KPMG
毕马威

2025年上半年
商业银行内审观察

毕马威 创见不同·智启未来

kpmg.com/cn

2025年9月

刊物简介

毕马威“内审观察”系列为商业银行内部审计服务专题报告。我们持续跟踪国内外内部审计理论发展、银行业重要法规及监管政策变化、监管检查与处罚动态、市场变化及舆情信息等，运用毕马威专家团队丰富的行业经验及专业解读，及时与您分享内部审计相关的风险洞察与应对建议。

目录

1 监管规则追踪

跟踪监管新规变化，对重点新规进行详细解读，提示内部审计需关注的重点事项 04

2 监管处罚洞察

跟踪监管处罚变化，洞察监管处罚重点及趋势，就重点关注领域及违规形态提请内部审计关注 12

3 敏捷审计专题

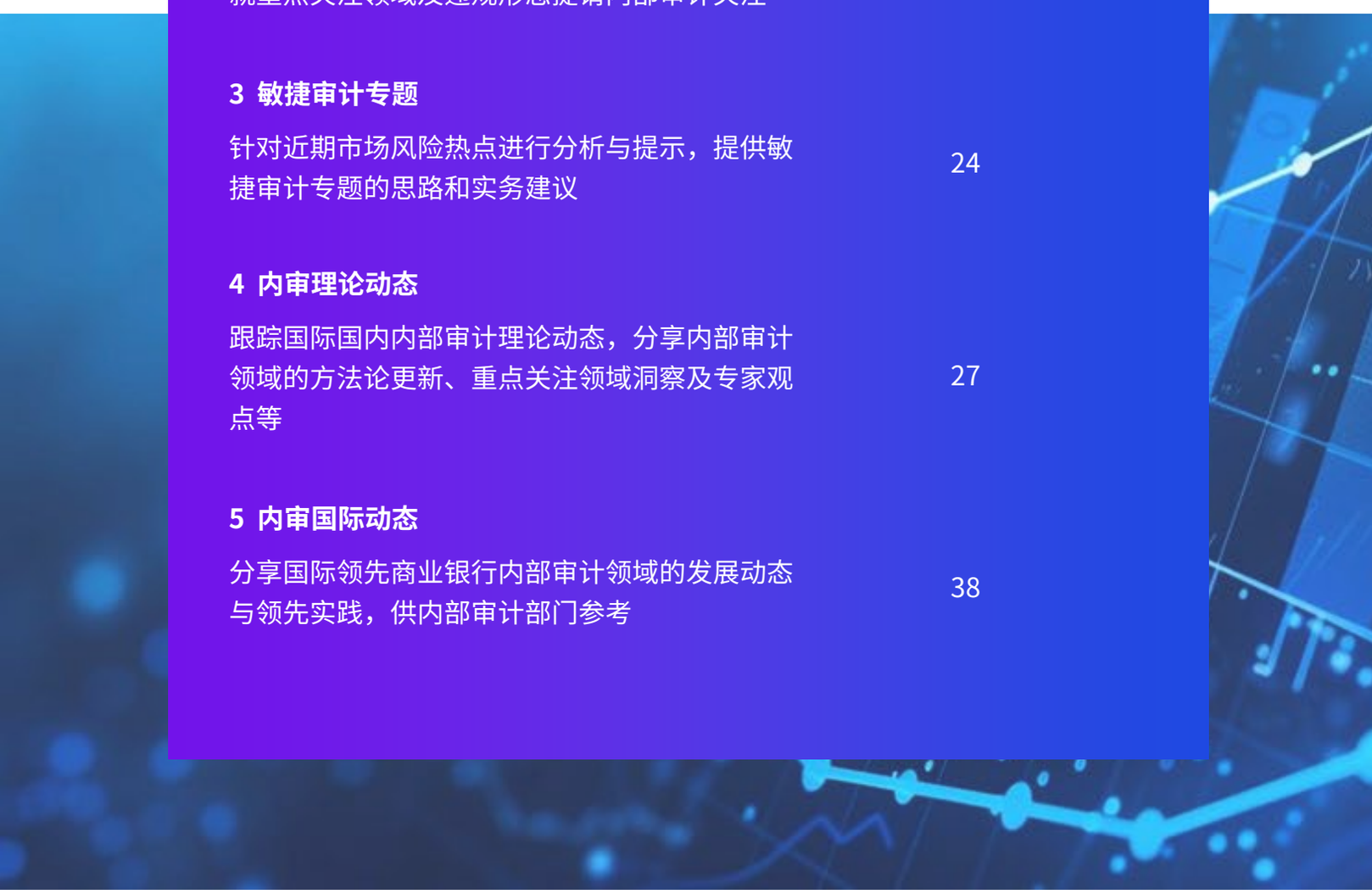
针对近期市场风险热点进行分析与提示，提供敏捷审计专题的思路和实务建议 24

4 内审理论动态

跟踪国际国内内部审计理论动态，分享内部审计领域的方法论更新、重点关注领域洞察及专家观点等 27

5 内审国际动态

分享国际领先商业银行内部审计领域的发展动态与领先实践，供内部审计部门参考 38



1. 监管规则追踪

监管新规变化

2025年上半年，全国人民代表大会常务委员会、国务院、财政部、中国人民银行（“人民银行”）、国家金融监督管理总局（“金融监管总局”）、中国证券监督管理委员会（“证监会”）、国家外汇管理局（“外管局”）等监管机构、行业自律组织、交易所等共发布154篇重要新规及征求意见稿。从涉及领域和重点规范事项来看，主要影响经济促进、资本市场、证券业务、债券业务、信贷业务、金融市场业务、非银机构管理、监管变革、“五篇大文章”、风险管理、反洗钱等业务及管理领域。科技创新与提振消费被共同列为政府工作重点，金融监管机构围绕这两个主题颁布了多项金融领域的工作方案与通知意见。

全国人大、国务院、人民银行、金融监管总局、证监会等亦公布2025年立法工作计划，《金融法》《金融稳定法》《中国人民银行法》《银行业监督管理法》《商业银行法》《地方金融监督管理条例》等金融业根本性重要法律法规均在酝酿出台，金融监管机构亦在加速制定针对各类机构、业务的更新规范。

内审关注要点

我们总结了重要的新规涉及领域、法规核心要点及关注事项，建议内部审计重点关注。

法规名称	涉及领域	法规核心内容暨内审关注事项
上市公司审计委员会工作指引	公司治理	• 明确上市公司设立审计委员会的要求，并明确委员会构成、成员任期 • 规范审计委员会工作职责、前置审议事项等
银行业金融机构董事（理事）和高级管理人员任职资格管理办法（2025）	公司治理	• 优化调整董监高人员选拔任用程序和标准 • 新增任职资格报告制度，针对无需适用核准制的董监高人员，规范了报告制的管理要求
《国家金融监督管理总局关于修改部分规章的决定》（涉及《银行保险机构关联交易管理办法》）	关联方及关联交易	• 要求按照实质重于形式和穿透监管原则，优化关联方和关联交易识别 • 明确在管理机制、穿透识别、资金来源与流向、动态评估等方面的具体要求
商业银行市场风险管理办法	市场风险管理	• 明确市场风险定义，不再包括银行账簿利率风险 • 完善市场风险治理架构方面要求，强调在集团并表层面加强市场风险管理 • 细化市场风险流程管理要求，包括内部模型管理、压力测试等
银行业保险业绿色金融高质量发展实施方案	对公信贷、绿色金融	• 要求完善绿色金融服务体系，优化银行信贷供给，丰富绿色金融产品服务 • 健全环境、社会和治理风险管理体系，加强风险识别、评估与监测，不断细化优化行业投融资政策 • 建立健全绿色金融统计数据管理制度，完善信息披露机制、建立绿色金融考核评价体系和奖惩机制

说明：根据监管机构网站公开发布信息自行编制。

法规名称	涉及领域	法规核心内容暨内审关注事项
关于做好金融“五篇大文章”的指导意见	对公信贷、个人信贷、养老金融、数据治理	• 要求丰富绿色金融和转型金融产品服务，强化绿色金融数据治理，防范“洗绿”、“漂绿”风险 • 推进“信易贷”工作、“一链一策一批”中小微企业融资促进行动，探索拓宽生物性资产、养殖设施等 抵质押资产范围，满足普惠小微主体多样化融资需求 • 加强养老资金投资管理，丰富产品体系，建设针对养老金融的统计指标体系 • 规范发展“贷款+外部直投”、知识产权质押贷款等产品服务模式，优化科技型企业贷款服务
银行业保险业科技金融高质量发展实施方案	科技金融、对公信贷、债券承销、债券投资	• 健全机构组织体系，优化内部考核和激励约束机制，鼓励做好科技创新重点领域金融服务，包括加强信 贷支持、提供债券承销服务、加大科创类债券投资配置力度等
关于加强商业银行互联网助贷业务管理提升金融服务质效的通知	互联网贷款	• 强调总行对互联网助贷业务的统一管理和业务分配 • 加强对第三方平台运营机构、增信服务机构准入管理，并明确平台和机构的营收模式
支持小微企业融资的若干措施	普惠金融	• 要求统筹运用无还本续贷、展期、调整还款安排等方式，做好小微企业贷款到期接续支持 • 加强贷款利率定价管理，优化小微企业融资服务定价管理，清理违规收费 • 优化线上、线下贷款业务，改进授信审批和风险管理模型，精简申贷材料清单，合理下放授信审批权限
银行业保险业科技金融高质量发展实施方案	科技金融、对公信贷、债券承销、债券投资	• 健全机构组织体系，优化内部考核和激励约束机制，鼓励做好科技创新重点领域金融服务，包括加强信 贷支持、提供债券承销服务、加大科创类债券投资配置力度等
银行业保险业绿色金融高质量发展实施方案	对公信贷、绿色金融	• 要求完善绿色金融服务体系，优化银行信贷供给，丰富绿色金融产品服务 • 健全环境、社会和治理风险管理体系，加强风险识别、评估与监测，不断细化优化行业投融资政策 • 建立健全绿色金融统计数据管理制度，完善信息披露机制、建立绿色金融考核评价体系和奖惩机制

法规名称	涉及领域	法规核心内容暨内审关注事项
商业银行代理销售业务管理办法	代理销售	• 明确对合作机构机构准入审查要求，并要求做好代销产品准入管理，履行尽职调查义务 • 稳慎评估客户购买产品的适当性，加强销售过程合规管理 • 明确要求对存续期产品持续跟踪，强调督促合作机构做好信息披露
个人信息保护合规审计管理办法	个人信息保护、合规管理、内部审计	• 明确开展个人信息保护合规审计的触发条件、机构选择与合规审计频次 • 细化个人信息保护合规审计的重要审查事项

相关刊物

毕马威《金融新规热读》为监管动态跟踪专题报告，我们持续关注金融业重要法规及政策变化，协助金融机构有效应对监管变化，以持续优化合规管理效率和效果。

重点新规精读

《商业银行代理销售业务管理办法》

近年来，商业银行代销业务快速发展，代销产品数量和类型日益丰富。在相关监管制度不断压实金融产品发行人、管理人责任的基础上，有必要进一步明确商业银行作为代销机构的义务。金融监管总局于2025年3月21日印发《商业银行代理销售业务管理办法》，新规将自2025年10月1日起施行。

主要内容

《办法》共八章54条，主要包括：

- 第一章：总则，明确商业银行开展代销业务应当具备的条件、基本原则。
- 第二章：代销业务内部管理制度，明确商业银行开展代销业务需建立健全管理制度、业务系统、内部管理、消费者保护等机制。
- 第三章：合作机构管理，强化商业银行对合作机构的管理责任，明确合作机构准入审查要求和退出机制，明晰商业银行和合作机构的法律责任。
- 第四章：代销产品准入管理，强化商业银行对代销产品的准入管理责任，明确尽职调查要求。
- 第五章：销售管理，对商业银行宣传推介和代理销售行为作出规范。
- 第六章：代销产品存续期管理，明确存续期内商业银行应尽的义务。
- 第七章：监督管理，明确对商业银行开展代销业务的报告要求和监管措施。
- 第八章：附则，规定《办法》的施行时间等。

主要变化

对比2016年《中国银监会关于规范商业银行代理销售业务的通知》，《办法》主要变化为：

一是新增部分整体要求，如坚持“了解产品”和“了解客户”的经营理念，代销产品实行准入制管理，建立健全代理销售全流程监测和管理机制，强化存续期管理，持续加强客户服务等。

二是结合近期新的风险特征与监管要求，强化了客户信息保护、网络和数据安全、消费者权益保护、电子渠道等方面的规定。

三是大幅修改了资产管理类产品的管理要求，整体更加细致、严格。

四是明确对于违法违规行为， 商业银行和合作机构均需承担法律责任。

五是开展代销业务的其他银行业金融机构范围中删除了汽车金融公司、消费金融公司。

说明：根据监管机构网站公开发布信息自行编制。

对商业银行影响较大的关键条款

管理体系

第十一条　商业银行应当明确履行代销业务管理职责的部门，由其牵头组织并督促指导相关部门开展代销工作。

第十二条　商业银行应当在合作机构准入、代销产品准入、宣传推介和销售等环节开展消费者权益保护审查，从源头上防范侵害金融消费者合法权益行为发生。

内审关注建议：

- 新规颁布前，商业银行普遍根据代销产品所属的管理部门，在总行根据对公、个人、私银等分类设立归口管理部门，并未设置统一的代理销售牵头管理部门。
- 多数商业银行将代理销售产品纳入消费者权益保护审查，未能全面覆盖合作机构准入、代销产品准入、宣传推介、销售等环节。

合作机构管理

第十六条 商业银行总行应当对合作机构实行名单制管理，确定合作机构资质审查标准，明确准入条件和程序，建立并有效实施对合作机构的尽职调查、评估和审批制度。对于已经准入的合作机构，商业银行应当加强日常管理，定期对其进行审查评估。

商业银行对资产管理机构进行准入审查时，应当对其信用状况、投资管理能力、风险管控能力、信息披露情况等进行审查。商业银行对保险公司进行准入审查时，应当对其偿付能力状况、风险管控能力、信息披露情况等进行审查。

第十七条 商业银行应当建立合作机构退出机制，及时对存在严重违规行为、重大风险或者其他不符合持续合作标准的机构实施退出，并平稳有序做好存量产品的客户服务。

第二十六条　商业银行应当确认合作机构具备产品发行资格，产品由监管部门或者其授权机构审批、注册、备案、登记或者取得符合规定的登记编码。

第四十七条　代销产品存续期内，商业银行应当督促合作机构按照规定披露代销产品相关信息。

对于公募资产管理产品，商业银行应当督促合作机构通过官方网站或者其余便于客户获取的方式披露产品评级结果、产品净值或者投资收益情况，并定期披露其他重要信息。开放式产品按照开放频率披露，封闭式产品和处于封闭期的定期开放式产品至少每周披露一次。

对于私募资产管理产品，商业银行应当督促合作机构按照监管规定和合同约定，及时披露必要信息，至少每季度向客户披露产品净值和其他重要信息。

对于保险产品，商业银行应当督促合作机构定期对分红型保险产品分红水平、万能型保险产品结算利率、投资连结型保险产品投资账户单位价格等信息进行披露。

内审关注建议：

- 商业银行普遍已对合作机构建议名单制管理、日常管理、准入审查与退出机制，但需关注相关管理标准及程序的科学性、可落地性及执行有效性，例如是否存在未进行动态管理、准入审查与日常评价流于形式等问题，亦需关注是否涵盖新规要求的审查要素。如实务中，个别商业银行由于未明确审查要素及评分要求，对于存在行政处罚、串标围标等负面行为的供应商，并未启动动态评分或退出流程。

对商业银行影响较大的关键条款

合作机构管理

- 需关注合作机构产品发行资格审查，并结合外部公开信息及行业信息等进行交叉验证。例如在准入审查环节制定明确的资格审查要求及资料范围清单，核验合作机构是否具有更新的经营业务许可证，是否获得金融监管总局、证监会的业务资格核准批复。
- 商业银行增加了督促合作机构披露代销产品信息的义务，需关注落实机制。例如在合作机构合同中明确信息披露范围、信息要素及标准化表述、信息披露格式模板等，以及合作机构未及时、有效履行信息披露义务的惩罚措施等。在合作机构准入环节了解合作机构信息披露管理机制，确保其信息披露流程与内部控制的有效性；在日常管理环节对其信息披露的有效性进行评价并将结果纳入动态评分体系等。

代销产品管理

第二十七条 商业银行应当对代销产品开展尽职调查，全面了解产品情况，对产品信息的真实性、准确性、完整性进行核实，结合本机构的客群特征、销售渠道、销售人员、信息系统等情况，形成独立、客观的准入意见。

对资产管理产品的尽职调查应当综合考虑产品结构、投资标的、投资策略、投资管理团队、风险管控措施、本产品或者同类产品过往业绩水平等因素。

对保险产品的尽职调查应当综合考虑产品类型、产品保障责任、保单利益水平等因素。

商业银行应当加强甄别，防范合作机构让渡主动管理职责，为其他机构、个人或者资产管理产品规避监管要求提供便利。

第二十八条 商业银行在对资产管理产品进行准入审查时，如该产品投向非标准化债权类资产、未上市企业股权、私募投资基金，或者聘请私募基金管理人担任投资顾问，商业银行应当由代销业务管理、风险管理、法律合规、金融消费者保护等部门进行综合评估，并获得本行高级管理层批准。

对于前款所提投向私募投资基金，或者聘请私募基金管理人担任投资顾问的代销产品，商业银行产品准入标准应当包括但不限于：其私募基金管理人管理的私募股权投资基金规模合计不低于五亿元、管理的私募证券投资基金规模合计不低于三亿元，在中国证券投资基金业协会登记不少于三年，近三年内未受到行政处罚和中国证券投资基金业协会纪律处分，符合法律、行政法规和国务院金融监督管理机构关于私募基金管理人的其他要求。政府出资产业投资基金可不受登记年限的限制。

内审关注建议：

- 新规对于代销产品尽职调查和准入审查提出了详细的管理要求，区分资产管理产品、保险产品等类别，并更加细化至资产管理产品的底层资产投向等，分别提出了调查审查的关注要素和审批流程要求，建议内审重点关注其落实情况。例如对于资产管理产品，如何实现实时穿透，确保底层资产持续合规，不突破投向要求。是否能够落实新规要求，在监管允许的过渡期内完成存量代销产品的整改等。

宣传推介及销售管理

第三十二条　商业银行仅限于在本行营业网点、官方网站及互联网应用程序（APP）等本行自主运营且不依赖于其他机构的渠道设专区销售代销产品，不得通过外包业务流程、让渡业务管理权限、将全部或者部分销售环节嵌入其他机构应用场景等方式违规开展代销业务。

代销私募资产管理产品的，应当通过本行面向合格投资者的专门渠道以非公开方式宣传推介和销售。

第三十五条　商业银行应当针对同类产品制定一致的代销产品展示规则。对于资产管理产品，应当综合考虑产品业绩比较基准（如有）过往达成情况、风险状况、信息披露、市场反馈等因素，不得简单依据业绩比较基准或者过往业绩高低进行展示排序，不得宣传预期收益率，不得使用合作机构未说明选择原因、测算依据或者计算方法的业绩比较基准。展示成立以来年化收益率的，应当明示产品成立时间。

第三十八条　商业银行应当向客户提供并提示其阅读相关销售文件，包括风险提示，以请客户抄写风险提示等方式充分揭示代销产品的风险，销售文件应当由客户签字逐一确认，国务院金融监督管理机构另有规定的除外。

对于六十五周岁以上的老年人、限制民事行为能力人等特殊客群，商业银行应当制定更为审慎的销售流程，加强宣传推介和销售行为管理，强化风险提示。

第四十一条　商业银行通过营业网点开展代销业务的，应当根据国务院金融监督管理机构的相关规定实施录音录像，完整客观地记录营销推介、风险和关键信息提示、客户确认和反馈等重点销售环节。

通过自助终端等电子设备向个人客户销售产品的，商业银行应当提示客户如有销售人员介入宣传推介，则需停止自助终端购买操作，转至销售专区内购买。

通过官方网站及互联网应用程序（APP）等互联网渠道向个人客户销售产品的，商业银行应当采取有效措施和技术手段完整客观地记录宣传推介、风险和关键信息提示、客户反馈和确认等重点销售环节，实现关键环节可回溯、重要信息可查询、问题责任可确认。

内审关注建议：

- 新规对于宣传推介和销售环节进行了严格的规范，特别限定了销售渠道为“本行营业网点、官方网站及互联网应用程序（APP）等本行自主运营且不依赖于其他机构的渠道”，并要求“设专区”，不允许通过合作机构等进行代销产品推介。内审需重点关注代销产品渠道合规性落实情况。对于私募产品，需关注认购者需满足合格投资者条件，并需要以“专门渠道”和“非公开方式”进行销售与推介。
- 新规特别明确了代销产品展示规则，要求同类产品采用一致的展示规则。针对资产管理产品，针对之前行业普遍存在的侵犯消费者权益的问题，特别强调了“不得简单依据业绩比较基准或者过往业绩高低进行展示排序，不得宣传预期收益率，不得使用合作机构未说明选择原因、测算依据或者计算方法的业绩比较基准”等要求。内审需关注实务中的落实机制及执行有效性。
- 针对具体销售过程，商业银行已普遍落实了风险提示、销售文件客户签字逐一确认等基础要求，内审需重点关注六十五周岁以上的老年人、限制民事行为能力人等特殊客群的客户甄别、销售流程设计、管理要求的执行有效性等。

宣传推介及销售管理

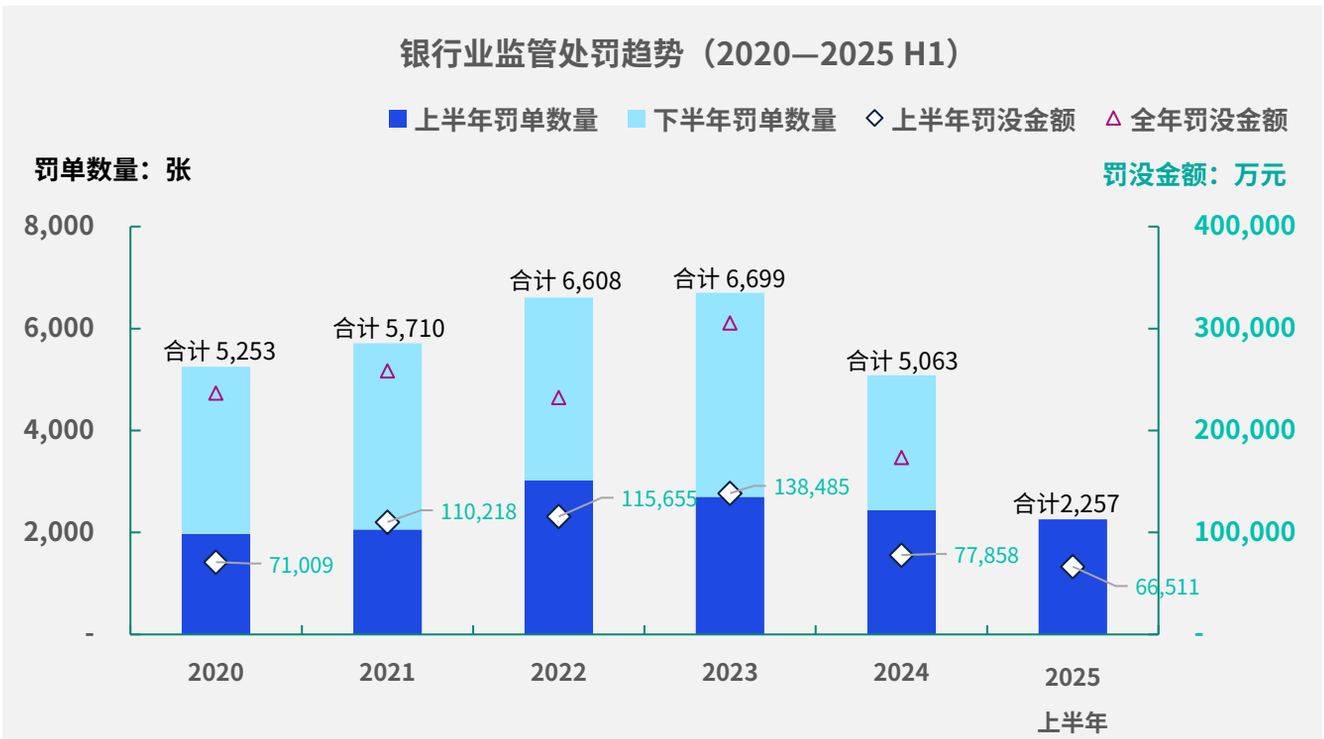
- 以往监管处罚中，涉及代理销售宣传推介及销售管理为处罚集中领域，典型处罚案由总结如下，供内部审计参考。
- 宣传推介：向超过规定年龄的客户销售保险产品、对特定人群的销售管理不到位，向特定人群销售保单利益不确定的保险产品、未收取合格投资者认定的相关证明材料
- 销售管理：未按规定进行保险销售从业人员执业登记管理、保险销售从业人员培训管理不到位、委托未通过本机构进行执业登记的个人从事保险代理业务、未对投保人进行需求分析与风险承受能力测评、客户风险评估操作不规范、保险销售可回溯管理制度执行不到位、代理保险销售未按规定实施双录、理财双录不规范、未按规定办理保险兼业代理许可证变更登记、违规允许保险公司人员在营业场所销售保险、违规代客操作购买理财、基金产品、误导投保人不履行如实告知义务、办理个人信贷业务过程中搭售贵金属、保险产品

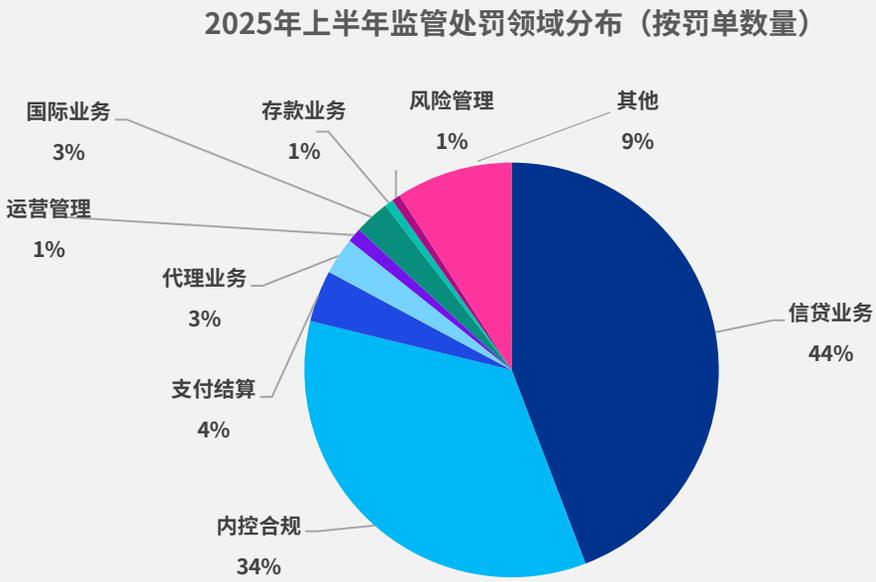
2. 监管处罚洞察

监管处罚整体观察

2025年上半年，监管处罚高压态势持续不减，人民银行、金融监管总局、外管局（含总部及其派出机构）针对银行业金融机构及从业人员共下发2,257张罚单，涉及罚没金额总计达人民币6.65亿元，虽然罚单数量及罚没金额较2024年上半年均有所下降，但整体仍呈现“严监管”趋势。从处罚涉及领域来看，主要集中在信贷业务、内控合规、存款业务、代理业务等领域。

2025年上半年人民币100万以上大额罚单共137张，占罚单总数的6.07%，罚没金额人民币3.16亿元，占罚没总额的47.45%，处罚行业典型加强警示效应的监管特征较为显著。其中，针对商业银行的最大罚单由国家金融监督管理总局对某全国性股份制商业银行开具，罚款金额为人民币1,680万元。





说明：根据毕马威监管情报站收录监管规则数据、监管处罚数据自行分析编制。由于四季度监管机构亦公布了处罚决定日在三季度的罚单，故罚单总数与罚没金额统计数据较三季度报告数据有所调整。

建议关注重点

通过综合分析上半年监管处罚特点、典型案例以及数据变化，结合近期监管动态及关注重点，我们总结了重点领域的典型问题及趋势苗头，提示内部审计部门关注：

观察一：信贷领域特殊案由及零售信贷需引起关注

信贷业务持续为监管处罚集中领域，往期《商业银行内审观察》已详细分享信贷业务处罚案由及变化趋势，本期我们主要聚焦信贷业务具有代表性的案由变化，以及结合近期零售信贷风险暴露的趋势，重点提示零售信贷业务风险。

涉及领域	主要违规形态
信贷业务 （近期变化）	向前期已存在异常情况的客户违规发放借名贷款
	以不正当手段发放贷款
	暂时经营困难企业支持政策执行不严，向不符合条件的企业进行续贷
	贷前客户资金需求测算流于形式
	供应链融资模式运用不合规
	信贷人员核保不尽职，导致冒名担保
	对已核销贷款追偿不到位
	违规向风险客户新增贷款掩盖不良贷款
	以贷收费
	超标准收取提前还款违约金
	贷款资金违规借名归集使用
	信贷资金被集团公司归集使用

在2025年上半年的监管处罚中，我们关注到监管对零售业务的合规性管理呈现出高压、精准、常态化的态势。处罚重点从以往准入管理、贷款三查、支付管理、资金用途监控等环节的业务流程瑕疵，全面转向业务实质、消费者权益保护、个人信息保护、合规营销与销售等领域，同时针对不同的业务品种的处罚案由亦不断丰富。结合近期零售业务发展与资产质量承压的背景，以及近期市场上诱导网络贷款，资金中介活动等乱象，建议内审部门对零售业务的风险变化予以关注。

涉及领域	主要违规形态
个人经营贷	违规发放个人经营性贷款
	个人经营性贷款管理不审慎，发放个人经营贷款过程中贷款管理不审慎
	个人经营性贷款尽职调查严重违反审慎经营规则
	向不符合条件的借款人发放经营性贷款
	人经营性贷款业务贷前调查不尽职、贷后管理不到位
	个人经营性贷款业务中签订空白合同，向保证人隐瞒实际贷款金额

涉及领域	主要违规形态
个人经营贷	个人经营性贷款贷后管理不到位
	个人生产经营性贷款资金被挪用
个人消费贷	个人消费贷款管理不到位
	个人消费贷产品存在合规漏洞
	个人消费贷款“三查”不到位
	个人消费贷款资金违规流入限制性领域，个人消费类贷款流入不合规领域，个人消费贷款被挪用于投资行为
个人住房贷	违规办理个人住房按揭贷款，违规发放个人住房按揭贷款
	违规发放房地产开发贷款和个人住房按揭贷款，严重违反审慎经营规则
	个人住房贷款贷前调查不到位，对首付款及收入证明材料真实性核实不到位
	个人二手住房贷款业务及代销业务管理不尽职，经办人员借二手住房贷款搭售产品
信用卡	信用卡业务不审慎，信用卡业务管控不到位
	信用卡分期业务电话营销不规范
	信用卡现金分期业务不合规
	信用卡透支资金用途管控不力
	信用卡资金被用于申购基金，信用卡资金被用于购买股票
其他案由	办理个人信贷业务过程中搭售贵金属、保险产品
	个人贷款用于偿还其他网络贷款

观察二：内控合规领域反洗钱与员工行为领域处罚问题突出

2025年上半年人民银行等共下发513张涉及反洗钱领域罚单，占罚单总数的22.73%，罚没金额合计达人民币8,589万元，占总体罚没金额约12.91%，较2024年上半年大幅下降。处罚案由及违规形态总结涉及基础管理、客户身份识别、客户风险评估、大额及可疑交易报告、资料保存等多个领域与环节。从处罚特点来看，全面覆盖反洗钱管理全流程，既关注整体机制建设，亦深入具体操作细节。

需要注意的是，新《反洗钱法》已于2025年1月1日正式实施，人民银行等反洗钱主管部门亦在密集酝酿反洗钱领域的新规出台，并把覆盖行业延伸至房地产、贵金属和宝石等。同时财政部、司法部等亦针对会计师事务所、律师事务所等发布反洗钱工作管理办法征求意见稿，强化反洗钱义务。预计未来反洗钱领域监管将持续强化。

涉及领域与环节	主要违规形态
基础管理	违反反洗钱法律法规，违反反洗钱业务管理规定
客户身份识别	未按规定履行客户身份识别义务
	与身份不明的客户进行交易或者为客户开立匿名账户、假名账户
	与客户建立业务关系时，未按规定识别客户身份
	与客户建立业务关系或办理一次性金融业务，未按规定识别客户身份
	未按规定对高风险客户采取强化识别措施
	未按规定重新识别客户，未按规定开展客户重新识别
	未对涉及有权机关查冻扣的对公客户开展有效的重新识别
	未按规定开展持续的客户身份识别（含重新识别）
	未按规定识别代理人身份
客户风险评估	未按规定开展客户风险等级划分、调整和审核工作
大额及可疑交易报告	未按规定对异常交易进行人工分析、识别，排除理由不合理
	未按规定报送大额交易报告或者可疑交易报告
	未按规定报送可疑交易报告
	未按规定时限报告大额交易
资料记录保存	未按规定保存客户身份资料和交易记录

近年来，监管机构对金融机构员工行为的监管持续强化，处罚力度显著加大，呈现整体从严、精细化的特征，体现了压实个体责任的监管导向。我们关注到2025年上半年公布的罚单中，涉及员工行为的罚单共计133张，约占罚单总数的5.89%；罚没金额为人民币6,726万元，占总体罚没金额的10.11%。同时，员工行为领域的处罚多与业务领域处罚伴生，严监管、零容忍，对违规个体严肃追责已成为常态，建议内部审计予以关注。

涉及领域	主要违规形态
整体管理	员工行为管理不到位，员工行为管控不到位
	员工异常行为管理不到位
	员工行为管理严重违反审慎经营规则
	员工行为管理薄弱
	员工合规管理欠缺
	未严格执行员工行为管理规定
异常行为排查	对员工异常行为排查不到位
	长期未发现涉案员工各类违法违规行为
	员工管理失察、员工从事违法活动

涉及领域	主要违规形态
业务及管理领域的具体违规表现	员工与客户不当资金往来
	员工与客户发生非正常资金往来
	原客户经理与贷款客户发生非正常资金往来
	银行员工违规借用客户资金和出借资金给客户使用
	员工为客户垫付贷款资金
	员工违规保管客户银行卡并违规操作
	员工违规销售理财产品
	员工违规代客操作购买理财、基金产品
	员工从事违法活动
	员工非法侵占客户资金
	员工冒用客户名义诈骗资金
	员工行为管理不到位，违规保管客户签章空白凭证

观察三：监管持续关注代理销售，代销保险问题突出

2025年上半年金融监管总局共下发67张涉及代理销售的罚单，占罚单总数的2.97%，罚没金额合计达人民币2,291万元，占2025年上半年总体罚没金额约3.44%，较2024年上半年有所下降。处罚案由覆盖的违规形态较为多样化，综合涉及整体管理、销售场所管理、销售人员管理、销售过程管理、数据、系统等多个事项与环节。从业务违规特点来看，代销保险领域存在的问题较为突出，销售行为管理亦是监管机构重点关注的事项。

值得注意的是，2025年3月21日金融监管总局在2016年《中国银监会关于规范商业银行代理销售业务的通知》的基础上，结合近年来代理销售业务存在的市场乱象与突出问题，更新印发了《商业银行代理销售业务管理办法》。新办法将于2025年10月1日正式实施，建议各内审部门重点关注代理销售领域新规落实和违规问题的整改情况。

涉及领域与环节	主要违规形态
整体管理	代理销售业务严重违反审慎经营规则，违规开展代销业务
	代理销售业务不规范，金融产品销售行为不审慎
销售人员及行为管理	违规销售基金产品
	员工违规销售理财产品
	理财双录不规范
	未收取合格投资者认定的相关证明材料
	客户风险评估操作不规范

涉及领域与环节	主要违规形态
销售人员及行为管理	销售人员管理不到位
	办理个人信贷业务过程中搭售贵金属、保险产品
	员工违规代客操作购买理财、基金产品
	个人二手住房贷款业务及代销业务管理不尽职
	经办人员借二手住房贷款搭售产品
数据与系统	错报1104系统代理代销业务报表数据
	销售系统管理不到位
代销保险	代销保险业务管理不到位
	保险销售行为不规范
	误导投保人，代销保险误导销售，代理销售保险存在销售误导行为
	在办理保险业务活动中欺骗投保人；欺骗保险人、投保人、被保险人或者受益人
	诱导投保人不履行如实告知义务
	隐瞒与保险合同有关的重要情况
	给予投保人保险合同约定以外的其他利益
	收受保险公司工作人员给予的合同约定之外的资金；收取保险公司及其工作人员合作协议以外利益
	代理销售保险业务未如实记录投保人实际地址
	允许保险公司人员在营业场所从事保险销售相关活动；非商业银行从业人员在商业银行营业场所从事保险销售相关活动
	代客操作购买保险产品
	代销保险业务可回溯管理不到位；保险销售行为可回溯管理不规范；保险销售行为可回溯管理制度执行不到位
	未按规定进行执业登记管理

观察四：数据统计与监管报送问题需引起内审高度关注

近年来，随着数字化智能化浪潮席卷银行业，监管机构日益重视数据质量，聚焦数据统计与监管报送领域的处罚也日益突出。2025年上半年监管机构共下发涉及该领域罚单106张，占罚单总数的4.7%，处罚金额总计人民币8,428万元，占罚没总额高达12.67%，整体呈现处罚趋严、趋重的特点。从案由特征来看，监管处罚事由日趋精细化，不仅涉及整体数据质量、不同来源数据一致性等，亦深入业务领域聚焦特定业务及产品品种。此外，监管机构亦在逐步提升自身的数字化监管能力，并对不同途径报送或采集的监管数据进行交叉核验与变动分析，监管力度逐年强化。

2025年8月7日，金融监管总局发布了《金融监管总局贯彻落实2024年常规统计督察反馈意见整改情况》，并表示将压紧压实防治统计造假责任，严格履行统计法定职责，预计未来该领域监管深度与力度将进一步提升。建议内部审计关注监管配合、数据统计及报送工作的规范性与严谨性。

违规事项	主要违规形态
违反管理规定	违反金融统计相关规定
	未按规定统计贷款数据
	执行境内大中小型企业贷款专项统计制度不到位
	EAST数据质量不符合规范要求
虚假或瞒报	虚报、瞒报金融统计数据
	提供虚假统计报表，虚报监管数据
	提供虚假的或隐瞒重要事实的统计资料
	瞒报相关信息，向监管部门提供隐瞒重要事实的报告
	监管统计数据不真实，监管数据报送严重失实
	监管指标反映不实
	虚增存贷款规模
	以贷转存虚增规模
	单位存款数据失真
	信贷数据不真实
	虚增小微企业贷款
	部分非现场监管统计数据与事实不符
数据不准确	非现场监管数据不准确，报送非现场监管数据不准确
	监管统计指标计量不准确
	贷款数据不准确
	重点领域数据不准确、表外金融衍生品类数据少计
	个体工商户及小微企业主经营性贷款统计不准确
数据错报、漏报	监管标准化（EAST）数据漏报
	贷款统计归属错误
	涉农贷款统计有误
	涉农贷款专项统计科目归属错误
	大中小微企业贷款统计划分错误
	错报单位活期存款统计数据
质量控制	数据质量控制不到位

观察五：网络安全和数据安全需重点关注

数字化浪潮影响下，商业银行数字化智能化快步发展，相关领域的关监管规则亦持续强化。未来随着数字金融的加速布局，数据要素的作用将进一步发挥，预计数据管理和网络安全方面的监管压力会持续抬升。我们关注到2025年上半年公布的罚单中，涉及网络安全领域的罚单共计36张，罚没金额为人民币1,805.56万元，占季度总体罚没金额的2.71%。此外，数据安全领域亦识别到多项新兴案由。

2025年4月，人民银行、金融监管总局、证监会等六部门联合发布《促进和规范金融业数据跨境流动合规指南》；5月，人民银行连续发布《中国人民银行业务领域数据安全管理办法》（6月30日已实施）、《中国人民银行业务领域网络安全事件报告管理办法》（8月1日已实施），未来相关领域监管将进一步强化，建议内部审计前瞻性地予以关注。

涉及领域	违规环节	主要违规形态
数据安全	整体管理	数据安全管控不足
	制度建设与执行	未制定数据安全管理制度
		未建立健全全流程数据安全管理制度，未按规定建立全流程数据安全管理制度
		违反数据安全管理规定，未按规定落实数据安全相关管理规定
	职责分工	未明确数据安全负责人和管理机构
		未落实数据安全保护责任
	风险监测、评估与报告	数据处理活动风险监测不到位
		未按规定在开展数据处理活动时加强风险监测
		未按照规定对其数据处理活动定期开展风险评估，未建立全流程数据安全管理制度和开展重要数据处理活动风险评估
		未向有关主管部门报送风险评估报告且数据安全管理风险评估报告要素不全，未向监管机构上报数据处理活动风险评估报告
		未及时处置数据安全漏洞风险
	保障措施	数据安全保障措施不到位
		未采取相应的技术措施或其他必要措施保障数据安全
		未采取加密、去标识化等安全技术措施保障数据安全
	教育培训	未组织开展数据安全教育培训
网络安全	整体管理	违反网络安全管理规定，未按规定落实网络安全相关管理规定
		网络安全和数据安全业务违法违规行为
		未落实网络安全保护责任，未按规定履行网络安全保护义务，未按规定履行网络运营者的网络安全保护义务
		未按规定对关键网络设备提供持续安全维护
		未按规定办理网络安全等级保护定级、备案

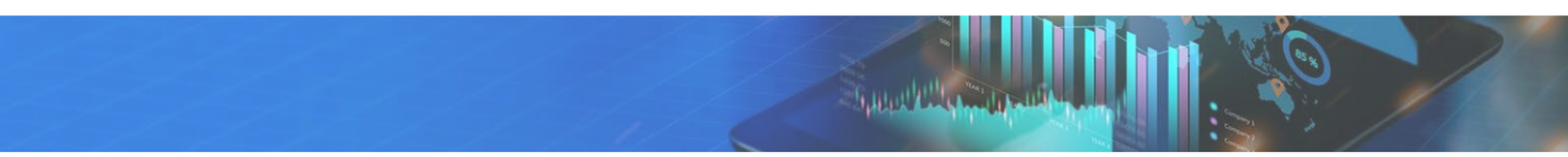
涉及领域	违规环节	主要违规形态
网络安全	职责分工	未按规定确定网络安全负责人
	技术措施	网络安全技术措施不到位
		未采取有效措施防范计算机病毒、网络攻击和网络侵入
		病毒库更新不及时，未及时更新计算机终端病毒库
		未采取防范计算机病毒的技术措施，未按规定采取防范计算机病毒的技术措施，未采取必要的防计算机病毒技术措施
		部分机器未采取防计算机病毒的技术措施
		办理人民银行代理发行库业务计算机终端未采取防范计算机病毒的技术措施
		未及时采取有效措施防范和处置计算机病毒事件
		未采取有效的防范网络侵入的技术措施
		弱口令风险监测存在隐患
		接入人民银行业务领域的通信网络流量未纳入监测、阻断范围
	网络日志	未按规定留存网络设备核心路由器网络日志不少于六个月
		未按规定留存终端系统网络日志不少于六个月
	应急预案	未制定网络安全事件应急预案
		未建立系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全事件应急预案，且未开展相关演练
	事件报告	未上报网络安全事件

观察六：数据统计与监管报送问题需引起内审高度关注

近年来，随着数字化智能化浪潮席卷银行业，监管机构日益重视数据质量，聚焦数据统计与监管报送领域的处罚也日益突出。2025年上半年监管机构共下发涉及该领域罚单106张，占罚单总数的4.7%，处罚金额总计人民币8,428万元，占罚没总额高达12.67%，整体呈现处罚趋严、趋重的特点。从案由特征来看，监管处罚事由日趋精细化，不仅涉及整体数据质量、不同来源数据一致性等，亦深入业务领域聚焦特定业务及产品品种。此外，监管机构亦在逐步提升自身的数字化监管能力，并对不同途径报送或采集的监管数据进行交叉核验与变动分析，监管力度逐年强化。

2025年8月7日，金融监管总局发布了《金融监管总局贯彻落实2024年常规统计督察反馈意见整改情况》，并表示将压紧压实防治统计造假责任，严格履行统计法定职责，预计未来该领域监管深度与力度将进一步提升。建议内部审计关注监管配合、数据统计及报送工作的规范性与严谨性。

违规事项	主要违规形态
违反管理规定	违反金融统计相关规定
	未按规定统计贷款数据
	执行境内大中小型企业贷款专项统计制度不到位
	EAST数据质量不符合规范要求
虚假或瞒报	虚报、瞒报金融统计数据
	提供虚假统计报表，虚报监管数据
	提供虚假的或隐瞒重要事实的统计资料
	瞒报相关信息，向监管部门提供隐瞒重要事实的报告
	监管统计数据不真实，监管数据报送严重失实
	监管指标反映不实
	虚增存贷款规模
	以贷转存虚增规模
	单位存款数据失真
	信贷数据不真实
	虚增小微企业贷款
	部分非现场监管统计数据与事实不符
数据不准确	非现场监管数据不准确，报送非现场监管数据不准确
	监管统计指标计量不准确
	贷款数据不准确
	重点领域数据不准确、表外金融衍生品类数据少计
	个体工商户及小微企业主经营性贷款统计不准确
数据错报、漏报	监管标准化（EAST）数据漏报
	贷款统计归属错误
	涉农贷款统计有误
	涉农贷款专项统计科目归属错误
	大中小微企业贷款统计划分错误
	错报单位活期存款统计数据
质量控制	数据质量控制不到位



观察七：其他值得关注的领域及案由

除以上处罚较为集中、典型的业务及管理领域外，我们还关注到部分新兴、趋势性、苗头性的处罚案由，建议内部审计关注。

金融监管总局、证监会公布的2025年规章制定工作计划中，《商业银行托管业务监督管理办法》（2022年12月29日曾发布征求意见稿）、《证券投资基金托管业务管理办法》（2025年4月3日已发布修订草案征求意见稿）等托管业务新规已纳入制定/修订计划。以往金融监管总局对于托管业务的罚单并不多，虽然2024年亦未对商业银行开具托管业务相关罚单，但2025年已有新的托管业务罚单落地，建议内审部门前瞻性地予以关注。

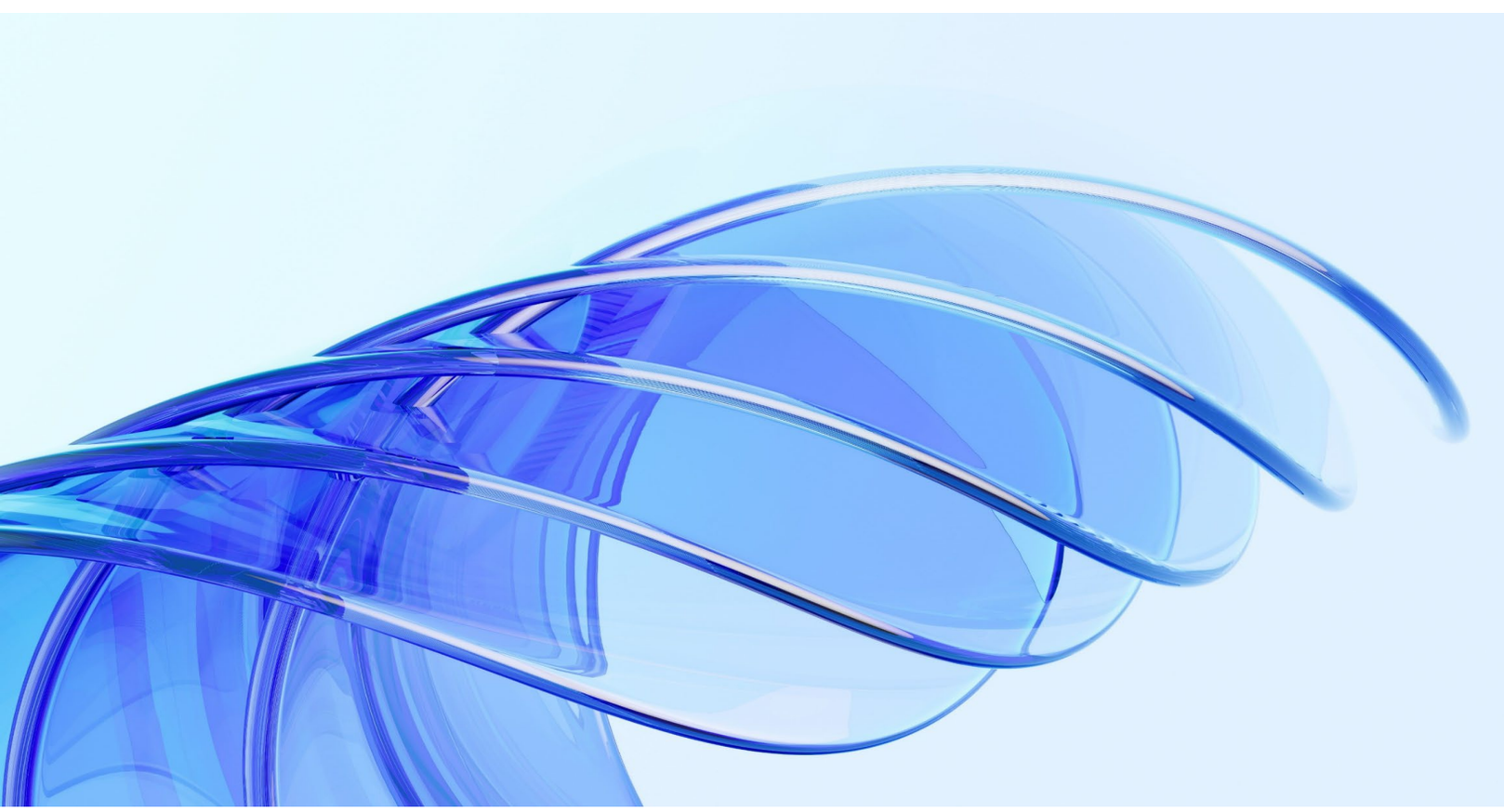
涉及领域	主要违规形态
托管业务	托管业务管理不到位
	逆程序开展托管业务
	未按规定对托管保险资产进行估值核算

近年来，监管愈加关注第三方风险，《商业银行代理销售业务管理办法》《国家金融监督管理总局关于加强商业银行互联网助贷业务管理提升金融服务质效的通知》等新规亦强调压实商业银行主体责任，提出强化合作机构管理的要求。在2025年合作机构管理处罚案由基础上，我们延伸对2022年以来的典型处罚案由进行了整理，建议内审部门酌情关注。

涉及领域	主要违规形态
合作机构管理	外包合作机构管理薄弱，对合作机构管控缺失，对第三方合作机构管理不审慎，选择合作机构不审慎
	放宽合作机构准入条件，未按制度规定对合作机构进行准入管理
	与合作担保公司业务管理不审慎
	理财投资合作机构名单制管理严重违反审慎经营规则
	对汽车分期业务合作机构管控缺失
	与不具备融资担保资质的第三方公司和个人合作开展融资担保业务
	未按规定程序选聘金融服务合作机构
	对合作机构日常管理不到位
	银行员工与第三方合作机构人员发生民间借贷
	合作机构催收管理不到位
	对合作机构管理不到位，准入尽职调查、审查不到位，日常管理缺失
	对第三方合作机构处理个人信息管控缺位

我们关注到监管意见落实领域的处罚案由，建议内审部门关注监管问题整改的有效性，以及监管处罚结果应用情况。

涉及领域	主要违规形态
监管意见落实	监管意见落实不到位
	监管发现问题整改不到位
	未将受行政处罚的考评对象调低考评等级



3. 敏捷审计专题

敏捷审计（Agile Auditing）是一种将敏捷软件开发原则和实践应用于审计活动的创新方法，其核心目标是提升审计的效率、响应速度和价值创造。敏捷审计通过将审计工作分解为更小、更频繁的交付单元，以聚焦于特定风险领域或控制要素，将审计资源始终投入到能带来最大价值的地方。敏捷审计的优势在于动态响应业务与环境的变化，通过持续改进与反馈循环帮助组织实现管理提升。

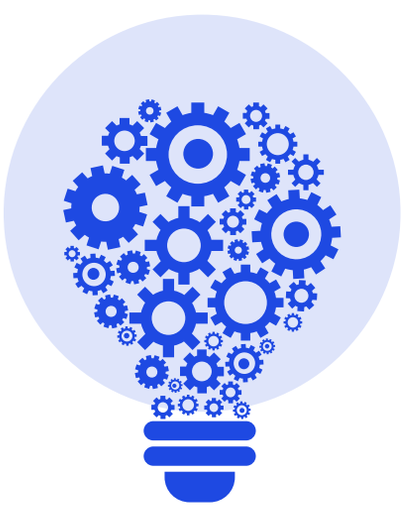
结合市场热点问题及专家洞察，每期我们将选择1至2个敏捷审计专题进行深入探讨，内审部门可以考虑将其纳入审计计划调整或融入现有的审计方案与程序中。

“贷款中介”与“职业背债人”

2025年7月，金融监管总局连续发布《关于防范虚假宣传诱导网络贷款的风险提示》《关于警惕“职业背债”陷阱的风险提示》，对不法贷款中介诱导网络贷款及职业背债人风险进行了提示。各地金融监管分局等亦结合区域业务特点，陆续发布警惕不法贷款中介陷阱、警惕诱导消费者“债务重组”等风险提示。2025年3月，《2025年最高人民法院工作报告》亦提出依法规制“职业背债人”“职业闭店人”等乱象，需引起商业银行的警惕。

近年来，伴随着经济结构调整带来的阵痛反应，以及普惠金融、消费金融市场的活跃，不法贷款中介活动频繁。部分中介机构以“低息快贷”“无条件放款” 为噱头，通过虚假宣传、隐瞒真实信息、包装材料、违规收费等手段误导消费者陷入高额债务与资金危机。更有不法中介以“快速致富”“无需偿还债务”为诱饵，锁定“职业背债人”目标人群，引诱不具有还款意愿与还款能力的消费者合谋骗贷，或在企业面临债务困境时通过“职业背债人”“职业闭店人”等帮助企业逃废债务，严重干扰了金融秩序，影响商业银行正常的信贷决策与资源配置，亦对资产质量产生严重的负面影响。需要警惕的是，不法贷款中介与职业背债人往往构成组织化的欺诈产业链，批量锁定目标机构、业务、产品进行套贷；同时可能伴随银行内部员工的不当行为与欺诈舞弊，以动态升级欺诈手段，规避银行内部监控，可能对商业银行信贷资产构成系统性风险。

“骗贷”及“逃废债”过程中的角色分工与画像



不法贷款中介：通常不具有金融业务资质或超出经营范围，选择内控环境较为薄弱的机构为骗贷目标，以不实宣传、欺骗手段招徕企业或个人作为“目标群体”，通过伪造材料等方式对贷款人资信材料进行包装，辅导或代替贷款人完成贷款流程，收取高额中介费、手续费等。

职业闭店人：专门为经营困难的商家策划实施“卷款跑路”方案以牟利的群体，闭店过程通常伴随转移资产、变更法定代表人及股东等。

这两类企业名称通常包括“互联网信息服务”“企业管理”“营销中心”“投资咨询”“助贷”“网络科技”等。

职业背债人：专门通过提供个人信息、签订虚假合同或配合他人完成一系列手续，以自身名义为他人背负债务，进而获取一定报酬的人，实质无还款能力或还款意图。通常包括被欺骗成为背债人的群体，如学生、中老年人、有急迫金融需求的人群；以及自愿背债的群体，如打零工群体、低保户人员、已有无法偿还债务的人员等。

说明：毕马威根据监管机构风险提示、公开新闻报道等整理。

“骗贷”及逃废债的步骤及特征观察

筛选内控环境薄弱的机构

- 选择内控环境和流程管理相对薄弱的机构及其分支机构
- 寻找银行内部员工，了解不同产品需要的材料、审查标准等
- 每年允许在一定范围内有坏账率，只要控制在合理区间
- 如非内部人配合，通常尝试“跑通”流程，再进行批量进件

选择“目标人群”

- 信贷白户，如学生群体、中老年群体、打零工群体、低保户人群等
- 已有债务但无偿还能力，有配合意愿的人群
- 对目标人群进行评估，选择合适的“人设”，与银行业务产品进行匹配。例如有学历群体，学历越高可贷出的金额越高，包装为企业高管或企业主等

量身定制“贷款资料”

- 包装：挂靠单位缴纳社保、养企业、个人账户的“资金流水”等
- 伪造：伪造收入证明、工作地点、银行流水、公积金缴纳记录、房产证、企业公章等
- 拍摄视频、打造社交账号记录，伪装成企业主、高管或员工

业务办理及中介分成

- “背债人”提供个人资料以及录制“自愿配合贷款”的意愿表达、签字视频等
- 选择“企业贷”、“房贷”、“车贷”等产品，通过线上或线下渠道申请，职业背债人案例中介分成比例或高达60%
- “背债人”配合完成企业法定代表人、股东变更等

贷款迅速劣变为不良

- 获得放款或完成变更后不再还款，贷款迅速劣变为不良

风险线索及内审思路

在制定详细审计方案阶段，可通过聚焦重要指标，分层分类开展数据分析，以从不同维度识别可疑风险信号，例如是否存在分支机构内控环境薄弱、风险文化激进，以至于被贷款中介利用；是否存在特定的业务/产品设计不合理，存在管理薄弱环节；是否有员工在不知情情况下被不法贷款中介机构利用，或者配合不法贷款中介机构骗贷等，提升审计对象锁定的精准性。

高风险机构

- 分支机构不良率畸高（整体、分品种、渠道等）
- 分支机构新生成不良率畸高（整体、分品种、渠道等）
- 分支机构首贷不良率畸高（整体、分品种、渠道等）

高风险业务

- 某业务或细分产品、某渠道（如线上、线下）不良率畸高
- 某业务或细分产品、某渠道（如线上、线下）新生成不良率畸高
- 某业务或细分产品、某渠道（如线上、线下）首贷不良率畸高

高风险员工

- 经办业务不良率畸高
- 经办业务新生成不良率畸高
- 经办业务首贷不良率畸高

可疑样本筛查

在开展敏捷审计阶段，可通过以下风险线索，通过数据分析快速锁定可疑样本，提升内审抽样的精准度。

问题特征	内审线索	筛查思路
批量进件	设备类	短期内同一 IP、MAC、手机号多次申贷
		多笔贷款申请源自同一个IP地址或相同的移动设备
		多个不同的借款人留存相同的联系电话或电子邮箱
	地址类	多笔贷款的借款人留存相同的联系地址
		多笔贷款的抵押物地址邻近
		多笔贷款借款人短期内来源于同一工作单位（中小企业）
		多个借款人工作单位注册地址位于同一幢大楼或同一条街道
虚假资料	个人类	借款人社保于近一年或6个月内新购买
		家庭住址、联系地址、工作地址虚假（如共享地址）
		同一客户频繁申请装修贷、购车贷等
		账户流水收入合计与纳税申报收入不符
		近期账户流水与以往资金流水趋势不符，存在包装嫌疑
	企业类	企业注册地址为共享地址（如联合办公、集群托管、虚拟产业园等）
		新注册或者近6个月才注册的公司申请贷款、对公账户无实际经营交易流水，或公司还未开通基本存款账户
		变更股东或法定代表人信息后，短期内即申请经营贷
		公司账户流水与以往经营趋势不符，存在包装嫌疑
		近期企业账户流水收入合计远高于纳税申报收入
账户及用款行为异常	账户行为	同一账户或控制账户为多名贷款客户提供周转资金
		账户转出转入交易发生时间短且金额近似
		贷款后账户资金流水对比贷款前资金流水断崖下跌
		账户/账户群发生规律性大额取现
	资金流向	多笔贷款的支付对象集中为某个人、某家企业
		受托支付后直接或利用关联账户回流至某账户/账户群
		贷款资金流向涉及担保公司、小贷公司、典当行、信息服务公司、科技服务公司、互联网信息公司、投资公司、咨询公司等

4. 内审理论动态

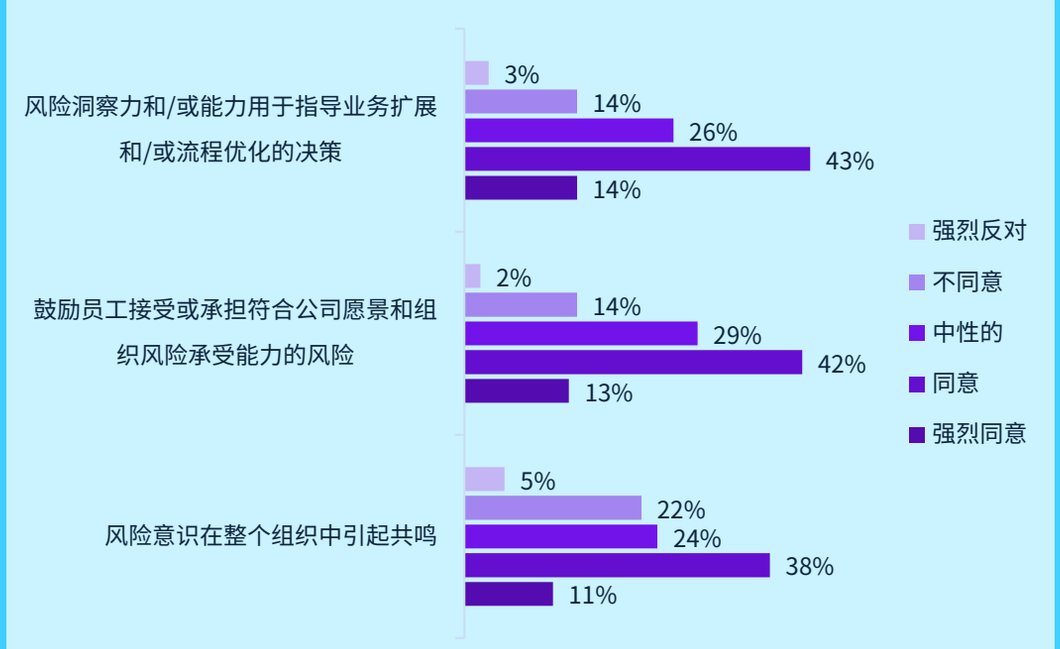
报告一：增强的企业风险管理与战略决策

国际内部审计师协会于2025年发布了《增强的企业风险管理与战略决策》。随着企业风险管理（ERM）的快速普及与发展，未来十年ERM市场将增长3倍，但多数企业并未真正发挥其价值。六成企业虽把ERM写进了战略规划，却并未将风险洞察真正融入决策过程中，且风险意识、技术工具与人工智能（AI）的应用均明显不足。报告呼吁通过及时的风险评估、内审协同以及技术升级三大策略，把ERM从“已有”变为“好用”。只有当企业领导者能够深刻理解风险以及风险管理如何影响组织各方面运作、明确风险缓释措施的有效性并能洞察新兴风险时，才更有可能制定并执行提升运营绩效和实现可持续成功的战略，这正是ERM的核心价值所在。若ERM体系未能与战略相结合，则难以发挥其真正的潜力。

目前企业在ERM与战略的融合程度及成熟度方面存在显著差异。部分企业尚未建立规范的风险战略体系，即便已建立正式流程的企业，其ERM活动与战略目标之间仍可能存在脱节。更根本的问题是，许多企业仍难以建立全员风险意识。最新调查数据显示：仅49%的受访者认同或强烈认同“风险意识已深入组织各个层面”；仅57%的受访者认可“企业鼓励员工承担符合公司愿景和组织风险承受能力的风险”；同时，仅57%的受访者认为“风险洞察和/或风险能力被用于指导业务扩张及流程优化决策”。进一步分析显示，公共服务部门参与者对这些表述的认同比例显著低于企业整体水平。

ERM活动与战略目标之间仍存在脱节

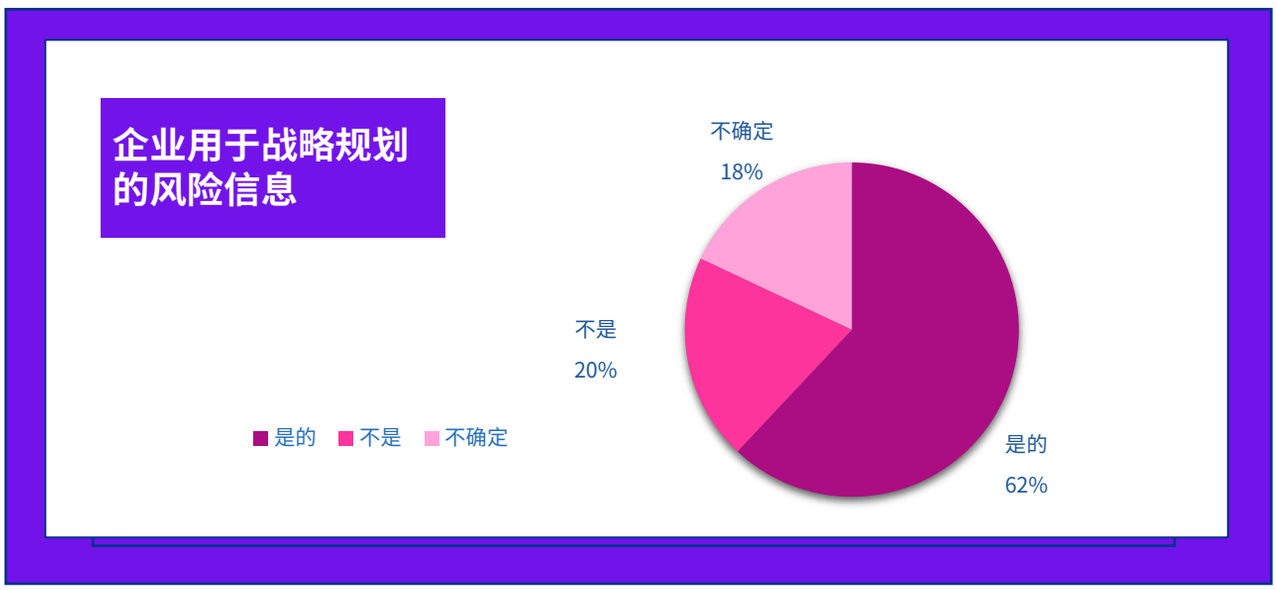
调查数据体现企业受访者对于结合公司前景与风险的意识：



说明：根据国际内部审计师协会《增强的企业风险管理与战略决策》编制。

ERM价值有待释放：仅六成企业将风险信息真正用于战略决策

ERM项目应促进风险信息在战略规划与决策中的应用。然而，调查显示，这方面仍有待改进。仅六成（62%）的受访者表示，其所在组织将风险信息用于战略规划。其中，公共服务部门的受访者反馈更差，仅有46%表示认同。



ERM领域的系统支撑和技术应用仍有待提升

01

ERM项目信息系统支持仍显不足

近六成（59%）受访者表示，其ERM项目仍依赖基础工具（如文字处理软件和电子表格）。仅有21%的受访者使用治理、风险与合规（以下简称GRC）平台，20%使用内部自主开发的技术

02

前言技术应用方面仍有较大提升空间

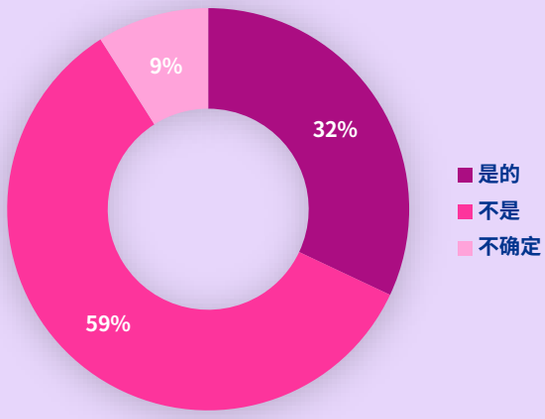
尽管越来越多机构已明确采用先进系统实现数据分析、报告生成和决策辅助，在人工智能（AI）、机器人流程自动化（RPA）、机器学习（ML）等前沿技术的应用方面，大多数企业仍处于初步阶段，尚未实现规模化部署

03

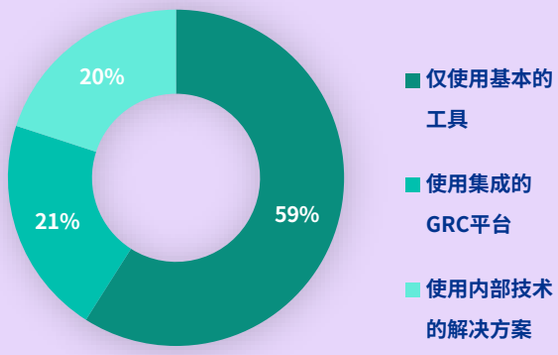
人工智能（AI）在风险管理中的应用潜力巨大

仅有不到十分之一的受访者表示，AI经常被用于风险识别（6%）或大量用于风险管理活动的数据输入（2%）

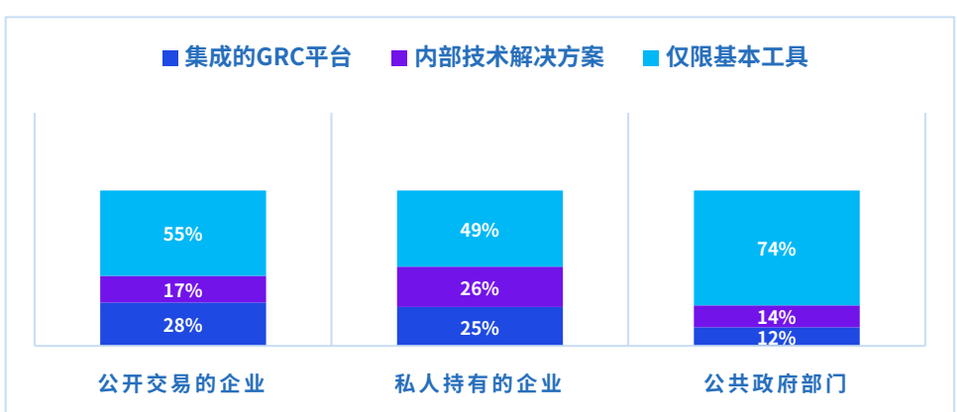
企业的风险职能是否使用了外部资源



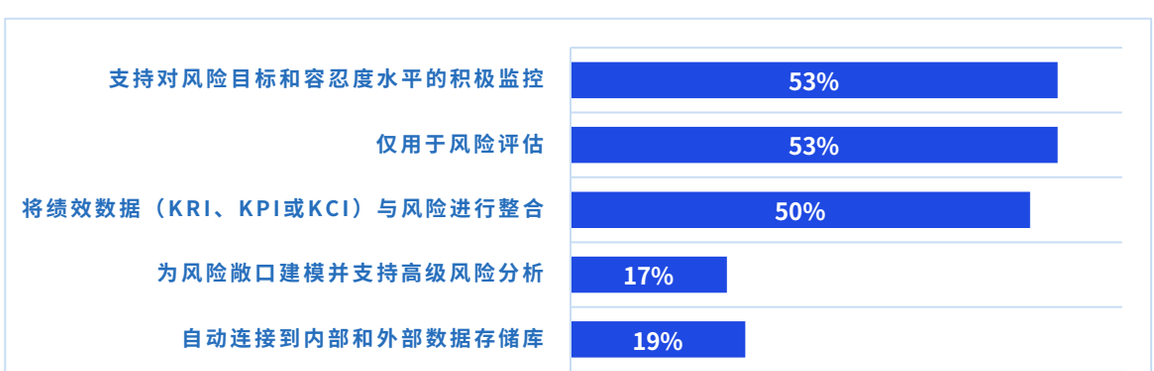
企业技术使用现状



不同组织类型的风险职能对技术的利用

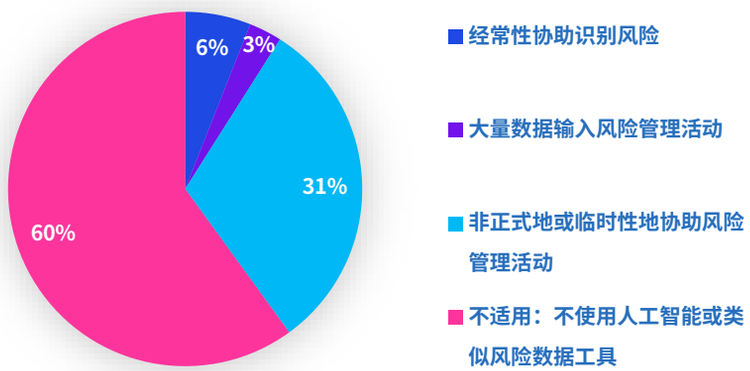


企业对于GRC技术平台不同功能的运用



尽管人工智能技术（尤其是2022年ChatGPT等大语言模型出现后）已在商业领域获得广泛应用，但其在ERM中的融合程度仍然有限。调查显示，60%的机构尚未引入任何AI或类似风险数据分析工具；31%的机构仅进行非正式或零散尝试，尚未形成系统性的应用。仅6%的机构能够较频繁地借助AI识别风险，而将AI深度应用于风险管理数据录入等核心环节的比例低至2%，反映出当前AI在ERM中的应用仍处于早期探索阶段。

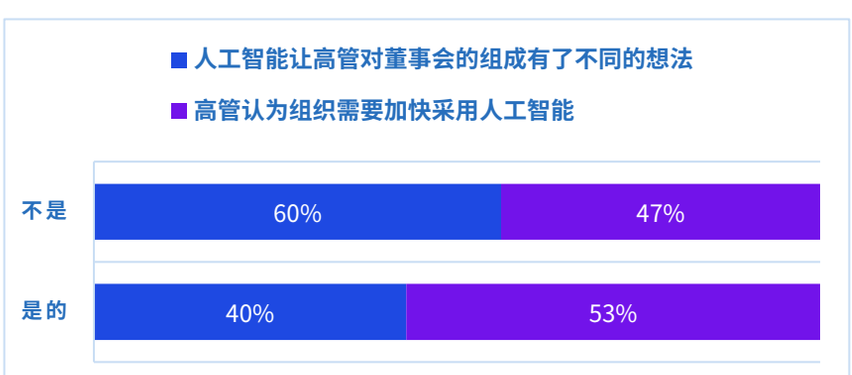
人工智能在风险部门中的应用



报告二：人工智能在董事会治理中的价值

内部审计基金会于2025年6月发布了第129期“高层基调”报告，主要讲述了人工智能正在深刻改变董事会的运作方式、战略决策和风险管理，要求董事调整监督实践以确保决策透明、负责且符合组织价值。与此同时，董事会也需注意AI应用可能带来的责任风险，并借助内部审计加强独立评估、治理框架审查及伦理合规风险管控。

对董事会成员和高管进行的人工智能治理调查



说明：根据国际内部审计师协会《人工智能在董事会治理中的价值》编制。

人工智能重塑董事会治理：价值、挑战与审计赋能

01 人工智能在董事会治理中的核心价值

- 人工智能技术正在深刻重塑董事会治理模式，为决策提供实时数据支持和前瞻性洞察。斯坦福大学研究显示，AI可提供“类顾问式”的辅助，使董事能够基于更全面、深入的信息进行战略研判。值得注意的是，预测性AI可在季度开始两周内识别收入问题，彻底改变传统依赖季度报表的滞后治理模式。这种技术赋能使董事会从被动响应转向主动引领，在战略规划、风险监督和绩效评估等方面产生根本性变革。AI的治理价值主要体现在三个方面：提升战略决策质量，通过大数据分析提供市场洞察；增强风险管理能力，实时监控风险指标并提供预警；提高治理效率，自动化日常监督工作。然而，要实现这些价值，董事会需要重新思考角色定位，培养数字素养，建立与新技术相适应的治理流程。只有在技术、制度和人员三个层面协同推进，才能充分发挥AI在董事会治理中的革命性价值，推动企业向更创新、更繁荣的方向发展。

02 发挥咨询角色作用，关注人工智能治理与风险管理

- 有效实施人工智能治理需要系统性的架构设计。企业应当建立清晰的AI治理框架，包括明确的责任分工、标准化流程和监督机制。具体而言，需设立专门的AI治理委员会，并组建跨职能团队，吸纳信息安全、合规、法律、风控和审计等领域的专家，共同制定监控标准和执行机制。实施过程面临多重挑战：技术层面，智能体行为可解释性不足，存在"黑箱"决策问题；权限管理方面，配置不当可能导致越权操作；系统架构方面，AI的自我演进能力使系统日趋复杂；风险管控方面，在缺乏人工监督时，AI行为可能产生不可逆的实质后果。此外，AI应用还带来治理结构的深层变革。传统董事会与管理层之间的信息传递和监督关系被重新定义，职责边界需要调整。海量实时数据可能导致决策信息过载，算法推荐可能使治理决策趋于"平均化"。这些问题需要董事会从治理理念、组织架构和运作流程等多层面进行系统性应对。

03 发挥审计独立监督作用，推动股权管理、公司治理再上新台阶

- 在人工智能治理体系中，内部审计部门承担着关键保障职能。内部审计需要为董事会提供三个层面的支持：评估AI控制环境的有效性，审计AI决策过程的合规性，以及评估AI应用的风险管理。这要求内部审计超越传统财务审计范畴，发展成为AI治理的专业保障力量。具体而言，内部审计需要评估AI治理框架的完整性，审计算法模型的公平性和透明度，监控AI系统的运行效果，并建立专门的AI风险图谱。特别重要的是，要协助董事会建立AI危机应对机制，针对算法偏见、隐私泄露、和系统故障等场景制定应急预案。为了有效履行这些职责，内部审计部门自身需要进行数字化转型。审计人员需要掌握数据分析、机器学习原理等新技能，开发能够对AI系统进行实时监测的新工具，并与数据科学家、算法工程师等建立新的合作机制。通过这些变革，内部审计能够成为推动AI治理成熟度提升的战略伙伴，帮助企业在拥抱人工智能的同时确保治理的有效性和责任感。

报告三：内部审计与网络安全的协作

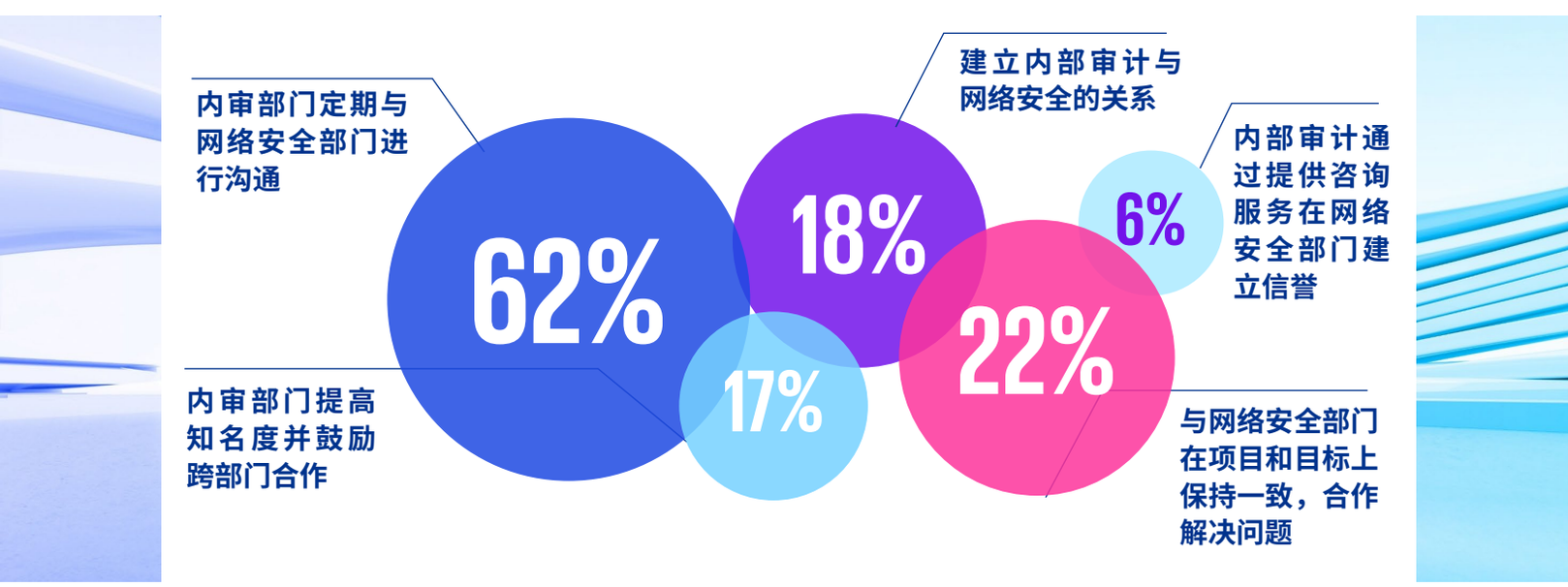
国际内部审计师协会于2025年发布了《天然盟友：通过内部审计和网络安全协作培育网络韧性文化》，围绕网络安全存在的风险展开讨论，以及强调内部审计和信息安全之间的协作对于构建网络韧性组织至关重要。网络攻击主要包括通过网络钓鱼，凭证利用和漏洞利用等三种途径。网络安全是各类组织面临的首要挑战，从初创企业到大型企业均受影响。根据《2025年聚焦风险》报告，网络安全仍是全球内部审计领导者排名首位的风险。勒索软件攻击是首席信息安全官（CISO）面临的三大主要网络安全威胁之一。该报告提议应培养信息安全和内部审计职能的协作关系，有助于加强网络安全并培育网络韧性。通过确保数据受保护的政策和流程，可以克服与内部审计共享信息相关的风险。

网络安全的问题与重要性

超过三分之二（73%）的受访者将网络安全列为公司前五大风险之一，远远超过了第二大风险人力资本（51%）	73%
在网络安全相关损失中，勒索软件和敲诈事件带来的损失中位数为4.6万美元	46k
内审协会的年度展望未来报告发现，82%的受访者将网络安全风险评为“非常高”或“高于平均水平”	82%
超过 80%的受访者报告称，内部审计和信息安全之间的会议很常见	80%

促进内部审计与网络安全的合作方法

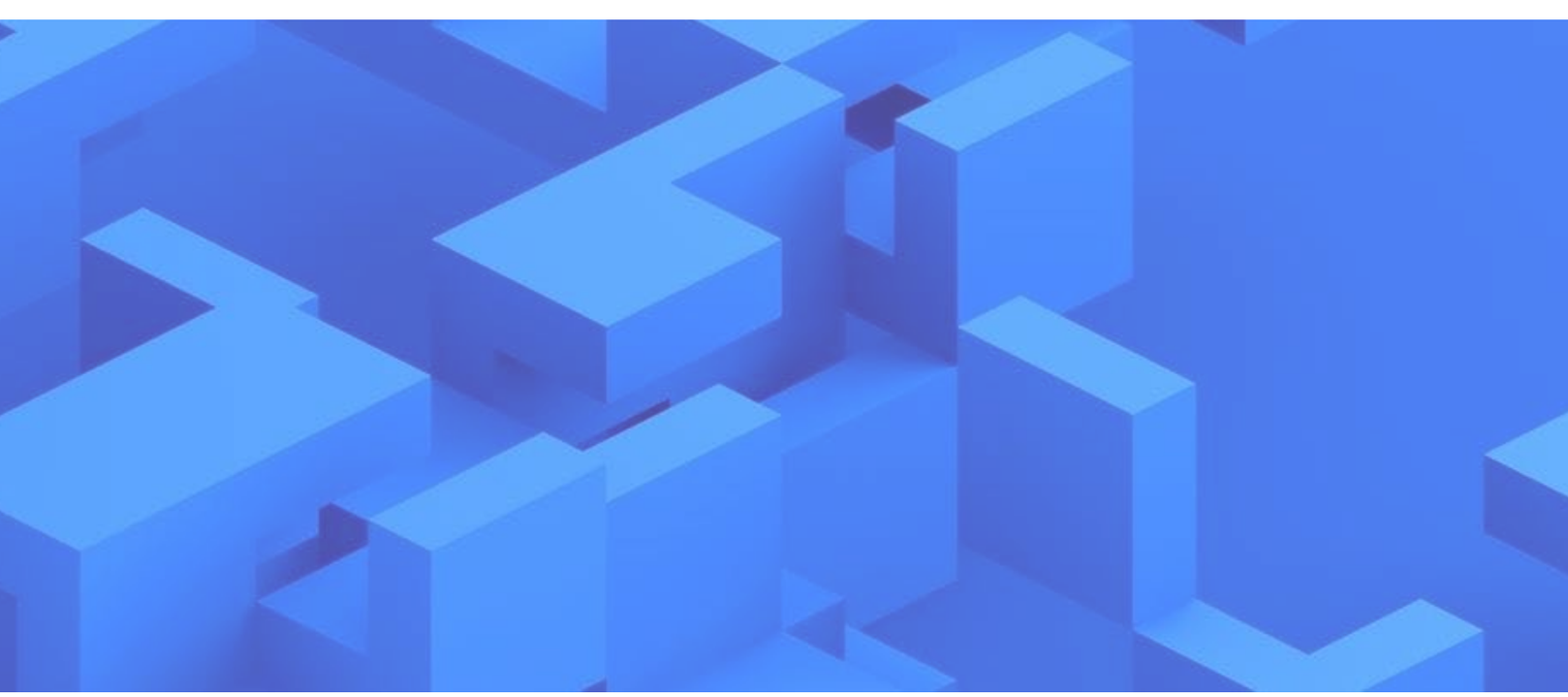
我们总结了五个提高内部审计与网络安全关系的步骤，以供内审从业者思考：



说明：根据国际内部审计师协会《天然盟友：通过内部审计和网络安全协作培育网络韧性文化》编制。

具体合作的应用细节与其带来的优势

		内部审计流程	合作益处	合作策略	网络韧性文化
	将网络安全融入所有审计中				
	提高内部审计对信息安全的了解				
	网络事件可以加速合作				
	设立联合风险委员会以加强合作				
	打破信息孤岛				
	支持综合保证				
	联合使用技术工具 / 软件				
	鼓励对齐 / 透明度				
	在人工智能采用 / 使用方面进行合作				
	改善数据共享 / 信息流动				
	增强信息安全对内部审计价值的认可				
	协调董事会沟通				
	支持向组织传达网络安全信息				
	支持监管合规				
	识别新兴风险 / 趋势				
	定位内部审计为信息安全倡导者				
	在审计工作中实现更大的透明度				
	关注声誉风险考量				
	双向培训 / 外部审计师				
	定位内部审计为战略顾问				



报告四：关于最新审计状况的调查

国际内部审计师协会于2025年3月发布了《北美内审脉冲：内审领导的基准》，主要讨论了2025年北美内部审计状况调查报告，介绍了管理、审计活动、内部审计预算、员工、及风险等五大主题的关键洞见。首席审计执行官（Chief Audit Executive, CAE）期望与组织建立更强的战略关系，并在风险管理方面也扮演重要角色，近三分之一的首席审计执行官亦负责企业风险管理（ERM），超过三分之二的首席审计执行官与风险管理职能部门协调和共享知识。同时40%的首席审计执行官表示正在使用生成式人工智能（GenAI）进行内部审计活动，千禧一代的使用率更高。数据分析技能被视为内部审计活动的基础，超过90%的首席审计执行官认为数据分析的采用对行业的未来发展至关重要。

部分洞察要点摘录如下，供内审部门参考：

审计现状调查报告的四大要素与12项发现

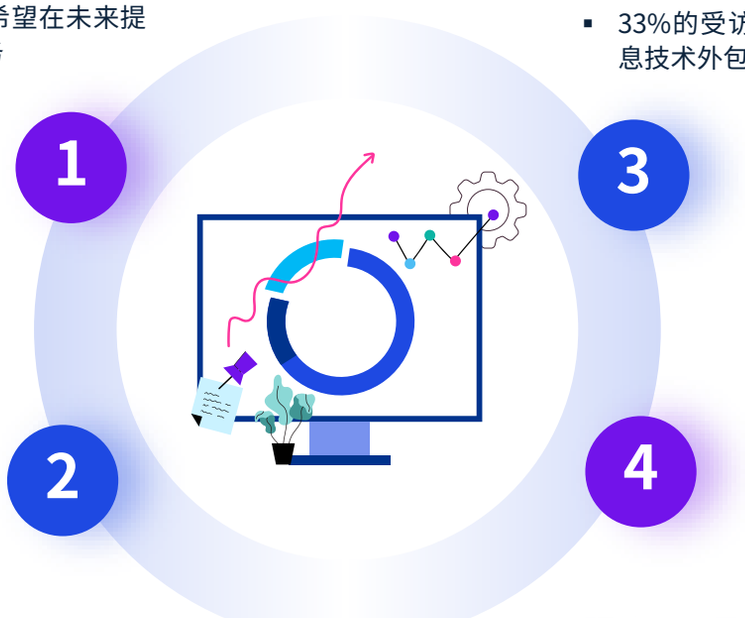
首席审计执行官（“CAE”）问卷，以供内审从业者思考：

战略与咨询服务

- 战略调整与更充足的资金有关
- 大约一半的受访者表示部门资金不足
- 首席审计执行官希望在未来提供更多的咨询服务

技术

- 92%的首席审计执行官表示，数据分析是未来最重要的技术技能
- 14%的首席审计执行官表示，他们的职能部门正在使用GenAI进行内部审计活动
- 33%的受访者使用网络安全和信息技术外包服务



职责与审计规划

- 首席审计执行官始终承担内部审计之外的责任
- 与9年前相比，首席审计执行官现在更有可能对风险管理内容负责
- 运营、合规和数据披露总体上占据了审计计划的大部分

预算与人员

- 内部审计预算和工作人员增长的趋势已稳定到接近新冠疫情前的水平
- 去年，近70%的首席审计执行官不得不招聘新职位或空缺职位
- 远程工作略有减少

说明：根据国际内部审计师协会《北美内审脉冲：内审领导的基准》编制。

战略与咨询服务

内部审计与组织战略对齐程度越高，获得的资金支持越多。超过一半的首席审计执行官表示内部审计与组织战略基本或完全对齐。

约一半的受访者表示资金不足，尤其在公共服务部门影响最大。资金不足会干扰内部审计功能的有效运作。

首席审计执行官希望未来增加咨询服务比例，从目前的25%提升至40%，审计服务75%降低为60%。

技术

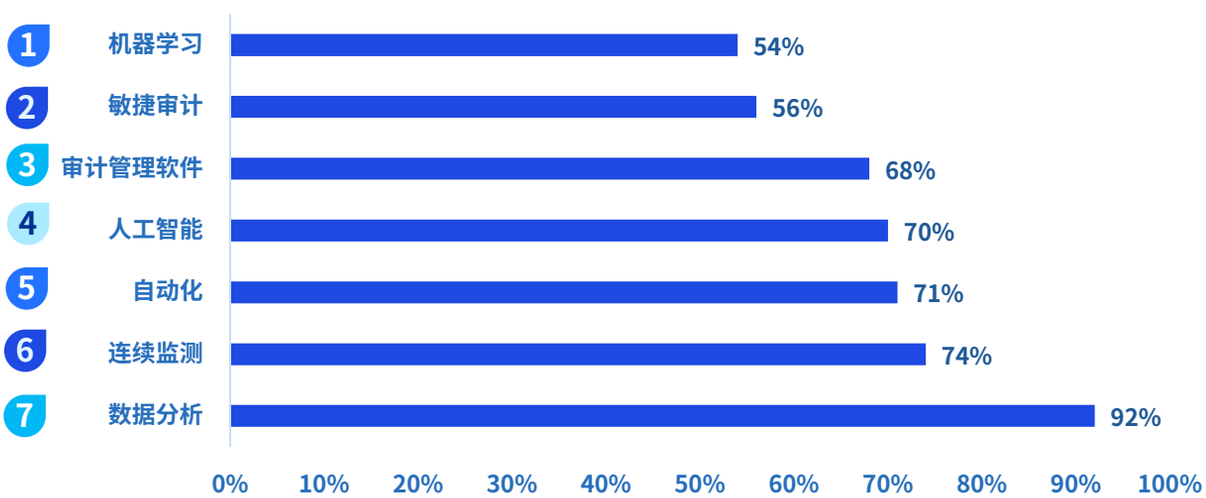
92%的首席审计执行官认为数据分析是未来最重要的技术技能。但仅28%的首席审计执行官表示其部门具有高级数据分析应用。数据分析也是CAE最希望提升员工能力的领域。

大约40%的首席审计执行官使用生成式人工智能（GenAI）进行内部审计活动。不同代际间存在显著差异，千禧一代最活跃（52%），其次是X世代（40%）和婴儿潮一代（31%）。

约三分之一的受访者将网络安全和信息技术服务外包。在金融服务领域，外包比例显著高于平均水平（约50%）。

内部审计职业未来最重要的技术技能?

数据分析为未来重要的技能



首席审计执行官职责与审计规划

近90%的首席审计执行官表示其职责超出内部审计范畴。主要领域包括反欺诈（47%）、披露准确的财务数据（SOX）（36%）和道德或举报程序（33%）。

首席审计执行官负责企业风险管理（ERM）的比例从2015年的24%上升至2024年的30%。

运营、合规和披露数据占据大部分审计计划。IT和网络安全合计占17%。

01

企业风险管理与内部审计角色

与九年前相比，如今首席审计执行官更有可能负责企业风险管理（ERM）

02

对风险管理拥有责任

在过去的九年中，声称对ERM拥有持续责任的首席审计执行官比例有所增加（从19%上升到23%），同时声称临时负责ERM的比例也有所上升（从5%上升到7%）

03

风险负责比例上升

当将这些指标合并时，数据显示2015年有24%的首席审计执行官负责ERM，而到2024年这一比例上升了6个百分点

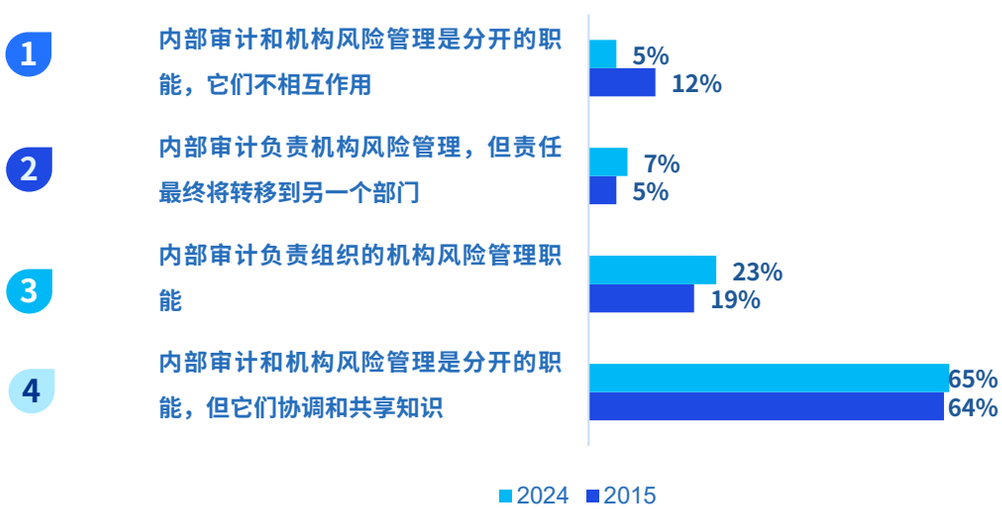
04

内部审计与风险管理不再相互独立

这一变化的原因是认为内部审计和ERM是不相互关联的独立职能的比例有所下降（从12%下降到5%）

内部审计与企业风险管理的关系

内部审计逐渐与企业风险管理职责相互交叉



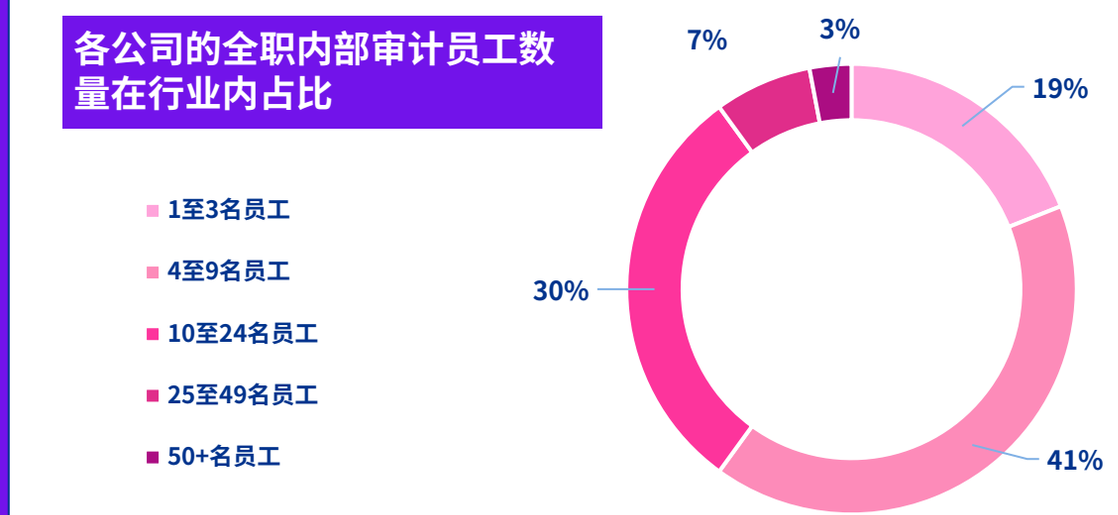
预算与人员

内部审计预算和人员增长趋势已接近新冠疫情前水平。

2024年，34%的首席审计执行官表示预算增加，25%的受访机构人员增加。近70%的首席审计执行官需要招聘填补新职位或空缺职位。

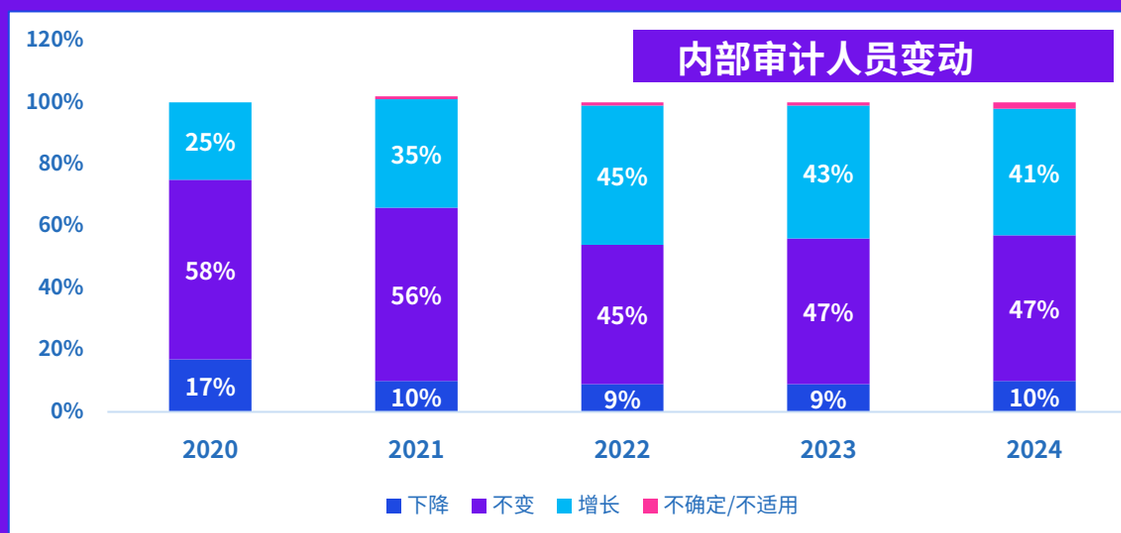
即便是规模较小的部门（4-9名全职员工），近一半的首席审计执行官也表示需人员招聘。

各公司的全职内部审计员工数量在行业内占比



41%的受访者表示，他们在过去一年增加了内部员工的预算，这代表着从最近的45%的高点逐渐下降。外包方面也出现了类似的下降趋势。工具和技术的预算基本保持稳定，几乎没有变化，只有4%的人表示他们的技术预算减少了。差旅预算的分配似乎高于2020/2021年，但可能仍低于疫情前的水平。

内部审计人员变动



5. 内审国际动态

巴克莱银行

亮点观察

- 积极拥抱技术进步，在内部审计计划与内部审计章程中体现审计前瞻性与技术融合，运用人工智能与数据分析提升审计质效
- 通过交叉任职提升董事会专业委员会之间的信息沟通与协作
- 迭代优化举报机制，进一步加强“畅所欲言”文化

1. 内部审计计划与方法的更新

巴克莱银行2024年度的财务报告显示，审计委员会审议批准了2024年度内部审计计划、方法论及交付成果，其中涵盖人才继任计划的审计方法。值得关注的是，巴克莱银行的内审职能已开始运用人工智能（AI）技术支持审计工作的有效实施。此外，审计委员会在年底批准了2025年度内部审计计划及修订的内部审计章程，更新主要聚焦于提升审计工作的前瞻性与技术融合。

2. 跨委员会协作与信息共享

审计委员会与其他董事会专业委员会保持紧密协作，以确保集团整体策略的一致性与高效性。通过交叉任职机制，例如风险委员会主席兼任审计委员会成员，审计委员会主席也参与风险与可持续发展委员会等措施，有效促进了不同委员会之间的信息共享与沟通协同，减少了职能重叠，强化了集团治理成效。

3. 进一步强化举报机制

审计委员会每半年获取来自管理层的有关举报机制的详细报告，内容涵盖举报案例数据、“畅所欲言”文化的建设情况及潜在报复行为的趋势等。审计委员会还定期就举报流程改进措施的效果征求反馈，包括员工体验以及如何进一步鼓励员工长期积极参与，以提升举报机制的有效性和员工信任度。

4. 科技与数据分析在审计中的应用

在“内部审计的技术应用”（ BIA T reach in ）交流活动中，审计委员会深入了解了内审职能在审计技术应用方面的创新，特别是人工智能（AI）在审计实施中的具体运用。这标志着巴克莱内部审计职能正积极拥抱技术变革，通过数据分析与智能化工具提升审计工作的准确性、效率与覆盖范围，推动审计模式的现代化转型。

说明：毕马威根据国际银行年报及公开新闻报道等整理而成。

美国银行

亮点观察

- 审计委员会积极识别可能妨碍审计部门有效履行职责的审计范围或资源限制问题，确保内部审计部门拥有足够的授权、预算及人员
- 内部审计工作成果直接作为公司战略及资本规划流程的关键输入，以保证银行实现“负责任的增长”

1. 确保内部审计的独立性与权威性

延续内部审计的核心架构以保持其权威性与独立性。首席审计执行官（CAE）及内部审计部门继续直接向董事会下设的审计委员会进行职能汇报，以确保审计结论的客观公正。同时，CAE在行政上向首席执行官汇报，以保障日常运营效率。美国银行的双重汇报机制是审计职能独立性的基石，以防止其受到业务部门的干扰。

2. 内部审计的核心职能

内部审计的核心职能为持续专注于对全行关键流程与控制进行独立的测试、评估与验证。工作重点包括通过检查和持续监控，对集团的信贷审批决策及信用流程有效性进行独立评估。内部审计作为风险管理“三道防线”模型中至关重要的第三道防线，旨在为前两道防线（业务部门与风险管理部门）的有效性提供最终保证，并向董事会和高级管理层提供客观的确认。

3. 审计委员会的履职重点

董事会审计委员会在过去一年里积极履职，不仅监督内部审计职能的整体绩效，更会主动质询高级管理层和CAE，以识别任何可能妨碍审计部门有效履行职责的审计范围或资源限制问题。此举旨在确保内部审计部门拥有足够的授权、预算与人员，能够无顾虑地执行其年度审计计划，应对当年出现的各类风险。

4. 三道防线的紧密协作

内部审计作为独立的第三道防线，与第一道方向（业务部门）和第二道防线（全球风险管理部）协同运作。其工作成果直接输入至公司的战略与资本规划流程，为董事会和高级管理层提供关于风险管控有效性的独立见解，以为银行实现“负责任的增长”战略和维持稳健财务地位提供关键保障。

联系我们

李砾
毕马威中国
金融行业研究中心主管合伙人
邮箱：raymond.li@kpmg.com
手机：139 1033 7443

靳蓓
毕马威中国
金融行业研究中心副总监
邮箱：catherine.jin@kpmg.com
手机：136 1115 0725

赵一诺
毕马威中国
金融行业研究中心副总监
邮箱：nicholas.y.zhao@kpmg.com
手机：139 1170 3295

本系列报告所使用之监管规则、监管处罚数据，承载于毕马威天罡智慧合规平台。如需进一步了解相关信息，请与我们联系。

特别鸣谢刘雨航、施雅童、侯亚男、陈希、赖恺靖等对本报告作出的贡献。

kpmg.com/cn/socialmedia

如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站：
https://home.kpmg/cn/zh/home/about/offices.html