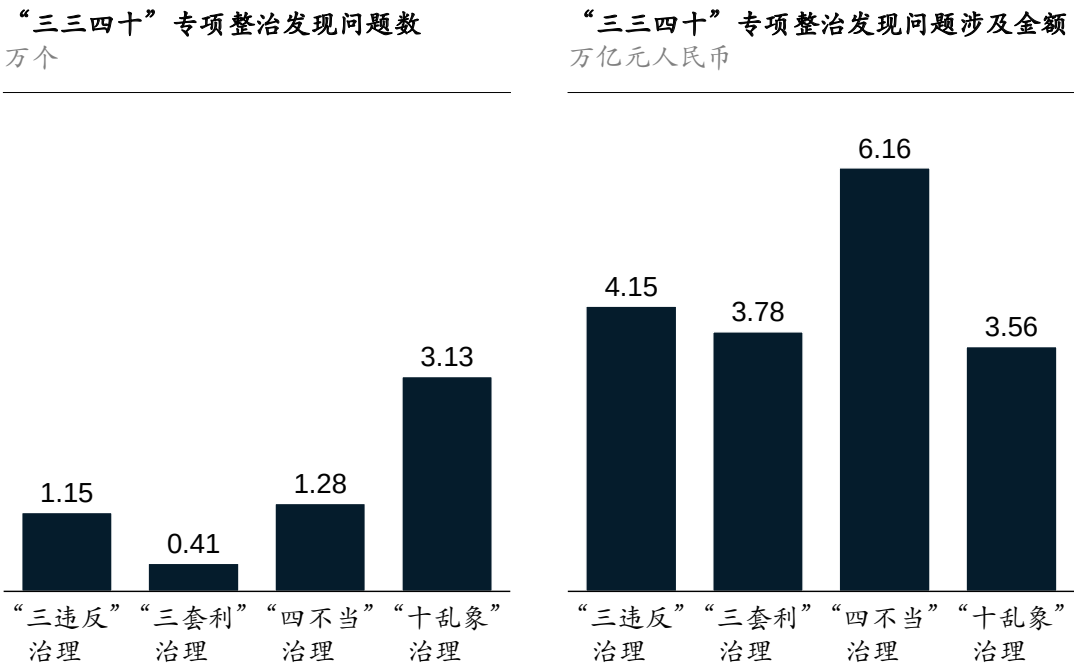
国际领先银行之所以重视建设完善的合规管理体系，既是监管高压下的必需，也是内部能力建设下的主动选择。因违背反洗钱和反恐怖融资相关法律规定，多家国际银行被美国监管机构处以高达十几亿美元的罚款；因涉嫌共谋操控法定汇率，5家国际银行被英美两国监管部门处以总计数十亿美元的罚款。面对愈加严峻的监管形势和企业自身的能力建设要求，许多领先银行已经开始在实践中搭建了完善的合规管理体系，帮助自身更好地履行对监管方、客户、员工和社会的责任，同时将法律法规转换为运营要求，不断提高企业的业务效率和可持续发展能力。

合规能力建设迫在眉睫。放眼国内商业银行的合规管理现状，行动滞后、管理被动和效率欠佳等问题无处不在。究其根本，是国内合规管理存在四大痛点：1）合规管理体系尚不健全，未形成自上而下的治理架构；2）缺乏可操作性较强的管理制度与流程；3）缺乏大数据等科技支持的系统建设；4）合规文化尚未充分建立，专业队伍建设亟待加强。

国内各大银行的唯一出路，是在完善和提升合规体系的过程中，视合规管理为内部风险控制的重要防线，不断强化制度先行的合规理念、牢记业务合规的把关意识，并将事后补救转化为事前防控，变外部合规要求为内部管理动力，从而真正有效地构建起合规管理长效机制，为业务腾飞保驾护航。

方兴未艾：金融严监管时代已至

图1 “三三四十”专项整治行动督促银行业加强合规管理



资料来源：麦肯锡分析

对于国内银行高管而言，2017年开始的金融市场乱象专项治理风暴仍然记忆犹新，监管机构的“三三四十”整顿波及千余家银行，开出的罚单高达数十亿元人民币，目标直指银行各类违规业务（见图1），引导商业银行回溯合规本源、回归业务本位。部分银行基础管理较为薄弱、内控制度不完善、重点业务合规管理不力，员工合规意识、风险意识和底线意识薄弱，严重触碰同业理财、金融套利等监管“红线”的案件屡见不鲜。

而风暴还在继续，随着政府继续将“大力整治违法违规业务，进一步深化整治银行业市场乱象”纳入到2018年监管的十大任务之一，金融合规监管的鼓声愈烈，呈现出三大关键趋势。

一、力度不减，坚决治理金融乱象沉疴

据统计，2018年全年，银保监会机关、原银监局及原银监分局针对银行业金融机构及从业人员共下发了超过3800张罚单，涉及国有大行、股份制银行、城商行等各类机构以及贷款管理问题、票据业务违规、同业投资违规、理财销售违规等多个领域。罚单数量较2017年陡增56%，平均每天开出10多张罚单，使**2018年成为“最严监管年”。**

步入2019年，严格合规监管的总基调毫未松懈，坚决治理沉疴。年初银保监会召开的2019年银行业和保险业监督管理工作会议提出，要坚持不懈治理金融市场乱象，下大力气补齐监管短板，把防范系统性风险与服务实体经济更紧密地结合起来。1月，银保监会发布《关于加强中资商业银行境外机构合规管理长效机制建设的指导意见》，明确了中资银行境外机构合规管理的工作目标和基本原则，要求其强化总部层面的日常监管沟通，及时回应监管关注事项，同时完善监管信息报送机制，加强对重点机构和业务领域的跨境监管，例如国别风险、反洗钱、反恐怖融资等。2019年开年第一个月，各级银行业监管机关披露的罚单数量达到683张，日均22张，创下近两年来的单月最高，总罚款金额高达1.67亿元人民币。同时，银行高管也被纳入严查范围之内，多位股份制商业银行和农商行的董事长、总经理、甚至党委书记/委员受到纪律审查和监察调查。

强调严格监管的同时，政府也提供了多项支持性政策，为金融机构开辟了业务调整之门，例如允许商业银行设立理财子公司，对银行理财表外业务与表内业务进行风险隔离、允许商业银行发行永续债补充资本金等。

二、巩固成果，雷霆直击重点风险领域

2019年5月，银保监会发布《关于开展“巩固乱象成果促进合规建设”工作的通知》（下称《通知》），提出2019年整治工作力争实现三个目标：一是查处屡查屡犯，消化存量，在推动银行保险机构合规建设方面取得新成效；二是查处重点风险，遏制增量，在推动银行业保险业生态修复方面取得新进展；三是推进金融供给侧结构性改革，在实现高质量发展和提升服务实体经济水平、能力方面取得新突破。至此，**金融乱象整治取得阶段性成果，**在对2018年工作“回头看”，巩固已发现问题整改、问责处理、机制建设成果的基础上，**下一步将寻求防风险、治乱象和稳增长、调结构的有机统一**，防止市场乱象反弹回潮的同时，推动银行业保险业实现高质量发展。

《通知》还明确要求银行机构持续推动**五大重点领域问题整治，包括股权与公司治理、宏观政策执行、信贷管理、影子银行和交叉金融业务风险、重点风险处置。**具体而言，同业业务违规、反洗钱和反恐怖融资、互联网金融风险等成为近期监管的重点和热点。

同业业务违规。随着许多“潜规则”，例如隐形担保、借同业资管通道违规处置不良资产、伪造资料办理同业理财和票据贴现业务等浮出水面，监管机构的处罚力度也不断加重。2018年开年，银监会对涉及票据违规的12家银行业金融机构开出“高价罚单”，共计罚没2.95亿元人民币，并惩处相关机构的多位业务负责人和领导班子成员。据统计，2019年1月至3月，银保监会公示的银行机构行政处罚中涉及同业内容的超过30件，其中200万元人民币以上的大额罚单超过5件，包括2019年的首张罚单，某农商行员工因对该行违规办理同业业务负直接责任而被“禁止从事银行业工作终身”，该行其他负领导和管理责任的人员也分别受到任职资格限制的惩处；3月，某股份制银行

因同业授信资金回流购买本行理财、同业理财产品误导销售等12项违法违规行为，被处以共计660万元人民币的罚款，成为年初以来银保监系统开出的最大单笔罚单；5月，某民营银行因同业投资等违法违规事项，合计被罚180万元人民币……**雷霆监管之下，银行资金利用同业渠道脱实向虚、以钱炒钱的行为逐渐得到遏制。**

反洗钱和反恐怖融资。自2017年国务院发布《国务院办公厅关于完善反洗钱、反恐怖融资、反逃税监管体制机制的意见》以来，监管机构加速出台相关政策。2018年7月26日，央行在一天之内连发4文，要求银行和非银行支付机构完善客户身份识别制度，建立大额交易报送机制。2018年10月，人民银行、银保监会、证监会、外汇局联合召开金融系统反洗钱和反恐怖融资工作部署会议，提出紧跟金融行动特别工作组（Financial Action Task Force on Money Laundering, FATF）国际标准，打好扩大金融业双向开放和防控金融风险的攻坚战。据人民银行官网公示，2018年全年反洗钱行政处罚共396笔，罚款金额合计1.3亿元人民币，其中银行业机构占比61%，且绝大部分为“双罚”，即对企业和相关责任人同时罚款，并将该处罚记入个人职业档案。进入2019年，随着央行163号文明确了大额交易上报标准，各地监管分支机构和金融从业机构将围绕多项政策的落地而忙碌，跨境支付和交易的进一步普及，也考验着我国现有条例的完善程度。**可以预见，未来对**

金融活动必须接受严格市场监管，任何金融活动不能脱离监管体系，不能以技术之名掩盖金融活动的本质；不论是金融机构、互联网企业还是金融科技企业，都应按照实质重于形式的原则，落实穿透式监管；互联网金融和金融科技并未改变金融的风险属性，其与网络、科技相伴生的技术、数据、信息安全等风险反而更为突出。

——中国人民银行副行长潘功胜在2018年中国互联网金融论坛上的发言

国内和跨境反洗钱和反恐怖融资的监管要求将愈加严格。

三、迎难而上，金融科技强监管常态化

近年来，互联网金融迅猛发展，在为消费者带来便利的同时，如何有效进行风控与监管亦成为一道难题，主要体现在：1）监管对象数量众多、类型复杂，且业务交易存在虚拟性，难以及时探测最新动向并在短时间内厘清交易对象和风险责任方；2）数据量级庞大，社会征信系统不完备、互联网金融机构信息核实缺漏、投资者对交易信息正确性判断失误等各个薄弱环节，都会导致风险的发生乃至指数型积累；3）技术时代的互联互通导致风险传播速度极快且呈现高隐蔽性，增加风险预警和风险化解难度。

尽管如此，监管方仍然迎难而上，自2016年来展开了对互联网金融风险的专项整治活动，并在网络借贷、第三方支付、虚拟货币交易场所和ICO（Initial Coin Offering，首次代币发行）等方面密集出台了多项严监管措施。2018年10月，人民银行、银保监会、证监会联合发布《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》，将网络支付、网络借贷、股权众筹融资、互联网基金销售、互联网保险等多个热点领域纳入监管范畴，并设立互联网金融反洗钱和反恐怖融资网络监测平台，要求中国互联网金融协会负责建设、运行和维护，并要求所有从业机构接入该平台，进行反洗钱和反恐怖融资履职登记。2019年2月，《中国人民银行职能配置、内设机构和人员编制规定》发布，明确指出中国人民银行应“统筹互联网金融监管工作”，同时下设科技司，负责指导协调金融业网络安全和信息化建设，拟定金融科技监管基本规则。

在加强互联网金融风控的同时，监管机构也积极引入科技工具，提升自身工作效率。2018年8月，证监会印发《中国证监会监管科技总体建设方案》，标志着监管科技建设工作顶层设计完成以及全面实施阶段开启。监管科技建设工作可分为三个阶段：1）监管科技1.0：通过采购或研制成熟高效的软硬件工具或设施，满足证监会内部门和派出机构基本办公和特定工作的信息化需求，提升监管工作的数字化、电子化、自动化、标准化程度。2）监管科技2.0：通过不断丰富、完善中央监管信息平台功能，优化业务系统建设，实现跨部门监管业务的全流程在线运转，为大数据、云计算、人工智能等技术在监管科技3.0阶段的应用打下良好基础。3）监管科技3.0：建设一个运转高效的监管大数据平台，综合运用电子预警、统计分析、数据挖掘等数据分析技术，围绕资本市场的主要生产和业务活动，进行实时监控和历史分析调查，辅助监管人员对市场主体进行全景式分析、实时监控监测市场总体情况，及时发现涉嫌内幕交易、市场操纵等违法违规行为，履行监管职责，维护市场交易秩序。

面对监管的持续高压，国内银行业唯有加快推进合规管理长效机制的建设，全面把握监管机构最新的合规管理方向和方法，才能确保银行经营上依法、合规，从而实现持续、高质量的发展。

他山之石: 国际领先银行最佳实践

国际领先银行在完成合规管理的转型前，曾因合规缺陷面临监管部门开出的巨额罚单。银行合规的体系建设和流程转型既是顺应“主动合规”的大势所趋，更是强化银行内部管理能力的主动选择。

多家国际银行曾因忽视合规管理而付出惨痛教训：因违背反洗钱和反恐怖融资相关法律和规定，多家国际银行被美国监管机构处以高达十几亿美元的罚款；因涉嫌共谋操控法定汇率，5家国际银行被英美两国监管部门处以总计数十亿美元的罚款。

面对愈加严峻的监管形势、迫于企业内部自身能力建设的需要，在实践中，许多领先银行已经开始搭建和完善合规管理的四大支柱，帮助企业更好地履行对监管方、客户、员工和社会的责任，同时将法律法规落实为运营要求，不断提高企业的业务效率和可持续发展能力。

一、欧洲某银行：合规组织及文化示范者

通过明确部门职责，开展高管之声与合规培训并加强结果管理，欧洲某银行建立了超越同行的强大合规风险管理组织及文化，成为银行合规经营的典范。

部门职责 – 该银行按照专门领域和风险类型，对合规部门的管理范围做出明确、全面的规定（见图2）。

高管之声 – 该银行高层管理团队通过“高管之声(Tone from the Top)”计划，树立管理层对员工理想行为的期望，监督并监测相关计划执行，领导层还以身作则以榜样的力量领导全员推进合规文化举措（见图3）。

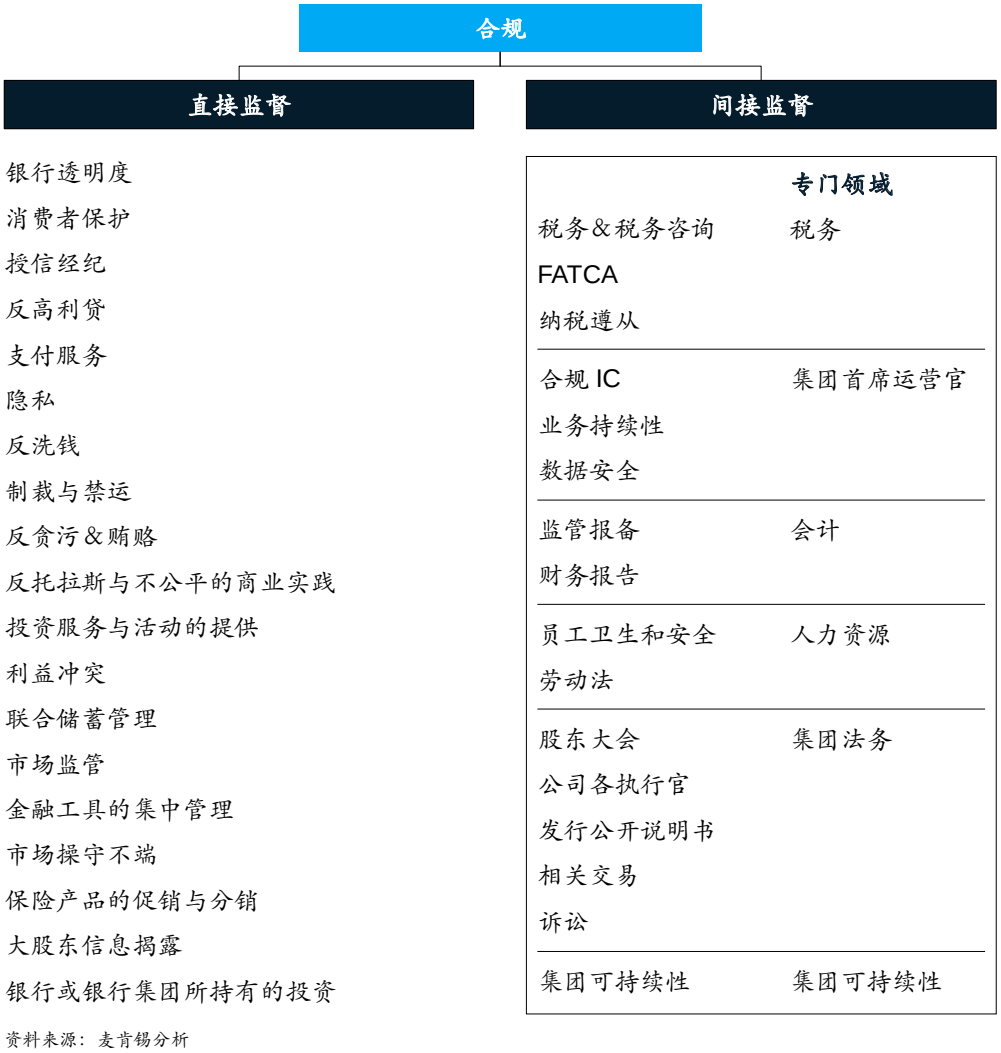
合规培训 – 欧洲某银行构建了三层合规培训体系与明确的培训原则，通过网络及面授课的形式，强力推动合规培训落地：

- **全集团课程：**针对约120家分行和代表处的所有员工进行强制培训，确保整个集团有统一的合规培训和知识；
- **条线/区域培训：**针对特定对象进行额外强制培训，这些特定对象通常是商业银行、对公投行或某些特殊国家和区域，通过此举进一步提高员工的法规知识；
- **针对工作岗位的特定培训：**针对高风险目标群体进行额外补救、强制培训，以确保其行为完全符合合规政策和流程，有将近12万名员工参与了这类培训，课程完成率在97%以上；
- **培训指导原则：**首先根据员工风险评估结果决定其是否需要培训，然后根据各岗位要求进行定制化培训内容设计，对培训过程进行严密监测和记录，并严肃处理未按要求进行培训的当事人。

结果管理–建立完备的“内部举报”机制，鼓励员工积极揭露“不当行为”，形成强有力的第一道防线。

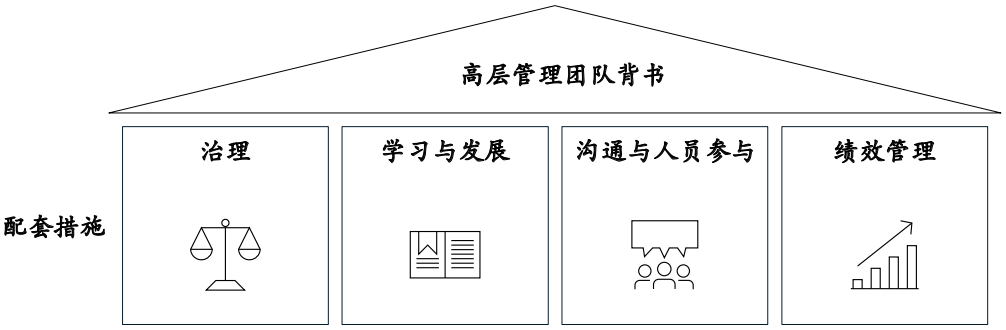
- 谁可以发起举报：所有员工均可以发起举报，不分层级、不分地域；

图2 欧洲某银行合规部门管理范围



资料来源：麦肯锡分析

图3 欧洲某银行“高管之声 (Tone from the Top)”计划



高层管理团队：

- **建立**对理想行为的**期望**
- **监督**并**监测**相关计划执行
- **以身作则**，树立榜样进行**领导**

设计了集团和各地的沟通计划，目前正在执行：

- 借由**Tone from the Top**将**文化散播到所有员工**
- 培养**个人担责意识**

资料来源：麦肯锡分析

- 如何举报：覆盖全公司的邮箱、热线、驻场办公机构等渠道均可接受举报；建立举报人保护制度，对举报人信息严格保密；
- 什么时候应该发起举报：任何人目睹不合规事件发生、或掌握不合规事项证据，该事件可能给公司运营或声誉、员工利益造成损害的，都应该发起举报；
- 注重消除偏见：通常人们评价非权限内事项或别的员工时会有所顾虑，该行鼓励大家打破成见，营造以公司和员工利益为本的氛围。

二、亚洲某银行：合规风险管理框架践行者

识别：三层次合规目标

亚洲某银行的合规风险管理目标包括三个层次：第一是遵守法律法规，这一层次属于外部约束；第二是遵守集团内部规定，这属于内部约束；第三是满足利益相关方（尤其是客户）的期望。前两个层次的目标与大部分银行相同，为刚性约束，只要合规部门密切跟进内外部规定并制定和实施了相应的举措，便能基本实现。第三层次的目标则提出了更高要求，旨在通过规范化经营，降低客户交易风险，提高客户综合体验和满意度。这一目标要求银行将合规风险管理水平作为满足客户需要、打造自身竞争软实力的一部分，从“被动合规”转向“以合规促发展”。

该银行总行合规部门统一负责对法律法规的解读。一般而言，在相关法律法规颁布后，合规部门首先应对条文进行预读，领会条文要义，并就其中不甚明晰的内容与相关政策部门及时沟通。而后，召集与本次法规内容相关的业务部门组成“联合工作组”，具体研究和评估法规对现有业务及流程的影响、确定应对举措

> 合规管理就是保证银行遵守其所在国家或地区的当地法律和法规，也保证银行遵守集团内部的政策和流程以及银行客户所期望的标准。
>
> ——该银行合规总监于银行业合规年会上的发言

我们银行的文化就像龟兔赛跑里的那只乌龟，虽然慢但是稳；这使得我们在多次金融危机中将影响降到最低。

——该银行前区域CRO（首席风险官）

并拟定实施计划。对确定需要改动的流程或系统，制作“责任分解表”分发至各业务部门，由相关负责人确认责任内容并予以落实，合规部门则持续跟踪完成情况，并就遇到的问题提供指导。对于地区性法律法规，地区分支机构合规部门没有解读权限，应及时将情况逐级上报，由总行合规部门统一按照上述流程协调处理。这种自上而下的制度安排，确保了该银行全行上下针对法律法规达成了正确而统一的认识，并能够及时做出反应。

管控：三条防线与三条信息渠道

该银行在全行上下强调，合规是各分支机构、各业务及每位员工的共同责任，而不仅仅是合规风险管理部门的责任。为此，该银行制定了全球统一标准宪法（“Global Standards”），对公司合规政策、员工行为与奖惩准则、各类别业务指引、合规问责机制等进行了详尽规定并设立了**合规风险控制三道防线：**第一道是业务部门。总行各业务部门下设业务风险及控制管理部，汇总本部门的合规事务并上报合规风险管理部统一处理；每个分支机构内也设立合规管理岗位，由本机构负责人或骨干员工担任，对本机构经营管理合规性负责。第二道是合规及内控部门，并与风险、运营、法律、IT等部门互相支持、协调和监督。第三道是内部审计部门，对合规相关问题进行复审，并参与调查合规薄弱环节及违法违规问题。

该银行开辟了三条渠道以保证法律法规要求传递到位：一是通过《合规工作手册》明确对员工的具体要求，不同部门和岗位的员工可以在内部网络上随时查阅到相关内容。二是合规总监通过内部邮件或内部网络公告等，以《合规传阅件》的形式向合规主任和合规代表传达最新要求。三是通过培训保证每个员工深入理解并严谨遵守合规要求。对于新入职的高级领导，必须参加“国际经理人”骨干培养项目，在风险条线轮岗至少1至2年，申请免除该项目的高管均应通过风险能力资格认证考试。对于新入职的初/中层领导，在参加“管理培训生项目”时（通常是高校毕业生），需在合规或其他风控岗

位（如风险、内审等）轮岗。对于非管理职位员工，需接受包括集团合规政策、员工行为守则、反洗钱等内容在内的集中讲解，并签收和确认《员工行为守则》书面文件，之后方可上岗。在岗期间，每年还需参加监管法规、反洗钱、反贿赂等方面的统一培训并通过网上结业考试。

合规风险管理部门广泛参与多个关键业务流程，包括新产品审定、市场宣传品审定、操作规程审定、培训内容审定、业务计划审定、外包计划审定等，牢牢把握各流程中的风险管控点并定期评估和更新。其中，操作规程审定最为重要，合规部门以全流程审核的方式，将各项外部监管要求和内部管理规定融入到业务部门的操作规程，尽力减少合规风险隐患。

监测与补救：体系化评估与现场检查相结合

该银行合规部门的工作主要包括两大方面，一是定期识别和评估各业务领域的合规风险，二是基于银行风险现状制定合规监察计划。具体内容包括分析客户投诉、分析自查或内审报告、查阅员工交易记录、关注疑似洗钱报告、开展年度综合合规性风险评估等。合规总监同时也是资产负债管理委员会、人事政策委员会、信息技术委员会等多个高层管理委员会的成员，以及时了解各项因素对合规风险的潜在影响，例如大幅招募或裁减员工、新产品开发、新系统启用等。

此外，该银行的多个部门（包括合规部门、内审部门、内控部门等）均具有现场检查职责，检查对象既包括业务部门，也包括合规部门。

对业务部门的检查往往深入到一线业务单元，采取自查和外部检查相结合的方式，具体分为三类：第一是业务自查，在业务部门内部自行完成，由对口的上级部门纵向逐级抽查。第二是合规检查，由合规部门负责，通常包括抽取具体交易档案、抽选员工检查其对法规的熟悉程度、观察业务操作流程中对相关法规及公司规定的执行情况等。第三是内控检查，由内控部门独立开展。

对合规部门的检查包括两类：第一是内审部门检查，主要对法规条文解读、合规监察计划制定、合规监察执行情况等关键工作开展审计。第二是上级合规部门的检查，以确保各级合规部门在获得必要资源的前提下，高度独立开展相关工作。

在检查中一旦发现问题，分行合规部立即向总行合规部实线报告，向分行行长虚线报告。总行合规部向分行提出整改要求，跟踪整改结果并收集反馈。同时，每季度出具对分支机构的问题检视报告，明确列示问题描述、严重程度和违规人，并实行违规“零容忍”的问责机制。将风险和合规指标纳入个人绩效考核，在平衡记分卡中的占比至少为25%，对于出现在每季度合规问题检视报告中的违规人，无论是否造成严重后果，均将影响其当期绩效考核。此外，采取奖金递延机制，初级及中级业务人员奖金递延三年，高管层奖金递延5年及以上，以避免过度追求短期效益的情况。

报告：合规事项双线负责

该银行合规风险管理实行“双线负责”制，即所有合规事项均通过经营管理条线和合规管理条线同时上报，基本保证了合规事项报告路线上下打通，体现了合规部门独立性。同时，该银行还设立“合规披露热线”，允许员工匿名举报违法违规、财务欺诈等事项。

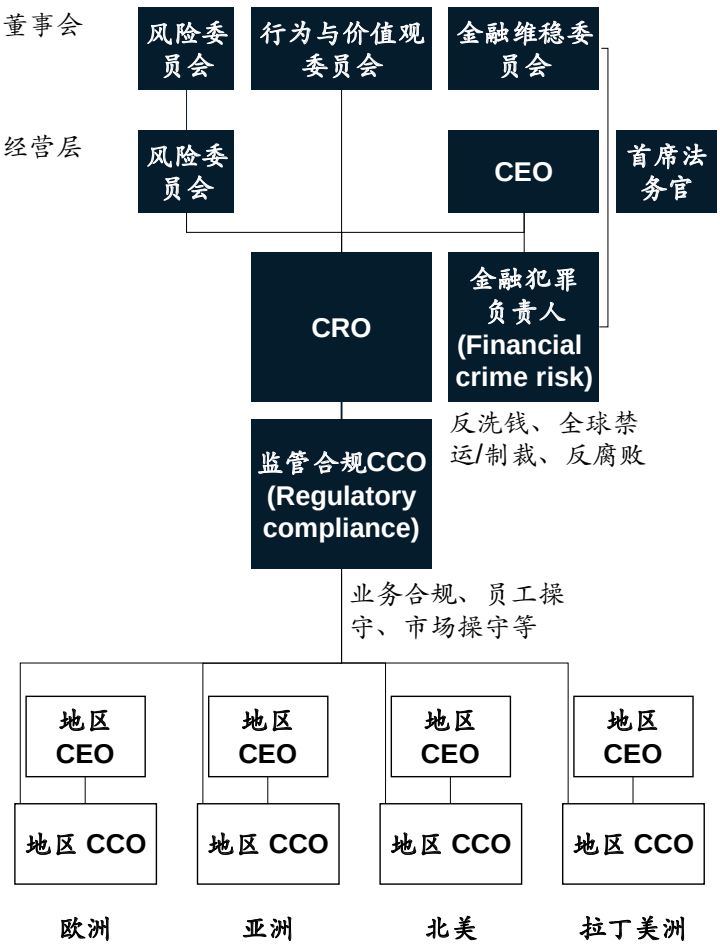
另外值得指出的是，该银行曾因反洗钱管理事故受到监管机关处罚，要求其重整反洗钱管理体系。于是该银行在集团层面将原归属于监管合规管理范畴的金融犯罪风险管理拆分成为独立部门，直接向CEO汇报，同时大量补充合规人员，其人数几乎占全球总员工数的2%，体现了该行针对突出风险动态调整合规管理及组织架构的做法（见图4）。

图4 亚洲某银行将金融犯罪与合规风险管理分离

设计思路

- 每个区域的监管环境有很大的差异，通过在区域和国家设置合规管理团队确保当地业务合规，双线汇报于地区负责人及总行合规条线
- 全球监管合规部门设置全球通用政策、行为守则等，地区合规官根据当地情况调整
- 将具有特殊监管意义的金融犯罪管理活动拆分，并直接汇报给业务负责人，确保得到足够的重视
- **CCO/CRO的汇报关系**
- CCO向CRO汇报
- 金融犯罪风险负责人直接向集团高管汇报

组织架构



资料来源：麦肯锡分析

三、北美某银行：数字化合规流程先行者

北美某银行全球合规部注重与业务部门的密切合作，确保各项业务符合法律法规要求，确定公司以适当方式追求全球市场机会，并跟踪各地监管趋势以及不同司法管辖权下业务模式的变化。

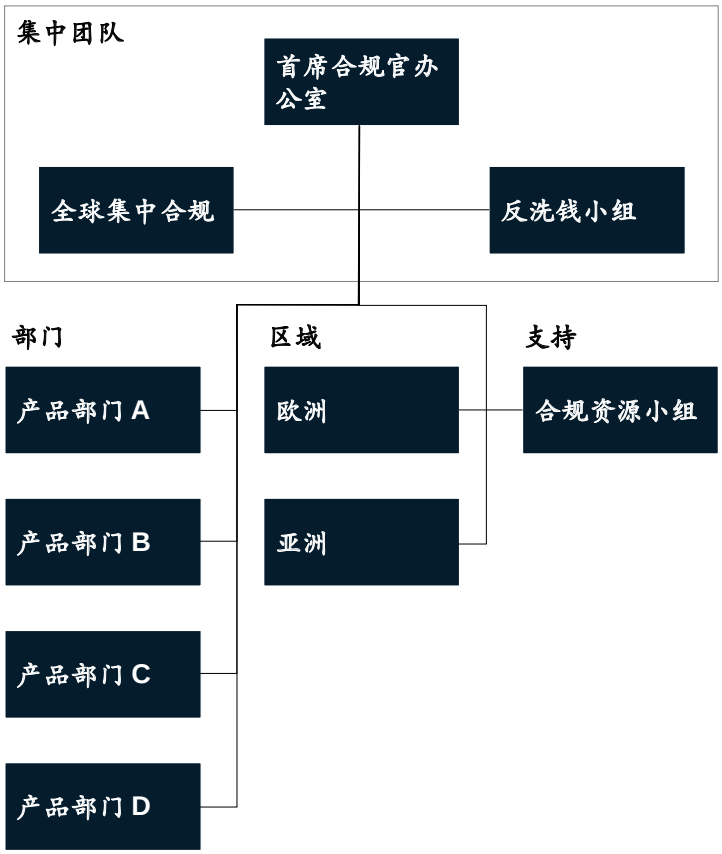
该银行合规部按照部门和区域划分管理条线，并采取矩阵式汇报方式，例如日本证券业务的合规负责人向日本分公司合规负责人与证券合规负责人报告。各合规团队之间没有严格界限，遇到重大合规问题时经常在线上或线下组织集体讨论，也经常进行跨地区轮岗（见图5）。合规部员工约500名，占全球总员工数的1.7%，包括三种合规职位：1）与主管机关对接，负责反洗钱、主管机关关系协调和报告等；2）与员工对接：提供交易建构建议，开展个人交易评估；3）与业务对

图5 北美某银行将合规与业务单元紧密结合

设计理念

- 少数工作有部分重叠的事业单位另外成立部门团队
- 依照各地监管机关设立区域团队，以反映对地方专业的需求
- 各部门与地区间采取矩阵式汇报，例如**日本证券业务的合规负责人向日本分公司合规负责人与证券合规负责人报告**
- **全球合规集中化以确保协作与监督**
- 完善的**支持团队**，负有合规运营与技术权限
- **首席内控官的定位**
- 首席合规官是全职职位，直接向首席执行官报告
- 首席合规官定期向稽核委员会与董事会报告

组织结构



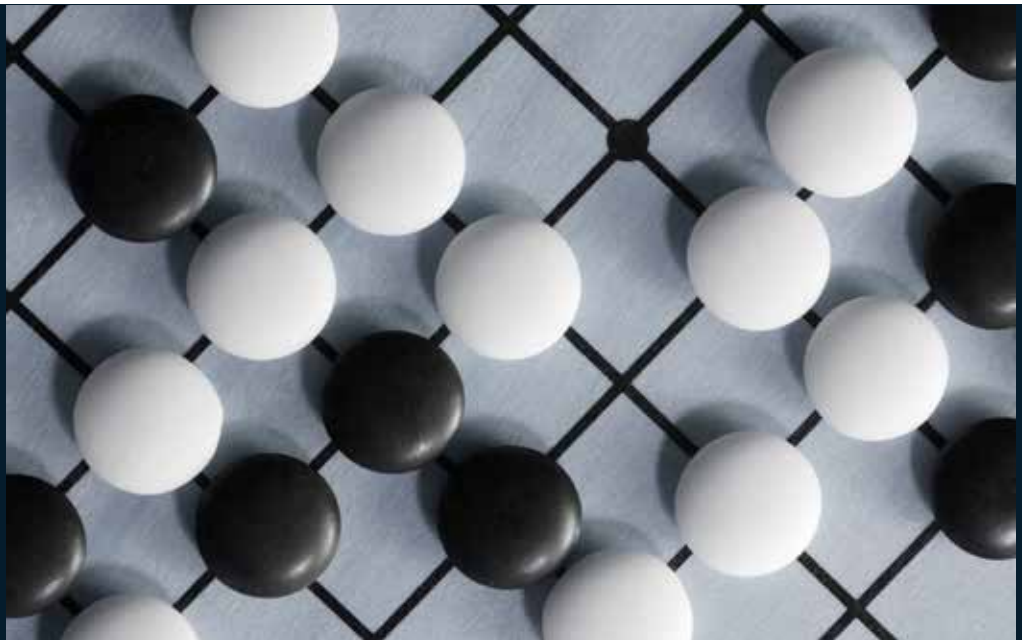
资料来源：麦肯锡分析

我们的风险管理理念并非规避、控制风险，而是主动经营风险。风险条线的人具有业务条线不具备的高级专业量化能力，是业务条线不可或缺的合作伙伴。

——该银行专家访谈

接：把控部门合规。**其中，与业务对接的合规员工占比达2/3，以确保每项业务工作合乎外部法规和内部规定要求。**

在合规与业务团队密切合作的基础上，该银行还自行开发了被业内公认为风险管理"秘密武器"的数据平台，该平台在服务交易中台的同时，从侧面支持了合规工作，增强合规管理自动化和即时性。该平台的发展历经三个阶段：1) 上世纪90年代，该银行为了交易目的而开发该数据库平台，采用统一的编程语言，可以灵活添加变量，并可与其他数据库对接。业务部门使用该数据库对交易的业绩表现、在未来不同情景下的波动情况、增持某项投资对整体投资组合的影响、新产品定价等内容进行检索，以辅助决策。2) 2000年~2008年，通过整合其他数据系统，该数据库演变成合规/风险管理和业务人员通用的数据工具。合规及风控部门使用该数据库统计风险敞口、审批业务以及获取和分析所有与风险相关的其他数据信息。3) 2008年以来，该数据库逐渐演变为大数据高级计量运行平台，每一位交易员和合规/风险管理人员均需要接受编程培训，以确保能够熟练地使用该平台，即时获取和监测任何风险事件和相关信息。



运筹决胜：对国内银行合规管理的建议和启示

随着国内银行业金融机构的经营活动日益综合化和国际化，业务和产品越来越复杂，合规失效事件不断暴露，银行业金融机构经营活动合规性面临严峻挑战，原有合规管理框架有效性受到质疑，合规风险管理理念和方法需要与时俱进。麦肯锡认为，国内银行要实现在合规管理上成功转型，需从合规治理架构、风险管理框架、数字化合规流程和主动合规文化四大抓手出发，构建全方位合规管理能力。

一、国内商业银行在合规管理方面普遍存在的问题

纵观国内商业银行的合规管理现状，普遍存在管理滞后、被动和效率欠佳的情况。究其根本，核心原因是尚未形成完善的合规管理体系，银行内也未形成“合规人人有责”的正确合规理念，与业务流程相匹配和适应的合规管理制度和流程也尚未到位。

1. 合规管理体系不健全，尚未形成自上而下的治理架构

国内银行普遍存在经营战略上重业务拓展与目标考核，风险管理及监管合规上重事后管理、轻事前预防，管理团队上重基层员工推动、轻高管人员约束的问题，导致未能形成完善的合规管理架构与支撑体系，在合规管理及时性、权威性和适用性上均有不足。合规部门在与业务部门的合作与角力中也常面临管理被动和滞后的难题，难以实现合规的全面和系统化管理。

2. 缺乏可操作性较强的管理制度与流程

国内商业银行普遍缺少系统化的识别机制、量化的评估标准和可操作性的管理制度，且各部门间合规管理相关权责界定不清晰，导致合规管理片面、分散和局部的问题。其中，合规报告存在渠道受限、真实性待考量、人为干预多的情况，导致合规报告真实性、时效性和前瞻性不够。

3. 缺乏大数据等科技支持的系统建设

许多商业银行、尤其是城商行的合规管理仍处于人工处理模式，尚未建立起相应的合规信息管理系统，导致合规管理信息质量、时效性方面不足。且未能充分利用大数据等技术改进并实现合规和监管信息的及时预警与多维度分析，难以为业务发展提供必要的决策支持和中后台支撑。

4. 尚未充分建立合规文化理念，亟需加强专业队伍建设

绝大多数商业银行尚未建立“合规人人有责”的文化理念，尤其是基层对合规管理的认识不够深入和充分，在合规管理上缺乏主动性。同时存在应付检查和重复检查现象，不仅未能达到有效管理，反而降低了管理效率。

合规管理团队同样缺乏科学、专业的合规识别、评估和处理方法，合规管理也难以由点及面、为银行整体经营管理提供必要的信息输入与决策支撑。

二、四大举措构建卓越合规管理能力

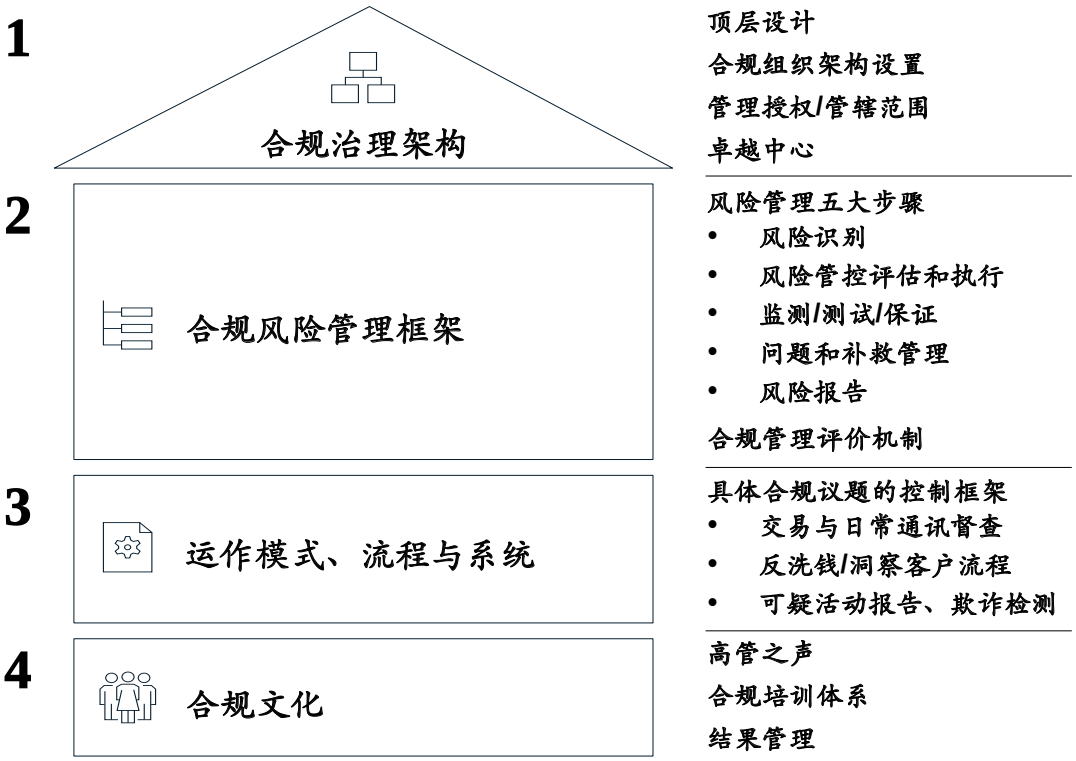
建设卓越合规管理能力，需要银行大力推动合规治理架构和管理框架，积极探索与业务相结合和适应的合规流程与系统，主动培养合规意识与合规文化，从而为合规能力落地提供必要基础与支撑（见图6）。

举措一：建立合规治理架构，明确合规管理权责和管辖范围

首先，在治理结构的顶层设计上，国际领先银行一般会根据整体组织战略与管控特性，**选择在董事会、经营层或业务线等不同层级设置与合规管理相关的委员会，**确保合规议题得到充分讨论，首席合规官参与所有重大决策讨论，或具有直接向CEO/董事会汇报的权利。

– 英国某领先银行将合规风险作为主要议题纳入董事会各委员会的议程中，在特定情况下，甚至会组建独立的同级别财务/非财务风险委员会，以凸显

图6 构建合规管理能力的四大举措



资料来源：麦肯锡分析

合规管理的重要性，并确保所有管控部门保持一致；

- 美国某领先银行针对重要的特定合规议题组建了专职的第二道防线委员会，常见形式包括：金融系统稳定性管理委员会（侧重反洗钱），声誉风险委员会，业务合规委员会等；

- 德国某领先银行则在第一道防线层面，将合规主管列为风险管控委员会中不参与投票的成员，让业务与参与管控各方之间形成从前台到后台的完整视图，确保对风险及其缓释计划形成综合全面的看法。

其次，针对合规组织设置，国际领先实践一般有三种模式：以法务为主、以风险为主及独立的合规部门。这三种模式在组织架构、汇报条线等方面各不相同，因而产生了不同的管控效果。

- **以法务为主**的组织设计下，合规隶属于法务部门，合规负责人向法务总监汇报。这也是过去银行合规最常见的汇报线结构。合规被视为法务部门内部的一个专业单元，法务和合规人员通常共同解决问题/案子，工作上并没有很明确的界限。在管控效果上，该模式确保了合规相对于业务的独立性，并与法务/监管实现专长共享，促进协同效应。

- 采用**以风险为主**的模式时，合规职能隶属于风险部门，合规负责人向首席风险官汇报。此时合规被视为类似于操作风险的一种风险，从而使风险部门对所有风险类型有一个综合看法。该模式有助于风险职能内部形成对业务的统一认识。北美某领先银行、亚洲某领先银行等多家国际领先银行的合规职能均采用该模式（见图7）。

- 而**独立的合规部门**设置下，合规负责人向CEO或COO（或直接向董事会汇报）。合规的定位类似于内部审计，与业务有清晰界限。该模式显著提高了合规职能的地位，确保合规独立于其他支持部门，尽管合规仍需与风险部门协调工作。例如德国某领先银行、法国某领先银行、意大利某领先银行等均采用了该模式（见图8）。

从国际银行业合规组织设置的最新趋势来看，合规与法务分离是普遍趋势。其原因在于法务更偏向于提供法律服务，而合规管理从风险管控的角度具有其专业性；同时，合规管理和风险管理（尤其是非财务风险）之间有很大协同性，例如都需要对重要流程进行拆分和风险评估、设置控制点、检查等。国内多家国有银行、股份制银行也都将法律与合规分离（见图9）。

此外，合规组织设置还有一个趋势：银行通过在总部设置统一的**卓越中心（COE）**，集中牵头管理具有重要监管意义和协同优势的议题，如反欺诈、反贪污、反洗钱等（见图10）。该组织一般由一名出色的全球领导带领一只小规模专家团队，接受董事会内执行运营委员会领导。

图7 北美某银行采用风险为主型的合规组织设置

设计理念

- 合规是**风险的一部分**并与法务剥离
- **合规独立于业务之外，由首席风控官直辖管理直到前线**
- 集团首席内控官**设定政策与内控活动**，确保整个集团内的规模经济（如反洗钱）

首席内控官/首席风险官的定位

- 集团首席内控官是全职职位，直接向集团首席风控官报告
- 合规的范围超过法务/监管事物，涵盖了人资与不动产，对客户与营收有直接影响但不负责客诉

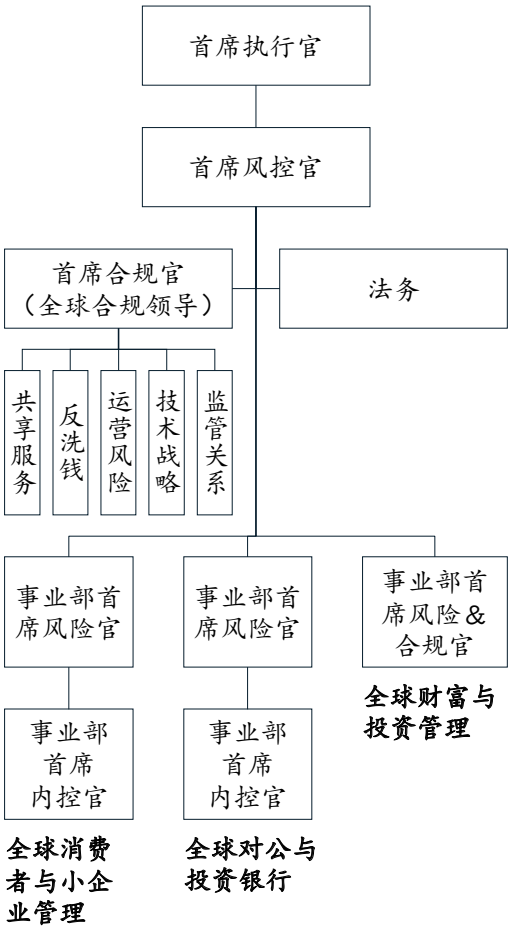
改革背景

- 欲提高效率并实现合规与整个风控组织内部的简化

其他考虑的选项

- 2004-2006：合规是独立组织，由首席内控官直接管辖到前线
- 2003：合规属于法务的一部分

组织结构



合规部门约950名员工

总部有300人

总员工（约17万7千人）0.5%为合规职能人员

所有合规人员有32%（950人中约300人）位于总部的合规职能

全球对公与投资银行的合规共有七个团队、60名员工，涵盖5,000-5,500名员工所从事的业务

资料来源：麦肯锡分析

图8 德国某银行采用独立的合规部门设置

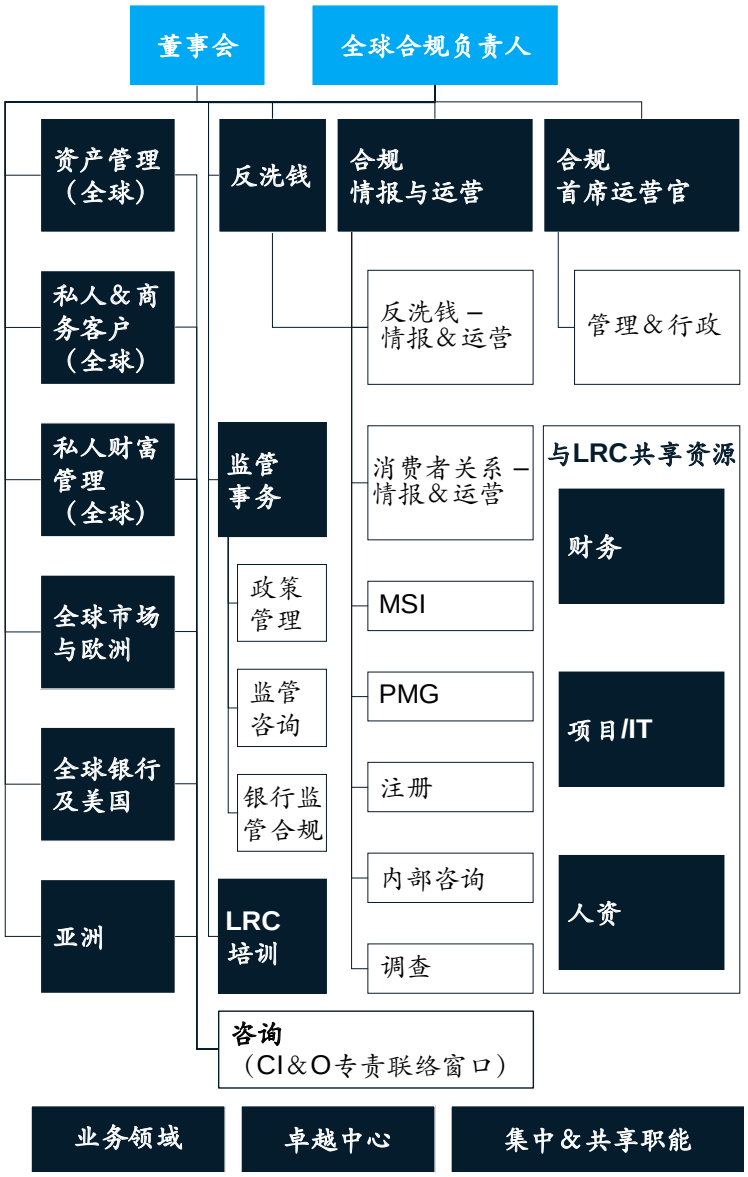
设计理念

- 合规是独立组织，由首席内控官直接管辖到前线
- **首席合规官/首席风险官的定位**
- 首席合规官**独立于风险条线**，独立向董事会及CEO汇报

改革内容

- 在总部设立**监管与培训的卓越中心，实现成本集约**
- 将所有的运营职能统一至合规运营官管理
- 强化**按业务领域进行的合规管理**，将一些**初级和合规职能下放和业务线合规管理总监**，如财务及人力决策等

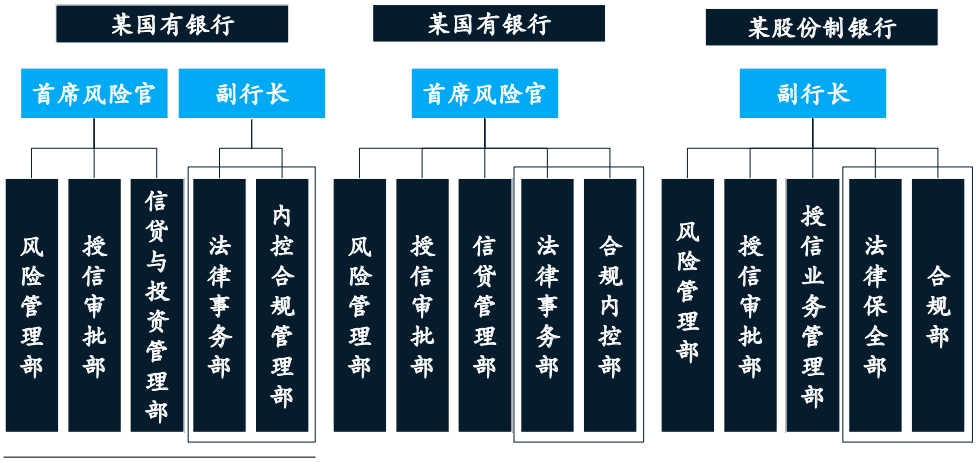
组织结构



启示：合规要与业务单元/经营机构紧密结合，同时对于一些有很强经济效应的模块在总部统一管理，如对接监管、培训及反洗钱等

资料来源：麦肯锡分析

图9 国内的大型银行机构采取法律和合规分离的架构

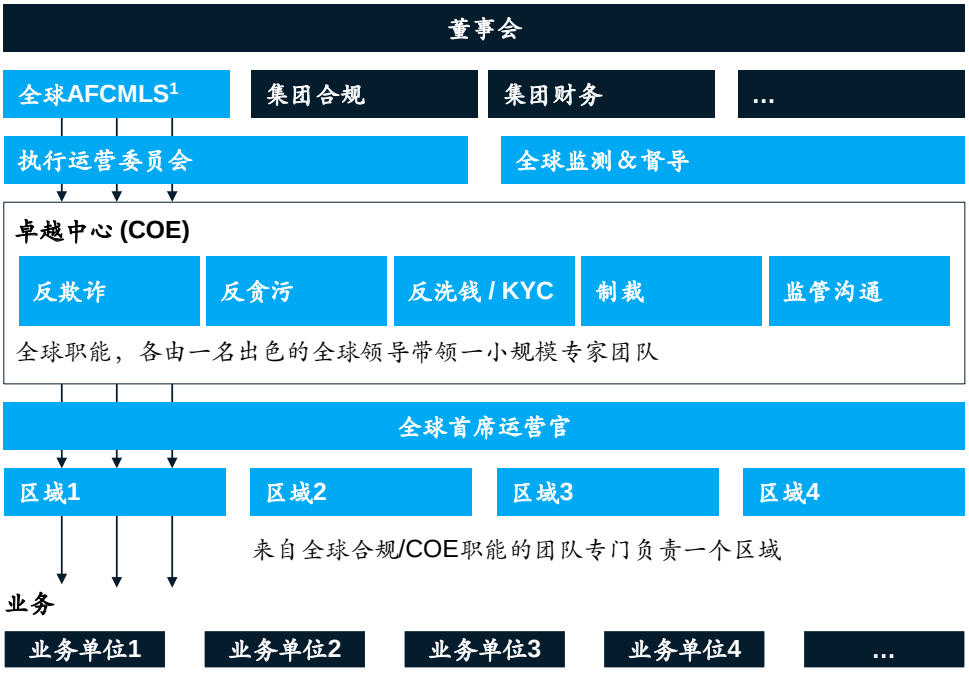


该国有银行的内控管理部统筹全行内控合规与操作风险管理，其下设置反洗钱管理、监测分析、操作风险管理、检查、集团合规管理、及按业务/产品分设不同管理中心等职能

资料来源：麦肯锡分析

图10 在总部设置反洗钱卓越中心 (COE)

示例: AML治理



第一道防线团队由各业务单位的内控领导带领

前线员工负责控管实施/保证

1 反欺诈/贪污/洗钱/制裁

资料来源：麦肯锡分析

举措二：构建全流程合规风险管理框架

全面的银行合规风险管理由覆盖端到端的五大步骤组成，即：识别、管控、监测、补救和报告（见图11）。概括而言，银行首先要对照适用的法律法规，将其转换成明确的政策要求，识别出具体合规风险；然后分解流程中的风险点，有针对性地设计、实施和管理管控点，并推行全行合规培训，确保规则深入人心；对接监管并做专项汇报，通过业务自查、合规独立监测的形式确保流程合规，期间设置结果型或预测型指标；对于内外部检查结果、法规变更等及时上报，弥补合规控制缺陷；最终整理关键风险指标（KRI）和违规事件，定期汇报，并为新的风险识别提供有效输入。以上这些工作，需要由银行第一道防线和第二道防线人员共同完成。

1. 合规风险识别

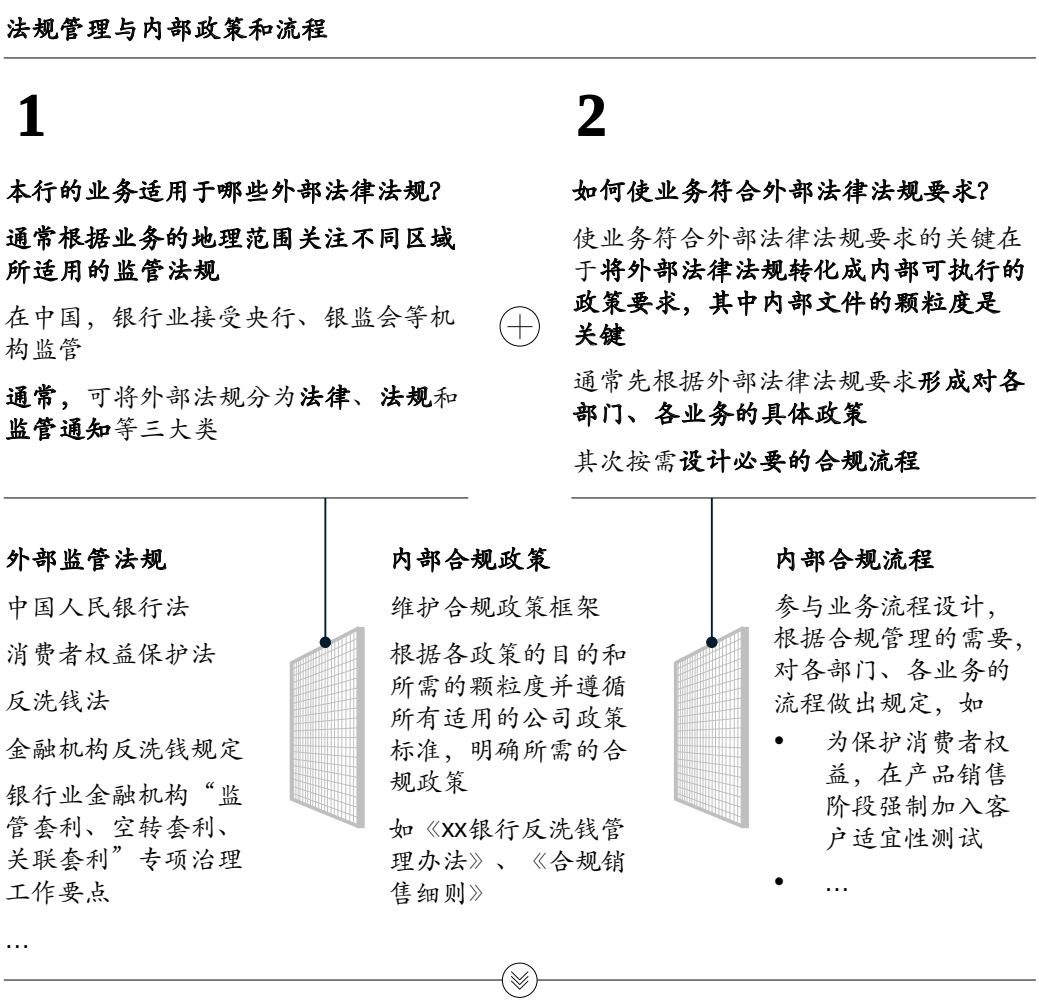
积极主动地识别和评估与银行经营活动相关的合规风险是银行合规管理的起点，包括新产品和新业务开发、新业务方式拓展、新客户关系建立或者客户关系性质发生重大变化所导致的合规风险等。而这个步骤的前提是要求合规部门持续盘点外部法律、法规并解读对业务的影响，并将其转换成明确的内部合规政策要求与合规流程（见图12）。

通过将合规风险整合入银行的风险与控制自我评估（RCSA）框架中，实施一体化

图11 合规管理的五大步骤

资料来源：麦肯锡分析

图12 将外部法律法规要求转换为内部适用的政策和流程



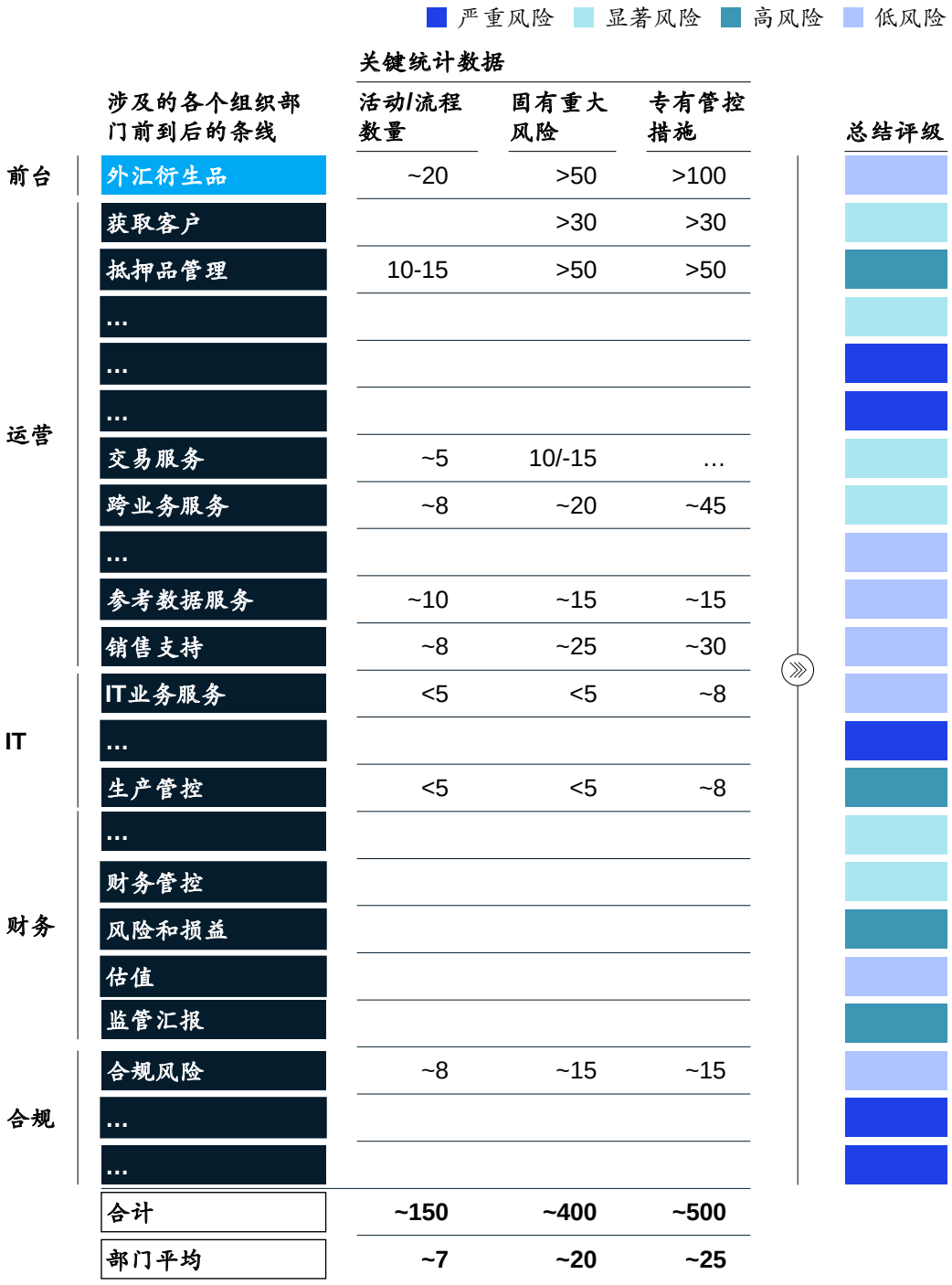
资料来源：麦肯锡分析

的风险评估，是识别合规风险的有效方法。系统化风控自评以一致的评分表为基础，可以提供沿价值链和流程各环节的风险视角（见图13），包括潜在合规风险。这些风险视角可以长期评估关键风险的重要性，并对未来风险治理进行优先排序。

2. 合规风险管控

风险管控设计有两大类，分别是检测型和预防型。其中，检测型管控通过对风险点进行检测，包括员工信件、资金账户监控、抽样检查等，及时发现可疑行为，一般用于事后管控、及时止损；而预防型管控则通过对风险点设置刚性控制，例如

图13 某银行一体化风险与控制自我评估 (RCSA) 结果



	涉及的各个组织部门前到后的条线	关键统计数据			总结评级
		活动/流程数量	固有重大风险	专有管控措施	
前台	外汇衍生品	~20	>50	>100	
运营	获取客户		>30	>30	
	抵押品管理	10-15	>50	>50	
	…				
	…				
	…				
	交易服务	~5	10/-15	…	
	跨业务服务	~8	~20	~45	
	…				
	参考数据服务	~10	~15	~15	
	销售支持	~8	~25	~30	
IT	IT业务服务	<5	<5	~8	
	…				
	生产管控	<5	<5	~8	
财务	…				
	财务管控				
	风险和损益				
	估值				
	监管汇报				
合规	合规风险	~8	~15	~15	
	…				
	…				
	合计	**~150**	**~400**	**~500**	
	部门平均	**~7**	**~20**	**~25**	

资料来源：麦肯锡分析

对交易系统设置严格的身份认证、禁止不明IP地址访问、设置第三人复核复验等，从而有效避免风险发生，一般用于事前管控，防患于未然。

因此，在实际应用中，管控体系往往结合两者所长，而且越是通过系统自动实现的预防型管控，效果越好。

此外，合规部门还需要通过开展合规培训进一步支持银行的合规管控。具体包括设计合规政策框架等培训计划，对业务、风险管理及合规部门员工进行需求评估、制定培训计划并实施和跟踪计划等。

3. 合规风险监测

合规风险监测通过监测已知合规问题，并致力于发现未知的新问题，可以帮助银行预防和预警各类合规风险，为后续补救措施提供依据，确保整体合规管理有效落地。典型的合规风险监测包括三大步骤：

- 首先，需要清晰界定监测问题类型，帮助银行确定所需监测的业务活动范围。领先实践一般通过对于监管检查的发现和内部自查的典型案例分析来确定该银行所面临的重点合规问题，通常是长期合规相关问题，例如交易行为、客户服务、员工行为等。

图14 合规数据收集与洞见示例

	数据源	分析洞见示例
交易	**静态账户数据**	根据免除特征确定**不属于怀疑授权缺失的帐户**，例如， 线上渠道发起 客户在该行的唯一账户
	交易数据	根据**资金到账和支出模式确定某帐户模拟资金**的可能性 根据账户利用情况调查客户需求
客户	**社会经济和人口数据**	**揭示不当销售的事例**（例如，储蓄产品不适合收入水平） 揭示**系统歧视问题**（例如，某地区某些种族的账户数不具有代表性）
	投诉	通过**模式识别**，识别**那些单个事例影响不大但高度系统化的做法**
	客户满意度调查	通过涵盖人口统计学的联合分析，揭示**系统性的歧视或不当销售问题**
员工	**HR数据**	**确定每个员工基于回归分析的风险评分**，例如，根据包括**年龄、工作时间、销售业绩变化、培训参与情况/测试成绩、过往问题**等因子的分析
	员工沟通	通过沟通内容（电子邮件、聊天、电话）或做法（例如，电子邮件串深度、发件人/收件人模式）来**识别问题**
	检举热线	通过**模式识别**，识别那些单个事例影响不大但高度系统化的做法

资料来源：麦肯锡分析

– 在确定所需监测的问题类型后，合规部门需要针对这些问题开展数据收集和汇总工作。通常而言，不同的待监测问题需要不同的数据信息，而最有效的监测需对多个数据来源进行独立及合并分析（见图14）。

– 根据业务特征和银行自身能力，可采用一系列方法分析合规数据，例如：关键词分析、异常值分析、基于规则和阈值的分析、风险评分和机器学习算法（见图15）。最基本和简单的方法是关键词分析法，通

图15 合规数据的可选分析方法

复杂程度：低 → 高

	具体说明	优点 ✓	缺点 ✗
关键词搜索	搜索表示销售做法有问题的关键字文本（例如，“不需要的”） 筛选投诉、检举和客户满意度调查数据	简单，成本低 容易适应	需事先知道关键词
异常值分析	通过风险指标及其偏离规范的程度，凸显出涉嫌账户或个人 检测受影响的帐户和员工	简单，成本低 可进行趋势分析	需事先知道风险指标
规则和阈值	根据预先确定的特征缩小涉嫌帐户或客户人群 检测/排除受影响的帐户和员工	简单，成本低	团队成员容易博弈 产生大量的误报 (> 80%)
定性风险评分	基于专家判断加权的风险因素对员工或账户的风险性进行排序 员工或账户的风险评分	简单，成本低	易受专家偏见的影响 只考虑变量之间的线性关系
量化评分模型	基于风险因子加权回归分析对员工或账户的风险性进行排序 员工或账户的风险评分	基于证据	非常依赖专家的变量选择假设 只考虑线性关系 需要高质量的数据 需要样本问题来训练模型
机器学习算法	有多种自适应算法使用方式来改进上述的分析： • 非直观变量 • 数据中的非线性模式 员工或账户的风险评分 筛选投诉、检举和客户满意度调查数据 检测/排除帐户和团队成员	基于证据 考虑变量的复杂关系（难以博弈，误报率低）	需要来自多个关联来源的高质量数据 可能需要样本问题来训练模型

资料来源：麦肯锡分析

过搜索代表有问题员工行为的关键词，如“不需要的”、“强制的”等，筛选客户投诉、检举和客户满意度调查数据，该方法简单有效，但需要事先知道尽可能多的关键词；另一种比较常见的方法是异常值分析，通过比对账户或个人的风险指标及其偏离规范的程度，确定潜在问题。

4. 合规风险补救

合规管理部门应根据监管调查、内部审计报告、法规变更、合规工作产出结果（如监测报告或测试中提出的合规控制失败问题）或经认可的优化机会（如减少某些导致合规控制不够严格的风险），对合规工作进行补救和挑战，弥补合规控制缺陷。

5. 合规风险报告

合规报告工作包含记录并追踪监测关键风险指标（KRI）和测试结果，收集所有相关合规工作中的指标、违规事件并审查，上报合规工作中发现的问题和异常情况。

举措三：打造数字化、有针对性的运作模式、流程与系统

银行需要针对特定高风险合规问题制定具体的风控运作模式、流程，并建立起相应的监控和分析系统，以强化其在这些合规风险领域的管控力度。同时，前沿国际领先银行的合规管理正聚焦在流程再造，通过机器学习和高级分析等方法实现人机结合的高效流程管理，在减少合规工作量、减少合规管理人工成本的同时，利用先进技术和方法提升管控能力。

1. 建设数据湖等合规数据平台，夯实数字化合规流程的数据基础

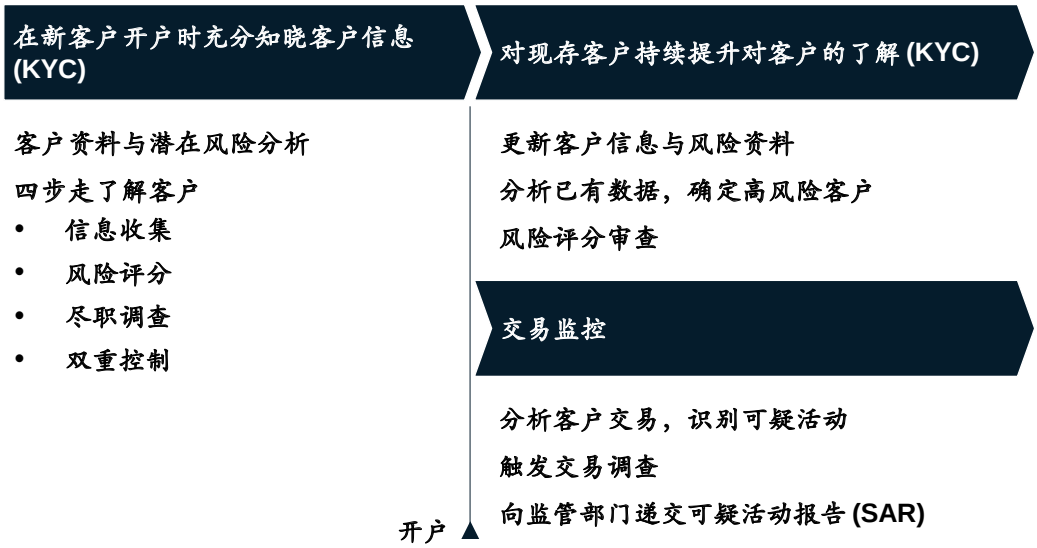
国内银行在数字化合规管理上的一大痛点和难点，是缺乏针对合规管理的数据湖等数据基础，仍普遍采用传统的报表式简单系统，且系统内未收集用户行为数据等可用、高价值的合规管理分析数据。数字化合规流程的打造，首先需梳理合规风险相关的业务数据，打造合规管理数据湖，借助高级分析和机器学习，收集并结构化整理各类合规管理相关数据。以德国某领先银行为例，其耗时两年时间，将100多个不同业务系统的数据串联起来，建成合规管理数据湖，方为合规管理流程的数字化和自动化奠定坚实的数据基础和系统基础。

2. 数字化流程改造，重塑与整合合规风险管理流程

传统的合规风险管理流程，不同环节由不同业务部门甚至是不同条线负责，导致很多流程和数据都未能形成有效整合。在已夯实合规数据基础的前提下，整合并数字化改造合规流程，将进一步提高合规管理的效率与质量。

以反洗钱为例，领先银行可以利用前述的卓越中心，由业务线或区域负责人指定一位高管负责制定并维护反洗钱体系和控制机制，具体职责包括：领导年度风险评估并基于评估结果制定和实施相应

图16 反洗钱合规风险管理的核心流程

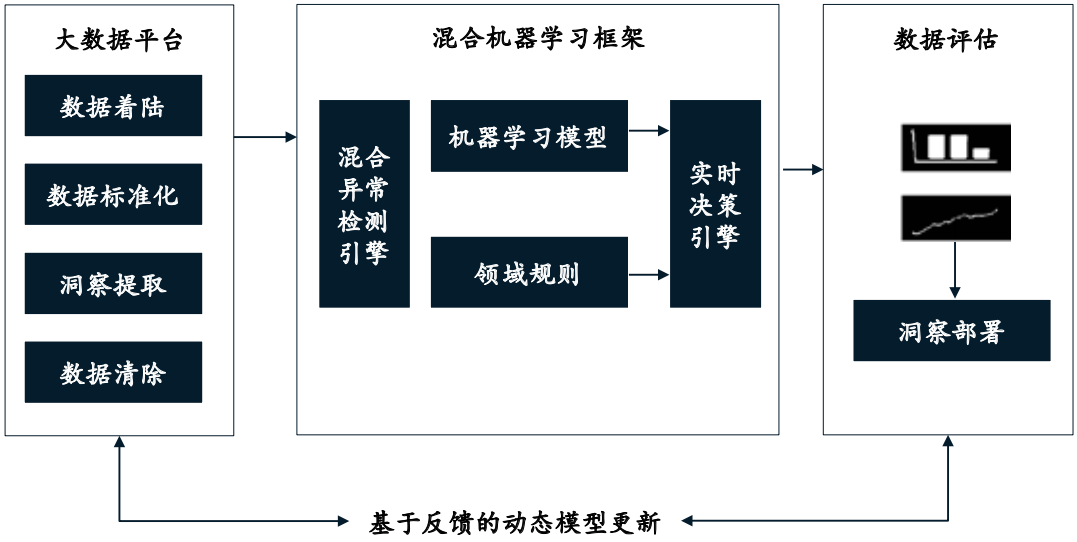


资料来源：麦肯锡分析

行动，听取反洗钱管理报告并制定应对举措，针对潜在短板实施及时、有效的提升方案，以及确保有足够的资源投入到反洗钱管理中等，从而让第一道防线深度参与到反洗钱管理中。进而有针对性的改造合规风控流程。典型的反洗钱管理流程包括掌握新客户信息、持续提升对现存客户的了解度以及账户交易监控（见图16）。充分掌握和持续更新客户信息是有效管控洗钱等违规问题的先决条件。领先银行机构更是实现了该流程的数字化和自动化，通过构建一个统一的客户信息平台（CIP），按既定信息维度将客户信息都存储在该平台上，并利用系统和模型对客户自动进行风险评分，主动识别出潜在高风险账户，必要时告知相应人员对特定客户进行深入的尽职调查。除了客户开设账户所提供的直接信息之外，银行内部的历史自查报告、外部审计报告、客户投诉和处理信息等，也能给合规管理提供大量有价值的数据。

在掌握了大量真实客户信息的基础上，银行可以借助系统和高级分析方法实施监控客户账户交易，尤其是高风险账户。合规监控团队可将过去的洗钱违规行为进行组合分析，总结常见的违规问题类型以及与之高度关联的定量指标，然后比对分析各指标的显著性，最终确定反洗钱监测的核心风险指标体系（KRIs）并构建合规风险预警模型。在这个过程中，银行需要持续完善监控合规风险的模型，通过机器学习等不断涌现的先进算法降低未识别出问题的概率，并提升自动化监

图17 基于机器学习的高风险及异常行为检测平台



资料来源：麦肯锡分析

测和处理的工作比例。同时，团队还需要制定相应的反洗钱调查流程，确保系统发出不同预警情景后，银行拥有全面的应对和升级处理机制，并在定位违规后向监管部门提交可疑活动报告。

3. 借助高级分析与机器学习等先进技术，实现人机结合的合规管理闭环

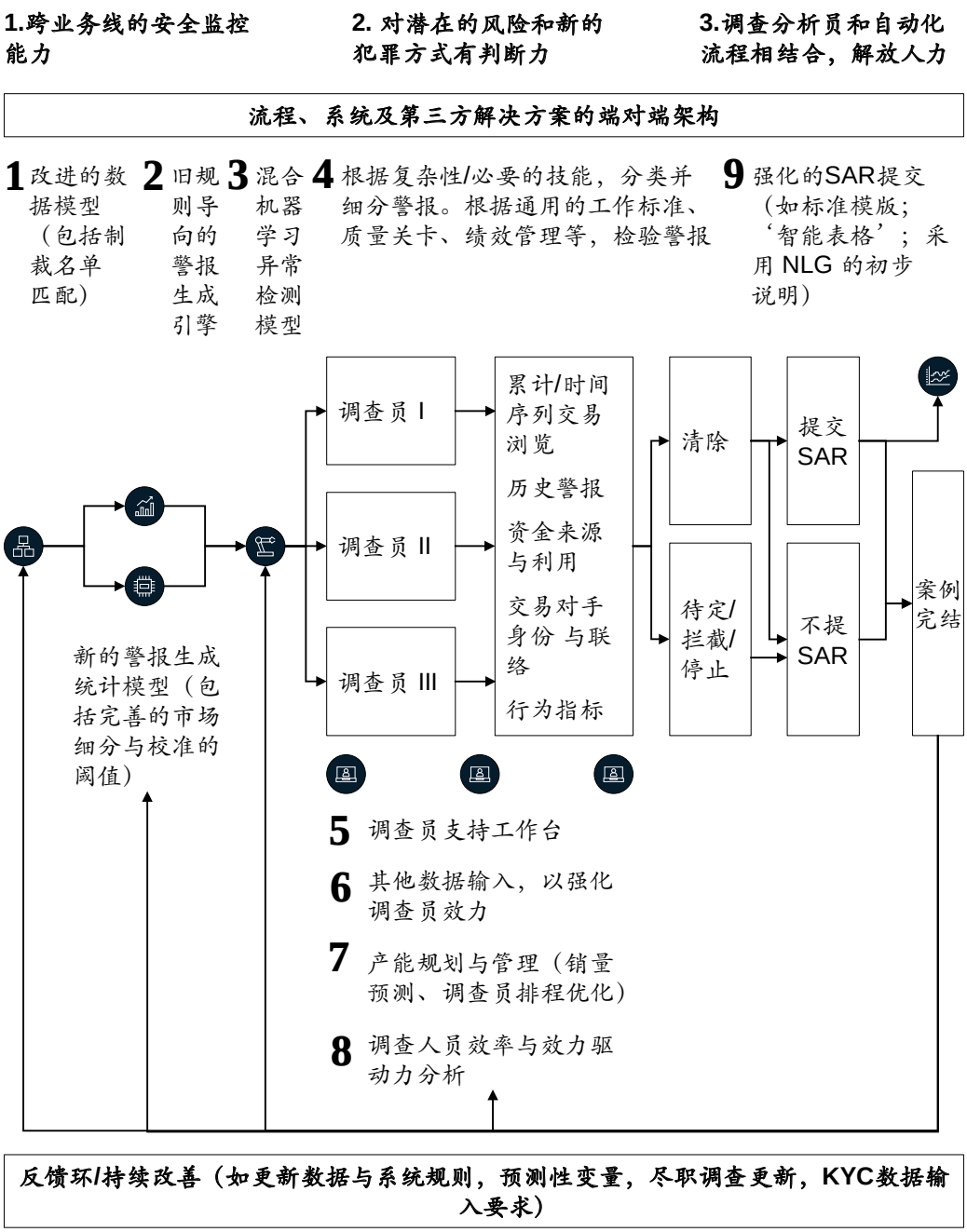
机器学习在数字化合规流程再造中扮演着重要角色：一是可将非结构化数据（如合同报表类文字数据、图片数据等）转化为结构化数据，大幅提高流程的数字化程度和工作效率；二是可实现行为数据的快速分析。例如，通过混合异常检测引擎和机器学习模型，可结合检测监督和无监督行为，并可检测不同领域的异常行为（含集群分析、密度分析、顺序分析和网络分析）；将领域规则评估融入实时决策引擎，再根据高风险可能性，可对客户和内部员工行为进行分析和排序（见图17）。

但我们仍需认识到，机器学习和高级分析不是银弹，无法承担全部合规风险管理职责。通过机器学习提高流程管理的数字化和自动化，提高合规人员的决策准确度和决策效率，并通过合规人员决策结果不断优化机器学习和高级分析模型，最终形成人机结合的合规管理闭环，才是构建数字化合规流程的最优解。

以德国某领先银行为例，传统警报引擎提供监管规则引发的合规案例分析，机器学习引擎提供传统规则外无法识别的异常点，并且收集案例相关事实信息，进而基于合规人员工作效能进行优先级排序，最终呈递给合规人员做合规案例判

断和决策。合规人员最终决策的结果及原因阐述，会收集进决策引擎中，帮助机器学习引擎不断优化和更新，从而最终形成人机结合的、高效高质的合规管理闭环（见图18）。

图18 德国某银行的数字化合规流程改造

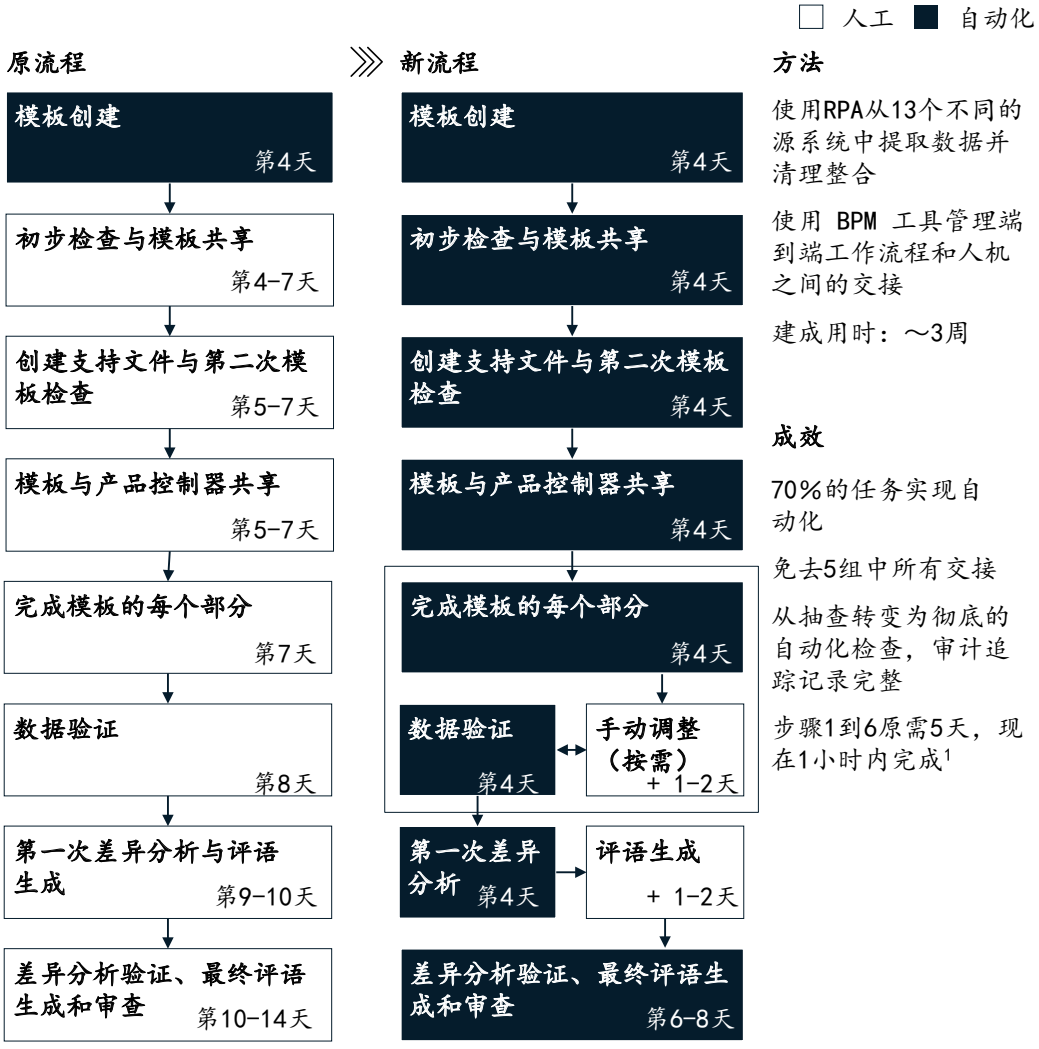


资料来源：麦肯锡分析

麦肯锡在数字化合规流程方面积累了丰富的经验和解决方案。例如，麦肯锡的合同到期报告流程自动化方案，可实现70%的任务自动化，报告周期能缩短4天以上（见图19）。

麦肯锡所收购的高级分析公司QuantumBlack，同样可为客户提供一个工业级的机器学习平台。以欺诈管理为例，该平台可帮助银行将回收价值提升95%，欺诈发生率降低86%（见图20）。

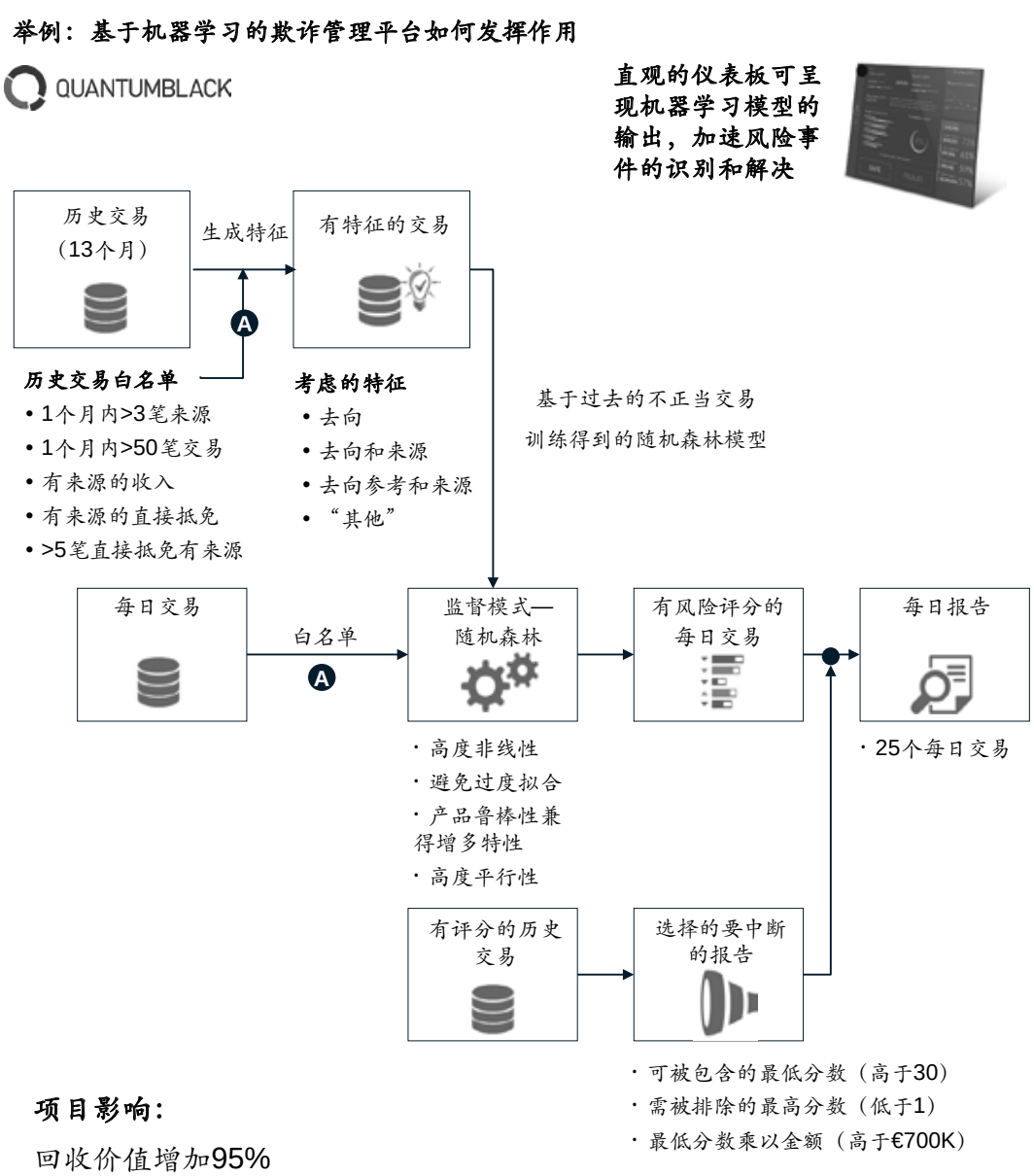
图19 合同到期报告流程自动化



1 假设在自动化流程执行中没有发现异常

资料来源：麦肯锡分析

图20 QuantumBlack 工业级机器学习平台



资料来源：麦肯锡分析

高级分析也可帮助企业极大改善风险监测效率，具体体现在三方面：

第一、数据整合和分析，包括明确定义要监测的风险问题分类、清楚了解并集成可用的数据源、通过标准化和数据清洗练习提高数据质量、为已知问题全面开发标准化分析方法等。例如针对财富管理业务开展数据整合和异常值分析（见图21）。

图21 财富管理中的数据整合和异常值分析

目标和方法

目的：

通过对客户投资组合的异常值进行分析来发现潜在的理财顾问的行为问题

方法：

整合各种来源的数据，例如投资组合头寸、交易、收入、静态账户数据、理财顾问相关信息

根据中小企输入和行业**对标选择指标**

定义适用的**投资组合子细分**（例如客户年龄、资产）

进行各组合的异常值分析，与各细分平均数相比对

样本输出

来自各种数据源的部分指标

相关细分群组

表示可能问题的异常值

	细分平均数：70+，$ 250k - $ 500k	**客户X**
本金周转率	32%	593%
权益本金周转率（Equity Principal Velocity）	46%	1406%
资产回报率（不含现金）	0.87%	6.78%
权益成本	0.40%	8%
新发股成本	3%	30%
每交易日交易次数	2.9	2.7
非现金头寸数	11.5	4
头寸集中度	29%	48%
管理账户的周转率较低（Low Managed Account Velocity）	46%	不详
权益集中度同比变化	-1%	-38%

资料来源：麦肯锡分析

图22 构建员工风险评分模型

目标和方法

目标：

根据**每个员工产生行为风险问题的可能性**给每人分配一个风险分数，然后对其排序

方法：

选择样本员工，包括有否行为违规先例（因变量）

从各种来源**收集原始数据**（例如人力资源数据、沟通数据、客户数据）

基于专家假设（例如，激励薪酬的同比变化）**将原始数据转化为自变量长清单**

进行**单变量分析和主成分分析**以确定变量的预测能力和敏感性

选择变量短清单并构建候选人回归模型

基于绩效和业务直觉选择模型

样本输出

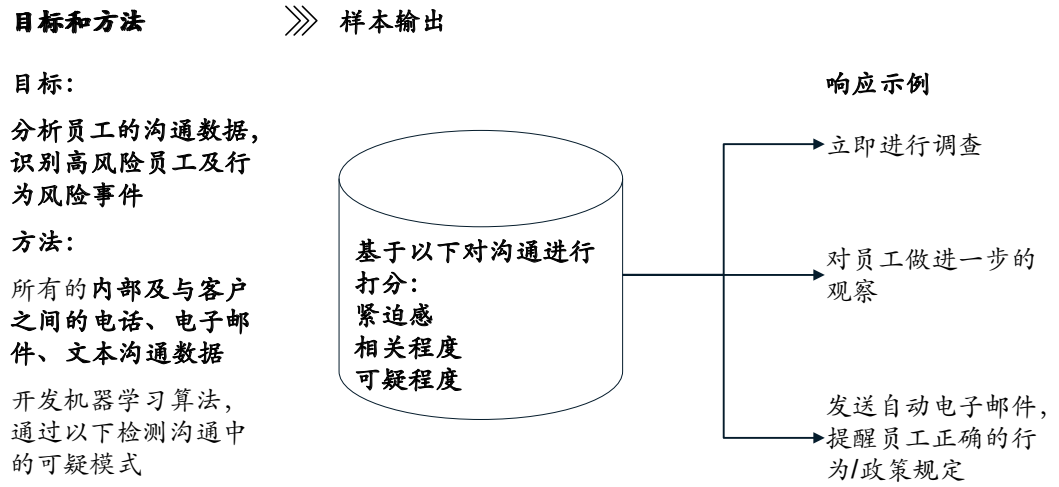
#	得分	员工 ID	事件数量	自首次事件后的天数	预警状态	严重性
1	5.7	1423254	4	2天	已创建	高
2	4.8	8347274	2	4天	已升级	中
3	4.6	4837658	5	3天	已创建	中
4	4.1	2834750	1	8天	已升级	中
5	3.9	3749390	4	1天	已创建	低
6	3.6	4938457	8	5天	已升级	低
7	3.5	7456432	5	2天	已创建	低
8	2.8	5743728	4	6天	已升级	最低

资料来源：麦肯锡分析

第二、应用传统高级分析技术，包括进一步集成数据源、改进分析方法，开发多类模型进行回归建模等，以准确识别已知问题。例如构建员工风险评分模型（见图22）。

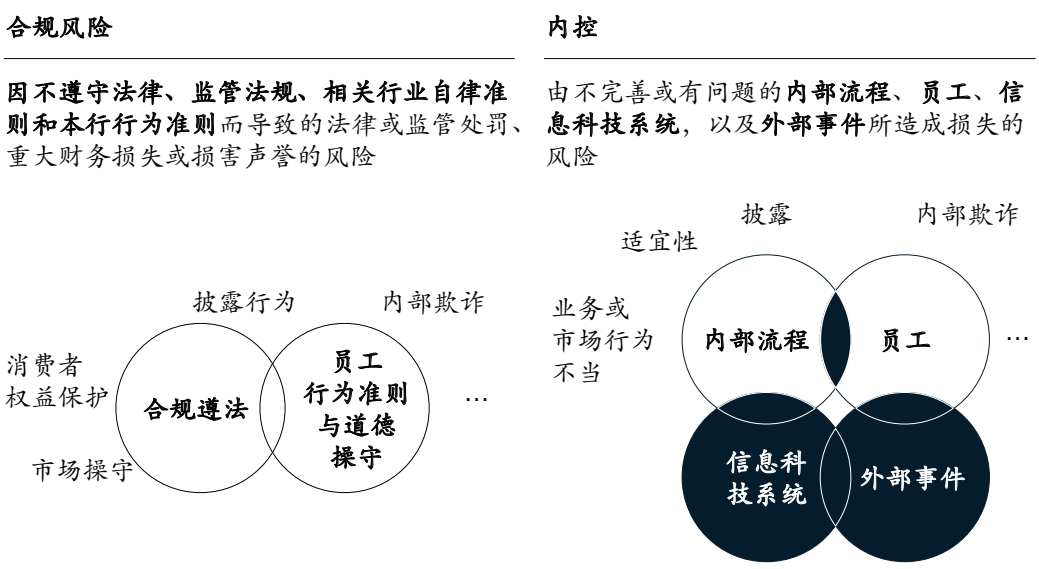
第三、应用机器学习技术。包括进一步改进识别已知问题的分析方法，例如监督式机器学习模型以及开发定制分析方法，如通过无监督式机器学习技术来识别新的未知问题（见图23）。

图23 开发机器学习模型



资料来源：麦肯锡分析

图24 银行合规风险与内控的区别



资料来源：麦肯锡分析

举措四：培养“主动合规”理念与文化

构建银行合规管理能力，需要在合规管理理念、合规管理范围等方面在全行建立起正确、统一的认知，并能敏感把握合规管理的最新发展趋势，进而在全行培养起“主动合规”的文化、重塑员工合规行为。

银行管理者首先需要认识到，合规管理的定义与银行内控有一定重叠，但二者的管理侧重有所不同：**合规侧重于从外部监管角度审视银行现有业务及流程、制度是否符合法律法规要求，而内控则侧重于监控银行流程中的风险管控设计是否合理、业务是否按章执行**（见图24）。

除保证外部法律法规在本行的落地外，越来越多的银行纳入了新兴的合规职责，例如员工健康和安全、不当业务或市场实践等，帮助企业在更大范围内履行对利益相关方的责任（见图25）。

与此同时，业界也在不断地探索和完善合规管理实践。金融危机后，随着监管升级与合规成本不断提升，全球银行业加强了对合规管理的重视与投入，并呈现出以下三大演变趋势。

- **从被动应对监管走向主动合规。**这是最为明显且影响深远的变化趋势。传统上，合规管理以制定规则、政策并控制业务活动为主；而今，合规部门开始更多地介入到业务活动改造过程，在积极协助业务部门制定目标的同时，致力于减少合规风险。
- **管理范围更广泛。**从原有的满足监管合规，扩大到关注员工行为、银行声誉和可持续性等更为广泛的议题，并增加了对内部规范、价值观和市场标准的关注。因此，利益相关者也从原来单一注重监管部门、应对审计发现，转变为更广泛的全面合规关系，包括股东、客户、员工和当地市场等。
- **管控强度进一步提升。**大部分银行加大了对合规负责人的管理授权，甚至将其业务汇报关系升级至董事会层面。同时，管控覆盖模式变得更为灵活，以平衡区域和业务层面的需要，包括利用集中化专家组和专职运营团队，帮助银行提升合规管理能力，更有效地配置合规管理人力资源。

基于追求“主动合规”、合规管理范围与强度不断扩大的行业趋势，银行建立一种强大的合规文化，是提高合规管理有效性的重要保障。而这背后，需要高层以身作则，董事会和高级管理层确定合规基调，树立正确的合规理念，并提高全体员工的诚信意识与合规意识，从而形成良好的合规文化。

全球领先实践经验表明，成功合规文化与行为塑造包含三项重要内容：**高管之声、合规培训体系和结果管理。**

- **高管之声：**从银行高管层面发声，显示出高管团队对合规文化和行为的关注，公司高管身体力行，建立对理想行为的期望、树立榜样并监督合规项目的执行，这是全行合规项目落地的坚实保障。高管之声可以帮助银行提高

图25 广义合规管理帮助企业履行对利益相关方的责任

监管方和股东

应对法律/监管要求	机构信息及公司治理	会计与财务报告	审慎经营合规监督	管理与监管方的关系	知识及工业产权

客户[1]		**员工**		**社会**	
识别客户	**公正对待客户**	**人力资源管理**	**行为端正**	**供应商**	**负责任的财务（部门）**
KYC了解客户	投诉及诉讼处理	寻找资源及资源筛选	利益冲突	供应商筛选	不当的业务或市场实践[2]
反洗钱	产品及业务审批	绩效管理	保密和隐私		税务义务
观察名单	隐私和数据保护	奖励	腐败		避税活动
	具体的客户保护规定	健康与安全	股市行为		
	信托	工会活动			

业务运营

将法律法规转化成运营要求	风险严重性标准以及识别/评估工具（取决于合规与风险管理部门之间的划定）	行为风险的职责定义

1 包括现有客户及联系过银行的潜客
2 反托拉斯、不当交易、市场操纵、内线交易、牌照外经营活动
资料来源：麦肯锡分析

合规文化和行为在全行的重要地位，建立对理想行为的期望、树立榜样。其中，监督合规项目执行是高管之声的关键，通过及时处理不合规业务及人员，明确高管层对合规管理的支持。

- **合规培训体系：**包括培训内容体系、培训形式、培训强化机制等三大方面。好的合规培训体系能实现培训内容“按风险事件、按岗位定制”、培训形式引人入胜、建立正式的培训监测机制并对未按要求进行培训的行为进行严肃处理。

- **结果管理：**注重对过程的违规问责，可帮助组织自我强化合规文化。通过设置完善的内部举报机制，鼓励员工成为管理不合规问题的第一道防线。同时，对于违规行为及时适当问责能强化正向合规文化。领先实践更注重过程违规问责，不仅要求当事人及时整改，还与当期个人考核直接挂钩。

■ ■ ■

面对愈加严峻的监管形势和企业自身的能力建设需求，国内银行应大力推动合规治理架构和管理框架，积极探索与业务相结合与适应的合规流程和系统，主动培养合规意识与合规文化，从而搭建起完善的合规管理体系，形成卓越的合规管理能力，帮助银行自身更好地履行对监管方、客户、员工和社会的责任，同时不断地提高企业的内部运营效率和可持续发展能力。■

关于麦肯锡中国区银行咨询业务

麦肯锡中国银行咨询业务致力于服务本地区领先和具有成长潜力的商业银行及投资银行，通过打造效益驱动的解决方案，帮助客户建立可持续的核心竞争力，取得持续的商业成功。

我们在中国拥有近300的银行业务核心咨询团队，专注于银行的整体转型、创新和并购等战略咨询，并提供端到端的方案设计和实施支持。主要包括五大类型：总体转型与创新战略规划，金控集团的战略及管控，具体业务业绩提升方案，客户体验提升，以及战略导向的风险管理和资产负债管理体系设计。同时，我们协助银行进行全面的组织能力升级和核心能力建设，包括领导力建设、事业部制改革、设立创新组织、打造大数据能力、协助双速IT转型等。与此同时，我们依靠麦肯锡遍布全球的金融机构专业咨询顾问和调研及分析人员的庞大资源体系，汲取智慧并有力地支持我们为本地区的客户提供服务。

关于作者

倪以理

全球资深董事合伙人
香港分公司
Joseph_Luc_Ngai@mckinsey.com

曲向军

全球资深董事合伙人
香港分公司
John_Qu@mckinsey.com

周宁人

全球董事合伙人
深圳分公司
Nicole_Zhou@mckinsey.com

徐天石

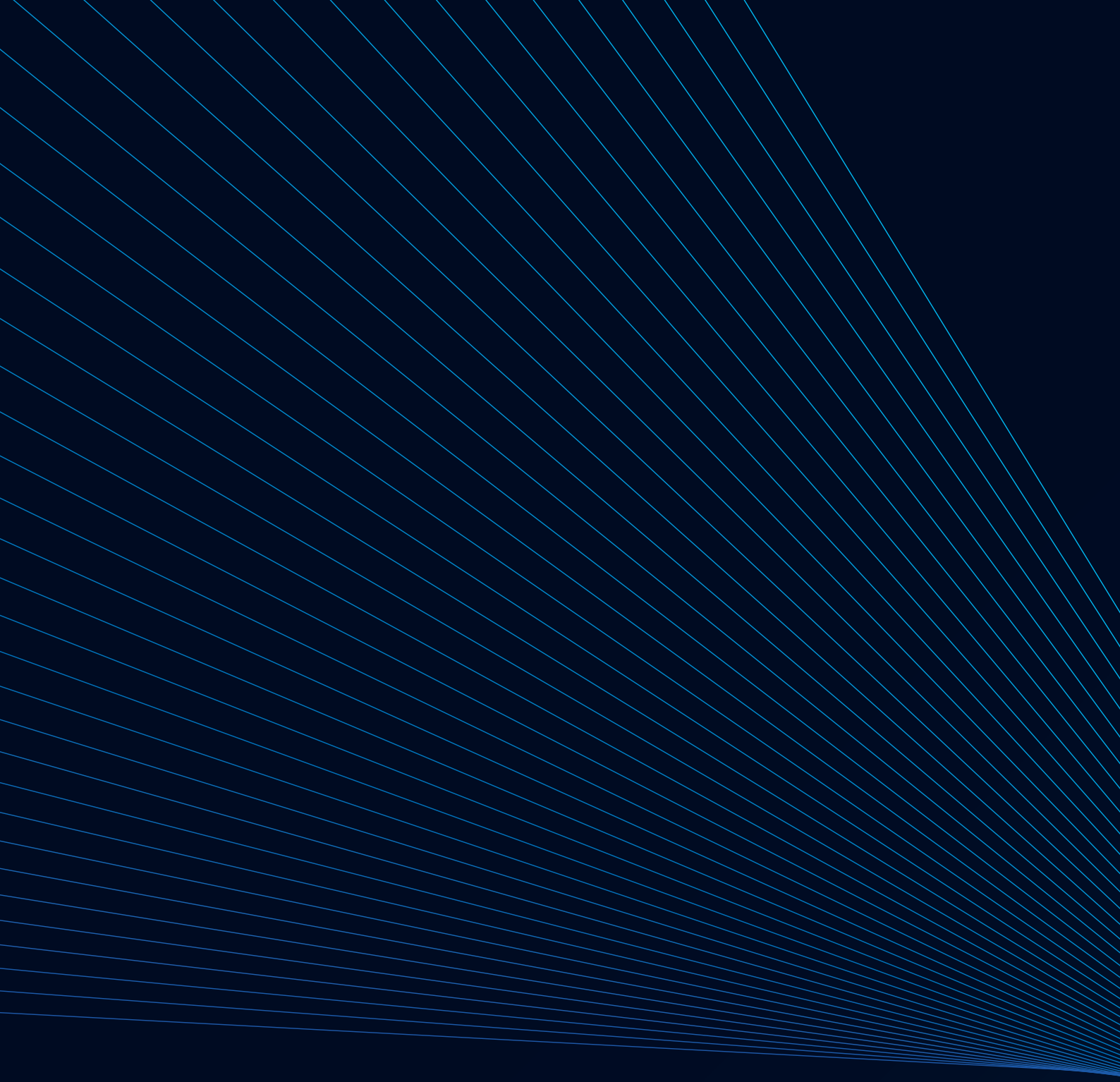
全球副董事合伙人
北京分公司
Kent_Xu@mckinsey.com

陆澄

咨询顾问
香港分公司
Michelle_Lu@mckinsey.com

王鹏

咨询顾问
深圳分公司
Jackie_Wang@mckinsey.com



麦肯锡中国银行业转型与创新系列白皮书
2019年8月

麦肯锡中国区新媒体设计出品

www.mckinsey.com.cn