KPMG

2022年
十大监管挑战

防范多米诺骨牌效应

kpmg.com

目录

引言

我非常高兴代表毕马威监管洞察中心发布《2022 年十大监管挑战》。我们预计监管“边界”将不断扩大，监管期望亦将迅速上升（无论是否推出新规）。以下十大方面将构成监管挑战，监管和执法活动将显著增加，金融服务公司应为此做好准备：

快速变革

- 公平与共融
- 气候与可持续发展
- 加密与数字资产
- 平台与操守

保持专注

- 网络与数据
- 欺诈与金融犯罪
- 估值风险

缓释风险

- 第三方与云技术
- 科技与韧性
- 风险“自满”

如果您希望更详细地了解本报告聚焦的问题和行动，或讨论贵公司面临的独特挑战，欢迎随时与我们联系。

谨致问候！

Amy Matsuo
主管
ESG与监管洞察

公平与共融

鉴于投资者需求、公众意识、社会动荡以及政府当局的首要任务和指令等因素，监管机构重点关注与消费者和投资者保护有关的监督和执法议题，并将公平条款的适用范围扩大到所有消费者触点。

将公平考虑因素嵌入整个客户旅程，涵盖产品/服务设计、营销/广告、信息披露、服务和客户互动（包括投诉管理），并将公平列为优先事项。
公平概念不再局限于贷款条件和产品的公平，而是涵盖所有渠道和触点。

实施集中化流程，并简化所有面向客户的沟通。
无论以何种形式或渠道，沟通应该清晰、准确、完整，披露充分信息，确保消费者了解相关信息、备选方案和/或利益冲突。

加强投诉管理流程、技术和数据分析；汇总问题，发现根源，并部署简单有效的响应措施。
在监管机构评估企业合规管理体系时，投诉管理是必不可少的方面，因为它可能预示着潜在新风险、管理或结构缺陷、第三方供应商问题，或说明企业存在反复出现的问题或需要对产品或服务进行改进。

设定清晰且可衡量的多元化、公平和共融目标；制定指标用于衡量和监测进度，并将其纳入管理层工作目标。
公众要求金融服务机构促进种族平等和共融的呼声越来越大，这与投资者需求、公众意识、社会动荡以及政府当局的优先事项和指令相一致。金融机构面临的压力势必将会越来越大。

气候与可持续发展

在投资者的巨大需求以及各种自愿披露框架推动下，金融服务公司正在采取行动，计量、监测和缓释气候相关金融风险。监管机构在这方面的期望发生了翻天覆地的变化。这种趋势将持续至2022年，监管机构的管辖权限亦将扩大。联邦金融机构必须制定并执行相关战略，以量化、披露和缓释气候变化对公共和私人资产造成的财务风险。政府政策目标是推动金融机构以“清晰、一致、准确、易于理解且可比较的方式披露气候相关金融风险”，并“采取行动减轻风险及其驱动因素，同时考虑如何解决气候相关金融风险对弱势群体和有色人种社区的不同影响。”

妥善管理所有气候和可持续发展报告（财务和非财务）的编制和发布以及已披露的指标和衡量标准，确保一致性。

如果没有建立有效的气候治理结构，企业可能难以在气候风险的基础上做出战略决策，管理气候相关风险，制定和跟踪气候相关指标和目标。气候风险问题同时带来财务风险和机遇；良好的企业治理应该包括有效的气候治理。然而，对许多企业而言，气候相关金融风险是一个错综复杂的问题，需要应对科学、宏观经济和政策方面的不确定性，时间跨度大，而且可能超出董事会的职权范围。

制定定性和定量指标和目标；确保业务部门、风险职能和管理层对报告整合和ESG绩效负责。

在投资者等利益相关者呼吁企业提升报告可比性和标准化的背景下，随着企业纷纷承诺实现气候相关目标，并积极行动提供指标和信息披露的基础数据，气候相关财务报告正在迅速演变。在短期内，虽然美国监管机构正在制定更详细的规定，但目前已有多个（自愿）报告框架可以为企业制定指标和目标提供指引。

气候与可持续发展

制定初步气候和可持续发展假设和模型，包括气候情景和/或压力测试（与辖区以及全球范围内的义务保持一致）。
尽管美国监管机构尚未就气候相关情景分析或压力测试提出正式要求，但毫无疑问的是，它们希望金融机构建立适当的制度来识别、衡量、控制和监测重大风险（包括气候风险）。在全球范围内，气候情景分析正在成为评估气候相关风险对金融机构和金融稳定影响的重要工具。

探讨气候风险导致严重影响的可能性，覆盖不同客户/社区和/或地域和行业；将结果纳入战略、运营和风险管理。
气候风险相关影响以及各方为遏制此类影响所做的努力（例如推进净零排放目标和气候韧性投资）可能导致目前的弱势群体/地区面临的处境恶化。实体风险事件（例如，洪水、火灾、风暴或海平面上升）在地理上较为集中，可能产生溢出效应，导致弱势群体、企业和市政当局的负担增加（例如保费飙升）；房地产和基础设施的价值和使用价值下降；以及投资者离场。转型风险（例如政策变化、消费者行为偏好）可能会引发突然的重新定价，并导致资产搁浅和价值受损。

政策制定者、监管机构、金融机构和行业团体正在探索各种选项，例如：

— 将“气候公平”和“气候公正”纳入关于气候风险（物理风险和转型风险）影响的讨论之中。企业应开发模型和指标来计量此类举措的影响（积极和消极），并制定应对策略。

— 在满足 LMI 社区的信贷和发展需求的同时，调整 CRA 以纳入和鼓励支持气候韧性的活动（纽约金融服务局针对国有机构采用这一规则）。

— 将气候相关金融风险纳入承保标准、贷款条款和条件以及联邦贷款政策和计划的资产管理和服务程序。

— 与州级保险监管机构合作，研究在特别容易受气候事件影响的地区私人保险承保范围发生“重大中断”的可能性。

加密与数字资产

随着投资者、企业以及部分央行使用加密和数字资产，表明零售和机构层面对数字资产的兴趣日益浓厚，围绕加密和数字资产的监管活动正在加强。在市场扩张的同时，美国的监管格局正在发生变化。为了明确监管法规，州和联邦监管机构和立法者正在审议不同的方案。重要问题包括特许、许可、欺诈和金融犯罪风险，以及消费者和投资者保护。

制定企业/产品能力评估以及风险合规策略，以适当方式许可、发行和/或使用数字资产。

当前，加密和数字资产监管格局高度碎片化，且正在快速演变。视资产结构以及相关事实和情况的不同，联邦和/或州级层面可能有多个监管机构对交易拥有管辖权。随着市场的发展，监管空白和重叠亦随之产生；加密科技公司正在接入传统金融体系，而受监管的银行正在构建加密基础设施（例如托管服务）。确立适当的监管制度（包括发放牌照和特许证的政府机构），可能需要法律变更，而这又可能改变相关市场。

建立/加强与数字资产和支付相关的内部风险政策、程序和控制。

监管机构聚焦消费者和投资者保护，审视广泛的风险领域，包括欺诈、网络安全、数据隐私、不当行为、结算、流动性、市场诚信、市场波动、透明度和洗钱/恐怖主义融资。执法环境同样复杂，部分原因是政府当局高度重视应对网络安全风险。值得注意的是，美国司法部成立了全国加密货币执法小组，对滥用加密货币的犯罪行为进行调查和执法；SEC 和 CFTC 继续在各自的管辖范围内积极开展执法行动。

编制实操性和相关性高的数字资产信息，并向董事会汇报。

监管机构希望董事会在充分的信息（范围、细节和分析均应充分）基础上，为企业战略和风险偏好设定一致、清晰的方向，以实现稳健决策并考虑潜在风险。

平台与操守

科技的迅猛发展、数字银行活动的增加、数据收集的日趋复杂以及社交媒体影响力的不断上升，正在以空前的方式重塑金融服务行业格局。我们正处于前所未有的时代，随着新冠疫情引发的社会与经济变化持续发酵，企业积极行动加速提升消费者体验——与数据安全、欺诈和利益冲突相关的新风险随之萌生。

设计合规的数字平台，并嵌入可验证且可计量的客户体验、访问、公平和共融原则和指标。
数字化提高了消费者对核心金融服务（包括支付、储蓄、贷款和投资）便利性的期望。一般而言，他们希望企业提供功能强大、直观的个性化界面，以便随时随地通过多种互联渠道（例如在线、移动、电话、线下）进行交易。作为标杆，社交媒体设定了消费者对个性化体验的期望。拥有大量数据的金融科技公司和大型科技公司正致力于在金融服务中满足消费者的期望。

在工作流程中的关键数据交接时，确保在数字平台和监督机制之间建立数据质量和完整性控制，以最大限度地提高市场行为监督的完整性。

评估利益冲突和市场行为风险，做出必要的改变，并积极监督和采取缓释措施。
长期存在以及部分新形成的市场惯例，目前正在面临更严格的审查，因为此类惯例可能导致经纪自营商、交易所和批发商存在利益冲突，并可能使投资者遭受不公正的市场行为。

监管机构高度重视投资者保护和利益冲突，将确保以下方面受到持续关注（详情请见下一页内容）：

网络与数据

金融服务监管机构将网络风险视为威胁金融稳定的首要风险——而政府当局则称网络风险为难以消除且日益复杂的威胁，对政府机构和金融服务企业均造成沉重压力。鉴于金融服务行业内部高度关联且依赖关键第三方服务提供商，金融体系的所有参与者都必须考虑网络威胁的频率和影响，实施相应的风险缓释和运营韧性计划。当前或新兴的威胁包括恶意软件（例如勒索软件）、供应链风险和复杂的分布式拒绝服务攻击（DDOS）。

改进客户和企业身份和访问权限管理方案，确保针对最新的帐户接管威胁采取适当的预防措施。
数据传输方式日益复杂，拓宽了金融服务公司资产和消费者数据的入口点，增加了恶意行为者的攻击类型。如果访问权限管理和身份验证控制薄弱，网络攻击者就有机会利用泄露的登陆信息访问机密资源和数据。

精心设计，使用自动化技术让有限的网络安全资源发挥最大效用，提升响应速度。
法律和监管合规要求日益提高，导致合规风险复杂化，成为推动企业增强网络安全能力的关键因素。通过结合安全设计、自动化和响应 (SOAR) 工具，企业能从多个来源收集安全威胁数据，通过有限的人工交互启动响应，并协调事后报告和信息共享。优势包括检测和反应更快；适用的威胁情景更广；数据管理保护措施集成化；以及成本更低——这有助于企业在 2022 年应对监管机构对网络和数据问题的关注，包括（详情请见下一页内容）：

通过嵌入“隐私设计”和实现数据保护自动化，（在数据管理生命周期中）识别、管理和保护企业信息资产。
企业正在收集越来越多的客户数据，用于开展预测分析、实现营销活动个性化以及推出/改进产品和服务。大多数消费者日益关注企业收集、使用和保护消费者个人信息的方式——这促使监管机构聚焦客户数据隐私和保护。“隐私设计”原则以防止隐私漏洞为目标，通过将隐私嵌入新应用程序（包括 IT 系统、人工智能平台和数字业务管理）的设计、操作和管理中，为稳健的数据保护设定基准。

欺诈与金融犯罪

随着监管机构重视创新方法（例如机器学习、增强型数据分析），采用创新技术来提高欺诈和金融犯罪风险管理的有效性，已势在必行。从网络安全到勒索软件，从加密货币到身份盗窃，层出不穷的威胁风险均是由技术驱动。政府当局已将许多此类问题列为重大国家安全问题，调动整个政府协同应对；重点关注的新兴领域涉及透明度和 ESG。

将自动化和分析技术整合纳入客户引导和维护流程，降低合成身份欺诈风险。
合成身份欺诈 (SIF) 是美国增长最快的金融犯罪之一。与传统的身份盗窃相比，合成身份欺诈同时使用真实和伪造信息，创建新身份，在一段时间内建立信用档案——因此，仅使用传统欺诈检测模型难以发现可疑活动。联邦储备委员会 (FRB) 指出了减轻合成身份欺诈风险的方法。

淘汰过时的身份验证技术，加强防御实时支付中的帐户接管和社会工程攻击。
快捷实时支付缩短了金融交易清算时间，增加了安全和欺诈风险的可能性，企业因此更加需要利用最新的敏捷安全和欺诈检测程序，包括身份验证和访问协议。需要重点防范的欺诈可能包括在线欺诈（例如恶意软件、网络钓鱼）、第一方欺诈（例如合成身份欺诈）和虚假声明。

建立成熟的内部人员风险计划（包括行为模型和情景分析），降低员工行为和金融犯罪风险（包括声誉损害、间谍活动、贪污挪用、市场和价格操纵）。
内部威胁因技术和人为风险结合而产生。在数字环境中，内部攻击可能导致金融和知识产权盗窃、资产受损以及企业范围内的内部系统和客户运营中断。然而，由于内部人员熟悉企业系统并在访问时受到信任，因此难以预防和检测；需要人工参与分析，发挥人类的智慧来解释技术数据（例如，来自网络安全工具的数据）并识别异常内部行为。内部人员的范围应涵盖董事、员工、承包商和第三方。

随着监管重点领域不断变化，加强相关控制。
FinCEN于 2021 年 6 月发布了政府范围内与反洗钱/打击恐怖融资有关的首要任务，包括腐败；网络犯罪（包括网络安全和虚拟货币方面的考虑）；恐怖主义融资；欺诈（包括合成身份欺诈）；跨国犯罪组织活动；贩毒；人口贩卖；和反大规模杀伤性武器扩散融资。

估值风险

金融体系的某些部门存在大量债务和杠杆，而且几乎所有资产类别（从公司股票、房地产到加密货币）的估值都处于历史高位。如果通胀上升导致利率大幅上升，这些领域的估值可能遭遇修正回调；即使是相对较小的回调，也可能对敞口集中或杠杆高的细分市场的资产价值造成巨大冲击。监管机构对公平和竞争原则的关注也可能对估值产生影响。

监测估值风险敞口，并制定情景和压力测试，以衡量资产对各种风险的敏感性。
随着新冠疫情带来的金融风险消散，监管机构正在将目光投向直接、间接、集中或杠杆高的敞口，以此监测其中长期的脆弱性。监管机构正在观察住房和金融市场（包括企业股票，以及加密货币等“风险较高的资产”）等资产类别的“繁荣”，分析多种因素单独或联合引致急剧估值调整的可能性。

确保制定有效的LIBOR过渡管理流程和控制。
联邦和州级金融监管机构已将 LIBOR 过渡列为 2022 年监管重点之一，以适当降低运营、合规、法律和声誉风险，并防止资产负债表不稳定，防范不利的财务影响。

评估并购目标可以产生的协同效应及其与公司战略的一致性。
数字化的普及，技术的现代化，科技公司带来的竞争，创造规模效应的期望，市场整合以及近期兴起的ESG潮流，正在推动金融服务公司寻求各种并购交易，并与第三方建立合作关系和/或联盟。

提升可量化和可衡量贷款标准的严格性，涵盖整个贷款周期。
由于支持不同市场板块表现的政府政策或计划力度不同，在新冠疫情时代量化和衡量不同市场板块信用风险，对金融服务公司构成了挑战。

第三方与云技术

为了增强竞争力、扩大业务和满足客户需求，金融服务公司正在大规模迅速与第三方公司建立合作关系，包括云服务提供商等专注于金融科技的企业。合作关系在为金融服务公司增添优势的同时，也可能降低管理层对业务活动的直接控制，这可能会给企业及其客户带来新风险或促使现有风险上升。

在实施稳健的供应商战略的同时，集中第三方风险管理流程，并推动流程自动化。

执行动态第三方风险评估，明确直接和间接风险评估、计量和突发事件。
风险评估是基于风险的第三方风险管理方案的核心，应贯穿整个第三方风险管理周期。任何的缺陷或不足可能会使企业面临战略、声誉、信用、运营、合规、流动性和/或集中风险。

确保第三方风险管理达到或超过全球和辖区监管机构的期望。
无论第三方（或第四方）处于何地，金融服务公司仍有责任遵守所有适用法律和法规，包括确保第三方履行此类义务。

在采购和第三方风险管理流程变更时，使用数据沙盒和并行数据概念验证。

使用现代安全工具，持续监测信息技术/网络控制，构建“零信任”安全环境。

科技与韧性

近期发生的事件（包括技术引起的故障、网络安全事件、新冠疫情和自然灾害）已清楚地表明，发生严重中断的可能性越来越大，并且可以相互关联（例如，此次公共卫生危机导致大范围封锁和交通瘫痪，进而引发金融危机）。尽管技术进步提高了企业识别此类中断并从中恢复的能力，但事件的频率以及相互关联和/或相互依赖的可能性（导致风险放大）仍然突显了企业确保运营韧性的必要，并促使领先企业采用更全面的复合方案。

针对服务韧性临界值，设定韧性标准和方法；将业务资产映射至相关服务。
良好的做法是优先考虑企业关键运营和核心业务线的运营韧性；然而，对于其他运营、服务和职能，如果发生中断可能对企业或其客户产生重大不利影响，亦应予以识别和应对。

衡量资产的财务和非财务风险敞口，评分并考虑相关因素对韧性的影响（例如，漏洞管理、生命周期结束、数据分类）。
识别财务和非财务风险敞口，应以公司内部受影响的各个领域为基础。随着风险不断演变，控制流程和程序应预见、测试和减轻未来威胁和潜在中断风险的影响。

定期向董事会和高级管理层提供信息，清楚地阐明最低服务水平和韧性强度。
公司董事会和高级管理层必须建立、监督和实施有效的运营韧性方案，以响应破坏性事件，迅速恢复并吸取教训，从而最大限度地降低中断的潜在影响，并在中断期间正常运营。

需要考虑的领域包括：

— 运营韧性方法和标准的全面性，包括治理、运营风险管理（包括网络安全风险）、业务连续性管理、第三方风险管理、情景分析、信息系统管理以及监测和报告。对于将资产清单映射至关键服务，信息技术资产管理仍然是首要主题。

— 识别和优先考虑商业服务的方法；对支持关键服务的资产进行映射分析；并定义韧性临界值。

— 制定和实施控制和富于韧性的信息系统，以维持关键运营。

— 将进阶标准应用于关键运营和核心业务线。

— 根据关键运营和核心业务线内部和之间的相互联系和依赖，识别潜在的风险传播渠道、集中度和薄弱环节。

— 确定服务质量退化引起的金融风险敞口。

— 结合业务连续性和解决方案规划进行测试并持续更新。

在漏洞管理方面，监管机构正在关注：

— 用于漏洞发现和验证（覆盖率和可见度）的工具。

— 确定补救活动优先级的策略。

— 未补救的老化漏洞。

— 不可修补的漏洞的管理情况。

— 遗留环境中的控制执行。

— 软硬件使用寿命终止风险分类的范围。

监管机构将关注以下方面的有效性：

— 考虑各种情景下的风险状况和运营能力，董事会对企业层面以及关键运营和核心业务线“中断容忍度”的审批。

— 高级管理层施行良好实践的情况以及董事会对相关工作的监督，包括维持风险管理文化；充足且适当的财务、技术和人力资源；并遵守中断容忍度。

— 业务线从头至尾对服务负责，明确划分管理职责，将运营韧性纳入治理框架，确保董事会清楚地了解相关情况。

— 建立信息系统和控制，及时发现异常活动并向董事会和高级管理层提供充分的数据（包括信息和指标的深度），以便及时、适当地做出响应。

— 网络事件期间的董事会报告（包括通知时间）。

风险“自满”

监管机构将金融服务公司的风险“自满”视为对利益相关者信任以及安全和稳健的潜在威胁。企业必须提高风险合规投入和宣传，谨慎避免过度自信——尤其是在业务增长、并购和创新时期。

赋予风险管理职能适当的地位和规模。
审慎的风险和合规管理（与规模、复杂程度和风险状况相称）必须伴随业务变化和增长，而且还必须提前预见和应对监管风险预期升级。

投资数据驱动型风险自动化、分析和流程效率。
金融服务公司必须不断从业务和风险的角度，确定如何以最好的方式利用数据和技术来满足消费者和客户的需求。监管机构希望企业采用数据驱动型方法进行风险和合规监测与评估。同样，监管机构越来越多地借力数据来开展监管和执法活动。

提前预见新兴风险并纳入考虑，积极发现问题并及时采取纠正措施。
金融服务公司必须将新兴风险和监管预期纳入考虑，同时还要持续及时发现问题并进行整改。

将风险意识嵌入业务、运营和技术变革中。
监管机构希望风险管理与控制职能成为持续的业务、运营和技术变革的一部分。以类似“这方面不可能发生风险”、“这个风险该第三方负责”或“我们从来都是这样做”的态度对待风险，都是不是稳健的做法。采取此类做法的企业将日益面临来自监管机构的压力。

在人力资本和风险文化和承担方面，监管机构将高度关注以下方面：

— 提出可验证且可信的质疑，包括风险评估的充分性以及在需要的情况下对内部控制进行监测和调整。

— 与其他战略职能相比，赋予风险、合规、信息安全和审计适当的地位（包括自主性、授权和影响力）。

— 人员配备充足且拥有适当技能，资金充足。

— 采用指标驱动的动态风险能力模型，以确定跟上业务增长或变化节奏所需的技术、运营和风险管理资源。

监管机构关注的领域将包括：

— 企业是否可以充分直接或间接访问相关数据源，以便及时有效地监测和/或测试政策、控制和交易。

— 企业是否建立了稳健的数据质量可审计性标准和方法。

— 企业是否使用数据执行更加动态和稳健的风险评估、尽职调查和监督（并相应地更新风险和合规方案）。

— 企业是否持续开展数据分析，对业务流程和控制提出质疑，并及时标记潜在问题（无论是系统性问题，还是孤立问题）。

— 在风险、检查管理和合规管理流程等领域使用工作流和自动化工具，以提高一致性和可审计性。

监管机构的关注点将扩大到以下领域：

— 建立有效的一线部门、独立的风险管理和内部审计和控制职能。

— 持续访问各个职能的运营数据和信息，以根据不断变化的合规风险更新和修订风险评估。

— 确保快速识别并适当纠正缺陷（包括数据质量，报告及时性和准确性，以及向董事会报告）。

— 对涉及系统性问题的投诉、争议和索赔信息进行稳健分析，并证明已采取相应行动（例如，修改产品或服务、加强流程控制以及产品或信息披露的清晰度）。

— 分析员工/内部人员威胁数据和行为模式以及从调查和访谈中获得的重要见解，以识别、确认和解决企业文化/行为风险或控制问题。

稳健风险治理和控制的重点领域将包括：

— 与大规模技术变革相关的持续举措，例如聚焦数据管理、数字资产、数字技术应用、云技术应用和迁移以及核心平台现代化。

— 提供支持或投入资金，促进风险管理职能访问各个职能和/或来自不同来源的运营数据和信息。

— 近期未发生变化但可能对消费者/客户群体产生过大影响的行业或企业惯例（例如，投诉处理、使用估价或其他估值模型、收取产品服务费）。

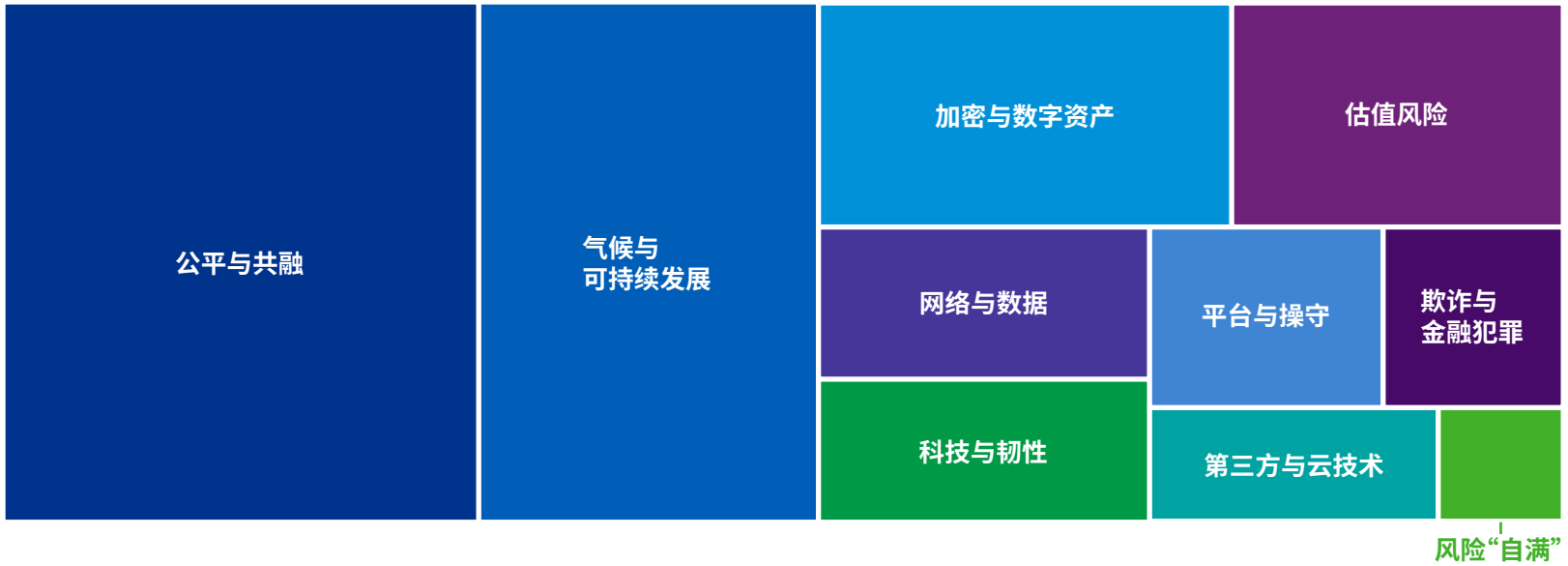
— 人工智能和其他技术风险和控制测试的适当性（例如，在访问和安全方面的潜在偏见、失当做法或漏洞）。

— 公开发布文件和监管响应的一致性（例如ESG承诺和报告以及监管问询和检查响应等领域）。

方法

毕马威监管洞察中心历来重视《十大监管挑战》系列报告。该系列以我们对政策公告、监管活动和客户讨论的评估为基础编制。去年，我们添加了一个新维度。毕马威智慧之光数据分析卓越中心利用毕马威 2019 年和 2020 年《Washington Report 360》快讯（金融服务行业公共政策、监管和新闻每周精选）开展自然语言处理和文本分析，将各期快讯及记录分类并按主题进行分组。在分析中，我们利用一种名为Guided Latent Dirichlet Allocation的技术，用户可以使用一串单词“播种”算法，引导他们将单词分类至既定主题（在本期报告中，指不同的监管挑战领域）。

今年，鉴于新冠疫情的影响、政府换届以及相关监管优先事项，我们将分析范围局限于 2021 年发布的《Washington Report 360》快讯。下图直观地表示了十大监管挑战中每个领域的记录数量。



Amy Matsuo
主管
ESG与监管洞察

Timothy Cerino
管理总监
数据分析

毕马威监管洞察

我们真诚期望本期内容为您提供有用的洞见。您还可以浏览毕马威思想领导力系列刊物中讨论的类似及其他主题。

毕马威监管洞察紧贴最新风险及监管趋势，以我们的视角助力客户预见和应对美国监管领域的变化。我们与毕马威全球监管领域的专业人士携手，洞察最新监管及执法趋势。

单击下方链接，访问毕马威思想领导力系列刊物。如果您有兴趣了解后续期刊，请点击此处订阅。

视点（Points of View）
深入分析影响金融服务业的新兴监管问题

监管快讯
汇总具体监管趋势，分析对金融服务业的影响

Washington Report 360
不超过360字的每周快讯，介绍影响金融服务业的立法和监管趋势

Amy Matsuo
主管
ESG与监管洞察

术语和缩写

ADA	《美国残疾人法案》
AML	反洗钱
AMLA	《2020 年反洗钱法案》
ANPR	拟议规则预先通知
BAU	照常经营
BCBS	巴塞尔银行监管委员会
CARES法案	《2020年冠状病毒援助、救济和经济安全法案》
CCAR	综合资本分析与评估
CCPA	《加利福尼亚消费者隐私法案》
CECL	当前预期信用损失
CFPB	消费者金融保护局
CFTC	商品期货交易委员会
CPRA	《加利福尼亚隐私权法案》
CRA	《社区再投资法案》
CSR/IR	企业社会责任/综合报告
DDOS	分布式拒绝服务
DEP	数字参与实践
DOJ	美国司法部
ECOA	《平等信贷机会法案》
ERISA	《雇员退休收入保障法案》
ERM	企业风险管理
ESG	环境、社会及治理
EU	欧盟
FCPA	《反海外腐败法》
FDIC	联邦存款保险公司
FinCEN	金融犯罪执法网络
FINRA	金融业监管局
FRB	联邦储备委员会
FSB	金融稳定理事会
FTC	联邦贸易委员会
GDPR	《欧盟通用数据保护条例》
GRI	全球报告倡议组织
HR	人力资源
LMI	中低收入
LOB	业务线条
KYC	了解你的客户
LIBOR	伦敦银行同业拆借利率
M&A	并购
ML	机器学习
MSB/MTL	货币服务业务/货币划拨许可证持有人
NCUA	全国信用合作社管理局
NYDFS	纽约金融服务局
OCC	货币监理署
OFAC	海外资产控制办公室
PFOF	订单流付款
PII	个人身份信息
PPP	工资保障计划
Reg BI	《最佳利益条例》
SAR	可疑活动报告
SASB	可持续会计准则委员会
SEC	证券交易委员会
SOFR	担保隔夜融资利率
TCFD	气候相关财务信息披露工作组（金融稳定理事会）
TFCR	气候相关金融风险工作组（巴塞尔银行监管委员会）
UDAAP	不公平或带有欺骗性或涉嫌滥用的行为或做法
TDR	总债务重组
TFCR	气候相关金融风险工作组（巴塞尔银行监管委员会）
UDAAP	不公平或带有欺骗性或涉嫌滥用的行为或做法

联系人

Amy Matsuo
主管
ESG与监管洞察

徐捷
金融业治理、风险与合规服务主管合伙人
毕马威中国
jessica.xu@kpmg.com

鸣谢

我们在此向以下协助编写本报告的人士表示衷心感谢：Amy Matsuo, Mark Dickemann, Steven Honeycutt, Amanda Kerr, Nisha Lane, Sam Mahler, Daniel Marchesani, Milan Patel, Jean-Gabriel Prince, Joe Slaninka, Karen Staines, Royal Thankachan.

毕马威审计客户及其附属公司或相关实体可能不允许使用本文所述的部分或全部服务。

kpmg.com/socialmedia