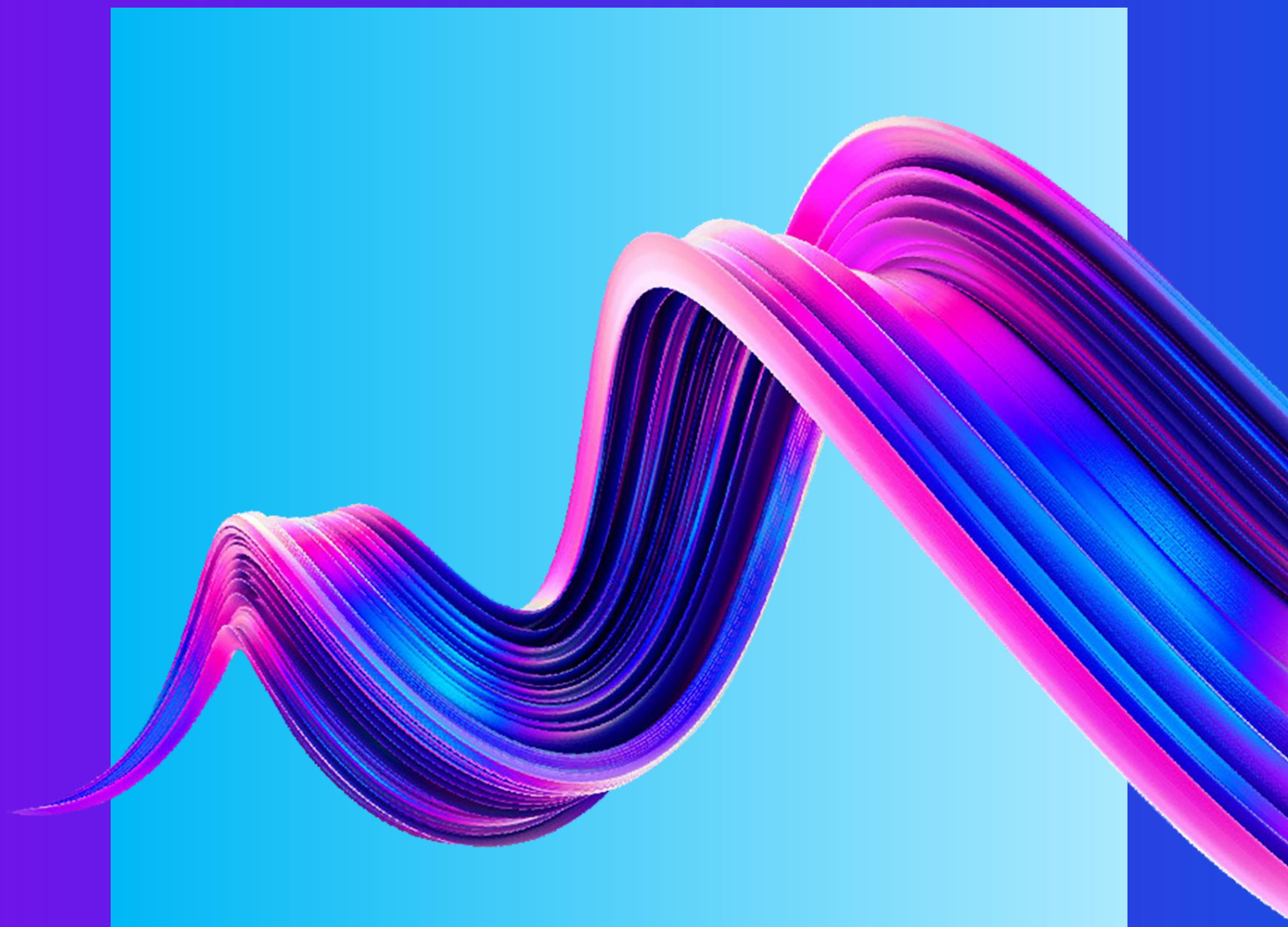
KPMG



2023年内部审计关键风险领域

在如今这个充满不确定性、不断变化的世界中，首席审计官和内部审计职能在审视风险和制定2023年审计计划时必须保持灵活。

在全球新冠疫情流行后，企业仍然面临着一系列的挑战（例如，供应链问题、员工心态变化等），过去几个月的情况表明，我们应该时刻关注新的威胁和挑战。与此同时，暴涨的通货膨胀以及地缘政治问题也将对许多企业产生影响。

新风险往往随着新挑战应运而生，内部审计部门在进行风险评估和动态计划年度内审工作时应考虑新生风险，且不应忽视关键的已知风险。因此，我们向您推荐2023年应该关注的重点风险领域。

01 经济和地缘政治的不确定性

02 气候变化

03 人才招聘与留用

04 ESG(环境、社会和治理)报告

05 网络安全与数据隐私

06 企业文化与行为

07 第三方关系与供应链

08 数字颠覆和新技术

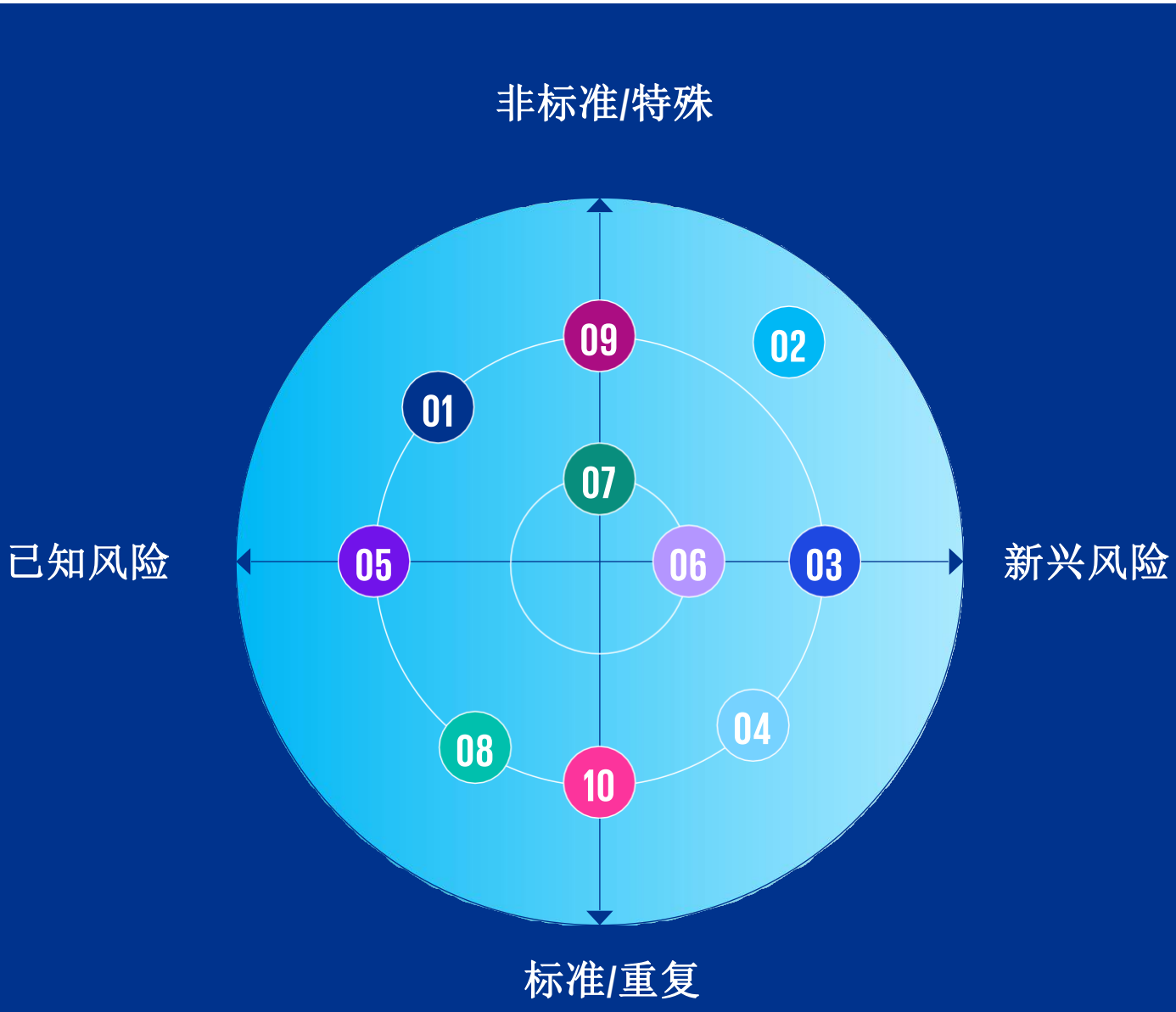
09 业务连续性和危机应对

10 兼并和收购

我们相信，在制定2023年审计计划时，本报告将为首席审计主管提供有关关键风险领域的见解。作为进一步的指引，我们已经在风险雷达上绘制了前10个风险领域(参见图1)。风险雷达图有以下两个维度：

1. **已知的关键风险领域**应该被内部审计部门识别和理解，而**新兴风险领域**正在发展，尚未得到充分理解。

2. **非标准/特殊风险领域**应考虑一次性审计，而**标准/重复风险领域**应考虑持续性审计。



2023年内部审计关注的十大风险

01 经济和地缘政治的不确定性

全球经济复苏势头强劲、消费模式向商品而非服务的转变、以及新冠疫情导致的物流网络的中断，都产生了巨大的通货膨胀压力。

在谈到乌克兰目前的局势时，就必须考虑商业、物流、法律和更广泛的地缘影响（包括复杂的制裁制度）。

此外，由于天然气和石油价格以及大宗商品价格的空前上涨，通货膨胀持续上升，许多家庭的购买力正在下降。作为一种控制措施，各国的中央银行已经开始采取行动提高利率。这些持续的全球发展正在为全球组织的商业议程带来新的日常风险。

内部审计的作用

基于“风险管理三道防线模型”,衡量风险管理的一线和二线部门如何识别和评估企业面临的风险和压力。内部审计还应审查易受经济变化影响的第三方供应商，并更广泛地考虑企业的资本规划和管理、净息差、信用/违约风险和债务回收、索赔管理和未来投资的业务案例。

内部审计还可以在识别和评估在遵守现行国际制裁制度有关的潜在的直接差距或控制弱点方面发挥作用，确保建立一个健全的框架，并采取适当的风险缓解措施，这些措施可以持续应用，以确保企业合规。

最后不能不提，内部审计可以在新生风险、三线模型的成熟度和治理相关事项方面，作为高级管理层的合作伙伴发挥积极作用。

02 气候变化

最近几年表明，气候变化的直接后果正在影响着全球人口以及企业。今年夏天，极端的气温在全球引发了新的问题，比如，由于河流流量惊人的下降而导致集装箱船运输减少、农业减产、甚至对基础设施造成直接破坏。企业在实现其可持续发展目标和减少其对气候变化的影响方面所面临的挑战和风险在未来几年内不会减少。

与此同时，投资者、监管机构、客户和员工也越来越希望企业在所有工作上都能从可持续发展的角度出发。

内部审计的作用

内部审计在确定企业是否准备好面对气候危机和支持企业有效管理气候变化风险方面发挥着关键作用。内部审计可以在运营层面审查这一领域，因为内部审计对从材料采购到运输、物流和废品管理等与可持续性相关并受其影响的流程有深刻理解和认识。

03 人才招聘与留用

在新冠疫情流行之后，人们在劳动力市场上的流动速度加快了，人才的招聘和留用仍然是一个关键的风险领域。员工的高离职率给许多企业带来了干扰，为确保招聘到所需的人才，企业进行了非常激烈的竞争。员工福利仍面临严重压力，这增加了人才流失、疲劳的风险， 在影响生产力的同时，也侵蚀了企业目标和文化。

每位员工的自愿离职都会给企业在业务中断、招聘和入职方面带来极大的损失。企业需要了解不断变化的员工心态，并设计长期的激励和薪酬计划，以提高留任率。

内部审计的作用

评估企业的劳动力规划和未来的技能需求、人才招聘和人才留用战略。这些应包括继任计划、能力管理、薪酬基准、福利计划以及培训和发展。内部审计应协助企业制定符合相关业务风险的人才衡量标准。

04 ESG(环境、社会和治理)报告

虽然ESG报告还处于起步阶段，但对ESG报告的要求更加广泛和全面是一个快速发展的趋势。香港交易所已将对ESG报告的要求纳入了气候相关财务信息披露工作组（TCFD）的若干关键建议。 与此同时，香港的绿色和可持续金融跨机构指导小组已宣布计划，到2025年强制披露与TCFD一致的气候相关信息。

因此，我们鼓励所有企业以适当的治理结构，应对ESG相关的话题，并对ESG风险和机会提供可靠和有用的信息。

企业应该确定他们的ESG披露和衡量标准，并确定需要采集和策划的数据，以便及时遵守当地最新的ESG法规。

内部审计的作用

对于处于ESG之旅早期阶段的企业，内部审计应在理解ESG风险方面提供咨询支持，并支持设计和开发强大的治理框架和控制环境。

对于在环境、社会和治理方面已经取得了进一步进展的企业，内部审计应该对相关的治理框架、企业战略和环境、社会和治理报告的完整性提供保证。同时，应对ESG风险管理和适用立法要求的遵守情况进行评估。

05 网络安全与数据隐私

远程工作和新技术(如云平台)被采用的速度加快，再加上全球参与者的加入越来越多地将网络破坏作为其武器库中的一个关键工具，这意味着组织必须对其网络安全风险保持警惕。这同时强调了对IT安全进行更严格审查和提高员工对恶意和非恶意网络攻击认识的必要性。

在以数字化为动力的数据驱动的世界里，监管机构正不断提高警惕，数据隐私和保护继续对企业构成重大挑战。《中华人民共和国个人信息保护法》(PIPL)和《中华人民共和国数据安全法》(DSL)，香港的《个人资料(隐私)条例》(PDPO)、以及欧盟的《一般数据保护条例》(GDPR)等相关法律法规不应被企业所忽视。持续地关注和遵守相关法律法规，将帮助企业避免巨额罚款和声誉风险。

内部审计的作用

评估用于降低减轻网络安全风险的相关控制措施的有效性，并考虑应用NIST网络安全框架：识别、保护、检测、响应和恢复。审查实例可能包括网络安全治理、身份管理、意识和培训、网络控制的安全评估(包括检测和响应管理)、新冠疫情后的新工作方式审查、数据安全实践、事件响应和恢复战略。

评估隐私和数据保护控制，包括如何收集、使用、存储、保护、保留和处理数据。这应该符合法规要求和行业领先的实践。衡量对第三方供应商可以访问的企业数据的管理。针对拟议的立法改革进行差距分析，或针对相关法律和法规进行成熟度评估。

06 企业文化与行为

企业对其内部和外部利益相关者负责，鼓励适当的文化和诚信标准的建设。为了实现这一目标，有必要确立一套员工在企业内应遵循的价值观。例如，在银行业，薄弱的文化与许多历史性的损失或欺诈事件有关。这导致当地的银行业监管人员更加关注风险文化。香港金融管理局（HKMA）已经启动了对银行文化的自我评估，并与个别银行进行文化对话。此外，管理层需要进行足够的监督，并制定明确的政策（如反贿赂和腐败）和要求。究其原因，最终是人们的行为推动了决策，从而影响了企业的绩效和现有控制的有效性。

内部审计的作用

“软性控制”审计旨在引发讨论，分享最佳实践和加强“控制中”活动。内部审计通常寻找的是多样的观点正在被传播，这些声音被听到，激烈的辩论正在发生，领导者愿意接受挑战的证据。审计采用工作人员调查，并辅以与领导者、关键人物和二线专业人士的访谈。内部审计应继续进行“软性控制”审计，以确保企业的当前文化及其对现有控制有效性的影响。

评估当前员工与企业价值观的一致程度，并通过数据分析识别潜在的欺诈风险。

07 第三方关系与供应链

企业越来越依赖第三方供应商向其客户和顾客提供关键业务产品和服务。企业还发现，第三方的失误会严重影响其有效运作的能力，并可能损害其社会信用和声誉。为了减轻这种第三方风险，企业应制定明确的战略来选择、审批和管理第三方。

内部审计的作用

评估情景和应急计划，包括供应商合同和其服务延续性。

评估端到端的采购流程，特别关注采购和第三方风险，以及该风险在供应商之间的分布。

协助企业建立一个合同管理框架、记分卡，以持续监测第三方关系，并全面了解所有的外包安排。

最新的全球事态发展和新冠疫情继续给全球和国内供应链带来巨大压力，从生产延误和劳动力短缺到主要港口的持续关闭和相关航运中断以及商品价格上涨。预计这种情况至少会持续到2023年。

审查供应链物流和连续性流程，包括与ESG相关的风险以及在其运营环境中对第三方网络安全风险的管理。

08 数字颠覆和新技术

在过去几年中，数字颠覆、转型和新技术的采用已经加速，包括人工智能（AI）、预测分析、认知计算和机器人流程自动化。这些新技术带来了新的风险，如数据和云存储、使用和隐私相关的风险，不应忽视。

内部审计的作用

评估数字化战略和计划以及相关的风险管理控制，对具体的数字化项目提供保证，包括人工智能设计的完整性、算法测试、异常管理和补救、变更管理控制、第三方供应商和软件供应商管理。提供治理和控制框架的建议，以确保人工智能和机器人的风险长期（实施后）得到监测和缓解。

内部审计还可以建议企业实施新技术，在整个企业内分享新技术的知识，使企业（重复的）流程更加有效。

09 业务连续性和危机应对

许多企业对新冠疫情产生的危机感到震惊，随后制定了灾难恢复计划和业务连续性程序。企业必须确保他们的业务连续性计划和危机管理程序是充分的，并不断更新以应对其他威胁，如网络威胁、自然灾害、其他疾病的爆发或政治不稳定。如果不这样做，可能会导致运营的深度中断。

内部审计的作用

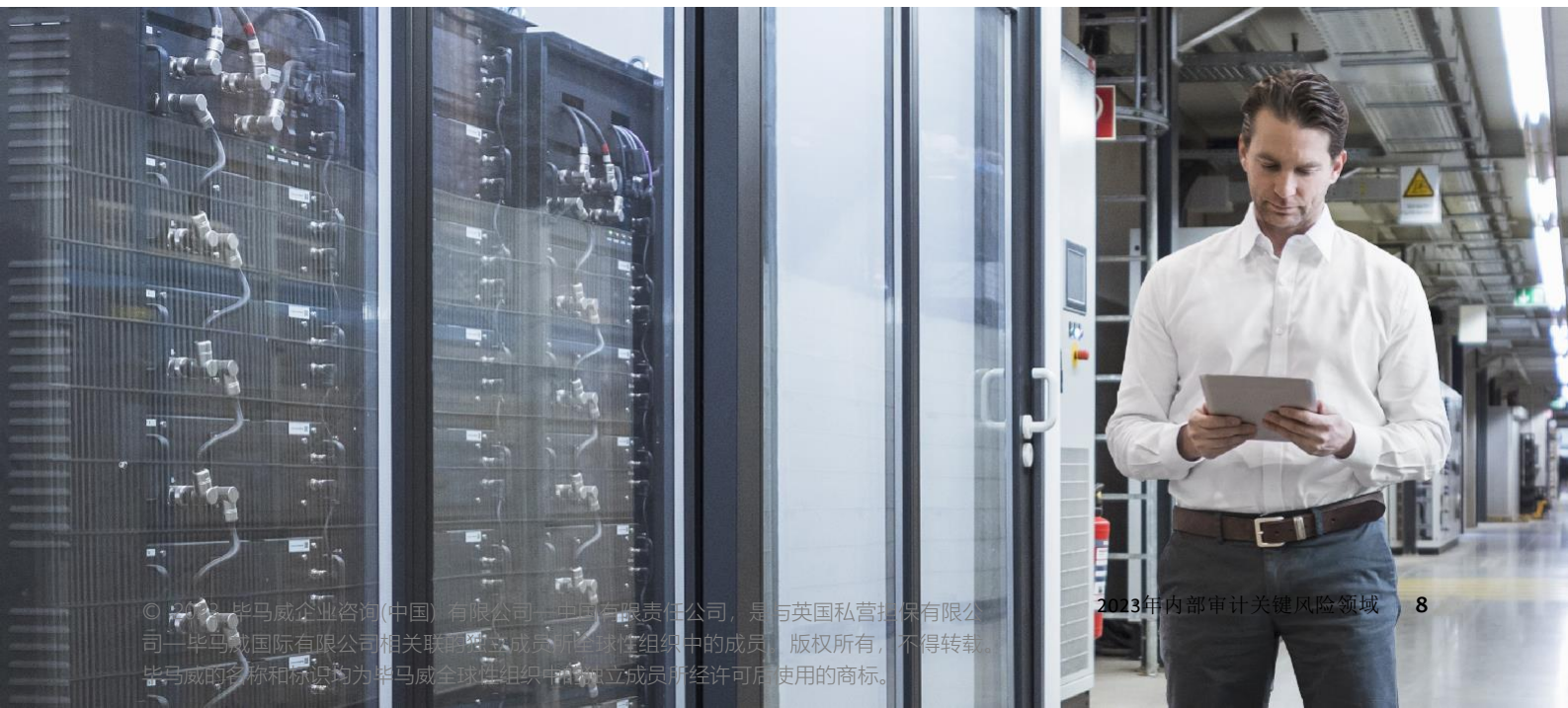
评估整个危机管理系统的质量，确保关键威胁已经被识别，适当的应对计划已经到位，并在应急演习中得到测试。内部审计应审查业务连续性或危机应对计划是否符合目的，是否考虑了新生风险和不断变化的关键威胁。内部审计还应该寻找围绕危机决策的治理以及向危机委员会报告的数据和信息的完整性的证据。

10 兼并和收购

新冠疫情暴发后，并购热潮加速，全球并购创下新高。在这个快速变化和需要实现交易利益的时期，并购带来了独特的 "交付 "和 "交付 "风险。

内部审计的作用

制定一个综合的并购风险保障(Assurance)战略计划，了解并购业务在其生命周期内将获得的保障类型，将内审对并购业务能否“过关”的保障类型从实时保障提升到即时保障，从而有助于企业做出明智的决策。重点领域可能包括：目标公司的控制尽职调查和补救计划，治理和整合审查，IT发展路线图规划，供应链整合和实现并购目标等。



请联系我们

华东及华西区

梅放
毕马威中国风险咨询及公司治理、风险和合规管理
主管合伙人
Tel: +86 (10) 8508 7188
frank.mei@kpmg.com

北方区

李斌
毕马威中国公司治理、风险和合规管理
北方区主管合伙人
Tel: +86 (10) 8508 5975
johnson.li@kpmg.com

华南区

梁安超
毕马威中国公司治理、风险和合规管理
华南区主管合伙人
Tel: +86 (755) 2547 3338
kelvin.oc.leung@kpmg.com

香港特别行政区

李懿玲
毕马威中国公司治理、风险和合规管理
香港主管合伙人
Tel: +852 2143 8764
alva.lee@kpmg.com

kpmg.com/cn/socialmedia

kpmg.com/cn