

商业银行内审观察

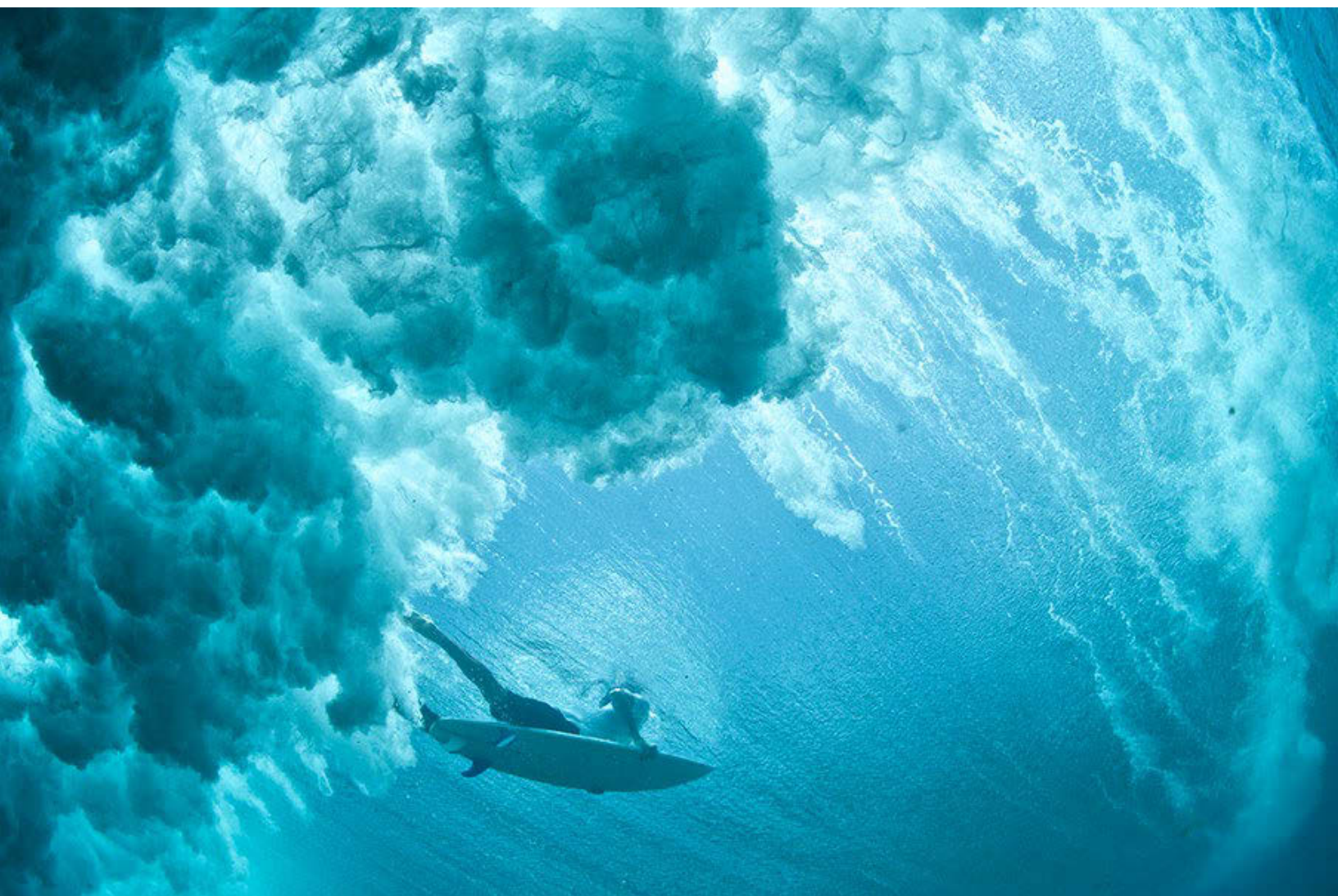
2026年度第一季度





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，并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

2026年一季度监管新规变化、《个人贷款业务明示综合融资成本规定》《金融机构个人消费类贷款催收工作指引（试行）》《保险产品适当性管理自律规范》等重点新规解读、内部审计关注事项及建议等	04
---	----

2 监管处罚洞察

2026年一季度监管处罚整体分析、监管处罚重点及趋势洞察，内部审计关注建议及参考程序等	19
---	----

3 敏捷审计专题

“端到端”视角的信贷业务模型及系统功能审计、生成式人工智能模型审计	26
-----------------------------------	----

4 内审理论动态

国际内部审计师协会报告《协同而不妥协》《内部审计与人工智能驱动的欺诈》《赋能下一代内部审计人才》主要内容及审计启示	31
---	----

5 内审国际动态

高盛集团、摩根大通、汇丰集团等近期内部审计动态及较佳实践参考	38
--------------------------------	----

1. 监管规则追踪



监管新规变化

2026年一季度，财政部、中国人民银行、国家金融监督管理总局、中国证券监督管理委员会、中国银行业协会、中国保险行业协会、中国证券投资基金业协会等监管机构、行业自律组织和交易所等共发布重要新规及征求意见稿54项。从涉及领域与重点规范事项来看，主要涵盖金融监管、信贷业务、同业业务、代理销售、托管业务、资本市场业务、运营管理、反洗钱等多个业务及管理领域，旨在进一步完善金融市场体系、强化风险管理、优化资源配置以及推动经济高质量发展。

从监管重点来看，一方面，在金融消费者与投资者权益保护方面，重点针对保险、基金、信托等产品强化了适当性管理和信息披露等要求，内部审计需关注代理销售、托管业务合规性与存量业务整改情况；另一方面，在信贷业务领域，综合强化了贷款贴息、催收、综合融资成本明示等内容，内部审计需在信贷业务检查中予以关注。



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
《国家金融监督管理总局行政许可实施程序规定》	行政许可	- 规范国家金融监督管理总局及其派出机构实施行政许可行为，明确行政许可程序，提高行政许可效率。适用于对金融机构设立、变更、终止、业务、任职资格及其他法定行政许可事项的实施程序，确立统一的申请与受理、审查、决定与送达、退出及公开等制度。 - 近年来，监管处罚案由中常见“分支机构未经批准终止营业”“董事、高级管理人员未经任职资格许可即履职”等处罚案由，内部审计需关注相应事项的落实工作机制以及实务中的落实情况。
《银行保险机构许可证管理办法（2026）》	行政许可	- 坚持金融特许经营、持证经营原则，适应金融监管实际需要，进一步规范、调整许可证分类及适用对象，压实银行保险机构许可证管理主体责任，加强许可证合规管理，坚持过罚相当原则，细化完善有关行政处罚标准，规范、优化工作流程，加强工作程序衔接。 - 对银行保险机构许可证实行分级管理。 - 近年来，监管处罚中常见“金融许可证管理不善”“金融许可证遗失”“遗失许可证未按规定报告”“损毁并丢失金融许可证”“未按规定公示许可证”“超期限未更换金融许可证”等处罚案由，内部审计需对照新规要求，关注金融许可证保管、公示、换证、遗失报告等事项。
《中国人民银行残缺污损人民币兑换办法（2026）》	运营管理	- 对残缺污损人民币的兑换明确了范围、标准、流程以及特殊情况处理。 - 近年来，人民银行在检查中关注现金存取业务，处罚常见“违反人民币流通管理规定”“对外支付残缺、污损人民币”“未按规定挑剔残缺、污损人民币”等案由，内部审计需在运营管理检查中予以关注。

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
《中国人民银行关于银行业金融机构人民币跨境同业融资业务有关事宜的通知》	同业业务 国际业务	- 覆盖人民币跨境同业融资各类业务，将银行业金融机构人民币跨境同业融资净融出余额与其资本水平、资金实力挂钩，促进合理开展业务。 - 设置宏观审慎管理相关参数，根据市场形势进行逆周期调节。 - 境内银行向境外机构净融出人民币资金余额不得超过人民币跨境同业融资净融出余额上限。
《反洗钱特别预防措施管理办法》	反洗钱	- 涵盖三类对象：恐怖活动组织人员、联合国安理会制裁名单、央行认定的重大洗钱风险对象。 - 对限制及制裁名单对象停止提供金融服务，限制其资金及资产转移；禁止事前通知。 - 名单发布或调整时需立即回溯核查存量客户；新建立业务关系时需核查新增客户及交易对手。 - 采取措施后续及时书面报告央行；涉及恐怖活动的还需同步报告公安、国安部门。 - 要求金融机构建立反洗钱特别预防措施内控制度，持续关注并及时获取三类名单。 - 内部审计需关注适用名单是否更新、准确；关注存量客户持续回溯管理机制是否完善；关注报告工作机制及留痕要求。
《关于优化实施个人消费贷款财政贴息政策有关事项的通知》	信贷业务 个人消费贷款	- 将个人消费贷款财政贴息政策实施期调整为2025年9月1日至2026年12月31日，居民在此期间发生的符合条件消费可享受贴息。 - 取消原实施方案中消费领域限制，个人消费贷款用于各领域真实、合规消费以及新发生的信用卡账单分期均可纳入贴息。 - 取消单笔消费贴息上限（原500元）及单户累计上限（原1,000元）；维持每人每年累计3,000元上限不变。年贴息比例1个百分点。 - 经办机构对借款人消费信息真实性、合规性识别负主体责任，对报送材料的真实性、合规性、准确性负责。监管将组织联合抽查，违规情节严重者将被取消经办资格。
《关于优化实施服务业经营主体贷款贴息政策的通知》	信贷业务	- 将服务业经营主体贷款贴息政策实施期限延长至2026年12月31日。 - 明确2026年新发放贷款单户可享受贴息额度上限提高至1,000万元，贴息期限不超过1年，年贴息比例为1个百分点。 - 支持领域在原有8类基础上新增数字、绿色、零售三类；文化领域界定调整。 - 四部门联合抽查；严禁贷款资金用于理财套利、房地产等；重复享受贴息将被严格追责。经办银行对资金用途真实性负主体责任，违规严重的取消经办资格。

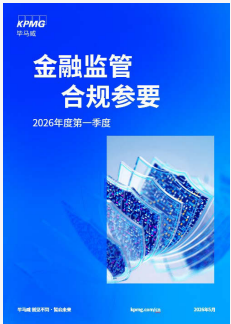
法规名称	涉及领域	法规核心内容暨内审关注事项
《关于优化实施设备更新贷款财政贴息政策的通知》	信贷业务 公司信贷	- 明确自2026年1月1日起实施至2026年12月31日。 - 将经营主体设备更新项目相关固定资产贷款纳入中央财政贴息支持，贴息比例为贷款本金的1.5个百分点，期限不超过2年；自贷款发放之日起贴息。 - 新增纳入科技创新和技术改造再贷款政策支持的、2026年期新发放的科技创新类贷款。 - 在原有工业、能源电力、交通运输、物流、文旅、老旧农具基础上，新增建筑和市政、用能设备、航空器材、电子信息、安全生产、设施农业、渔船、冷链设施、粮油加工、废弃物循环利用、小水电、消费商业设施、人工智能、养老等14个领域。 - 财政贴息不再以贷款获得再贷款支持为前提。 - 四部门将联合抽查，严禁资金用于投资理财等套利活动；避免重复享受中央财政贴息。经办银行对资金用途真实性负主体责任，违规严重的取消经办资格。
《关于实施中小微企业贷款贴息政策的通知》	信贷业务 普惠金融	- 适用对象为中小微民营企业固定资产贷款和参与项目使用的新型政策性金融工具资金。 - 按贷款本金给予年化1.5个百分点、期限不超过2年的中央财政贴息，单户贴息贷款规模上限5,000万元实施期限暂定1年，同一笔贷款不得重复享受其他中央财政贴息。 - 投向领域包括新能源汽车、工业母机、医药工业、工业软件、民用大飞机、轨道交通装备、农机装备等重点产业链及上下游，以及生产性服务业、农林牧渔和农副产品加工业、人工智能等新兴领域。 - 严禁用于投资理财等套利活动；违规严重的取消经办资格。
《金融机构个人消费类贷款催收工作指引（试行）》 (本篇纳入重点篇章分析)	信贷业务 个人消费贷款	- 适用范围覆盖信用卡及个人消费贷款产品，其他类型个人贷款可参照执行。 - 明确定义催收行为，将电话、信函、外访、司法及短信、企业微信等催收方式全部纳入范围。 - 建立催收行为规范，对社会广泛关注的催收时间、频次、联系信息获取等热点问题进行了全面梳理，突出强调易理解可执行，设置了禁止红线。 - 强化外部机构规范治理，明确了会员单位对外部催收机构管理的各项要求，建立约束机制。实行名单制管理，在官网公示合作机构。 - 加强催收业务内控管理，要求全面提升机构内部管理能力，实现“治管结合”。

法规名称	涉及领域	法规核心内容暨内审关注事项
《个人贷款业务明示综合融资成本规定》 (本篇纳入重点篇章分析)	信贷业务 个人贷款	• 适用对象包括所有商业银行、消费金融公司、汽车金融公司、信托、小贷公司等机构。范围覆盖营销获客、担保增效等合规机构，合作机构行为纳入银行主体责任。 • 明确“综合融资成本”内容涵盖贷款利息、分期费用、增信服务费等正常履约成本及逾期罚息等或有成本，要求贷款人依法合理确定年化水平。 • 除已明示项目外，不得收取其他任何与贷款相关的息费；合作机构违约须终止合作、追偿损失。 • 2026年8月1日起施行。按照新老划断原则，新增业务严格执行相关规定。
《关于做好帮扶小额信贷工作的通知》	信贷业务 普惠金融	• 明确帮扶小额信贷支持对象为防止返贫致贫对象及需继续帮扶的原建档立卡脱贫人口，以户为单位发放贷款。 • 贷款金额较原政策的5万元提升至为10万元（含）以下。贷款期限与原政策保持一致，为3年期（含）以内。贷款利率合同期内保持不变。担保方式为免担保。管理方面允许续贷或展期1次。 • 坚持户借、户用、户还，精准用于发展生产和开展经营；严禁用于结婚、建房、理财、购置家庭用品等非生产性支出；严禁“户贷企用”或以入股分红转贷等方式交由企业使用。 • 建立差异化监管容忍度，不良率高于自身各项贷款不良率3个百分点以内的，不作为监管和考核扣分因素；续贷不因办理续贷单独下调风险分类。 • 过渡期内（2025年12月31日前）及通知印发前合同政策在合同期内不变。
《境内企业境外放款管理办法》	委托贷款 外汇业务	• 适用对象为境内非金融企业（放款人）向符合条件的境外企业（借款人）提供资金跨境融通；放款人与借款人须有直接或间接持股关系。将境内企业人民币和外币境外放款业务纳入统一管理。 • 将境内企业境外放款纳入宏观审慎管理，明确境外放款余额上限与其所有者权益挂钩，支持企业在余额上限内办理业务；将境内企业境外放款宏观审慎调节系数由0.5上调至0.6。 • 须使用自有资金；不得使用个人资金或利用自身债务融资为境外放款提供资金来源。 • 期限原则上6个月至5年；同一笔境外放款展期不得超过一次；逾期不得对同一借款人新增放款。 • 不得用于借款人经营范围之外；不得规避境外直接投资、证券投资等管理政策；需遵守反洗钱、反恐怖融资、反逃税规定。 • 开立境外放款专用账户，多笔放款可共用；收回金额不得超过本金及利息等合理收入之和。 • 及时、准确地进行国际收支统计申报及RCPMIS数据报送。

法规名称	涉及领域	法规核心内容暨内审关注事项
《公开募集证券投资基金业绩比较基准指引》	代理销售 托管业务	- 突出业绩比较基准的表征作用。基准须与基金投资目标、风格严格匹配，具备市场代表性。基准一经选定不得随意变更；仅允许在要素无法运作、编制方案重大调整等情况下调整，且需提前30日公告。严禁因基金经理变更、短期排名等原因变更。 - 明确基金托管人的监督职责，符合基准合理性、监督投资组合与基准的相符性、复核信息披露。 - 规范基金销售机构、基金评价机构对业绩比较基准的展示、运用等行为。销售机构展示基金业绩需同时展示基准表现。 - 相关要求与存量产品基准调整过渡期为1年；托管人系统改造过渡期为6个月。
《公开募集证券投资基金业绩比较基准操作细则》	代理销售 托管业务	- 托管人须建立健全覆盖合同条款评估、投资监督、信息披露复核的工作机制；与管理人协商明确基于基准的投资监督指标；跟踪基金偏离情况并定期报告。 - 基金销售展示主动管理型基金业绩须同步展示基金表现，且原则上不得展示非合同约定的其他基准；不得将全市场选股基金与行业主题基金混合排序。 - 定期报告须披露多周期基金与基准的收益率、波动率对比；股票基金须额外披露行业分布对比，债券基金须含久期分布对比；须定性结合定量分析差异原因。 - 过渡期要求同上篇。
《私募投资基金信息披露监督管理办法》	代理销售 托管业务	- 压实各主体的信息披露责任；全面明确细化披露要求强化穿透披露；强化风险揭示，更好保护投资者权益实施差异化信息披露安排；发挥托管、审计的外部监督作用；加大信息披露违法违规行为处罚力度。 - 外部审计：私募基金年度财务会计报告，财务会计报告应当对关联交易情况进行专项说明。按照规定应当进行外部审计的，同时披露外部审计意见。 - 穿透披露：投向其他私募基金或资管产品的，须穿透披露底层资产情况；被投机构负有配合义务。 - 托管人职责：披露托管协议；出具托管人报告；复核资金头寸、证券账目、基金净值、申购赎回价格、资金流向；发现净值计价错误须督促纠正。
《保险产品适当性管理自律规范》 (本篇纳入重点篇章分析)	代理销售	- 保险业首部聚焦产品适当性管理的自律性文件，“卖者尽责、全链匹配、源头治理”。2026年7月1日起实施。 - 人身保险产品分级为P1至P5，财产保险产品分级为P1至P2；P4、P5类保险产品及投资账户进一步划分为R1至R5。 - 通过“适当性评估问卷”，从保险需求、财务支付水平、风险承受能力等维度评估；评估结果有效期原则上为12个月；65周岁以上投保人购买P3至P5类产品，须履行特别注意义务。 - 建立销售人员资质分级体系，能力等级与产品分级挂钩；最低等级智能销售基础类产品，最高等级方可销售P4、P5类复杂产品。

法规名称	涉及领域	法规核心内容暨内审关注事项
		代销机构可使用本行客户风险承受能力评估测试结果用于P4、P5类产品销售；评估结果应回传保险公司或指导客户在保险公司平台完成测评。
《资产管理信托产品适当性管理自律规范》	代理销售	- 划分产品风险等级（R1-R5）并动态管理，将合格投资者区分为专业投资者与普通投资者，对普通投资者进行特别保护，包括强化风险承受能力评估，充分履行告知义务，开展风险提示等。 - 严禁公开宣传，不得通过营业网点/APP等向不特定对象推介；严禁拆分份额变相降低投资门槛；严禁承诺保本保收益。 - 禁止向无民事行为能力人/非合格投资者销售；禁止代替投资者评估或先销售后评估；禁止向普通投资者推介高于其风险承受能力的产品。 - 代销机构应独立审慎划分风险等级；产品代理销售机构在产品风险等级划分、销售管理、投资者分类与评估分级、适当性匹配、内控管理等方面可参照《规范》执行。 - 相关资料保存至信托终止或关系解除后15年。 2026年7月1日起实施。
《关于进一步防范和处置虚拟货币等相关风险的通知》	虚拟货币	- 明确虚拟货币不具有与法定货币等同的法律地位，境内虚拟货币兑换等业务活动属于非法金融活动，一律严格禁止并依法取缔。 - 未经同意，境内外单位和个人不得在境外发行挂钩人民币的稳定币，境外单位和个人不得非法向境内主体提供相关服务。
《理财公司监管评级暂行办法》	子公司管理	- 监管评级以日常监管信息为基础，每年开展一次，评价期间为上一年度1月1日至12月31日，原则上于每年4月底前完成。 - 评级结果作为市场准入、监管资源配置和差异化监管措施的重要依据，监管机构据此调整现场及非现场监管强度、检查频率和范围，对评级下降导致不符合业务条件的理财公司，禁止新增相关业务并要求有序压降存量。

相关刊物



2026年5月，毕马威《金融新规热读》已全面改版为《金融监管合规参要》，综合收录国际国内金融业重要法规及政策变化、同业合规管理动态、典型合规案例分析、合规风险热图等，协助金融机构有效应对监管变化，持续优化合规管理效率和效果。



重点新规精读

《个人贷款业务明示综合融资成本规定》

新规背景及影响

为维护个人贷款市场秩序，保护金融消费者合法权益，提升金融服务质效，2026年3月15日，国家金融监督管理总局、中国人民银行联合发布《个人贷款业务明示综合融资成本规定》（金规〔2026〕2号），自2026年8月1日起施行。

《规定》共11条，是在现有贷款业务信息披露监管制度框架内，细化个人贷款业务息费信息披露的涵盖范围、操作方式和环节等，要求贷款人向借款人展示综合融资成本明示表，清晰披露个人贷款息费成本。

《规定》旨在推动解决个人贷款业务息费信息披露不规范、不透明问题，将更好保障金融消费者合法权益，畅通金融惠民政策传导，促进行业规范健康发展。内部审计需在《办法》生效前关注新规落实机制，并在未来审计中关注以下问题。

对商业银行影响较大的条款及审计关注建议



综合融资成本计算口径与年化准确性

《办法》明确了个人贷款业务综合融资成本是指由借款人承担的与贷款相关的各项息费，包括但不限于贷款利息、分期费用、增信服务费等正常履约成本，以及逾期罚息等违约情形下的或有成本。

内审关注建议：

- 综合融资成本计算口径是否完整，是否覆盖利息、服务费、增信费等，以及可能的逾期罚息、违约成本等；计算逻辑是否准确，年化水平计算方式是否符合《中国人民银行公告》要求的内部收益率法，对各项息费逐项折算为年化水平后加总。系统设置是否与业务规则相符。
- 对于分期产品、随借随还产品等，年化计算逻辑是否已准确适配。



综合融资成本明示表展示

《办法》要求综合融资成本明示表应注明贷款本金金额，并逐项列明贷款人及其合作机构收取的各息费项目及其收取方式、收取标准和收取主体。同时，逐项列明贷款逾期或被挪用等违约情形下的或有成本项目及其收取标准和收取主体。还应明确提示，除已明示的成本项目外，贷款人及其合作机构不再向借款人收取其他与贷款相关的任何息费。

说明：根据监管机构网站公开发布信息自行编制。



综合融资成本明示表展示（续）

内审关注建议：

- 是否实质遵循了“明示之外无收费”的要求，是否存在以“财务顾问费”“融资安排费”等名义收取其他费用。是否将合作机构的平台服务费、增信服务费等全部纳入明示表。
- 是否设计了相应管理机制，并在合作协议中明确合规机构行为约束，以防合作机构额外收取费用。
- 是否将罚息、违约罚款等或有成本明确纳入综合融资成本明细表中。



业务流程合规性要求

新规要求贷款人应当在营业场所、官网等渠道清晰披露借款人正常履约情形下的个人贷款综合融资成本上限。现场办理个人贷款业务的，应当在签署贷款合同或办理分期前，由借款人在综合融资成本明示表上签字确认。线上办理个人贷款业务的，应当通过弹窗方式向借款人展示综合融资成本明示表，设置强制阅读时间，由借款人在签署贷款合同或办理分期前确认。

线上消费场景下办理分期付款业务的，应当在消费订单支付页面以显著方式清晰展示贷款本金、分期安排及收取的服务费用、收取主体、正常履约情形下的年化综合融资成本，以及违约情形下的或有成本项目及收取标准。应明确提示，除已明示的成本项目外，不再收取其他任何息费。

因利率定价基准调整、开展优惠活动等原因导致相关融资成本发生变动的，贷款人应当及时告知借款人。

内审关注建议：

- 是否已在营业场所，官网等渠道清晰披露个人贷款综合融资成本上限。
- 对于现场业务，是否在流程中要求贷款合同签署或办理分期前，借款人在综合融资成本明示表上签字。对于线上业务，是否设置弹窗向借款人展示综合融资成本明示表，是否设置了必要的强制阅读时间，是否要求借款人在签署贷款合同或办理分期前确认。是否明确提示“除已明示的成本项目外，不再收取其他任何息费”。
- 对于发生利率定价基准调整、开展优惠活动等导致融资成本变动的，是否设置了主动、及时通知借款人的机制。



合作机构管理

新规要求贷款人在与合作机构签署的合作协议中，应当明确各方落实综合融资成本明示要求的责任和义务。贷款人应当加强合作机构管理，对合作机构违规违约行为及时采取纠正措施，情节严重的，应采取终止合作、依法追偿损失、追究法律责任等措施。

内审关注建议：

- 是否在合作机构协议模版或合同拟定管理流程中，要求明确各方落实综合融资成本明示要求的责任和义务。
- 是否建立合作机构日常管理机制，并明确违规违约行为的处理措施。

《金融机构个人消费类贷款催收工作指引（试行）》

新规背景及影响

2026年1月30日，中国银行业协会发布《金融机构个人消费类贷款催收工作指引（试行）》，规范会员单位和外部催收机构对信用卡及个人消费信贷催收行为，促进行业健康发展。

从主要内容来看，《指引》共七章五十四条，从加强行业自律、规范业务发展的角度，通过催收行为定义、催收行为规范、外部催收机构管理、内控管理、促进行业健康发展五个方面制定了相关规则。

《指引》旨在配合近期监管机构强化金融消费者权益保护和个人信息保护相关要求，在行业自律方面对个人消费类贷款常见乱象进行规范，特别强化了催收行为以及外部催收机构管理，重点治理高频电话短信催收、深夜骚扰、爆通讯录、外包催收层层转包、债权层层转让至暴力催收机构等侵犯金融消费者合法权益的现象，为消费金融催收工作定立统一的合规标尺。

对商业银行影响较大的条款及审计关注建议

催收行为规范性

【严格催收时间】未经债务人同意，严禁在每日晚22:00至次日早8:00进行电话催收、外访催收及其他催收。

【合理频率】债务人电话未接通的，催收人员对债务人同一联系方式尝试拨打次数当天不宜超过6次；与债务人另有约定除外。

【规范联系第三人】严禁对无关第三人进行催收。催收人员在债务人本人失联的情形下可联系第三人：债务人本人手机号码无效（如空号、错号），可直接联系第三人；连续三次拨打债务人本人预留手机无法联系上本人的情形下，次日可联系第三人；连续三日拨打债务人本人预留手机无法联系上本人的，可直接联系第三人；如后续联系上债务人本人，时间重新开始计算。催收人员在联系无关第三人时不得透露债务人的金融信息，无关第三人未表达代偿意愿的，其只能作为获取债务人联系信息的渠道或请其代为转告，上述情况与债务人另有约定的除外。当无关第三人主动表示愿意为债务人偿还欠款时，可提供还款所需必要信息（如还款卡号、欠款金额等）。当无关第三人明确要求不得联系时，则催收人员应限制后续联系行为。

【规范催收记录】会员单位和外部催收机构应记录催收全过程，确保相关录音、录像及其他催收记录真实、客观、完整反映催收过程，录音录像资料保存年限应参照相关监管规定执行。会员单位采取司法催收的，在相关司法机关、仲裁机构、公证机构形成的录音、录像及其他催收记录按照其管理要求执行。

【电话催收规范】催收人员应核实接听人身份，当确认为债务人本人时可实施催收。催收过程应全程录音。会员单位应要求外部催收机构使用的设备符合与其签署的协议规范。

【信函催收规范】发函过程中应注意保护债务人的个人信息及私密信息，信函封面不应展示债务人欠款信息。设立固定化催收信函模板并留存备查，催收信函模板应由会员单位事先审定，未经会员单位审查同意，外部催收机构不可变更信函模板内容。纸质信函需严格密封、不得随意张贴，并应加盖相关印章（含电子印章）。



催收行为规范性（续）

【外访催收规范】外访催收应安排不少于两名催收人员。催收人员应出示工作证件或受托催收身份证明。催收人员应遵守基本礼仪。催收行为应全程录音（或录像）。外访催收人员应着装得体，不得穿着特殊服饰或有不当言行。

【催收人员告知规范】会员单位应要求外部催收机构明确告知其所代表的委托方（金融机构）或其负责催收的金融产品名称信息。催收人员联系债务人时应表明所代表的金融机构、催收机构（如有），向债务人如实告知催收事由、逾期欠款金额。催收人员应使用符合会员单位催收作业规范的话术，客观规范陈述事实。

【权属关系转移告知规范】对于不良贷款转让等情形，会员单位应当按照合同约定或法律规定允许的方式及时告知债务人债权关系转移情况。对于失联的债务人和担保人，可采取公告等方式履行告知义务。会员单位与相关合作方签订权属关系转移协议时，可要求其遵守本催收工作规范要求。

【禁止行为】催收人员在实施催收过程中严禁出现以下行为：（一）冒用行政机关、司法机关等名义追查债务人信息、寄送催收信函、开展催收行为。外部催收机构以会员单位身份开展催收。（二）通过散布他人隐私、非法获取个人信息，采用恐吓、辱骂、欺诈、威胁、暴力、涉黑等不当手段开展催收。（三）采取误导性表述虚构或夸大事实。以列入虚构的黑名单、虚构的不良信用数据库为由开展催收。以虚假承诺、夸大债务数额、性质、法律后果为由开展催收。（四）以催收名义收取额外费用，诱导或逼迫债务人通过新增借贷或非法渠道筹集资金偿还债务。（五）在公众场所张贴催收公告、律师函等文书。（六）外部催收机构在未经会员单位同意的情况下，使用私人手机电话联系债务人等，使用私人手机或社交软件发送催收语音、文字类信息等。（七）未经同意，进入住宅等私人场所或债务人所在的相关办公区域实施催收。（八）采取其他违法违规的手段实施催收。

内审关注建议：

- 对于催收时间及催收频次，是否在系统或操作流程中设立相关控制，对22:00—6:00期间，或每日6次的频次上限催收电话进行拦截。
- “联系第三人”为以往催收投诉重灾区，是否对照新规规范了联系第三人的情形、催收时点、催收话术等。例如联系第三人是否以债务人本人失联为前提；系统或操作流程中是否设置失联判断标准的确认节点；是否要求不得透露债务人金融信息；对于明确要求不得联系的第三人，是否进行标注等。
- 对于电话、信函、外访等催收方式，新规要求是否纳入操作规程；是否要求保留完整的录音、录像并保存相关年限。是否要求联系催收告知及权属关系转移告知。是否设立协会禁止行为。
- 以上要求是否纳入催收合作结构的合同条款中。是否要求催收机构在催收过程中明确告知其所代表的委托方（金融机构）或其负责催收的金融产品名称信息；是否不得以金融机构身份开展催收。



外部催收机构管理

【审慎管理】会员单位应当落实催收管理主体责任，审慎管理外部催收机构。与外部催收机构开展业务合作时，应当落实业务合规审查主体责任，加强与外部催收机构在从业人员合规和金融消费者权益保护培训等方面的协作。会员单位应实行名单制管理；建立并持续完善相应的业务管理制度，明确外部催收机构信息管理、业务培训、法律责任和经济责任等；对单笔债务在



外部催收机构管理（续）

同一时期内仅可委托一家催收机构实施催收；在本单位官方网站等官方渠道统一公开委托催收机构名称、联系方式等有关信息。

【外部催收机构准入】会员单位应制定外部催收机构的准入、退出标准和日常管理制度，合理评估业务集中度。会员单位应与选用的外部催收机构签订管理完善、职责清晰的委托协议，在双方委托协议中要明确双方权利义务、催收规范要求、个人信息保护、金融消费者权益保护、投诉处理、违约责任、就违规催收行为及涉及机构向银行业协会报送共享等内容，并在有效期内开展催收业务。

【人员管理】会员单位应要求外部催收机构组建专业的债务催收团队，对催收人员定期开展催收业务、金融消费者权益保护、信息安全、合规操作等方面的培训及考核。

【信息保密义务】会员单位应与外部催收机构以协议约定方式，明确外部催收机构对个人信息的保护义务和具体违约责任。会员单位应要求外部催收机构制定信息安全标准、政策和流程，包括但不限于出入管理、人员管理、业务操作管理、数据信息管理、权限管理、作业场地及机房安全管理等方面。委托协议终止时，外部催收机构应按协议约定销毁相关信息，并继续承担个人信息保密责任。

【合规管理】会员单位应切实履行外部催收机构催收行为管理主体责任，持续加强日常管理，通过现场检查、非现场检查、培训等方式，督促外部催收机构依法合规开展催收。会员单位每年对外部催收机构的现场或非现场检查频次不低于1次。

【投诉管理】会员单位应切实承担金融消费者权益保护主体责任，认真记录并处理债务人对外部催收机构的投诉意见，结合投诉意见持续推动优化外部催收机构债务催收的流程和行为。委托协议终止，会员单位应要求外部催收机构按协议约定继续配合处理受托期间催收行为产生的客户投诉。

【考核机制】会员单位应建立对外部催收机构的科学合理考核机制，制定合理的绩效考核与奖惩机制，优化考核方式，将催收效果、催收行为合规情况、催收记录完备情况、信息安全、投诉管理、违规处罚及整改情况、金融消费者权益保护等纳入综合考核范围，不得简单以债务回收率作为单一考核指标。

【禁止转包】会员单位应严禁外部催收机构将委托催收的业务转包或变相转包。

【互联网平台催收行为约束】会员单位应加强对互联网平台催收行为的约束，将互联网平台催收业务全面纳入管理，坚持统一的催收管理标准，严格执行本指引相关规定。互联网平台按约定从事催收业务的，会员单位应将其作为外部催收机构进行管理，传导并督促其按照监管要求规范开展催收，落实金融机构监督、检查、培训、追究违约责任等穿透管理要求。

内审关注建议：

- 外部催收机构是否纳入名单制管理，是否在本单位官方网站等官方渠道统一公示，是否落实业务合规审查。
- 外部催收机构准入审查是否涵盖机构资质、从业经验、合规记录、信息安全能力、从业人员管理、金融消费者权益保护培训等。外部催收机构考核机制是否将以上重点方面纳入考核范围。退出机制是否明确，触发条件是否清晰。
- 是否对存量合作机构每年开展不低于1次的现场或非现场检查。
- 是否将人员管理、信息保密义务、投诉、禁止外包等要求纳入外部催收机构合同条款中。

《保险产品适当性管理自律规范》

新规背景及影响

为落实国家金融监督管理总局《金融机构产品适当性管理办法》，中国保险行业协会于2026年3月27日发布《保险产品适当性管理自律规范》，《规范》将于2026年7月1日起实施。

《规范》是保险业首部聚焦产品适当性管理的自律性文件，旨在构建统一、科学、可操作的适当性管理标准，以“卖者尽责”为出发点，通过构建覆盖产品、人员、客户、销售、内控的全链条自律框架，致力于从源头上化解销售误导与产品错配风险，提升销售行为的专业性和规范性。《规范》全文共九章四十六条，配套《保险产品适当性评估问卷》《保险产品适当性评估结果反馈》等五个操作性附件，形成了涵盖产品分级、销售资质、客户评估、匹配销售、内控管理及自律监督的全流程管理体系，各核心环节均明确具体操作标准。

《规范》紧密围绕消费者实际需求和行业突出问题，注重可操作性，通过配套标准化工具为保险机构落实监管制度提供清晰指引，既是对监管要求的有效承接，也是对消费者知情权、选择权和公平交易权的切实保障。实务中，金融监管总局每年均会对商业银行开具大量涉及保险代理销售业务的罚单，内部审计需重点关注《规范》的外规内化有效性以及业务操作合规性。

对商业银行影响较大的条款及审计关注建议



产品分级、客户评估与匹配销售

【保险产品分类分级】《规范》明确，保险机构需综合考虑产品设计类型、保障责任、保险期间及保单利益是否确定等因素，对保险产品实施分类分级管理。人身保险产品划分为P1至P5五类，其中P1为低等复杂程度、保单利益确定的短期产品；P2为中等复杂程度、保单利益确定的普通型长期产品；P3为中等复杂程度、保单利益浮动有保证的分红、万能等产品；P4涵盖投资连结型、变额年金等利益浮动无保证或高等复杂程度产品；P5则为高等复杂程度且保单利益浮动无保证的产品。财产保险产品则根据复杂程度分为P1和P2两类。

针对P4、P5类利益浮动型产品，保险机构还需对产品或投资账户进一步划分风险等级，由低到高至少分为R1（低风险）至R5（高风险）五级。

【客户保障需求及财务支付水平评估】保险机构应当在了解投保人相关信息的基础上，根据投保人的保障目的、收益期望、保障期限、保费承担期限等方面的保险保障需求，结合投保人的收入、资产、财务预算等方面的财务支付水平，参考需求的优先重要性、已购买保障情况，对投保人进行保险需求及财务支付水平评估，向投保人提供适当的保险产品。

【客户风险承受能力分级评估】《自律规范》明确，保险机构需对客户进行评估。对于普通产品，重点评估保障目的与财务匹配度；对于P4、P5类可能导致本金损失的浮动利益产品，还需开展风险承受能力评估，将客户由低到高分C1（谨慎型）至C5（激进型）五级，并与产品风险等级建立明确的匹配规则。

投保人在同一保险机构自营平台单日评估次数不超过2次，十二个月内累计不超过8次。投保人风险承受能力评估等级与最近一次结果不一致的，保险机构应当对其进行提示，请投保人对变动情况再次确认。



产品分级、客户评估与匹配销售（续）

内审关注建议：

- 保险代销系统是否对接保险公司产品分级数据，是否保证信息的及时性、准确性。
- 网点及线上销售保险，是否在流程中嵌入《保险产品适当性评估问卷》，是否设置刚性控制未完成适当性评估，不得签署销售合同。银行是否复用银行自身客户风险评估体系，评估结果是否传送至保险公司。现有评估标准是否与保险风险等级相匹配，是否与保险公司达成一致。对于评估有效期12个月，是否设置临期重评提示。是否系统限制单日评估次数不超过2次，十二个月内累计不超过8次。
- 系统是否强制或在流程中人工校验客户等级与产品风险等级的匹配性。是否设置系统刚性控制，不允许突破评级匹配销售保险产品。



销售人员管理

《规范》要求保险机构建立保险销售人员资质分级管理体系，以销售人员的保险知识、诚信合规守法记录、销售履历等为主要标准进行分级，与保险产品分类分级管理制度相衔接，区分销售资质实行差别授权。

《规范》要求保险机构构建科学合理的销售人员激励约束机制，考核标准应当包括但不限于销售行为和程序的合规性、客户投诉情况等，不得以销售业绩作为唯一考核指标。

《规范》要求保险机构对销售人员持续开展产品适当性管理相关培训，销售新产品之前，保险机构需针对销售人员组织产品售前培训或学习，确保销售人员充分了解所销售产品的属性特征及风险水平。

内审关注建议：

- 银行代销保险人员是否已完成资质认证。保险代销系统是否设置了销售资质与产品等级的权限配置或关联校验。
- 代销保险人员的考核机制设计是否合理，是否包含合规性、客户投诉等要素，是否以销售业绩作为唯一考核指标。
- 销售人员是否定期参加产品适当性管理培训。销售新产品前是否参加对应培训。



销售过程中的适当性匹配要求

【P2至P5类人身保险】保险机构销售P2、P3、P4、P5类人身保险产品时，当保费交费金额与交费期限存在以下情况之一的，应当在取得投保人签名确认的投保声明后方可承保：（一）趸交保费超过投保人家庭年收入的4倍；（二）年期交保费超过投保人家庭年收入的20%；（三）保费交费年限与投保人年龄数字之和达到或超过75；（四）保费大于或者等于投保人保费预算的150%。

【人身保险疑似风险行为】（一）保单退保后重新投保：同一客户退保后的30天内（含），再次投保同一险种类型的新保一年期以上保单，且退保金额超过新保保费的50%；（二）保单贷款后新投保：同一客户保单贷款后的30天内（含），再次投保新保一年期以上保单，投保时客户



销售过程中的适当性匹配要求（续）

保单贷款未还清，且30天内保单贷款金额超过新保保费的50%；（三）保单效力中止后新投保：同一客户存在效力中止的保单，再次投保同一险种类型的新保一年期以上保单。

【告知义务】根据产品特征，使用便于接受和理解的方式向投保人告知以下信息：（一）产品的基本信息，包括产品名称、保障范围、保险期间、交费期限、等待期、赔偿限额、索赔程序、保单现金价值、续保条件、减轻或者免除保险人责任的条款等；（二）保险利益的不确定性、可能导致保费损失或者保单利益不及预期的事项；P4、P5类保险产品的投资风险，重点是已交保费亏损可能；P4、P5类保险产品投资账户的风险等级，存续期间风险等级可能会进行调整的情况；（三）P4、P5类的保险产品或保险产品的投资账户风险等级发生由低到高变动，且超过投保人风险承受能力等级的，保险机构应调整适当性匹配意见及时告知投保人，由投保人自主决定是否持有存量产品；（四）犹豫期及投保人在犹豫期内的权利；（五）退保可能遭受的损失；（六）需要投保人支付的保费总额、保单初始费用、保单管理费等各项费用或费率；（七）本规范规定的产品适当性匹配意见；（八）其他应当告知的信息。

【禁止行为】推介、销售过程中禁止下列行为：（一）代替投保人确认投保人适当性评估结果，进行不当提示，诱导投保人提供不实信息，先销售后评估，或者通过其他形式影响评估结果的真实性、有效性；（二）对投保人进行告知、风险提示时，内容存在虚假、误导或者重大遗漏，包括但不限于混淆存款、基金、理财、保险等产品，违规承诺保本保收益，夸大产品收益或者保障范围等；（三）在已进行保险投保人适当性评估后，主动推介风险等级高于投保人风险承受能力的产品，欺骗、误导投保人购买不具备适当性的产品；（四）通过操纵业绩或者不当展示等方式误导或者诱导投保人购买有关产品；（五）其他违反产品适当性要求，损害投保人合法权益的行为。

内审关注建议：

- 是否获取客户适当性评估的相关信息，是否设置系统校验规则，识别客户不具备适当性需要额外进行风险提示并签署投保声明的各类情形。
- 是否更新销售流程管理要求，嵌入信息告知义务并杜绝禁止行为。是否已做好必要的系统控制及人员培训。



特殊群体投保人的保护性规定

【65岁以上】《规范》要求向65周岁以上投保人销售P3至P5类保险产品时，应当履行特别的注意义务，可通过大字展示、语音提示、电话讲解、现场讲解、新契约回访等方式强化告知和风险提示，可以依据老年人具体情况给予投保延长阅读时长等更多的考虑时间，以保障老年投保人了解相关信息。

通过互联网等线上方式向65周岁以上投保人开展保险产品适当性评估或销售产品的，流程设计、界面展示应保障适老性、易用性、安全性。

【无民事行为能力】保险机构不得直接向无民事行为能力的投保人销售保险产品。

【限制民事行为能力】经法定代理人同意，保险机构方可向限制民事行为能力的投保人销售P1、P2类保险产品。



特殊群体投保人的保护性规定（续）

内审关注建议：

- 保险代销系统或销售流程是否支持识别65岁以上的投保人群体。销售流程中是否针对特别的注意义务设置风险提示、讲解、回访等环节，保险产品资料、销售合同、系统与APP界面等是否支持大字显示相关信息，是否给与必要的阅读时间与考虑时间。
- 保险代销系统或销售流程是否支持识别无民事行为能力人和限制民事行为能力人。系统是否锁定限制民事行为能力人仅可开放P1、P2类保险产品。流程是否设置环节，要求获取限制民事行为能力人法定代理人的书面同意。



客户回访

保险公司应对购买保险期间在一年期以上的个人人身保险产品的新单业务的投保人进行回访，回访应当在投保人签收保单后的合同约定的犹豫期内进行。保险公司可通过电话回访、电子化回访或监管部门认可的其他方式进行，应由从事销售推介以外的人员开展。

在回访中不得有误导、欺骗、隐瞒等行为，并如实记录回访过程。保险公司在回访中发现存在销售误导的，应当按照规定及时予以处理。

内审关注建议：

- 是否建立回访机制，在犹豫期内对客户进行回访。回访话术是否覆盖《规范》第三十条要求的内容。是否做好回访记录。
- 是否对回访过程进行定期检查，以防止回访中误导、欺骗、隐瞒等行为。
- 如实施简化回访或对特定产品类型实施简化回访，检查保险产品销售行为可回溯管理机制是否合理，运行是否有效。



内控管理

《规范》要求保险机构将产品适当性管理纳入公司内部控制体系，加强内部控制和自查，并纳入消费者权益保护内部审计范畴。并在消费者权益保护审查、互联网销售、信息系统及设施、适当性管理记录与资料保存、投诉处理等方面提出了具体要求。

内审关注建议：

- 银行是否已将适当性管理要求纳入内部控制体系，制定相关的制度要求。是否已配备必要的信息系统及设施，以及记录与资料保存机制、投诉处理机制等。

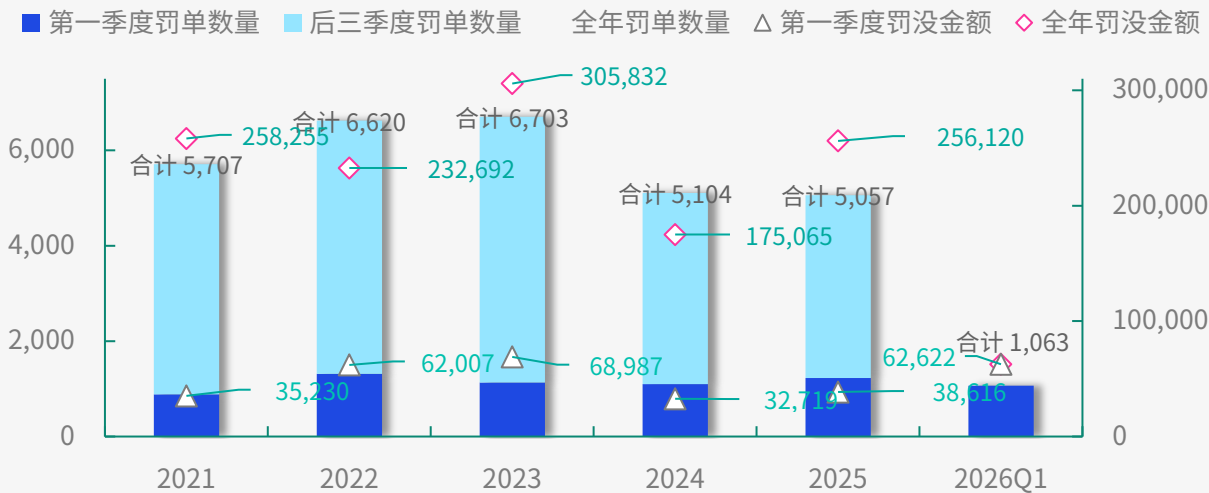
2. 监管处罚洞察



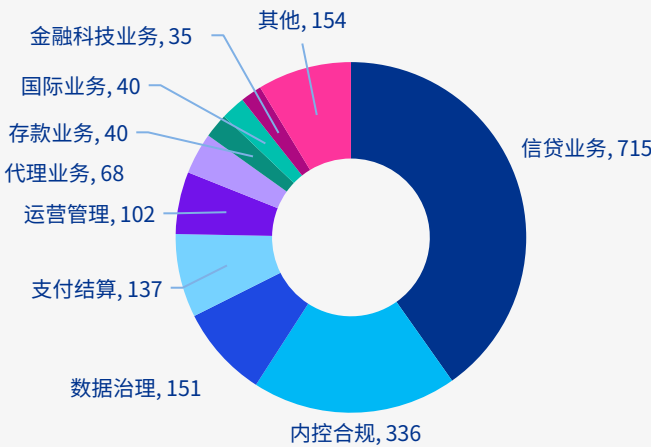
监管处罚整体观察

2026年一季度，银行业监管处罚整体呈现“数量回落、金额抬升”特征，中国人民银行、国家金融监督管理总局、国家外汇管理局等三大金融监管机构及其派出机构，针对银行机构及其从业人员共下发罚单1,063张，罚没金额共计人民币6.26亿元。从整体监管处罚趋势来看，较去年同期，虽然罚单数量下降约一成，但罚没金额上升超六成；单均罚没金额约59万元，上升超八成。罚单数量下降的同时，处罚金额与单笔处罚金额均大幅抬升，严监管、重处罚的威慑力持续加大。从受罚机构类型来看，国有大型商业银行罚没金额同比变动明显高于行业平均值。从大额罚单来看，前十大罚单合计处罚金额高达1.1亿元，监管机构对银行业金融机构重大违规行为的处罚力度持续加大，警示效应显著。从处罚最为集中的前三大业务及管理领域来看，分别为信贷业务、内控合规、数据治理。其中值得关注的是，监管统计数据错报、漏报、未报相关罚单同比增长255%，配合数字金融高速发展，穿透式、数智化监管不断完善的业务背景，需引起内部审计重视。

银行业监管处罚趋势（2021年—2026年Q1）



2026年Q1监管处罚分布（按罚单数量）



2026年Q1监管处罚十大案由

案由	罚单数量	罚没金额
报送监管统计数据错报、漏报、未报	156	1.69
未按规定履行客户身份识别义务	130	1.82
贷后管理不到位	112	0.67
消费者金融信息使用管理不到位	101	1.65
非法查询、泄露客户信息	100	1.65
账户管理不到位	94	1.70
贷款“三查”不尽职	92	0.49
违规发放贷款、办理信贷业务	80	0.36
假币鉴别、收缴和保管不当	70	1.59
信贷资金被挪用	61	0.37

备注：罚单数量，单位张；罚没金额，单位亿元。

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。



建议关注重点

综合分析2025年全年及2026年一季度的监管处罚特点、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：关注信用卡业务风险与全流程合规性

人民银行发布的《2025年支付体系运行总体情况》与已披露的2025年商业银行年报信息综合显示，信用卡业务整体呈现收缩趋势，业务发展正遭遇瓶颈。自2025年起，部分商业银行密集关停信用卡分中心，并停发部分信用卡产品。国有大型商业银行信用卡业务更是集体缩水，信用卡贷款余额与发卡量均呈现明显的收缩态势，资产质量亦出现明显下滑。除了业务发展承压外，信用卡业务的风险暴露亦不容忽视。2026年一季度，某国有大型商业银行信用卡中心受到金融监管总局处罚，罚没金额人民币575万余元，处罚事由覆盖整体管理、业务营销、发卡、合作机构管理、收单机构管理、资信调查、风险监测、资金用途管理等多个业务环节。建议内部审计关注信用卡业务风险，排查全流程环节的内控有效性与操作合规性。我们整理总结了近三年来信用卡业务的常见罚点，供内部审计部门参考。

涉及领域	主要违规形态
整体管理	信用卡业务管理严重不审慎
	信用卡业务管理不到位
合作机构管理	对合作机构管控缺失
	外包合作机构管理薄弱
	放宽合作机构准入条件
	对合作机构日常管理不到位
	信用卡催收外包管理严重违反审慎经营规则；信用卡中心外包催收机构管理不严
收单商户管理	收单商户准入管理不到位
新业务/产品管理	新增信用卡业务产品种类未按规定期限报告
	违规办理信用卡车位分期业务
业务营销	信用卡分期业务电话营销不规范
	未经资格认定从事信用卡发卡营销活动
授信管理与资信调查	信用卡授信管理不审慎
	信用卡授信额度管理严重违反审慎经营规则
	客户资信水平调查严重违反审慎经营规则
	信用卡申请人资信调查不充分
发卡	信用卡发放严重违反审慎经营规则
	发卡业务管理严重违反审慎经营规则
风险管理与交易监测	信用卡风险监测机制存在缺陷
	对信用卡业务可疑交易的监测和风险管理不到位

涉及领域	主要违规形态
风险管理与交易监测	可疑交易账户管理严重违反审慎经营规则 对高风险持卡人未采取审慎监管措施
资金用途	信用卡资金管控不到位；信用卡资金监测管控不到位 信用卡中心监测策略存在缺漏，刷卡资金流入非消费领域 信用卡套现 信用卡分期业务交易背景不真实 信用卡分期资金管理严重违反审慎经营规则 信用卡透支资金未按规定用途使用 信用卡透支资金被挪用；信用卡透支资金用途管控不力 信用卡资金流向限制性领域 员工信用卡预借现金被挪用于限控领域 信用卡资金被用于申购基金 信用卡资金被用于购买股票
分期业务	未按规定退还分期利息 信用卡现金分期业务不合规
汽车分期	信用卡汽车分期付款业务严重违反审慎经营规则；信用卡汽车分期业务管理不审慎 信用卡汽车分期业务贷前调查不审慎 信用卡汽车分期业务调查不尽职 信用卡汽车分期业务风控缺位 信用卡汽车专项分期贷后管理不到位
公务卡	信用卡（公务卡）业务管理不到位
预借现金	预借现金分期业务严重违反审慎经营规则 信用卡预借现金业务额度超过非预借现金业务额度
其他	信用卡中心员工行为管理不到位 信用卡中心隐瞒与保险合同有关的重要情况



观察二：人民银行在征信领域处罚集中，需引起高度重视

2026年一季度，人民银行累计下发涉及征信领域的罚单113张，罚没金额合计人民币1.65亿元，受罚机构广泛覆盖国有大型商业银行、股份制银行、城商行、农村金融机构、外资银行等，体现出行业在该领域管理工作中普遍存在薄弱环节。从处罚案由看，涵盖的环节及违规形态较为多元，主要涉及制度建设不完善，用户管理不到位，非法查询、泄露客户信息，征信异议处理不及时、不合规等。

近年来，人民银行的检查深度覆盖征信领域，相关罚单频出；征信领域的案由亦为处罚数量与金额快速增长的典型案由。随着国家大力推进建设社会信用体系与征信业务的快速发展，以及消费者权益保护与个人信息保护领域监管要求的持续强化，建议内部审计关注征信领域的问题暴露。我们整理总结了近三年来征信领域的常见罚点，供内部审计部门参考。

涉及领域与环节	主要违规形态
整体管理	违反征信管理规定；违反征信管理法律法规；违反征信管理业务方面管理规定
	违反信用信息采集、提供、查询及相关管理规定（金融机构及其他机构、个人）
	违反个人信息信息基础数据库管理规定
制度管理	征信内控制度有缺失
	未按规定对征信制度进行备案
用户管理	未按规定进行征信人员和用户管理
	征信用户超期备案和未备案
	未按规定对征信用户变更情况进行备案；未按规定向中国人民银行变更备案征信系统用户
	征信用户发生变更未按时报备；未在用户变更两个工作日内向人行备案
	创建查询用户未得到相关授权
	未根据操作规程创建（重启）征信查询用户
	违反安全管理要求，征信查询用户未按规定备案；征信查询用户变更未向当地人民银行备案
	征信查询前置系统个人查询用户新增和停用未备案；征信用户（前置系统用户）变更，未按规定进行用户报备
	二代征信系统管理员用户离岗未及时停用
	违反安全管理要求，征信查询用户调岗离岗未及时停用；征信查询用户调离未及时停用
	征信查询用户公用
信用信息采集、提供、查询	未准确、完整、及时报送个人信用信息
	提供个人不良信息，未事先告知信息主体本人；提供个人不良信息前未履行告知义务
	违反征信业务管理规定，未在查询信用报告前取得信息主体本人书面同意；未经同意查询个人信息

涉及领域与环节	主要违规形态
信用信息采集、提供、查询	违反征信业务管理规定：未经同意查询企业信贷信息
异议处理	未按照规定处理征信异议
	异议处理超期
	未按照规定对异议信息进行标注
	未按规定对异议信息进行核查和处理
	征信异议答复超期
数据安全与信息安全	未按规定对异议进行书面回复；未将异议处理结果书面答复信息主体
	未严格落实个人信用信息安全管理制度
	违反个人征信信息安全管理要求
	违反征信安全管理要求；未按规定执行征信安全管理要求
	违规保存征信数据，存在数据泄露风险

观察三：监管机构高度关注人员履职有效性

2026年一季度，人民银行、金融监管总局、外管局等三家监管机构发布涉及“人员不尽职”相关罚单157张，罚没金额达人民币7,439万元，受罚机构覆盖国有大型商业银行、股份制银行、城商行、农村金融机构等；涉及方面广泛涵盖各类业务与管理领域、产品品种和业务环节；受罚人员亦覆盖业务管理链条的各层级，如客户经理、审查人员、审批人员、管理人员以及董事长，对人员的处罚措施包括警告、罚款、禁止从业一定年限，乃至禁止进入相关行业。

此外，我们亦关注到，一季度信贷、存款、运营等领域存在大量基础违规问题；同时，“人员不尽职”等案由通常与违背业务管理规定、严重违反审慎经营原则等案由伴生。综合来看，伴随着长期低息差环境及商业银行迈入存量竞争阶段，机构及从业人员普遍面临营收考核压力，“不尽职”等问题仅为表象，实质反映了业务发展困境及业绩压力对风险合规文化的侵蚀，以及“降本增效”下人员超负荷运转对执行质量的放松，因此需引起内审人员的高度关注，综合从公司治理、发展战略、绩效考核、人员产能负荷等维度识别业务管理中的问题动因。

普遍性表现一：“不尽职”行为涉及业务全流程管理环节

涉及领域与环节	主要违规形态
整体管理	相关贷款业务严重失职；贷款管理失职
	贷款业务管理不尽职；贷款管理不尽职，严重违反审慎经营规则；贷款管理严重不尽职
授信管理	授信管理不尽职

涉及领域与环节	主要违规形态
贷前调查	贷前调查未尽职；贷款调查审查不尽职
	贷前调查不尽职，对资料审核不严
	贷前调查不尽职，贷款形成不良
贷中审查	贷款审查不尽职
	资本金审查未尽职
贷后检查	贷后管理不尽职
	贷款“三查”严重不尽职，导致贷款资金未按约定用途使用
支付管理	贷款资金支付管理不尽职

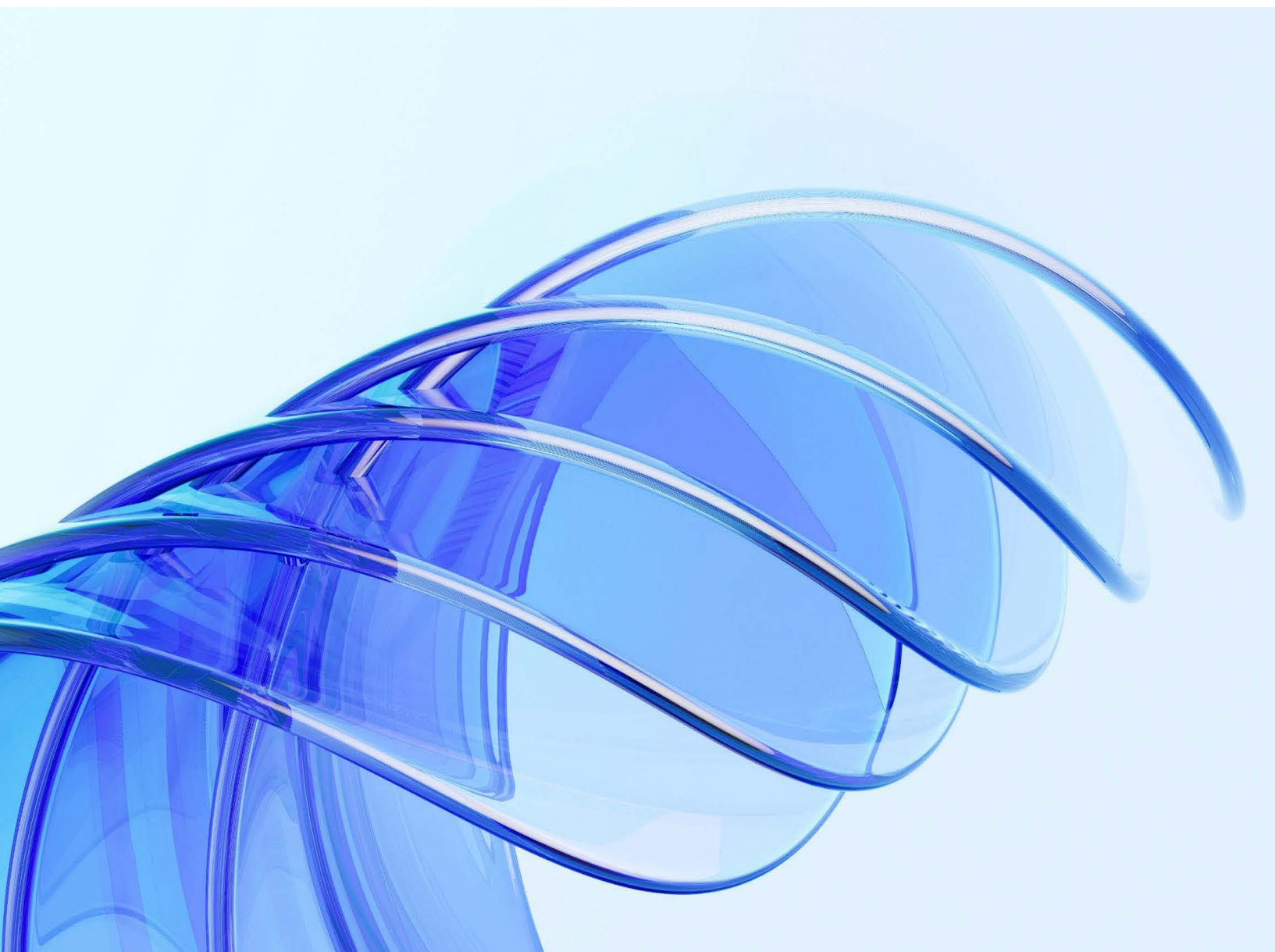
普遍性表现二：“不尽职”行为涉及多类业务、产品及管理领域

涉及领域与环节	细分领域	主要违规形态
贷款业务	对公贷款	对公贷款管理不尽职
		固定资产贷款管理不尽职
		流动资金贷款贷前调查不尽职
		项目贷款管理未尽职
	个人贷款	个人贷款“三查”不尽职
		个人经营性贷款贷前调查不尽职
票据业务	票据业务	个人消费性贷款贷前调查不尽职
		银票业务管理不尽职
		银行承兑汇票保证金管理不尽职；票据保证金审查不尽职
信用证业务	信用证业务	对票据承兑申请人资信调查不尽职
		信用证业务管理不尽职
外汇业务	外汇业务	国内信用证业务管理不尽职
		办理付汇业务未尽职审核
		未尽职审查办理货物贸易项下收汇
管理领域	公司治理	未尽职审查办理资本金结汇业务
	系统安全	董事长未勤勉履职
	员工行为管理	系统安全管控不尽职
		员工行为管理不尽职

观察四：其他新兴或苗头性问题需引起关注

2026年一季度的监管处罚中，人民银行与金融监管总局在运营管理领域发现了大量基础性问题，如“现金运营管理具有重大缺陷”“违反反假货币业务管理规定、违反人民币流通管理规定”“假币收缴流程不规范”“部分网点现金从业人员不具备判断和挑剔假币的专业能力”“未按规定上缴假币，超期解缴”等。当前随着数字经济的快步发展，现金业务正逐步萎缩，导致部分网点与业务人员对现金业务不重视不熟悉，商业银行仍需关注基础运营与网点人员能力。

此外，人民银行出具的罚单中，涉及金融科技的罚单共35笔，罚没金额人民币3,198万元。随着商业银行陆续实施人工智能战略，不断推进人工智能、自动化等在业务营销、风险管理、业务流程、管理场景的应用，内部审计需关注其蕴含的实质风险，并审计其合规性。



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。

1、“端到端”视角的信贷业务模型及系统功能审计

随着金融科技快速发展，特别是AI信贷模型的普及，许多互联网银行和金融科技公司依赖算法进行极速放贷，其资产规模的扩张速度往往与模型的激进度高度绑定。传统商业银行亦运用模型开展业务营销、客户信用评级、授信额度测算、业务决策、贷后风险监测、资产质量分类等活动，并不断推进数字化、智能化工具建设与流程自动化水平。

如今人机协作已成为主流工作模式，模型与系统的重要性日益凸显。未来随着人工智能特别是生成式人工智能的普及应用，更会由“人在环中（human in the loop）”迈向“人在环上（human on the loop）”，人机深度融合为“人工智能主导、专家监督调优”的工作模式，需在起步阶段高质量夯实作业基础。同时，模型与系统建设走过了信息化、数字化、智能化漫长的发展阶段，经历了局部功能建设、工作流程再造、专业系统整合、内外部其他系统对接融合等沿革历程，在沉淀知识资产与专家经验之外，亦积累了大量冗余、效率损失、不可解释性等问题。因此需要内部审计以独立视角综合审视，既关注模型的输入、输出、逻辑合理性，亦关注端到端流程中人机协作的设计有效性及运行效率。



快速诊断：您在信贷业务内部审计过程中是否关注到以下问题？

虽然已经访谈了业务人员、作业人员、系统开发人员、系统管理人员等众多角色，但仍无法了解模型、系统全貌以及特定功能变更原因。没有一个人能说得清整体设计思路与具体功能点，仅能通过碎片化信息反复核实、艰难拼图。

前台人员可以反复修改业务基础信息，测试模型评分及决策阈值。

不法中介利用线上产品进件渠道填写信息、准备支持性材料试探模型阈值与反欺诈能力，成功后仿照“成功案例”批量进件。



模型系统技术债

- 迭代过程缺乏充分的文档记录，无法追溯设计逻辑与决策逻辑。
- 会议纪要等只记录“共识”，但对于问题背景、讨论过程、决策中不同角色的考量缺乏充分记录。



行为信息与日志审计

- 信贷系统未要求记录关键字段修改的操作用户、时间及原因，难以追溯或实施监督。
- 未定期审计日志、文档相似性等，并对高频修改行为进行调查。

说明：根据监管处罚信息、银行业风险案例及研究报告等编制。

业务决策阶段，客户提供的过渡性/替代性信息与真实信息存在差异。但审批节点后，由于缺乏信息二次校验机制，利用时间差进行决策操纵。

- 客户在审批阶段提供未经审计的财务报表，获得高评额度，经审计财务报表信息差异巨大。贷后阶段虽要求客户经理采集更新信息，但不要求录入系统，或仅依赖客户经理判断手工填写指标或结论。
- 不填写不利信息，利用数据“空值”下的替代规则规避特定规则。
- 汽车消费贷款中，客户先提供购车发票，审批后进行发票红冲，后续未校验发票异常状态，亦无法识别合同金额、发票金额、实物不一致等异常。
- 客户踩着银行数据采集期间要求包装信息通过审批，如个人社保、企业资金流水、购销合同等，获得贷款后即“变脸”。
- 科技贷款企业名下专利在放款环节已失效，并被撤销“科技型中小企业”资质，仍进行了放款。
- 个人贷款贷前及审批阶段联系方式为客户本人，放款后即变更为“贷款中介”联系方式。



单一环节合规，端到端存在漏洞

- 从全流程视角来看，信贷业务流程设计普遍“头重脚轻”，业务决策“大考”后放松信息追溯与校验，难以震慑准入阶段不符合标准的业务进件，亦难及时识别风险与欺诈。
- 对于提供过渡性/替代性信息的情况，由于其个性化较强，未有效设定后续信息校验的控制，为数据舞弊和决策操纵提供了空间。关注“空值”原因，加强后续跟进及校验。
- 合理加强数据交叉校验与持续采集，识别数据疑点。
- 对于人员输入数据，加强支持性材料的数据自动化采集、计算与校验，提升作业效率并避免操作风险。

行内数据未有效采集与充分利用。随着业务发展，新产品、新渠道不断出现，系统监测范围与监测规则未同步变化。

- 系统未充分采集内外部信息，并对同质性字段进行校验。例如客户提供资料中，工作单位与征信报告信息不一致；工作单位已注销但仍获得授信；该工作单位有多人申请贷款且已出险。
- 对于第三方数据，由于系统功能不完善或节约成本考量，部分信息调用本地数据而非实时查询数据，数据时效性不佳。
- 资金流向监测规则遗漏新型支付渠道。
- 定期重检清单以上一期清单为准生成，上次未执行则一直被遗漏。额度即将到期前结清存量贷款再次支用，规避重检。
- 各系统间的管理框架、数据标准、接口规范等不一致，导致不同机构、业务条线信息无法交互或传递。
- 系统建设总体上与业务发展速度不匹配，功能更新不及时，无法有效支撑业务。



数据与系统功能

- 对于具有业务意义，可以进行交叉验证以提高风险识别效能的信息，充分复盘内外部信息来源及文件，将相关信息转化为结构化数据，并设置交叉校验规则。
- 关注第三方数据的接入、更新频率以及调用规则等，以实现有效的交叉校验。
- 对于新业务、新产品、新渠道，关注系统功能与业务规则是否充分覆盖，规则设计是否合理。
- 关注系统间的管理框架、数据标准、接口规范等，是否做到有效的信息交互。
- 关注系统、模型等建设是否与业务发展速度相匹配。

业务流程中的“人机协作”问题。

- 模型输出欺诈评分高风险推送预警，但未充分解释原因和预警逻辑（担心一线反推规则或系统功能不支持），人工难以充分了解需要核查的疑点。而且对于模型基于复杂特征作出判断，人工难以理解，亦无法转化为调查动作。
- 模型存在系统间的重复部署，重复推送至一线人员造成冗余工作量。
- 模型转人工量巨大，一线人工难以负担，且核查手段有限，未配备交叉验证的信息源及工具。
- 智能客服等模型难以处理复杂的业务投诉，与客户互动多轮无效后转入人工，人工面临的派单都是“愤怒的客户”。转入人工处理后，客户仍需将已向智能模型叙述的事件经过再次向人工客服复述，严重影响客户体验。
- 由于系统功能设计不合理或人员作业习惯未改变，仍是线下操作，线上录入，造成重复工作与人力浪费。
- 应当设置刚性控制的环节未严格落实刚性控制，或者刚性控制设置不合理，需要大量后台核实解锁或特殊审批。



人机协作深度融合

- 对于需核实的预警信息，模型是否提供预警方向、缘由，并提供“调查SOP”。
- 检查不同系统、不同功能模块之间规则部署是否存在重复。
- 模型有效性及模型产生的需人工核实的工作量是否合理，是否超出一线人员负担能力。
- 评估当前模型能力水平，业务流程“人机协作”设计是否匹配当前模型能力与人力配置。
- 是否对系统上线、功能变更提供必要的培训，促进人员工作习惯与行为的改变。
- 评估是否可以通过部署系统刚性控制减少人员基础操作、操作错误等问题（例如按照资料清单分类上传，自动校验完整性等）。对于经常需要突破的刚性控制，分析原因并迭代优化，或建立分支流程。



审计关注建议

从业务端到端视角，重新审视模型、系统的信息上下游、逻辑及在业务流程中的应用方式，特别是人机协同方面。

- 针对同一对象（例如客户）的多种材料相关字段、多种信息来源梳理，寻找可以交叉核验的信息，强化内部数据采集与外部数据的应用。
- 在风险高发领域，将业务准入或办理时的一次资料核验，变为批量定期核验。对于使用过渡性/替代性信息，或者“空值”的数据字段，提供合理逻辑，加强留痕与后续信息的追踪。
- 关注由于业务发展带来的问题：确认模型数据采集口径、覆盖渠道、业务品种等与实务中最新情况和管理要求一致。关注系统、模型等建设是否与业务发展速度相匹配。
- 关注人机协作的有效性：模型、系统实际应用情况及普及度，是否存在“两张皮”。模型成熟度是否与当前业务流程中承担的角色相适应，系统、模型功能的增强是否与一线人力资源配置与人员作业能力相匹配。

2、生成式人工智能模型审计

生成式人工智能（Gen AI）正被越来越广泛地应用于银行业，用于信息摘要生成、辅助专家决策及自动化处理等知识密集型任务。尽管这类技术有望显著提升生产力，它们也从根本上改变了模型风险的本质。与传统模型输出确定性的数值结果不同，生成式AI系统会产生概率性的叙述、建议和解释——这些内容即使存在信息缺失、偏见或事实错误，也可能显得合理可信。

生成式人工智能应用也带来了新的风险。首先，对于董事会和高管层而言，它带来了全新的责任挑战。生成式人工智能的结果会影响客户交互、业务决策与管理报告，而且它并不与当前的控制体系与概念完全相容。其次，生成式人工智能要求模型所有者和开发者重新思考系统设计、文档记录及测试流程——风险来源不仅包括数据和算法，更延伸至提示词、检索机制及运行环境。再次，在模型验证与风险管理领域，传统验证框架是为输出定义明确的透明模型设计的。而生成式AI系统具有动态性、不透明性，且往往依赖第三方供应商。因此验证工作的重心将从数理正确性核查，转向持续确认其长期运行方式是否符合银行的风险偏好。

基于毕马威国际报告《在模糊性中探索控制之道：生成式人工智能模型验证》，我们将与您分享开展生成式人工智能审计的方式方法。

验证相关的模型特征

虽然模型验证已有一套成熟的方法论，但考虑生成式人工智能模型的特性，针对它的审计方法必须根据具体的部署模式（云端API还是本地部署）、模型规模（大语言模型还是小语言模型），以及系统架构（对话式、RAG还是智能体）进行定制性调整。在开展审计前，需识别以下模型特征：

部署与模型控制：黑盒 vs. 玻璃盒

- 云端部署的大语言模型（API集成）
- 小型语言模型与本地部署

核心模型验证领域

- 功能正确性与推理
- 语境敏感性
- 信息检索限制

架构特定验证：检索增强生成与智能体

- 检索增强生成（RAG）
- 代理式AI与函数调用

安全、误用与鲁棒性

- 对抗性红队测试
- 数据泄露防护
- 沙盒技术

组织价值观、运营与文档

- 价值一致性与公平性
- 运行遥测
- 可追溯的证据

战略整合：监管要求与模型风险管理

- 优化现有模型验证流程
- 跨职能协作



说明：根据2026年毕马威国际报告 *Seeking Control in Opacity: Validation of Generative Artificial Intelligence Models in the Banking Sector* 编制。



验证方法及程序建议

基于已识别的生成式人工智能特有考量，建议内部审计应用结构化的验证框架开展模型审计工作，各项要求对应的具体验证活动如下：



步骤一：模型目标及应用分析

- 了解底层架构、模型输入数据的类型、模型输出的性质
- 详细审阅模型相关文档，访谈模型开发者并执行独立分析

步骤二：模型设计与输入质量

- **模型使用范围分析：**需超越算法本身，结合数据溯源及模型运行的具体场景，确立有效性边界
- **架构解构与系统设计：**解决方案的模块化拆解；考量组件交互效应与系统涌现行为；基础模型、检索层、提示词工程与系统指令
- **数据评估（预训练 vs 上下文）：**确定基础模型的知识截断点（训练数据截止日期）；评估上下文窗口利用效率
- **有效性边界定义：**明确能力边界、涵盖语言文化局限、区分确定性与创造性任务
- **风险分级与监管映射：**对标监管要求及银行内部风险分级框架，确定模型风险分级；评估模型重要性
- **模型与输入质量：**系统结构完整性（含数据与配置项）
- **模型假设与局限评估：**识别隐性假设、量化局限影响程度、界定可靠性边界
- **数据质量（训练/验证/检索）：**数据集代表性评估、数据污染流程审查、偏见与伦理风险分析、模型配置与超参数
- **生成式AI专项：**提示词工程；模型对齐，检查模型行为是否与目标、价值观保持一致

步骤三：模型实施与输出质量

- **验证技术实施与基础设施：**检查整个端到端的基础设施。对于使用RAG（检索增强生成）的架构，检查向量数据库或图数据库
- **独立测试与概率性复制：**独立测试依赖于“黄金数据集”。采用影子测试或“模型对模型”基准测试
- **解锁黑盒：**注意力分析与反事实测试。应用经过调整的可解释人工智能（XAI）技术。利用注意力权重分析。使用反事实测试来评估稳定性和公平性
- **评估输出性能与鲁棒性：**应用语义性能指标，使用基于嵌入的指标，例如BERTScore或“LLM即评审（LLM-as-a-Judge）”框架。关注模型的鲁棒性，压力测试的表现

步骤四：模型弱点与局限性

- **整合与问题严重性评估：**整合所有问题与观察。根据问题的严重性和重要性对其进行评级
- **评估补偿性控制：**评估补偿性控制措施；评价剩余风险
- **治理、沟通与应对措施：**问题沟通与对话、确定整改措施、撰写报告等

4. 内审理论动态



报告一：《协同而不妥协》

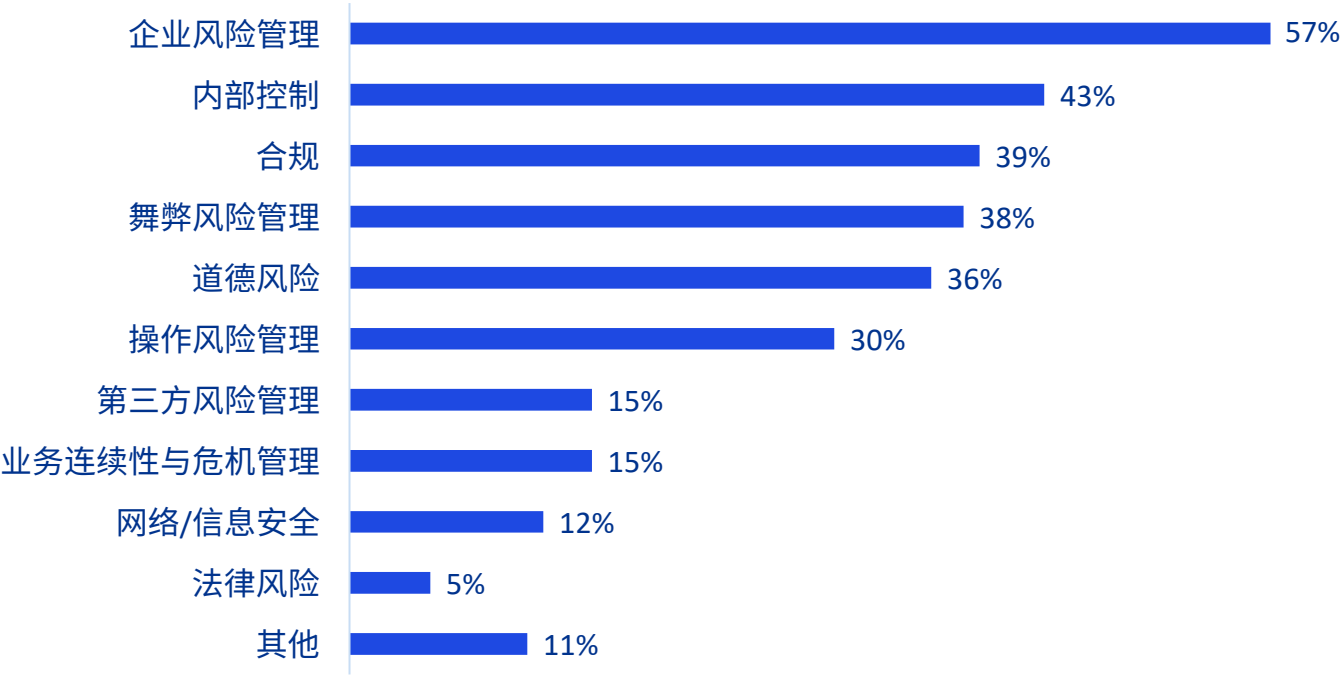
国际内部审计师协会于2026年发布了《协同而不妥协》报告。报告基于全球3,000多位内部审计与风控专业人士调研编制，重点讨论了内部审计如何与风险管理、合规等职能协同。目前第三道防线与第二道防线协同已成主流趋势，32%的内审负责人兼任二道防线职责，90%的组织从协同中获得风险覆盖提升、重复工作减少等收益，但报告提示仍需在协同效率与内审独立性之间做好平衡；20%的组织认为职责重叠存在独立性风险，需通过清晰角色边界、制度保障等防护措施实现有效协同。

内部审计师：在职责拓展与独立性之间取得平衡

三道防线模型不仅敦促组织为管理层、第二道防线和内部审计设定清晰的职责并理解履职要求，也鼓励它们之间相互协调。该模型亦明确指出，尽管内部审计在职能设计上独立于管理层，以确保其在工作规划与执行中不受阻碍和偏见，但这种独立并不意味着完全孤立。

- 调查中，32%的首席审计执行官（CAE）至少承担部分第二道防线职责。最常见的领域是企业风险管理（ERM），占57%；其次是内部控制，占43%；再次为合规，占39%。调查列示的第二道防线职能均有受访者选择，这表明内审负责人在实践中可能被期望参与的职责范围非常广泛。
- 71%的CAE及其他高级内部审计人员表示，其职责范围涵盖内部审计以外的一个或多个领域。

? 内部审计负责人监督与管理的职能领域

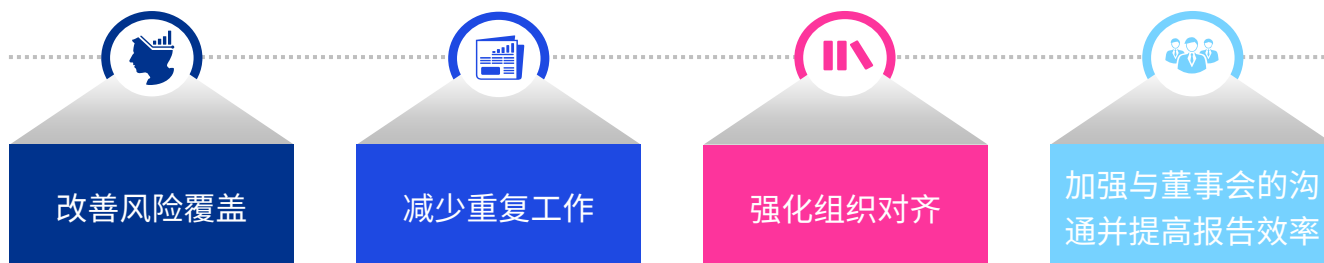


说明：根据国际内部审计师协会《协同而不妥协》编制。

内部审计实践中的协同效应

? 内部审计职责拓展的积极成果

内部审计职责的扩展为提升其作为治理与风险管理有效性和效率的独立评估者角色带来了机遇。在实践中，组织发现跨职能协调风险评估与风险管理具有价值。90%的受访者表示，第二道防线与第三道防线之间的协调带来了积极成果。



? 内部审计职责拓展的关键挑战

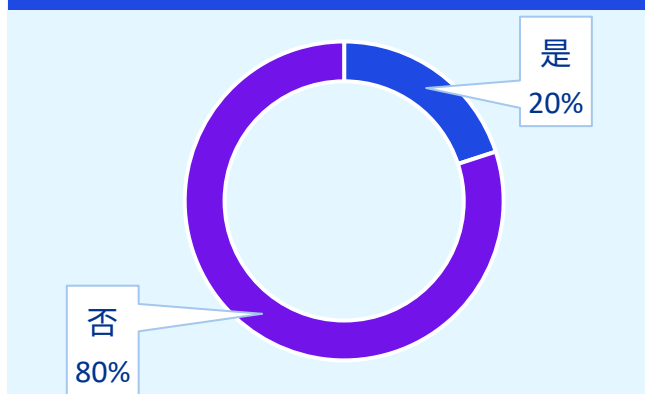
随着组织日益成熟，整合式风险管理与控制流程的价值也愈发凸显。内部审计领导者通常具备足够的能力，可以在ERM及其他第二道防线职能（包括合规、舞弊风险管理以及道德风险）中发挥作用。对于CAE而言，这种变动带来了三大关键挑战：

1. 利用职责重叠与共享责任，提供更优的风险管理和战略洞察
2. 对其管辖范围内的第二道防线职能提供客观无偏的鉴证
3. 维护其内部审计职能的独立性

? 内部审计职责拓展的独立性风险



共享职责及其对独立性的影响是否构成风险



调查结果表明，内部审计独立性的风险在理论上值得关注，但在实践中较为有限。八成受访者表示，第二道防线与第三道防线之间不存在对内部审计独立性构成风险的职责共享。然而，对部分组织（20%）而言，共享职责及其对独立性的影响确实构成风险。

调查数据显示，风险职能与内部审计职能之间呈现协同增强态势。39%的受访者表示，过去五年间，其所在组织的内部审计与风险职能之间的关系趋向更加整合。展望未来，这一比例将在五年内升至60%。通过信息共享、活动协调及优先级对齐等精心设计的工作方式，此类实践有助于确保董事会获取可靠信息，从而做出明智的决策。



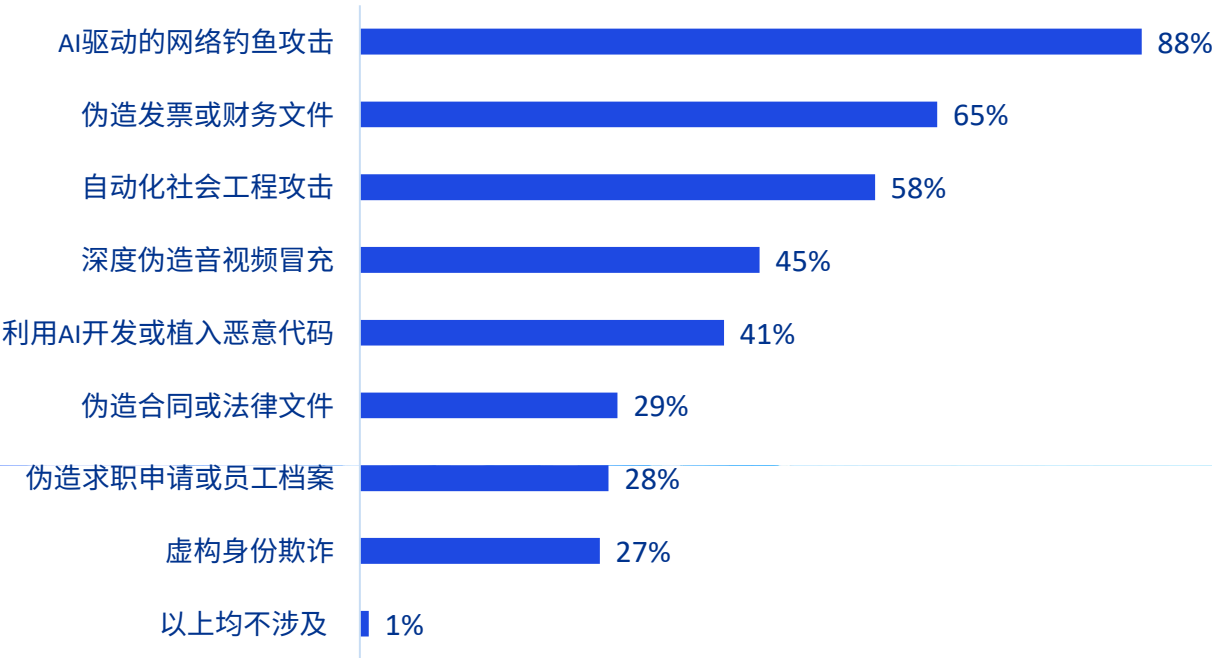
报告二：《内部审计与人工智能驱动的欺诈》

国际内部审计师协会于2026年发布了《内部审计与人工智能驱动的欺诈》。报告基于373位高级内部审计人员的调研反馈编制而成。人们对人工智能驱动的欺诈风险关注度不断提高，但熟悉程度参差不齐且应对信心有限。尽管85%的受访者认为人工智能驱动的欺诈风险为中高风险，但只有不到四成的受访者认为内部审计职能能够充分准备监测此类欺诈行为。内部审计部门对人工智能的使用不断增加，大多数受访者预计在短期内将继续延续这一趋势。对人工智能驱动的欺诈行为的熟悉程度日益增长，这为内部审计团队提供了机会，以加强识别滥用行为、评估控制措施并更有效地向管理层提供建议。

组织对AI驱动的欺诈的关注

人工智能具备高度灵活性，威胁者可以利用它来实施各种欺诈活动。人工智能驱动的网络钓鱼攻击是最常被提及的关注点（88%），其次是伪造发票或财务文件（65%），以及自动化社会工程攻击（58%）。

人工智能驱动的欺诈的主要关注点

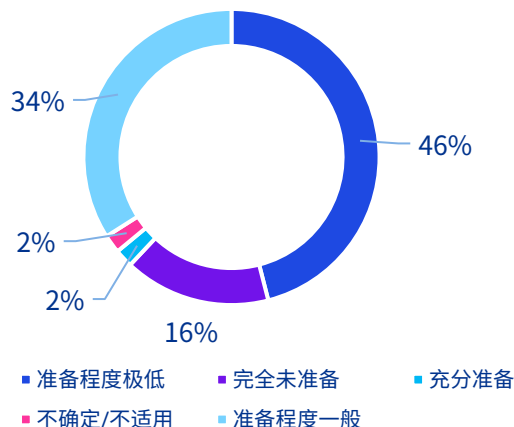


说明：根据国际内部审计师协会《内部审计与人工智能驱动的欺诈》编制。

内部审计应对AI驱动的风险的准备

评估内部审计团队是否准备好应对人工智能驱动的欺诈风险至关重要。研究结果反映超过六成的受访者（62%）认为他们的内部审计职能要么完全没有准备，要么仅有一些基本准备来监测人工智能驱动的欺诈，只有36%的受访者认为自身准备程度达到中等或以上水平。

内部审计团队对监测AI驱动的欺诈的准备程度



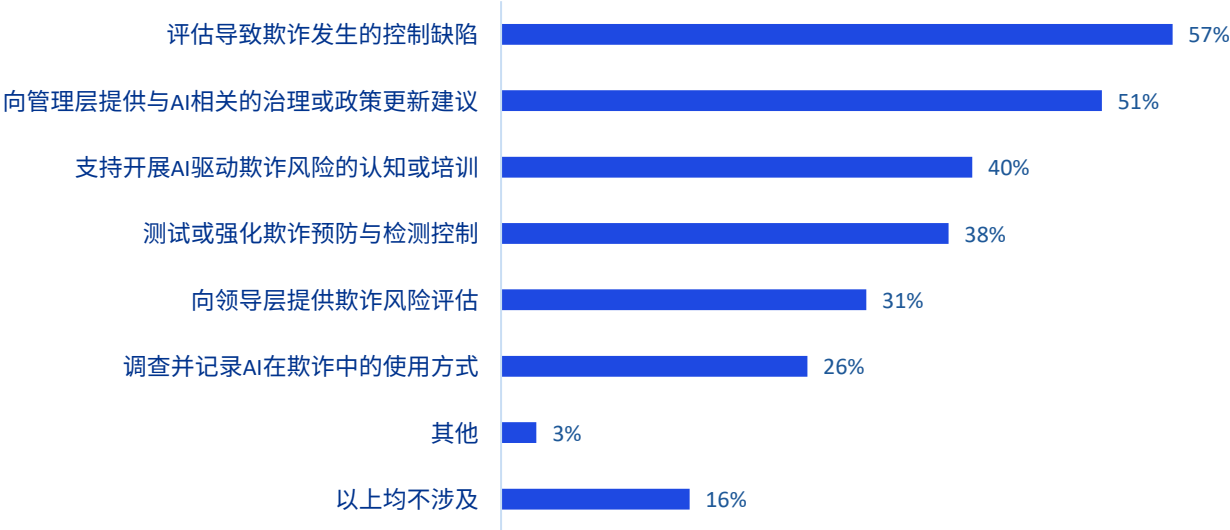
这些数据表明，内部审计团队在应对人工智能驱动的欺诈方面存在显著的准备不足和资源限制。以下是一些关键的障碍和挑战：



内部审计对于AI驱动的风险的应对

内部审计主要通过提供鉴证与洞察，促进威慑与响应，并协同其他承担运营责任的管理及职能条线开展工作。内部审计在组织中的独特定位，使其能够在评估组织准备情况与抵御新兴风险方面获得显著优势。随着人工智能日益广泛地嵌入组织流程，内部审计面临进一步拓展自身角色的契机。这包括更积极地参与管理层主导的欺诈风险评估，确保决策层了解人工智能可能被滥用的风险，并通过更深入地参与调查与记录涉及人工智能的欺诈事件，以强化鉴证职能。

内部审计对AI驱动的欺诈的应对措施



防范AI驱动的欺诈采取的关键行动

技能建设

培训必须具备适应性，要与AI快速迭代的能力及相关欺诈风险同步演进。技能培养是一项持续性工作，旨在让内部审计人员及整个组织，掌握识别、评估和防范AI赋能欺诈所需的知识与实操能力。

- 内部组织技能建设项目，在可控环境中开展实操演练，让审计人员测试相关技能
- 引入具备专业特长的外部机构或顾问，对内部培训进行补充
- 技能建设的规模可根据组织成熟度与风险敞口灵活调整
- 面向全员开展基础认知培训
- 针对核心人员提供进阶技能提升与专项培训
- 为承担AI赋能欺诈检测与防控深层职责的审计人员，提供正式资质认证

AI使用的协同对齐

大量受访者强调，组织范围内就AI使用达成组织层面的协同对齐至关重要。受访者指出，需要更清晰地掌握AI在业务流程中的部署位置与应用方式，他们频繁提及AI资产清单（AI inventories）以及跨业务单元开展结构化调研的价值。这种更全面的认知，能让内部审计在审计规划、风险评估和审计程序中，纳入全组织层面的AI相关考量。

内部审计负责人也明确表示，防范和应对AI驱动欺诈的工作绝不能各自为战、形成信息孤岛。相反，这类工作需要建立能够跟上风险快速演变节奏的治理与协调机制。组织内部的协同对齐，有助于确保AI相关风险（包括欺诈风险）得到持续识别、评估和管理，而非以碎片化、被动应对的方式处理。

跨部门协作

受访者一致认为，有效的AI欺诈防范准备是一项共同责任，需要与技术、网络安全和风险管理团队进行密切协调。同时，受访者也强调了联动业务部门的价值——这些部门往往已具备更丰富的AI及相关技术使用经验，这一点在AI应用与认知仍处于起步阶段的组织中尤为重要。

管理层进一步指出，协作的意义不仅在于知识共享，更是提升欺诈检测与缓释工作效率的核心手段。通过跨职能协同，内部审计能够：

- 更清晰地掌握AI在企业内的部署情况
- 充分利用现有技术专长
- 确保建立起适配的安全防护机制

协作与充足的资源投入至关重要，其价值远超单纯的培训与组织对齐。



报告三：《赋能下一代内部审计人才》

国际内部审计师协会于2026年发布了《赋能下一代内部审计人才》。随着职业不断适应新需求，内部审计领域的人才格局正在发生变化。新一代员工怀揣着不断演变的期望进入职场，而技术也在重新定义组织中各个岗位的角色。内部审计职业及其领导者亟需从战略层面重新评估如何识别、吸引和培养未来所需的人才。

随着人工智能的持续发展和普及，许多传统入门级、重复性职责——如数据收集、文档整理、抽样和核对等，这些曾构成该职业早期经验基础的任务，如今均可由机器完成。因此，许多新专业人士的职业生涯可能将从审查、分析和评估AI生成的输出开始，从而打破传统培训中“高数量、低复杂性”的工作模式。技术不应成为发展的障碍，而应被用于加速成长进程，赋能下一代人才不仅能在当前岗位上取得成功，更能推动岗位本身的演进与拓展。

这一转变需要从两方面予以回应：

内部审计部门应为新员工配备必要的技能和信心，使其能够更早地承担更具战略性的职责。

1

2

雇主应提供结构性的支持，帮助他们在这些更高层次的岗位上取得成功。

未来内部审计师职责

内部审计师需要超越纯粹的技术合规角色，转而将自己定位为战略顾问，提供实时洞察、创造价值，并助力企业应对不确定性。为成功实现这一转变，审计人员需在以下六个核心领域建立优势：



技术敏捷性

快速学习、适应并应用新兴技术，以提升绩效并在不断变化的环境中保持有效性。



适应力与学习敏捷性

迅速调整以应对变化，并在不断发展的环境中持续获取新技能或知识以保持有效性。



战略思维

预见未来趋势，跨复杂系统连接洞察，并做出决策以使短期行动与长期目标保持一致。



商业敏锐度

理解和应用组织的运营和战略知识，以做出明智决策。



创新思维

挑战现有假设，拥抱新理念，并尝试创意解决方案。



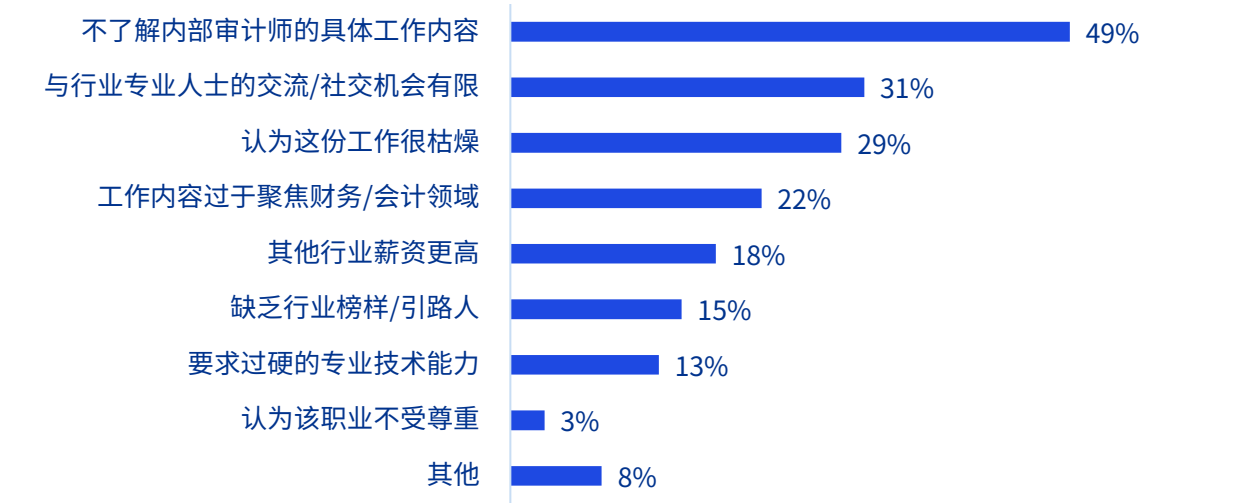
跨学科专业知识

整合来自不同领域的知识和视角，以解决复杂问题。

六大能力体现了从纯粹的技术熟练度，向更广泛、更具前瞻性的综合能力体系的转变，融合了内部审计专业知识与强大的分析思维、沟通能力及领导素养。审计人员愈发需要提升数字素养，尤其是在理解新兴技术与评估相关风险方面。同时，鉴于变革步伐持续加快，终身学习已从可选变为必要。为在未来数年内保持公信力、有效性及影响力，内部审计师必须依据不断演变的风险与技术环境，持续更新自身能力。

说明：根据国际内部审计师协会《赋能下一代内部审计人才》编制。

阻碍从事内部审计工作的因素



调研结果反映，未考虑从事内部审计职业的学生表示，他们对内部审计师的工作内容缺乏了解。这突出了显著的认知差距。若未能清晰传达该角色的职责、目标及影响，多数学生将难以将内部审计视为可行或有吸引力的职业方向。排名第二的常见回答中，学生指出与领域内专业人士接触的机会有限。这表明许多学生缺乏通过导师计划、实习、客座讲座或校园活动等途径与内部审计师建立实质性联系的机会。此外，29%的学生认为该工作看似乏味。尽管这一看法可能源于过时的刻板印象，但对于追求动态且有意义的职业发展的年轻一代仍是显著障碍。

为未来做好准备的内部审计

随着宏观趋势重塑未来工作方式，学生与年轻专业人士的期望也在迅速演变。下一代人才，特别是Z世代和Alpha世代，拥有一套新的价值观、优先事项和职业抱负，这些正在挑战传统的职业模式和雇主实践。2025年学生职业调查的数据显示，学生在做出职业与教育决策时，会基于实际因素，如就业机会、薪资潜力和晋升机会考虑，同时也非常重视工作与生活的平衡及灵活性。未来的内部审计师需要具备技术熟练度、商业敏锐力和适应性思维方能胜任。内部审计的未来将由那些能从变革中识别机遇、在洞察与预见中找到价值的人才所塑造。吸引下一代人才不仅需要适应，更需要重新构想该职业的未来可能性，并致力于以具有前瞻性的方式培养人才。

吸引并留住下一代人才的核心措施：

1

为初级专业人士提供结构化、技能提升的体验

2

内部审计团队及整个行业应专注于通过早期接触和教育来弥合认知差距

3

优化职业路径的设计、结构和保障

5. 内审国际动态

2026年一季度，国际银行内部审计在人工智能与数智化审计、技术能力布局、人才技能升级等方面呈现出主要变化。



高盛集团



亮点观察

- 部署AI“数字员工”执行审计任务：2026年初，高盛与AI公司Anthropic深度合作，部署其Claude模型作为“数字员工”，专门处理交易会计、客户尽职调查等核心内审工作。
- 谨慎的人才策略：高盛在英国的内部审计职位招聘量微降了5.9%，反映了顺应智能化趋势，以AI提升效率而非单纯扩充人力。



摩根大通



亮点观察

- 将AI列为“核心基础设施”进行战略投资：摩根大通已将AI投资提升至战略高度，视其为与电力、网络同等重要的核心基础设施。该行已明确要求员工放弃使用公共AI工具，转向使用其自主开发的内部AI套件，以保障数据安全与合规。
- 软件开发审计：内部编码助手已使数万名软件工程师的效率提升10%至20%。
- AI工具推广：摩根大通银行要求其约6.5万名工程师和技术人员在日常工作流程中使用AI工具。管理层正在追踪员工使用这些工具的频率，这种情况还可能影响绩效评估。



汇丰集团



亮点观察

- 设立首席AI官：2026年汇丰任命了首位首席AI官，将AI提升为集团层面的核心战略。
- 战略性投资Elliptic，用于区块链与加密货币审计：为应对日益增长的加密货币合规风险，战略性入股了区块链分析公司Elliptic，并将集团金融犯罪负责人派驻其董事会。此举旨在利用AI技术和链上监控工具，优化内部审计，加强对数字货币洗钱风险的管控。

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。Goldman Sachs teams with Anthropic as AI agents go beyond coding to automate accounting, compliance, and onboarding, UK Internal Audit Jobs Surge 18% Due to New Banking Demands, 《摩根大通把6.5万员工塞进AI监控》《摩根大通开始追踪员工AI工具使用情况》《银行业的AI时刻：国际案例与启示》《汇丰银行押注Elliptic：利用AI震撼区块链监管》《首位首席AI官上任！汇丰银行“大象转身”，开启金融全自动化元年》。

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

特别鸣谢侯亚男、赖恺靖、刘雨航、区颖蓉、范嘉怡、孙旭晖等对本报告作出的贡献。

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。

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://kpmg.com/cn/zh/about/office-locations.html>

所载资料仅供一般参考用，并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的资料，但本所不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

© 2026 毕马威华振会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所，毕马威企业咨询(中国)有限公司 — 中国有限责任公司，毕马威会计师事务所 — 澳门特别行政区合伙制事务所，及毕马威会计师事务所 — 香港特别行政区合伙制事务所，均是与毕马威国际有限公司(英国私营担保有限公司)相关联的独立成员所全球组织中的成员。版权所有，不得转载。在中国印刷。

毕马威的名称和标识均为毕马威全球组织中的独立成员所经许可后使用的商标。

刊物编号：1777538018168

更多免费行业报告

并购家

www.ipoiipo.cn