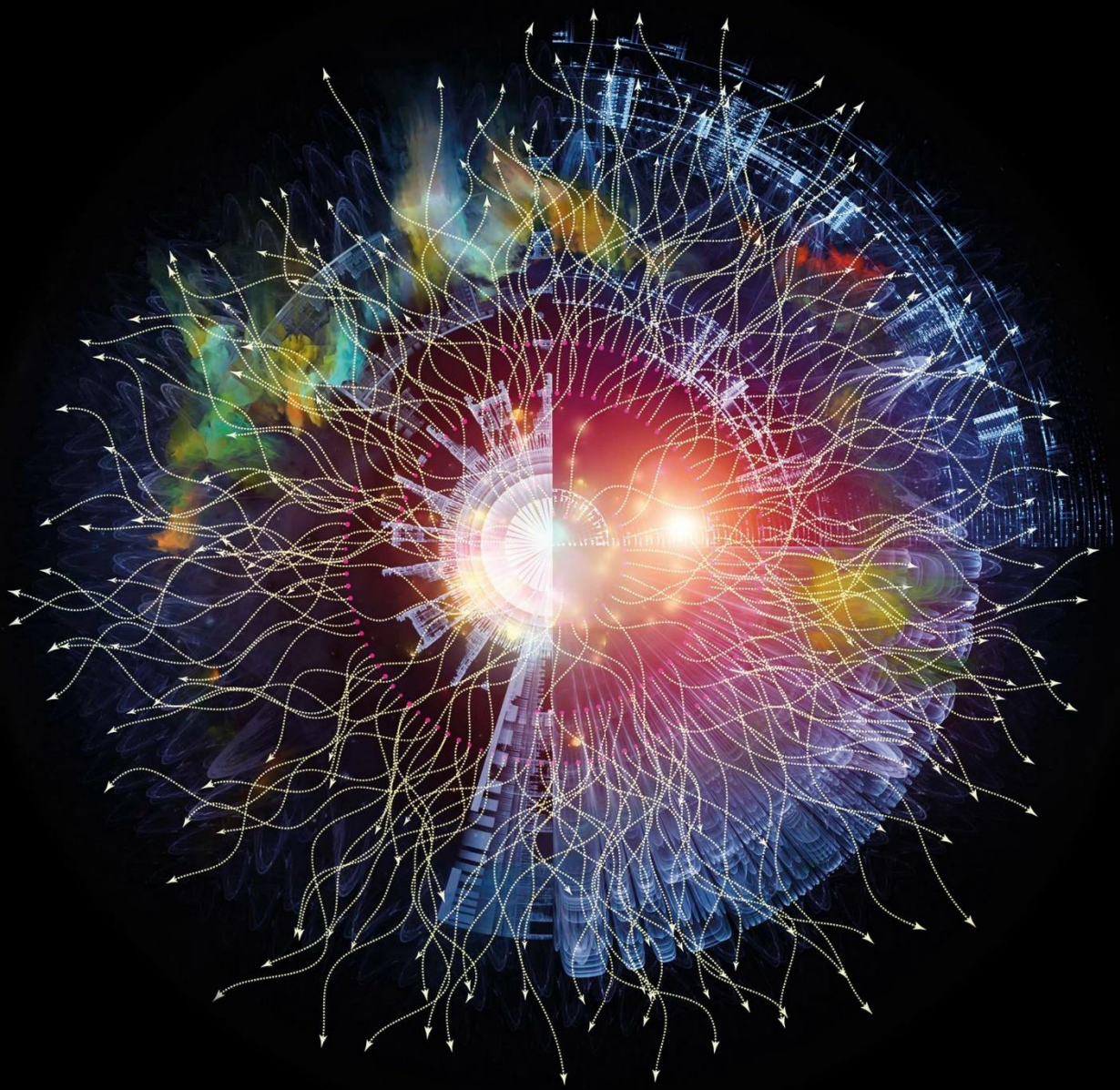
Deloitte.



认清趋势，抓住机遇

2019年全球数字化风险调查

目录

序言	01
关于本次调查	02
颠覆性技术对企业的影响	04
数字化转型治理	11
数字化转型带来的全新风险领域	16
风险运营模式	22
运用颠覆性技术数字化管理风险	28
人才	33
作者和参与者	38
全球联系人	39
注释	40

序言

我欣然与您分享我们首次全球数字化风险调查结果。我们采访了160多家企业，其中大多数正经历一定程度上的数字化或真正意义上的数字化转型。受访者开诚布公地向我们讲述了其数字化愿景——从建立全新商业模式到创造更具个性化的产品和服务，而这些产品和服务均依托人工智能（AI）、大数据和云技术来实现。同时，他们亦谈到了当前所面临的巨大挑战，包括变革速度、文化采借、网络威胁、技术资源匮乏和监管合规等问题。我们希望本报告对您的数字化之旅有所启发和帮助，并期待与您共同探讨本调查报告中涉及的关键问题。

概况

建立客户忠诚度需花费数年时间，但在数字化世界中，这种信任一夜之间即可逝去。因此，企业须在迈向数字化时代的转型过程中觅得持续掌控的方法。本报告介绍了我们2019年全球数字化风险调查的结果，从全球角度阐述了运用颠覆性技术降低风险时所面临的机遇和挑战，并就如何克服其中某些挑战提出了最新思路。

我们旨在阐明采用新兴技术后的“实际”进展状况，并强调有效的风险管理能推动企业实施其数字化战略。因此，贯穿本报告的共同主题即是如何最大程度地转化数字化经济所带来的商业机遇，而强劲的领导力、明晰的归属划分和高效的执行力将有助于加快这一进程。

我们在此感谢参与本次调查的全球客户，他们坦率地分享了其观点及挑战——其中许多观点及挑战在多个区域和行业均相似。

Stephen Ley
全球领导合伙人，技术与数字化风险



报告结构

1. **颠覆性技术对企业的影响**——企业运用颠覆性技术到达何种程度？他们能否迅速部署颠覆性技术？在运用此类技术过程中面临哪些困难？
2. **数字化转型治理**——企业是否有信心充分掌控颠覆性技术的运用？是否对其治理方法的适用性和可扩展性具备信心？
3. **数字化转型带来的全新风险领域**——随着数字化转型速度及程度日益提高，将出现哪些风险类型？这些风险类型拥有多大的关注度？
4. **风险运营模式**——颠覆性技术的运用对风险管理方式有何影响？
5. **运用颠覆性技术管理风险**——企业是否基于当前所需的速度和规模管理风险利用颠覆性技术？
6. **人才**——企业需要哪些技术来应对管理数字化风险所面临的挑战？

关于本次调查

概况

本次调查衡量了三道防线的高管对颠覆性技术的看法及此类技术对其企业的影响。166名受访者来自欧洲、中东和非洲（EMEA）、美洲和亚太地区的各个企业，所属部门分别为数字化、转型、技术、风险和内部审计部门。上述参与调查的企业涉足金融服务、消费品与零售、电信、公共卫生与生命科学、石油与天然气以及科技等领域。

方法

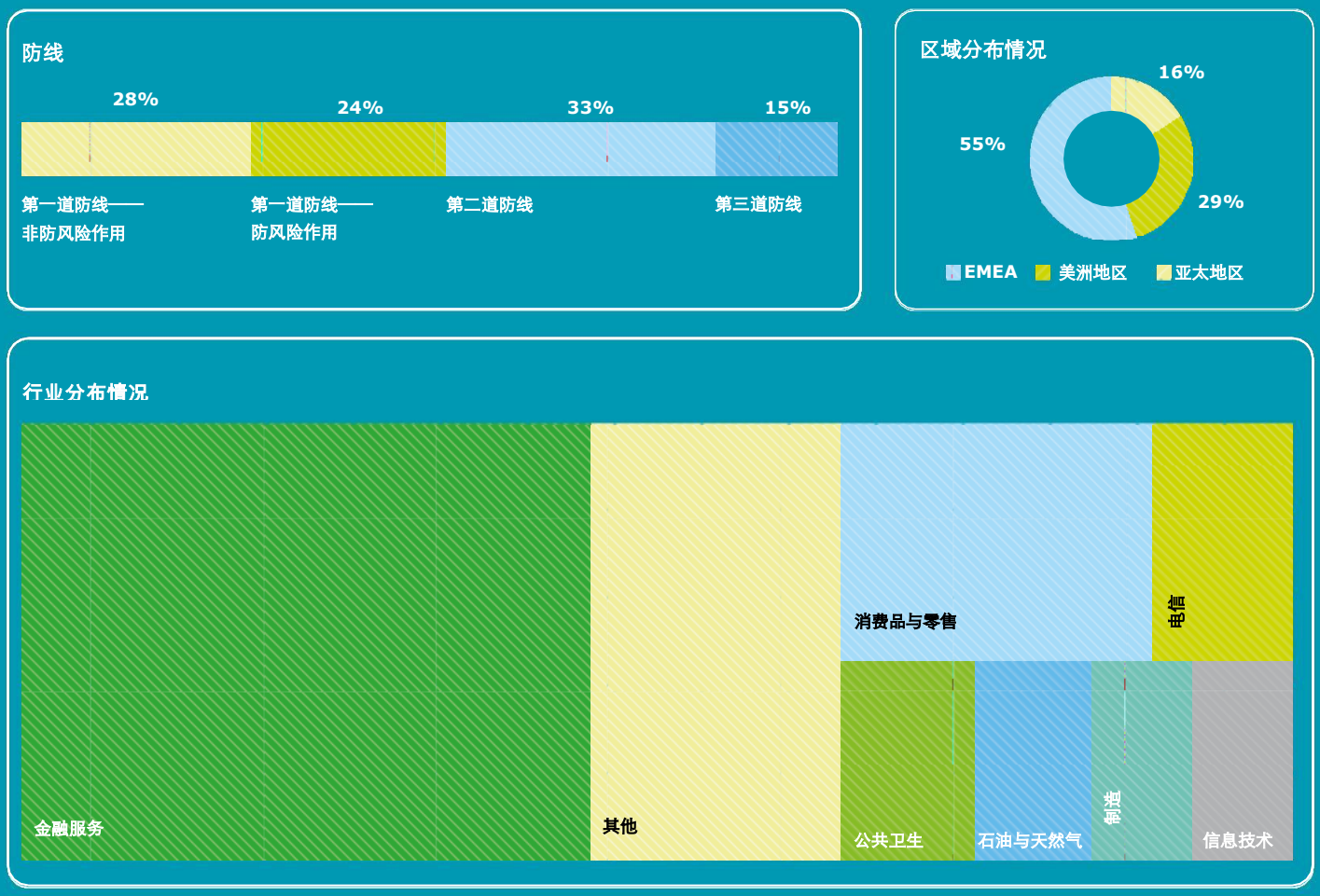
本次调查受Deloitte LLP委托，持续时间从2018年12月至2019年3月。

调查团队通过线上和线下两种方式访问调查参与者。

在此之后，内部行业专家对实际调查结果进行分析并确定共同风险类型、关键经验教训和问题，以供深入考量。

受访人员情况

图1.受访者分布情况





颠覆性技术对企业的影响

颠覆性技术对企业的影响

对于能成功冲破壁垒的企业而言是千载难逢的机遇

技术以多种方式助力当今企业完成其梦寐以求之事，化不可能为可能。讽刺的是，实现真正数字化转型过程中面临的诸多壁垒不再与技术有关，而是与文化、技术、执行能力和风险管理能力有关。因此，需结合这些要素来决定和阐明提高颠覆性技术采用率的商业作用——许多机构似乎仍在适应这一点。

机遇无限，障碍重重

来自各地区、行业及职能部门的意见均趋同于一点，即颠覆性技术蕴含创造极大价值的潜力。从缩短上市时间到更好地了解客户，再到创造具备全球规模的新产品类型，受访者表示新业务模式可释放出巨大的商业价值。然而，赢得此类机遇并非畅行无碍。受访者谈及的数字化转型壁垒大相径庭，范围从传统流程、文化抵触、人才及能力匮乏到基础设施老化。

从缩短上市时间到更好地了解客户，再到创造具备全球规模的新产品类型，受访者表示新业务模式可释放出巨大的商业价值。

当前最具影响力的颠覆性技术是什么？

就采用颠覆性技术的总体形势而言，调查显示，占据主导地位的技术为云（85%）、敏捷开发（80%）、敏捷交付（77%）及应用程序接口（76%）。大规模采用其他新兴技术似乎仍处于初始阶段，如物联网、机器人、机器学习、区块链及自然语言处理等“规模化运用”的相关占比均低于10%。

有关颠覆性技术的详细列表，请参见图2。

创建数字化优势的良机



鉴于当前云、敏捷及应用程序接口等技术的采用程度和需求情况，风险团队应充分考量三类技术的各项治理方法，确保此类方法易于理解并能推动上述技术进一步普及。

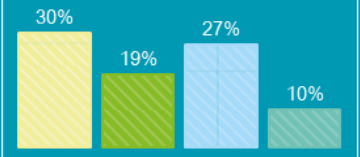
认清趋势，抓住机遇——最广泛采用的技术趋势有哪些?

图2：按整体采用水平和使用类型分列的技术趋势

领军者——云、敏捷和API等成熟的技术及方法在调查参与者中的整体采用率超75%。同时，以下四项技术在“规模运用”和“客户使用案例”方面的比率最高。

云

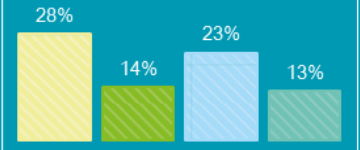
整体采用率： 85%



扩大采用规模的三大障碍
- 风险偏好
- 治理模式成熟度
- 监管审查

敏捷开发

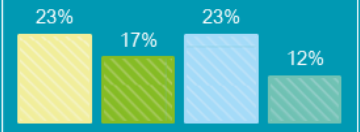
整体采用率： 80%



扩大采用规模的三大障碍
- 文化抵制
- 治理模式成熟度
- 人才匮乏

敏捷项目实施

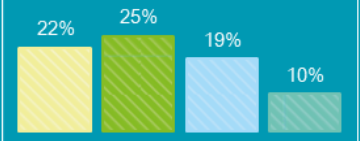
整体采用率： 77%



扩大采用规模的三大障碍
- 文化抵制
- 治理模式成熟度
- 人才匮乏

API

整体采用率： 76%

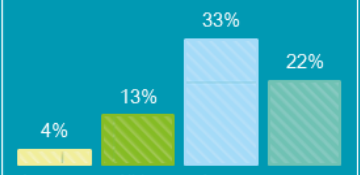


扩大采用规模的三大障碍
- 人才匮乏
- 难以阐明商业作用
- 带宽不足

追赶者——自动化与机器人、机器学习和物联网（IOT）的采用率为50%至75%。以下技术还具备最高水平的概念验证实验，该实验可发掘这些技术最具价值的用途。

自动化与机器人

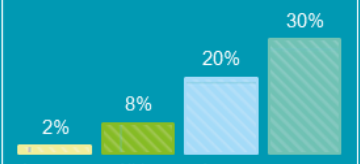
整体采用率： 71%



扩大采用规模的三大障碍
- 难以阐明商业作用
- 功能成熟度
- 预算限制

机器学习

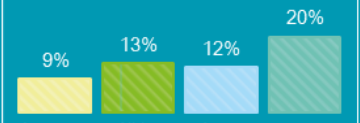
整体采用率： 60%



扩大采用规模的三大障碍
- 难以阐明商业作用
- 功能成熟度
- 人才匮乏

物联网

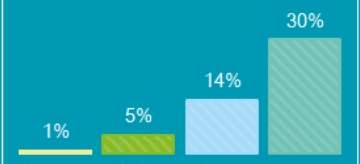
整体采用率： 54%



扩大采用规模的三大障碍
- 难以阐明商业作用
- 功能成熟度
- 人才匮乏

自然语言处理

整体采用率： 50%

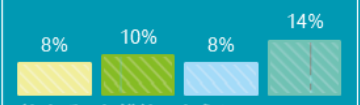


扩大采用规模的三大障碍
- 难以阐明商业作用
- 功能成熟度
- 人才匮乏

未来参与者——如微服务和区块链等其它技术趋势的整体采用率在本次调查中最低。区块链的实验远远超过其它类别，而微服务在每项使用类别中的划分大致相当。

微服务

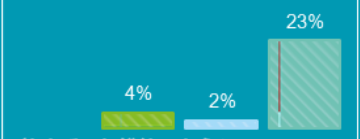
整体采用率： 40%



扩大采用规模的三大障碍
- 难以阐明商业作用
- 功能成熟度
- 人才匮乏

区块链

整体采用率： 34%



扩大采用规模的三大障碍
- 难以阐明商业作用
- 功能成熟度
- 董事会接纳程度与理解程度

关键

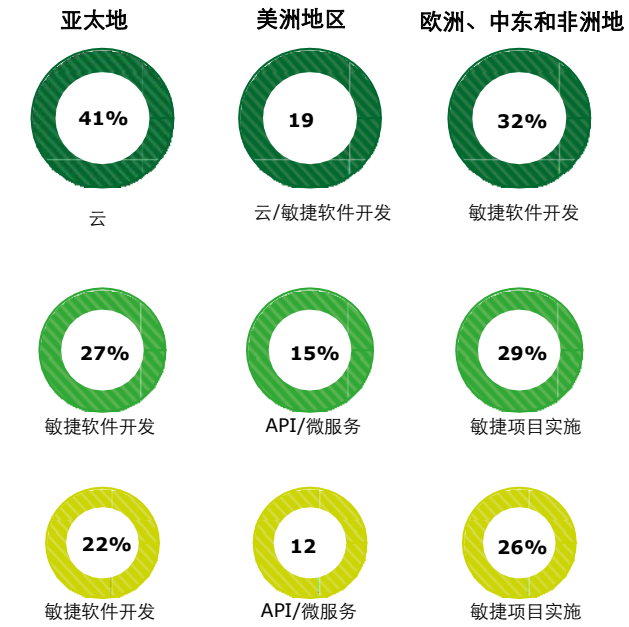
- 规模运用
- 客户使用案例
- 内部使用案例
- 实验

哪些地区在运用颠覆性技术方面处于领先地位?

每个地区颠覆性技术的应用水平大致反映了全球颠覆性技术的应用趋势——云、敏捷开发、敏捷交付和API是应用最广泛的四大技术趋势。在亚太地区和美洲地区大规模应用的技术中，云技术位居榜首；而在欧洲、中东和非洲，敏捷开发技术最普遍。结果表明，亚太地区在云技术的应用处于领先地位，该地区大规模应用云技术的企业数量几乎为美洲的两倍（参见图3）。

哪些地区在颠覆性技术的运用方面处于领先地位？哪些技术的采用位居榜首?

图3：受访者大规模应用颠覆性技术的占比（按地区划分）



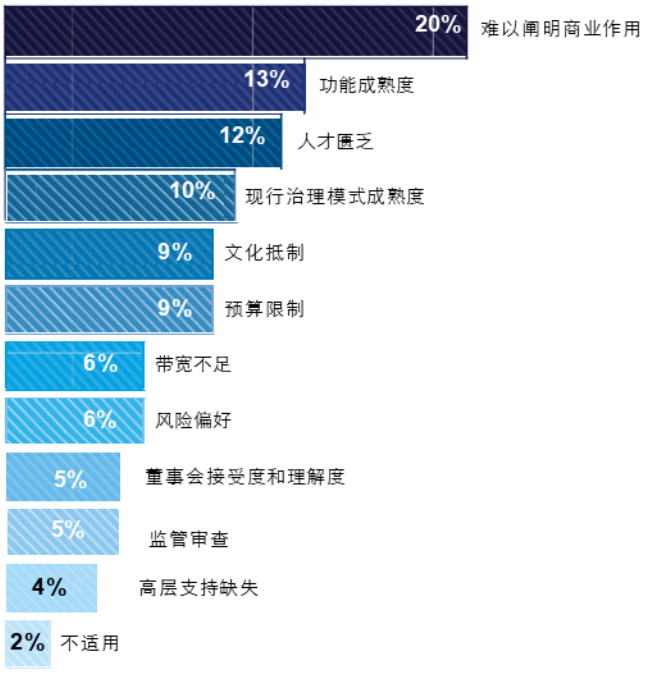
扩大颠覆性技术应用规模最常见的壁垒是什么?

难以阐明商业作用（20%）是扩大颠覆性技术应用规模最常见的壁垒（参见图4）。现有选择多样化，企业似乎专注于决策如何最佳地应用新技术来创造商业价值。很明显，位居第二和第三位的答案分别是功能成熟度和人才匮乏，两者在阐明如何应用技术方面均发挥着十分重要的作用。

扩大颠覆性技术应用规模最常见的壁垒并非监管审查、缺乏高层支持和董事会接受度低，而是源自阐明商业作用、人才、功能、治理模式和文化方面的挑战。

扩大颠覆性技术应用规模的壁垒

图4：扩大技术应用规模最常见的壁垒——难以阐明商业作用

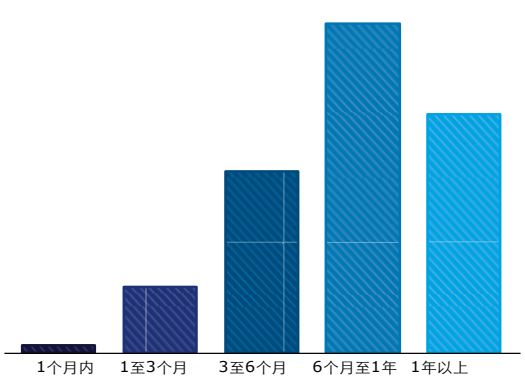


企业能否迅速将创意转化为实际解决方案?

大多数企业（69%）报告称，他们难以在六个月内将创意推向市场（参见图5）。虽然各地区间差异不大，但美洲地区和亚太地区的报告显示，其在制造业和IT业的技术部署速度较之其他地区更快（就行业而言）。但从总体来看，各研究结果表明，不同地区和行业间并无显著差异，这表示许多企业面临同样的挑战，即如何在保持控制权的同时缩短“实现价值的时间”。

能实现快速部署的情况鲜见

图5. 将创意转化为实际解决方案的平均时间



对于需要6个月或更长时间将创意转化为实际解决方案的企业而言，相关壁垒主要聚焦于文化（如更加保守的瀑布式资金分配方法）、传统流程（如人工环境配置）和人才匮乏。对于能较快展开技术部署的企业来说，加快部署的最大壁垒并非文化和传统流程，而是人才匮乏的问题（参见图6中的完整列表）。

大多数企业需要6个月甚至一年多的时间来构想和实施一项新的解决方案。此现象在所有行业及地区几乎是一致的。

不论部署时间长短，各项研究结果均表明风险团队在减少实现变更时间和成本方面可发挥重要作用。在解决由风险及控制需求而导致的延迟问题时，安全要求、文化和敏捷团队与非敏捷团队的相互沟通等要素均可促进问题解决进程。

超过三分之一的受访者（36%）称其经历了因颠覆性技术出错而导致的重大事故。他们中许多经历了影响更为重大的低发事故——此类事故由采用曲线下的技术（自动化、区块链）所引发，以及较低影响的高发事故——此类事故由现行技术（云、API）所造成。该观察结果存在偏差，体现在颠覆性技术所产生的风险状况随采用曲线有所差异。随着颠覆性技术采用率的日益提高，服务中断的可能性不断增加，这意味着需要根据技术采用情况扩大治理方法的适用范围。

风险管理团队的价值创造机遇——助力企业缩短实现价值的时间

图 6——影响将创意转化为实际解决方案的最大壁垒，按转换创意所需的平均时间划分

将创意转化为实际解决方案（6 个月内）



将创意转化为实际解决方案（6 至 12 个月）



将创意转化为实际解决方案（1 年以上）



规划前进之路——企业应把工作重心放在何处?

由于数字化环境的市场动态变化迅速，扩大规模和提高速度的任何壁垒均可能成为对业务造成严重潜在影响的战略风险。因此，风险职能部门可通过安全可靠的方式改进快速应用新技术的方法，从而在帮助企业消除这些壁垒时发挥重要的作用。

- **聚焦业务转型需求，而非技术——**当今世界，技术日新月异，人们很容易将主要精力倾注在技术上。然而，业务转型需求应是主要驱动因素。待真正的业务需求确定后，应聚焦创建经充分研究且令人信服的业务案例，并找到具备相关技能的员工，以实现此类业务需求。
- **了解并突破速度壁垒——**调查结果显示，传统流程、技能差异、文化及应对风险和控制需求的方法是影响变革速度的主要因素。应明确影响价值实现时间的问题，并将其逐一解决。
- **将灵活性融入治理框架中，优先考虑与当前相关的技术——**企业高管不太可能愿意承担不必要的风险，但如因此导致效率低下或治理流程过于僵化，或使创新和承担风险的能力受限，其亦无法承担。随着颠覆性技术采用率的不断提高，治理和风险管理日趋重要，因此，为确保颠覆性技术的安全采用，需定制一套通用方法，使其与常规风险框架保持一致。

创建数字化优势的良机



当今，快速市场化至关重要，通过设计缩短价值实现时间的治理流程，风险团队有机会为企业创造真正的商业优势。



数字化转型治理

数字化转型治理

乘风破浪

新技术具有增强优化、颠覆甚至替代现有业务模式的巨大潜力。新技术带来的风险可能会在整个企业中产生广泛的影响，因此，企业考量其现有治理模式是否符合未来需求，并且能否应对当下及即将发生的纷繁变化是至关重要的。此类考量包括深入理解关键的新兴风险领域是什么，谁来负责并管理、监控和降低这些风险。

数字化风险的定义是否明确？谁来负责这些风险?

许多行业经历了翻天覆地的转型，我们的调查显示，数字化风险尚未在众多企业中得到明确定义，这一结果并不令人讶异。大多数企业将数字化视为附加在现有风险领域（例如信息安全、网络、数据隐私及转型）中固有的风险驱动因素。有趣的是，一些受访者表示，数字化风险作为战略执行风险（即在实现董事会战略目标时技术和数据所产生的风险）已被明确定义，而更精细的运营风险仍未被定义。另一个普遍现象是，数字化风险在第一道防线中往往被视为战略或营销风险抑或会影响数字化渠道（例如移动应用程序）的稳定性，而内审部门则倾向于从更广泛的角度将其视为在云转型、大数据及人工智能等新兴技术应用中产生的风险。

大部分企业似乎更关注于网络和监管合规性等热点领域，这表明他们尚未探索在数字化转型进程中所产生的端到端的风险影响，与网络、数据及监管相比，数字化转型对风险管理的影响更大。

一些受访者强调，缺乏对数字化风险的更多关注的原因之一是控制职能部门中的数字化专业人员不足，企业通常依赖负责数字化风险相关人员的“直觉”，而非结构化治理方法来管理这些风险（网络等通俗领域亦是采用该方法）。

对风险责任归属的影响

由于对数字化风险的构成难以达成一致，导致诸多企业缺乏相应的数字化风险责任人或对其定位不清。根据我们的调查，在大多数企业中，数字化风险可来源于 IT、战略抑或营销等职能部门，因而并未被明确界定。

33%的调查参与者表示，数字化风险应由首席信息官（CIO）负责，该回答在所有受访地区中最为普遍。14%的受访者给出了自己的答案，比如数字化部门的首席执行官或是视情况来确定风险责任人（例如，移动应用程序所产生的问题较之数字化渠道所提供的较差客户成果的情况）。12%的受访者认为并未对风险责任进行明确界定，而表示由首席技术官、首席执行官及首席风险官等负责数字化风险的受访者合计达 8%左右。

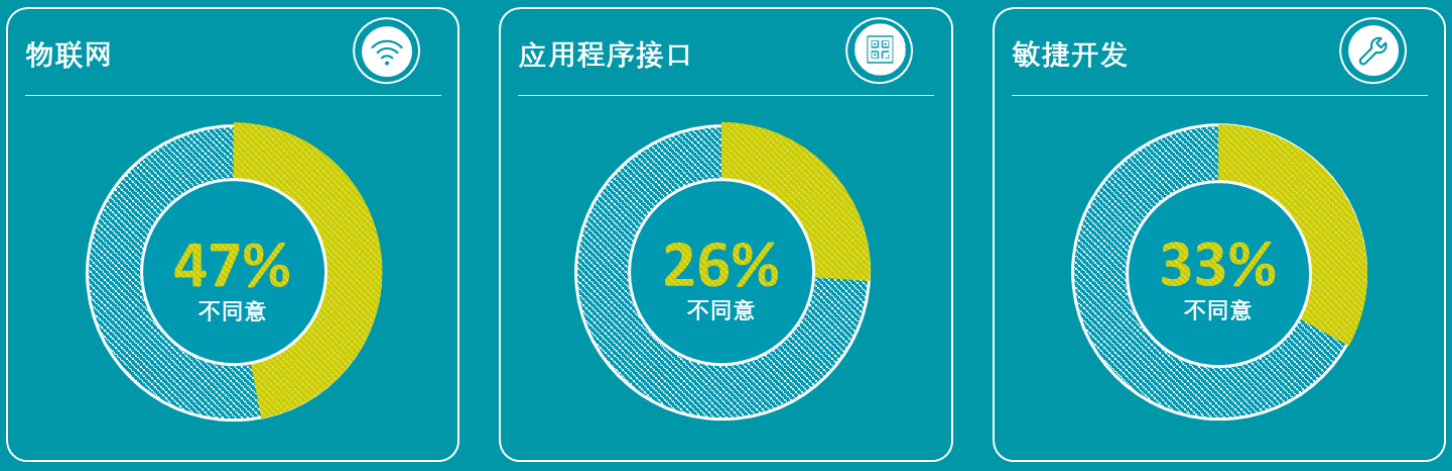
鉴于数字化会对企业的许多方面（如变革、供应商、财务、房地产、战略和组织设计与文化）产生广泛影响，建议将管理数字化风险的职责进行明晰地划分。

目前，仅有金融服务和消费品行业提及首席数字风险官这一新兴岗位。

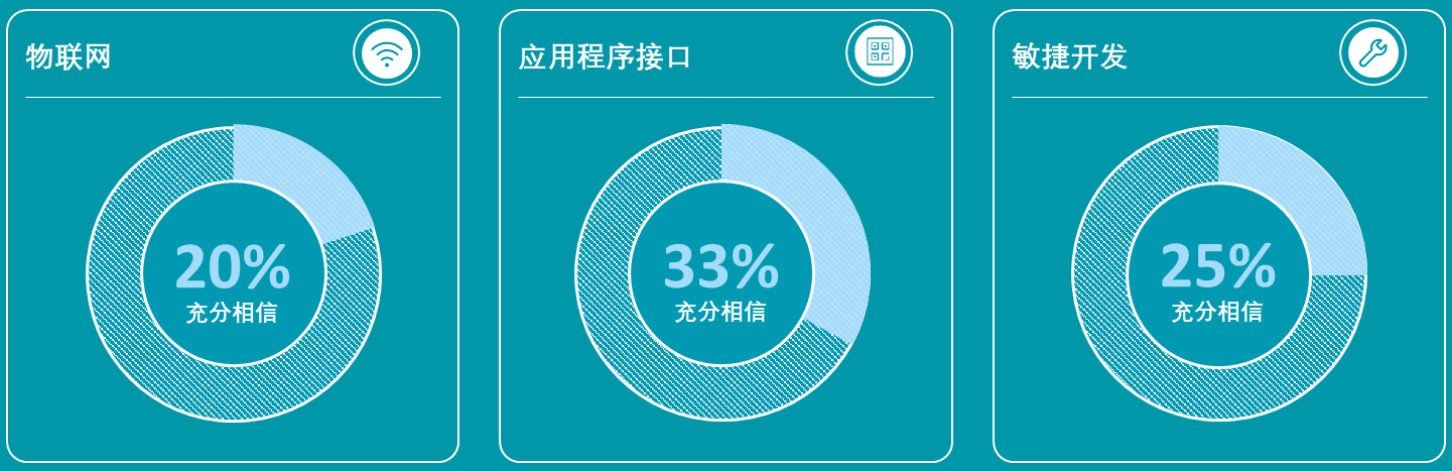
当前风险治理模式是否与技术的应用水平保持一致，且具有可扩展性呢?

图 7. 针对技术应用周期不同阶段所采用风险治理方法的适当性开展调查，并对受访者就治理方法随技术应用的普及而扩展的可行性所回答的信心水平进行对比。

您在多大程度上同意以下说法：“我们的治理方法符合当前的技术应用水平”



对于以下颠覆性技术，您是否相信您现有的治理方法能有效推动其被广泛应用?



创建数字化优势的良机

数字化转型的广泛影响促使企业各风险责任人之间相互沟通和关联，从而有效防止或减缓风险。风险管理团队应确保风险治理模式依照正确的信息使相关人员充分发挥其作用，并以透明、协作的方式加以运用。

企业的哪些领域参与到数字化转型治理?

目前，有 73%的受访者表示其技术部门作为治理主体一般负责管理数字化转型，而将相关高层、运营部门、战略部门、风险部门和首席信息安全官作为治理主体的也不少，这在受访公司中的占比达 37%。然而，仅有16%的企业以人力资源部门作为治理主体负责数字化转型治理，且不到 10%的企业选择供应、制造、物流和采购部门作为治理主体。

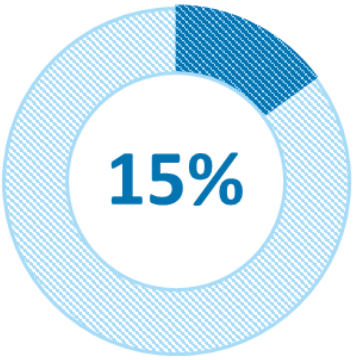
受访者指出，推动数字化转型治理的关键职能部门是技术部门、风险部门和相关业务部门（占比分别为74%、40%和39%），这表明风险部门在数字化转型中虽占有一席之地，但也未成功将有效的风险治理转变为数字化优势。有一半的受访者表示，其作为治理主体负责数字化转型的职能部门数量有限（三个或以下）。



仅有7%的受访者表示风险治理主体所提供用来帮助他们高效管理风险的数据是真正完整有效的。

企业是否已针对数字化转型定义其风险偏好?

仅有 13%的企业表示，他们已经明确定义了数字化转型相关的风险偏好。46%的受访者表示已经讨论过在数字化转型下的风险偏好，但并没有正式定义或发布此类偏好，还有 33%的企业根本未考虑过专门针对数字化转型去定义风险偏好，这种情况在那些从事数字化项目工作人数不足 1,000 的企业中更为普遍 。



仅有15%的受访者表示其内部审计部门能对数字化转型治理产生巨大影响。

企业是否使用指标来衡量风险?

大约一半（49%）的受访者表示，他们正在整个企业范围内采用运营风险衡量方法来定义风险指标。鉴于本报告第 3 节中着重提及的新兴风险，这些传统指标在数字化环境中能否充分覆盖数字化各领域仍值得商榷。仅有 7%的受访者指出，他们提供给治理主体的各类指标信息是全面有效的，这说明还有待加大此方面的工作力度。

受访者所关注的改善风险治理方法的五大机遇

许多受访者都对如何优化现有风险治理模式发表了意见。其中最普遍的观点是现有风险治理模式应与企业数字化总体战略保持一致，而非独立运行。五大反复提及的观点如下所示：



对那些未受到技术发展直接冲击的利益相关者进行教育——普遍认为，业务团队并不总是能够认识到技术产业变化（无论是数据还是技术方面）对客户体验和品牌声誉产生的潜在影响。提升团队对此类影响的理解程度可有效提高企业的风险识别及管理能力。



消除企业“筒仓效应”——这需要业务、技术和风险团队之间的共同努力，从而避免产生单向的风险治理模式或是个别团队认为定义风险治理模式是其他团队责任的情况。



确定技术应用与实施框架——受访者表示，基于一致的框架及结构有助于实现报告输出的统一性，还可制定协商一致的方法来根据从概念证明到规模的应用以扩大治理工作的范围。建立一致性框架亦可避免风险管理工作是基于项目，而非计划——这可能导致管理方法产生差异。



识别并确认企业相互矛盾的优先事项——无论是在削减成本的同时加快市场化进度，还是在投资全新构筑的同时延长年久失修基础设施的使用寿命，整个企业中存在诸多相互冲突的优先级事项需要得到确认和管理。



明确内部审计作用——从我们的调查结果来看，内部审计为数字化转型提供的保障性作用似乎并不明确，仅有 15%的受访者认为其内部审计职能发挥了显著作用。鉴于该职能所涉及的各类技能，这说明部分企业并未依照一定程度的严谨性及结构化方式开展数字化转型工作。



数字化转型
带来的全新风险领域

数字化转型带来的全新风险领域

聚焦全新风险领域，应对日益复杂的已知风险

毫无疑问，风险格局正持续快速地发生变化，企业自身在戮力管理网络、数据隐私等已知风险的同时，还需了解并解决全新的风险领域。业务团队与技术团队之间的界线日趋模糊，新兴风险领域将比过去传统的技术风险更具战略影响力。

新兴风险的主要来源

在调查中，受访者普遍认为，业务与技术的融合对传统风险管理框架内各类传统风险（非仅限于运营风险）的影响日益增加。现有众多风险框架基于当今技术应用水平之前所确定的主要风险类别而建立，因此仅从这一角度可能不足以评估数字化转型的影响。

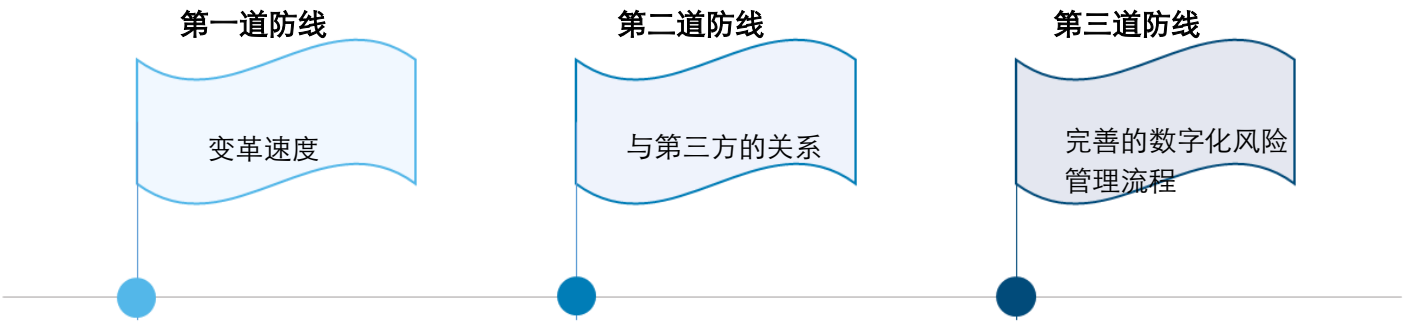
近年来，人们对网络安全和数据隐私愈发关注，企业将新兴风险所涉及的三大领域认定为网络（21%）、数据隐私（17%）和监管不合规（12%），这也并不足为奇。各防线受访者对这三大风险领域的观点是一致的。 但是，一些受访者认为这些领域不再属于“新兴”领域，因为对这些领域的认知度已经很高，而且为降低三大领域相关风险已在多种情况下开展了大量工作。

然而，数字化转型的确进一步加大了这些已知风险领域的复杂性，如数字化资产的不断增加及第三方集成增加了其他网络威胁切入点，数字化资产相关数据的大量使用带来了隐私及道德方面的问题，以及在缺乏规范性监管指导的情况下难以获得监管合规的保障。

除网络、数据隐私和监管不合规三大风险领域外，各防线受访者回答的其他领域有所差异。第一道防线受访者将“变革速度”列为新兴风险的第四个领域；第二道防线受访者为“与第三方的关系”；而第三道防线受访者为“完善的数字化风险管理流程”（见图 8）。出现此类回答合情合理，原因在于运营团队较关注对其交付速度的要求；风险团队更关注扩展企业的影响；而审计团队则关注企业是否提升自身风险管理能力以与数字化企业的发展保持一致。这些都是很有价值的关注点并彰显了跨防线治理和协作的必要性，而这种必要性有助于确保风险补救措施的优先级是根据企业需求而非特定职能而确定的。

是否充分了解新兴风险的影响?

图 8. 除网络、监管不合规和数据隐私外，受访者认为企业的最大风险源类别因防线而异。



风险格局日趋复杂

我们的调查还包含以下洞见，例如会在哪些方面加剧已知风险的复杂性（见图 9），在哪些方面需要新兴技术知识以便从与新技术相关的控制角度（例如云实施相关的逻辑访问控制）了解需要改变之处，以及先期未深入探讨的具体风险——尽管有可能根据现有运营风险类别对这些风险进行分类。上述洞见包括：

- **数字化渠道对不同客户群欺诈风险的影响**——也就是说，如果银行客户仅通过网络或移动设备等特定渠道（而非支行等实体渠道）进行交易，银行客户是否更容易被欺诈?
- **扩展风险**——调查反映出一项巨大挑战，即对数字化职能部门以外团队的依赖性，以及这些团队能否随着数字化职能部门相关数据处理量、客户旅程及变革组合的发展变化而快速扩展。
- **工具类风险**——随着数字化产业的不断发展，支持其发展的工具亦在大量增加。其中许多工具可能在过去并未引起风控团队的关注，因此应仔细考虑对相关工具（如用于代码部署的自动化控制平台）的控制级别。
- **变革延迟风险**——调查显示，许多数字化团队希望更频繁地将变革举措应用到生产环节，但由于企业内某些限制因素而无法得以实施。除了因无法快速实施变革举措而产生的成本及战略风险外，从准备部署到能够部署之间较长的滞后时间通常意味着每次会推出大量累积的变革项目，这导致在事件发生后更难查明问题的症结所在。
- **企业文化和体系架构风险**——随着企业数字化转型架构不断演变，其自动化程度、报告体系及治理结构各异，因而未达最佳标准的组织结构设计将在很大程度上影响企业的交付能力。

创建数字化优势的良机

帮助企业了解并主动管理在数字化环境中不同风险种类之间的相互依赖性（如行为风险、第三方风险与运营风险之间的相互关联），将助力企业提升运营弹性。数据和自动化技术的应用在迅速完成此类工作方面呈现巨大优势。

企业在数字化转型中是否需要重新考量其传统风险框架?

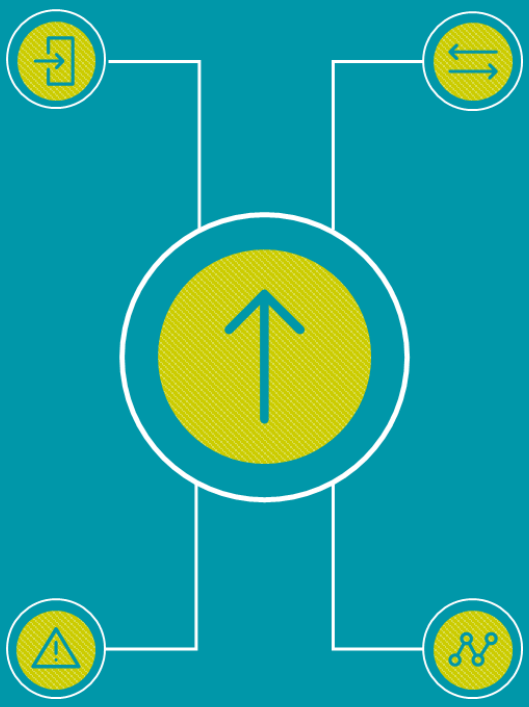
图 9. 传统风险领域愈发复杂

对系统及数据的逻辑访问

交付团队成员所承担的角色越来越多，这说明传统角色在设计、开发、测试、环境控制、发布管理和应用支持等方面的界限日趋模糊。由此提出一个疑问，即当个人需承担多个角色时，“基于角色”的访问控制方法是否仍奏效?

变革管理

数字化产业越发复杂，需求变革的呼声日益高涨，因此采用“一刀切”的方法来管理变革会产生瓶颈问题。



事件管理

代码部署和发布管理等跨不同团队的传统流程日益自动化，谁将在事件中发挥主导作用?

数据治理

数字化渠道提供了大量有关客户行为的数据，由此对商业成功而言，相关数据质量极其重要。而遵循监管要求及道德规范的情况愈显复杂。

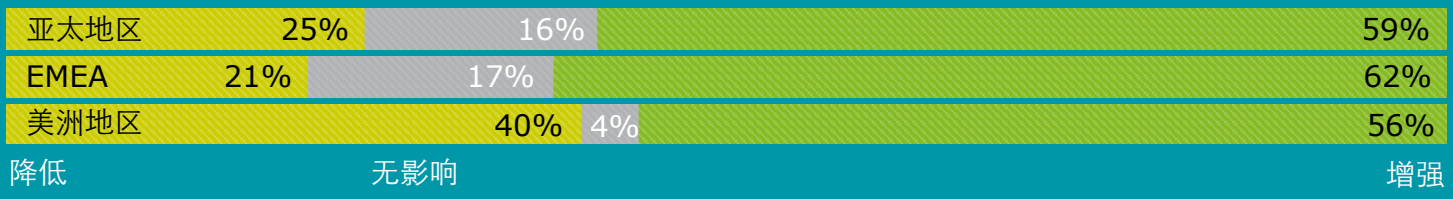
全球视角——受访者认为数字化转型整体会增强还是降低运营弹性?

图 10. 受访结果汇总（按受访者）



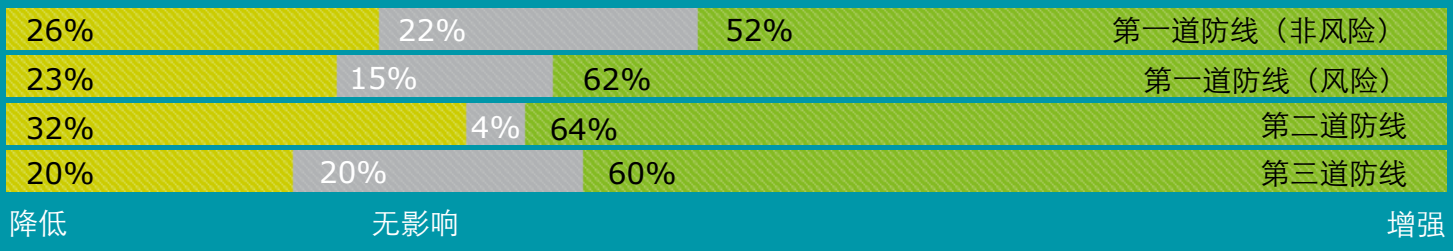
美洲企业倾向于数字化转型降低了运营弹性

图 11. 受访结果汇总（按地区）



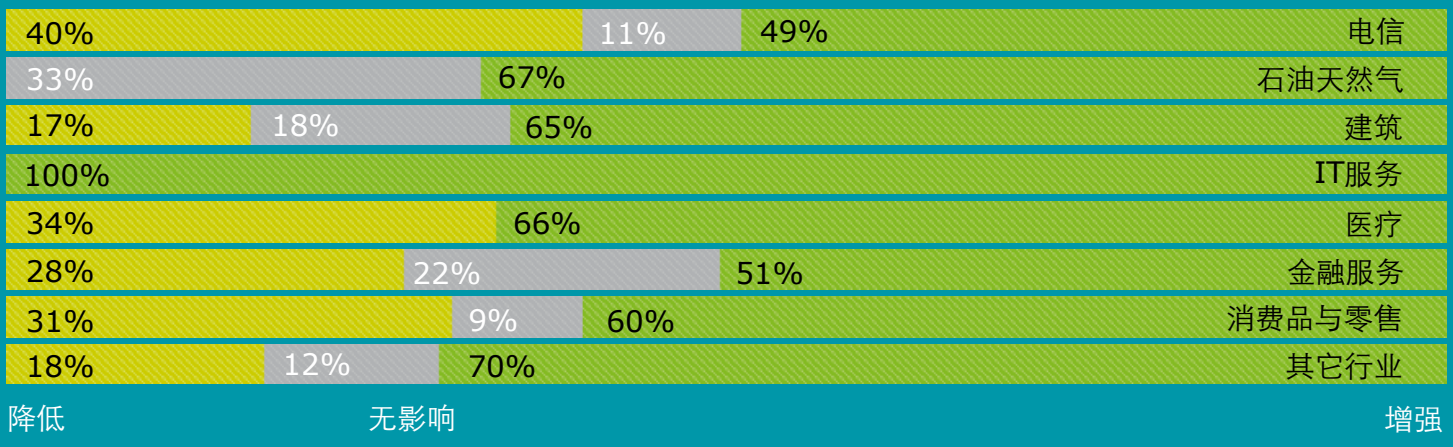
从事风控及审计工作的人员更倾向于数字化转型对运营弹性产生积极影响

图 12. 受访结果汇总（按防线）



科技型企业更倾向于数字化转型正在增强运营弹性

图 13. 受访结果汇总（按行业）



在未来三年，风险格局将如何变化？同时带来哪些挑战？

许多受访者认为，风险格局正迅速变化，在此背景下，企业的应变能力将决定其风险敞口是增加还是减少。

受访者关注的某些主要挑战包括：

- **第三方整合力度不断提高，企业需保持控制力**——企业报告显示，将加大将第三方（无论是成熟的技术供应商或是 IT 初创公司）纳入其价值链的工作力度。我们的调查结果表明，销售与营销、战略与技术部门在整合工作中处于领先地位，并对整合工作从易到难的进展态势有着全方位的认识。相关挑战主要围绕风险治理在安全、业务连续性和数据等方面是否从初期及规模上均达到合理水平，尤其是在风险团队事先未介入或合同早已签订的情况下。应对这些挑战的方法如下所示：将第三方视为合作伙伴而非供应商；较大企业应为初创企业提供技能和资源，以帮助其达到要求水平；在风险团队前期参与的情况下开展概念验证，以确保风险在一开始阶段即受到重视。

- **认识集中风险**——无论将基础设施迁移至单个云供应商，还是将客户旅程关键部分（如入职培训）外包给单个第三方，抑或核心流程自动化、集中化风险、对单一流程或提供商关键依赖，均呈上升趋势。我们在调查中强调的挑战主要是风险归属问题，即由谁来负责了解集中风险并代表企业对该类风险进行监控。

- **变革呈常态，应随之调整运营模式**——持续、渐进地进行变革是产品开发的核心部分。随着变革数量和频率的急剧增加，变革俨然成为部分变革类别的 BAU 流程，但并非全部类别。变革不断推动流程变化（例如增加自动化技术的使用）、文化差异（数字化团队与非数字化团队之间）以及组织结构变化（如增加交付团队自主权，以快速实现变革）。

- **充分监督自动化流程**——通过部署机器人流程自动化（RPA）软件、在端到端客户旅程相关系统之间实现数据流自动化或自动配置环境并运行测试脚本等，可不断提高企业自动化程度。实际上，当前亟待解决的关键问题之一是确定跨多部门自动化流程的责任制，其中涉及企业某些需人工处理的半自动化流程。

- **缩小技术团队以外团队的技术知识差距**——某些企业担忧，数字化产业的变革速度正超越其能够理解和管理相关风险的速度。这对于传统技术风险团队和审计团队而言尤其重要，即技术虽并非其专职工作，但需紧跟技术趋势。



风险运营模式

风险运营模式

在变革与充满不确定性的时代中运筹帷幄

组织结构正缓慢发生变化——数字化转型推动商业模式、技术实施方法、流程和工作方式的革故鼎新，以及组织结构的不断演变。这种持续性变化对确定风险归属及问责制，以及执行核心风险管理流程并将这些流程应用于企业不同环节提出了挑战。传统的风险管理功能模式须相应地进行调整。

颠覆性技术的应用如何变革运营相关风险管理的需求?

我们的调查显示，在企业适应数字经济过程中，风险管理活动无疑也在不断变革。所有受访者中最普遍认可的影响包括：

- 与回溯性鉴证相比，持续性监测需求愈显重要（47%）
- 对技术的需求更多（46%）
- 需重新定义风险与控制的项目模式（46%）
- 需为每项颠覆性技术量身定制风险管理方法（42%）

虽然这四大影响在受访者中被广泛认同，但在本报告所述不同防线中存在某些差异。

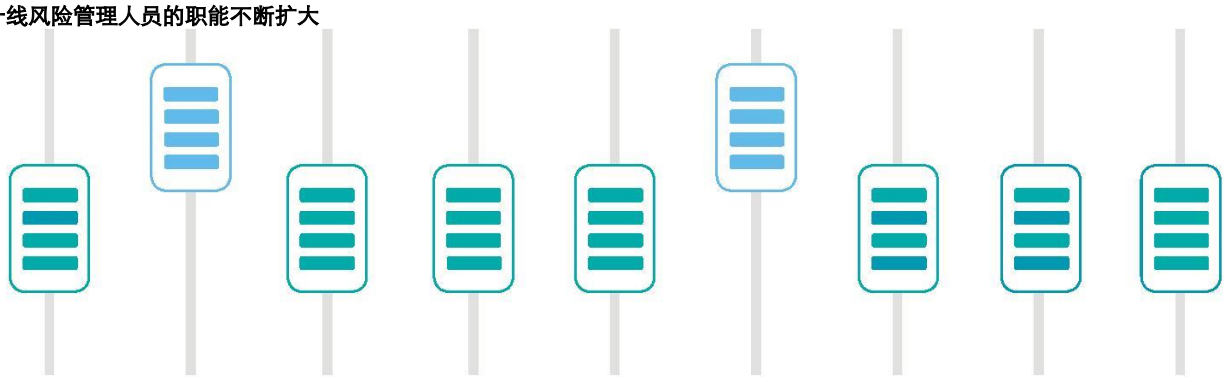
第二道防线和第三道防线的受访者把重新定义项目模式作为优先事项，这表明这些团队认识到需改进与运营团队的沟通方式，以确保模式行之有效。而在第一道防线担任非风险角色的受访者则把持续性监测的重要性放在首位。这是意料之中之事，原因在于第一道防线的利益相关者更加重视来自风险团队的洞察——此类洞察推动日常调整升级与决策，而非回溯性的时间点干预措施。

有趣的是，身处第一道防线风险岗位的受访者将对技术的更多需求作为其首选，并将“提速”需求视为前四大影响。这是可理解的，因为他们可能需要处理日常技术问题。

风险管理职能角色的诸多变化增加了一线风险管理的重要性，以及运营团队和变革团队对风险能力的需求。一位受访者巧妙地将这些变化概括为 “赋能作用”，而非仅是传统意义上由风险职能发挥的“保护作用”。

开展一线风险工程与风险分析

图14. 一线风险管理人员的职能不断扩大



风险管理职能的作用及职责范围将如何演变?

调查受访者迅速指出，传统风险管理活动的总体目标依旧重要，但执行方式正发生变化，以便目标结果更好地契合高级管理层的需求——即执行方式需具备主动性、预防性与预测性，而非被动的、回顾性的与需经检测的。这意味着，风险管理活动正在不断演变，本调查关注的主要变化如下所示：

- **更多地参与到解决方案设计中**——有明显的迹象表明，风险团队的职权范围正在扩大，扩展范围涉及“制造者”——即负责交付产品和解决方案的数字化交付团队，而产品和方案有助于推动数字转型带来诸多变革。对于企业而言，在开始阶段即从风险与控制的角度设计解决方案有助于其大幅降低鉴证成本；

- **更加重视数据分析**——当前呈现的普遍趋势是，管理层期望获得预测性分析，而非检测性结果，因而更加依赖数字化环境中生成的数据进行分析。

- **风险覆盖范围扩大**——受访者指出，数字化转型正日益触及企业的诸多领域，随之扩大了风险团队需要了解和挖掘的潜在风险数量。这表明，对熟知数字化企业的风险团队领导者的需求正在增大；

- **将控制措施嵌入到流程自动化方案中**——随着企业不断扩大自动化的使用范围，某些领先企业正积极探索将控制措施嵌入到新建的自动化流程中，由此可将手动且周期性的鉴证模式变革为自动化持续的模式；

- **摆脱每年瀑布式的鉴证周期**——许多传统的鉴证计划遵循年度周期，逐年实施重复性的既定计划、测试、报告和整治活动，以确保管理层有效执行控制措施。各企业正在探索如何制定出一种可持续、敏捷的鉴证方法（见图15），这种方法可通过可视化手段来为决策提供有效信息，而非两年一次的鉴证报告。

创建数字化优势的良机



通过设计自动化控制措施来降低鉴证成本的潜力巨大。如果设计得当，这将使鉴证团队能够专注于自动化控制的设计，而非进行成本高、人工且基于样本的运营有效性测试。

敏捷工作方式的差异对企业有何影响?

我们的调查结果表明，很少有风险管理职能部门能够成功采用敏捷文化，仅有9%的受访者表示其风险管理职能部门成功采用了敏捷文化。这与我们在数字化交付团队中看到的情况形成了鲜明对比，敏捷文化已经在此类团队中成为默认的工作方式。这种采用差异在某种程度上说明了为什么超过一半的受访者（55%）认为其采用敏捷文化不成功，或仅在针对敏捷交付调整风险管理技术方面取得了有限的成功。一些受访者表示，其风险团队在评估敏捷交付相关风险时，某些情况下“甚至未能发挥有效作用”。我们的观察反映了双方的挫败感——数字化交付团队认识到，从战略上来说，企业的延迟成本很高，因此希望更快地交付项目，而风险团队则担心，在没有明确说明如何保持正确控制水平的情况下加快交付所带来的负面影响。

仅有9%的受访者表示，他们的风险管理职能部门成功地采用了敏捷文化。



当被问及企业在针对敏捷性交付而调整风险管理技术方面有多成功时，55%的受访者表示“不成功”或者“努力后的成效有限”。

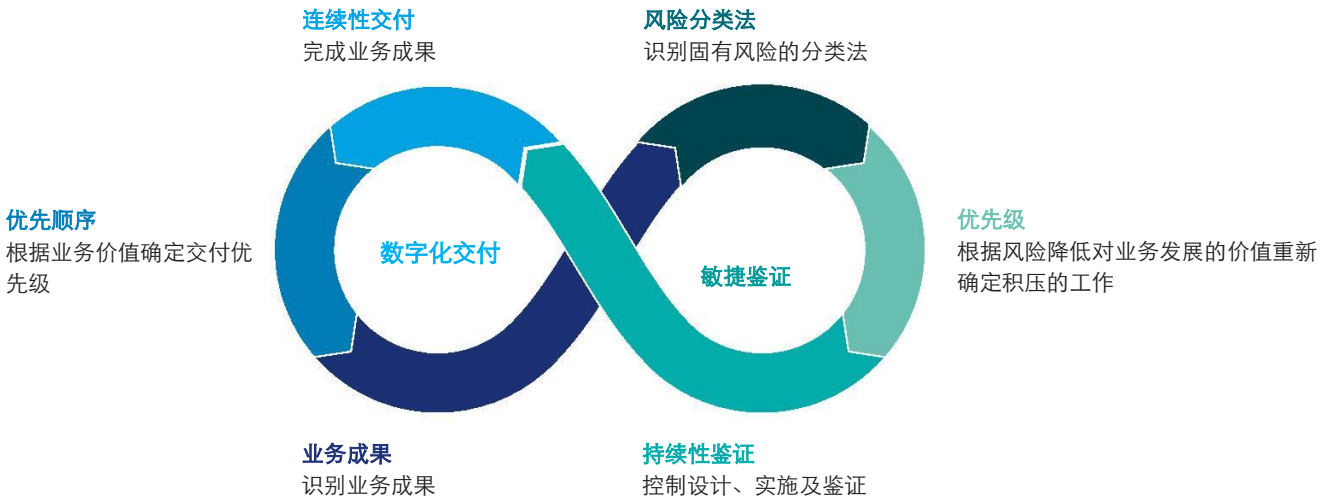


创建数字化优势的良机

鉴于开发全新数字化产品和解决方案所需的投资金额，风险团队需采取行动以明确其与数字化交付团队的合作模式，并通过缩短企业变革时间及降低相关成本来彰显其所能提供的价值。

何为敏捷鉴证?

图 15. 敏捷鉴证模型遵循的原则



何为未来管理风险的运营模式?

当人们尝试将为前数字化时代设计的运营模式来管理现今风险环境时，会发现这样的做法并不理想。我们认为，对于希望从自身风险管理能力中获得较大价值的企业而言，可能需要一个真正的跨领域模式——未来构成风险管理能力的潜在要素包括：

集中化能力

- **技术智能**——经验丰富的技术专家，他们了解与各类技术及企业架构相关的风险，能够监督风险分类的完整性和一致性。
- **数字风险解决方案工厂**——软件工程师，他们能设计、建造、测试和部署解决方案，无论是基于技术开展风险管理活动，抑或在现有技术栈中建立有助于持续监测的风险与控制框架。
- **风险运营**——风险与控制专家，他们能设计和运行核心风险管理流程，向解决方案制造者反馈需求，并提供“服务平台”功能以帮助运营人员在日常对风险进行管理。
- **风险分析**——数据科学家，他们在大数据分析领域经验丰富，可将不同数据集融合在一起进而主动识别潜在风险（例如，与不同数字化渠道均有关联的欺诈交易）。
- **风险经验**——服务设计专家和产品经理，他们与内部利益相关者合作开发并改进风险产品，由此消除矛盾并提高整个企业对于风险流程的满意度和参与度。详见图16。
- **风险与控制鉴证**——集中化鉴证能力，即可代表其他团队开展独立的鉴证工作，不受相关团队在企业中所处位置的影响。

非集中化能力

- **产品/服务/渠道风险责任人**——经验丰富的数字风险专家，他们负责在技术层面和商业层面管理与特定产品、服务或数字化渠道相关的风险。
- **风险团队**——跨职能团队，他们由来自不同领域的成员组成，旨在短迭代中实现特定目标，即控制设计迭代、控制实施任务或风险补救迭代。

由数字化驱动的人工任务

案例研究——控制库质量和覆盖率的自动化评估解决方案

一位客户希望审查其控制库中记录的8,000多个控制项的质量，预计人工操作将花费26周。然而，采用德勤自动化控制库评估工具“控制智能”（Controls Intelligence）可在45分钟内上传并分析8,000个控制项。

基于根本原因分析法，可制定补救路线图并深入了解补救优先事项。经调查发现，某些团队在控制创建方面低于标准，因此可对这些团队进行相关培训。

继续前行中，风险团队如何充分发挥其能力来实现转型?

诸多行业总是专注于成本，这使除维持运营所需的资金外，为变革计划筹集资金变得愈发困难。因此，企业如何使现有团队充分发挥其自身能力来逐步达成最终目标，俨然成为需要解决的问题。我们可对三大重点领域进行探讨：

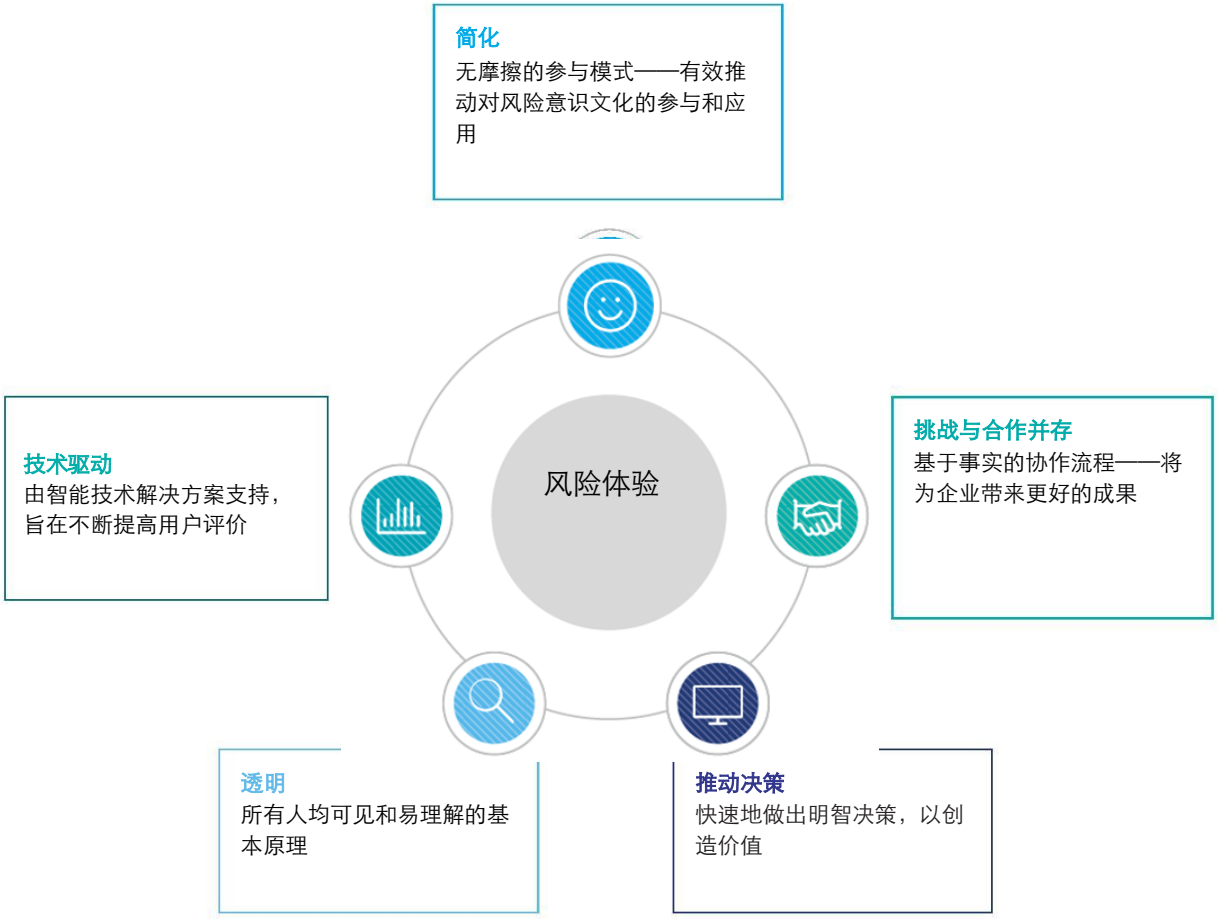
许多日常的风险管理活动仍靠人工执行，但此类活动可由技术驱动——这包括风险报告相关数据人工处理工作、风险状态的及时更新、现有控制库覆盖范围评估、对世界各国的控制评估执行质量保障。其中许多活动可通过低成本的技术解决方案加以改进（详见上一页的案例研究）。

与企业现有的技术专家建立合作关系——许多企业将拥有越来越多的技术专家，他们致力于开展有效的控制以推动更多技术被深入采用。风险职能部门可主动确定相关专家并与其建立合作关系。

继续减少低价值的工作——任何具备多步骤的流程均存在可优化之处。基于“精益”的思维来重新审视现有流程，则可能将有价值的资源重新导向更多价值创造活动中去。

提升风险体验

图16. 通过技术推动，在企业内获得更好的风险体验





运用颠覆性技术数字化管理风险

运用颠覆性技术数字化管理风险

一个很大程度上尚未被发掘的机会

大规模管理风险是一项复杂的任务。虽然某些行业在应用技术管理风险方面较其他行业更为成功，但许多企业仍依赖独立运行的传统系统或电子表格来管理关键资产和流程，如风险分类、控制库和风险评估。应用新的现代技术从风险管理投入中获得更高价值的机遇正在显现，但为了使相关计划成功实现，必须夯实好基础——即建立好一致且易被理解的风险分类、控制库和完善的流程，其中最重要的是明确好风险归属及责任划分。

现行风险管理工具效果如何?

我们的调查显示，从整体来看，在总分设定为10分的情况下，**60%**的受访者对现行风险管理工具的有效性评分为五分或更低（**77%美洲地区、56%EMEA、59%亚太地区**）。评分结果令人担忧，这说明企业无力应对数字化转型在提升变革速度、增加复杂性和加大风险活动量等方面所带来的变化。

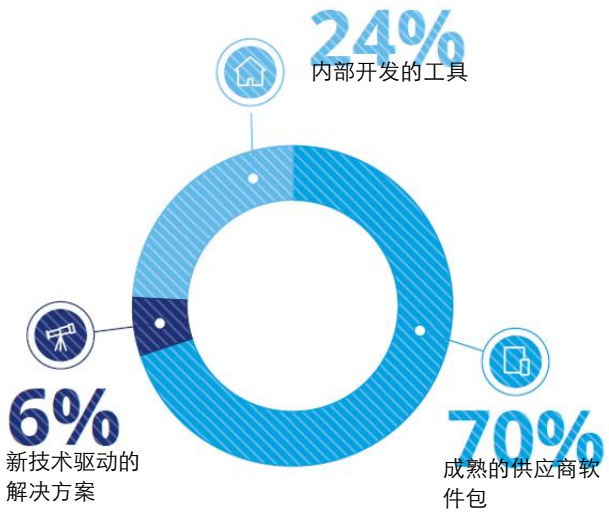
当被问及妨碍企业提高风险管理工具有效性的相关壁垒时，受访者提到了某些关键问题：

- 对当前可能发生的情况缺乏了解，也没有时间去思考
- 无法将工具与传统系统和软件包相整合
- 运营工具与风险管理框架及流程之间缺乏一致性
- 数据质量低下
- 变革速度使各团队和职能部门难以就方法及工具达成共识
- 企业控制框架结构存在的差异使各团队和职能部门难以收集数据
- 难以阐明投资风险管理工具的商业作用
- 对变革的文化抵制。

值得注意的是，上述壁垒几乎不与技术能力的匮乏相关。从这些壁垒可以看出，工具缺乏有效性的根本原因更多地与潜在风险管理框架、流程、责任划分模式、决策者技术知识和企业文化等有关。这说明，如果企业能解决这些方面的问题，那么技术将在提升其风险管理能力方面发挥巨大的作用。

技术工具

图17. 采用颠覆性技术的企业所使用工具的类别



有多少企业运用颠覆性技术管理风险?

调查显示，大约有五分之一的企业在风险管理生命周期的核心阶段运用了颠覆性技术——风险识别（19%）、风险监控（21%）和风险报告（17%）。当前试用方法的企业（35%）正构建用例以扩大适用范围，由此我们预计这个比例会得以提高。

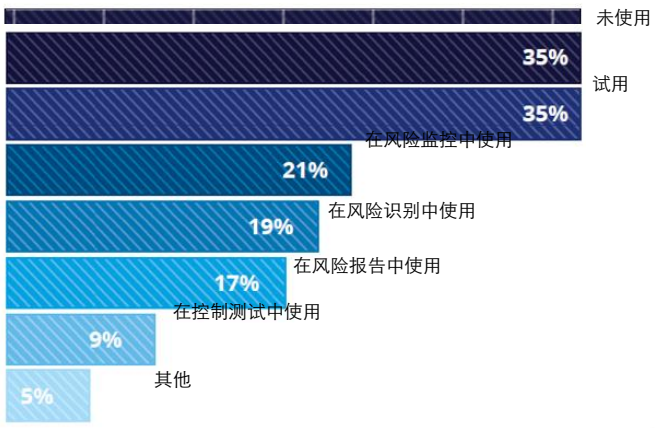
当被问及使用现代技术的具体用例时，受访者给出的例子主要涉及反洗钱、欺诈和网络等利用先进分析功能的领域。目前，采用技术已能对整体数据集进行分析，而在过去采用的是基于采样的方法，这对于通常大型的运营数据集而言是合乎逻辑的起点。

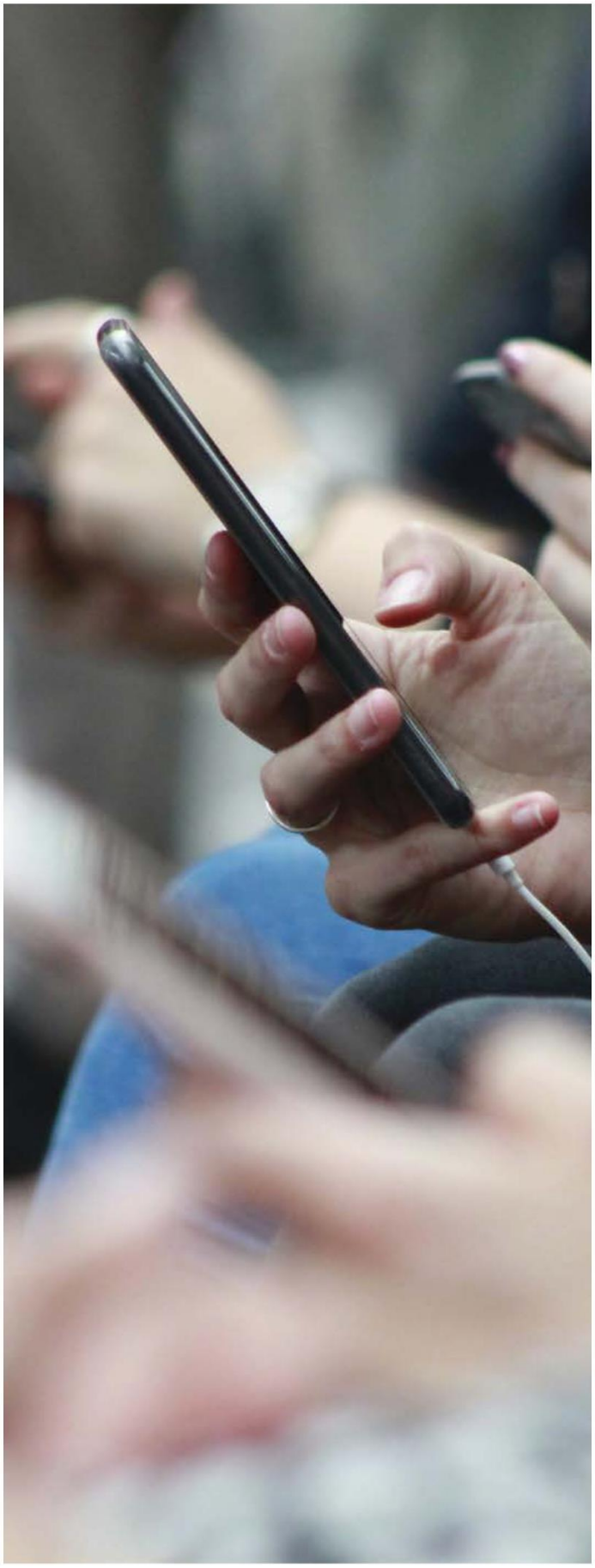
在上述领域，新技术还带来了明显的商业优势，例如欺诈性支付的百分比显著降低，这证明对此类技术的前期投资是非常合理的。调查结果显示，大多数企业极度依赖成熟的供应商软件包（70%），鉴于上述用例，这是意料之中的（见图17）。

调查报告中还列出了许多典型的人工型风险管理流程相关新兴用例（见图18）。其中，仅有9%的受访者表示将新技术应用于控制测试等涉及大量人工的鉴证活动中，因此有待进一步提高效率。

从涉足到实践

图18. 运用颠覆性技术管理风险





风险管理工具现状产生的影响

毫无捷径可言——事实证明，识别和整合支持风险管理的恰当工具组合是非常困难，而且在一定程度上，随着数字化转型推动企业文化、流程、架构和技术的变革，这似乎愈发困难。业务及技术团队、风险经理和企业风险团队在管理风险方面均发挥着重要作用，但他们常常面临不同的需求、压力和要求，这导致调整风险工具战略的工作变得越加困难。

虽然为特定用例（如欺诈分析）设计技术解决方案是相当容易的，但当涉及到跨团队或部门地支持人工风险管理流程和需一致的聚合框架来按层级进行汇报时，我们发现诸多企业存在难处。许多企业的常规做法是使用现有工具并辅以人工合并、分析和报告等手段来汇集不同的数据源。这或许可以解释我们调查中所提到的对效率低下的评价，尤其是在风险管理工具极为有效且人性化并成为日常工具而对其期望值大大提高时。同时，鉴于数据是经人工汇集的，这也在一定程度上解释了为什么受访者对提供给治理论坛相关信息的充分性给出了较低的评分。

当前格局产生的主要影响是，管理层可能更难发现问题的本质，因此影响其专注于最重要的事情上及做出降低风险的正确决策。在许多情况下，监管、网络等风险最常发生的领域均受到积极监控，但其他不大明显或直接的风险类别可能未被充分管理，由此可能损害企业的相关价值。

调转话题——有效风险管理系统的需求到底是什么，如何利用技术来发现相关需求?

从颠覆性技术运用到特定风险管理用例，其间蕴涵的潜在价值愈发明朗，但许多企业可能希望，在大规模投资新的解决方案之前重新审视其稳健的风险管理文化基础。需考量的某些关键问题包括：

- 各级文化是否真切理解企业管理好风险的价值，以及各层人员的需求是否明确?
- 内在风险分类是否在整个企业内得到一致了解，是否与反映实际情况的控制库相一致?
- 企业风险管理流程是否成熟可靠，一线团队是否了解如何将其应用于日常工作?
- 是否拥有流程对数据进行分类和提高数据质量，而非仅用于获取和报告数据?
- 合理的决策流程和升级路线是否得以明确，是否根据正式的风险治理管理层要求进行了相应调整?



随着更具现代化的技术解决方案成为主流，由此将开启哪些新的可能?

我们发现，需利用现代技术对“工具如何支持风险管理日常工作”进行重新定义的情况越来越多：

- **通过设计，利用投资流程自动化嵌入控制措施**——许多企业开始实行自动化计划，无论是通过机器人流程自动化，还是核心IT流程（如发布管理）的自动化，从流程建立之初就嵌入控制措施，这将切实减少对人工型鉴证工作的需求及相关成本。

- **在日常运营工具中嵌入控制视图**——根据企业风险框架，在日常使用的运营工具（例如，用于维护面向客户服务或监控数字化渠道的可用性）中构建控制效果视图，或许有助于管理层通过某种能被更多风险管理角色容易理解的语言来展现是如何管理风险的。

- **通过整合来自不同系统的数据，获得新的见解**——一般情况下，实时服务通过将来自不同团队的多种流程相结合来提供。企业筒仓效应通常会阻碍知识和数据的有效共享，但当这些知识和数据与来自另一个团队的知识和数据相结合时，可为产生洞察提供有价值的依据。举例而言，将某个事件的数据与控制库的数据相结合来了解发生的问题。

- **技术赋能人工风险管理生命周期**——从基于评估识别到补救与报告，风险管理活动始终存在需人工完成的部分。依托技术而非电子表格来执行此类人工流程，可通过有效的分类、跟踪和监控补救措施来提高数据质量，实施连续一致的工作流来了解决策和自动化处理报告。

- **改善用户体验**——许多企业致力于改善其风险管理文化，和增进对完善风险管理措施所产生价值的理解。简而言之，为推动这两方面的变革并吸引劳动力，所采用的工具需要把简单的事情做好。人们势必希望使用可获得的工具，因为这会使其生活更加简单轻松。

- **推动协作**——线框图等协作工具和技术的应用对于设计数字化方案而言十分必要，此类应用可根据用户需求来确定内容形式和最合适的布局（如网页布局）。在风险场景中也可采用类似的方法和概念来改进关键风险报告的格式和布局，从而使通常由数据结构驱动管理层能够专注于正确的事项上。

创建数字化优势的良机

对风险管理相关行政层面进行自动化对于企业而言是一个巨大机遇，其由此可提高数据质量、加速决策、更多地从战略层面思考问题，而非仅出于维系运营。



人才

人才

最大的数字化风险是人才风险吗?

尽管围绕颠覆性技术对人才未来影响一直被不断讨论，但一个企业能否充分利用人才资源，将始终是决定其成功的关键驱动力。人才是企业工作的核心，虽然让合适的人员担任恰当的角色一向都是至关重要的，但现在让合适的人员管理风险比以往任何时候都更加重要。

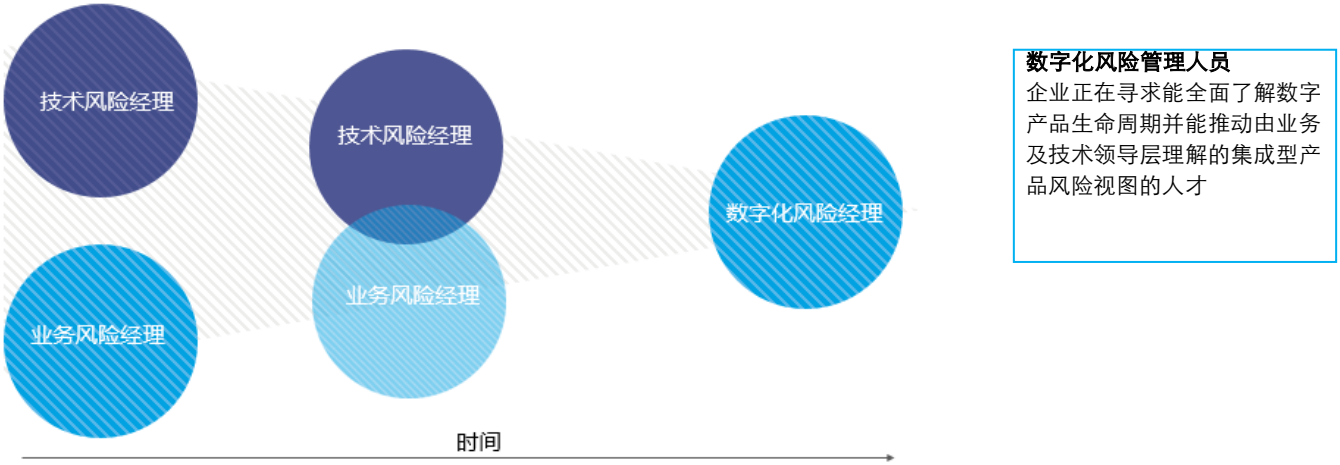
在日益错综复杂的环境下，重新审视技术风险管理人员这一传统角色是否已刻不容缓?

技术不断进步、变革步伐日益加快和企业各层面就优先事项达成共识及调整所面临的挑战，均导致管理技术风险日趋复杂。因此，领导层对其现有团队是否具备适当技能在数字化企业中管理风险缺乏信心——我们将其称之为信心落差，这也就不足为奇了，而仅有19%的受访者对其团队具备此类技能“充满信心”（见下图19）。

我们的调查结果显示，风险管理人员岗位愈发侧重于影响企业中的其他人员并与其相互协调、协作和沟通，这通常超出了风险职能本身，即“风险管理人员”这一职称意指的那样仅承担管理风险的职责。

产生信心落差的原因 ——数字化风险管理人员崭露头角

图 19. 在数字化交付团队中，业务团队与技术团队的整合度日益提高，从而促发了对数字化风险管理人员的需求

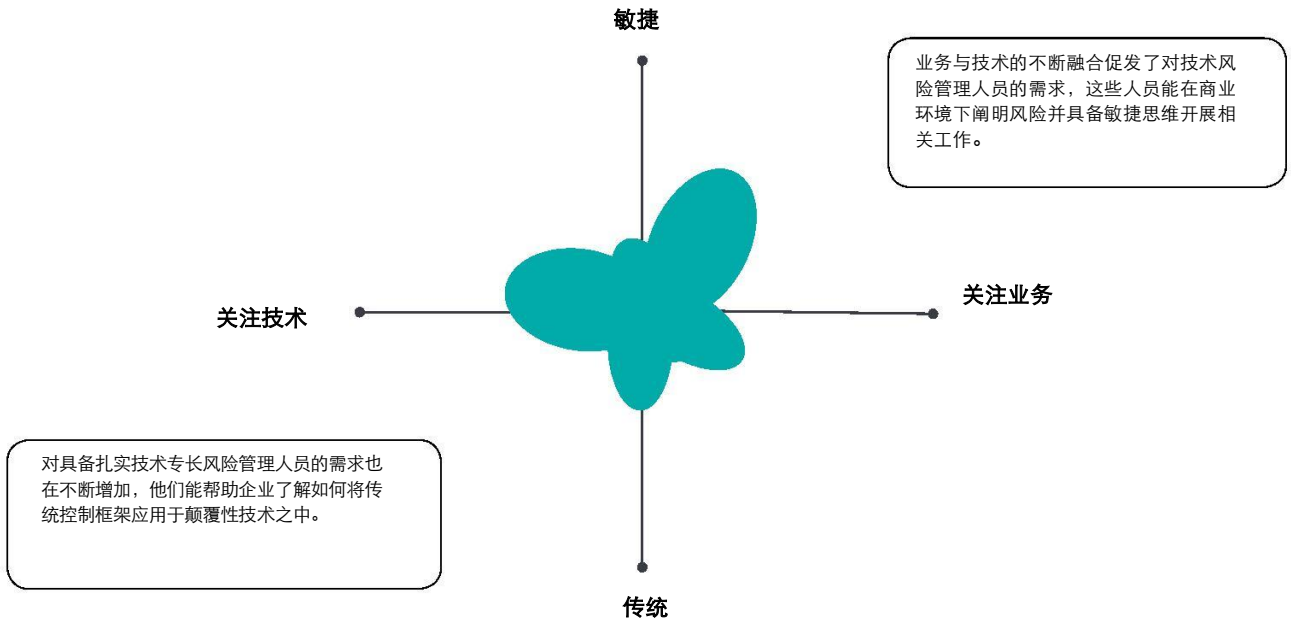


对风险管理人员技能要求发生了哪些变化？

我们的调查显示，在招聘技术风险岗位相关候选人时，最重要的技能要求是技术与业务经验（72%）+先期风险管理经验（66%）。更有趣的是，数据显示，招聘具备特定技术经验（49%）和“敏捷”思维解决问题（46%）的候选人愈发重要。我们称之为“蝴蝶效应”，因为传统的风险管理人员技能要求已扩展至更加重视技术+商业技能，以及在敏捷和传统的企业环境中适应及发展的能力（见下图20）。

这些附加技能在最难招募的技能排名中也很高，如果优先考虑具有相关先期经验的候选人，则意味着企业或许正继续从其以往招募的同一群人员中开展招募工作。这可能会使企业受限于招募仅具有传统风险管理职业技能的人员，很难招募到具备新近所需技能的候

图20.当今运营环境是如何改变风险专业人员所需技能的



创建数字化优势的良机

- 明确需求——明确所需技能，有助于在正确渠道寻找候选人。可考虑在传统招聘渠道之外招募相关人才。
- 设置灵活的岗位要求——对候选人必须具备的风险管理经验进行限定，这可能会阻碍招募到具备所需技能的候选人。
- 了解所需候选人的需求——这有助于候选人主动上门应聘，而非被动地搜寻他们。

未能缩小技能差距所产生的影响

我们的调查表明，在过去数年中，应对不断变化的风险格局所需的技能与传统技术风险管理人员所具备的技能之间差距在不断扩大。 无法缩小此类差距的企业可能会意识到愈加难以有效地管理风险。数字化转型将继续颠覆众多行业，我们认为，对于那些在风险管理能力上缺乏核心技能的企业而言，存在五大关键影响：

- **新技术的采用缓慢，变革实现步伐缓慢**——我们的调查强调，缺乏人才是扩大颠覆性技术应用的主要壁垒之一，也是缩短将创意转化为实际解决方案所需时间的关键障碍。 这凸显了业务需求与人才战略相匹配的重要性。

- **企业中的风险盲区**——由于缺乏识别、理解和管理风险所需的知识和经验，或具备相关经验和知识的人员不认为是其责任管理风险，导致某些风险无法得到管理。

- **缺乏对企业基层风险管理活动的参与**——最成功及成熟的企业能够使日常管理风险的一线团队与企业运营风险流程相对应。专业风险管理人员的技能和影响力在促进此过程中发挥着至关重要的作用。

- **在未纳入风险职能部门的情况下，风险管理资金被重新分配**——由于企业其他职能部门负责确定更有效的鉴证流程，无法展现其所创造价值的风险管理职能部门可能会被削减资金。

- **难以留住优秀人才** ——随着第一批“数字原住民”担任高级管理职位，对顶级人才的需求日益加大，企业应使风险管理职位长久具备吸引力，以保留优秀人才。 行业领头羊不断给出具有吸引力的薪资，许多优秀人才不会坐等所在企业“迎头赶上”。

人才策略——短期内如何充分利用现有人才库?

- **利用人们固有的求知欲，提供与业务需求相匹配的框架**——对与时俱进的需求从未如此迫切，但每个人都想通晓一切并不可取，这将适得其反。

- **入职流程中嵌入风险意识文化**——当企业受雇员工来自其他行业时，在员工从非监管行业跨入受监管行业的

- **培养风险管理人员在日常工作中应用“数字化”技能**——“数字化”技能以及研究用户行为、定义问题陈述、制定解决方案、执行可行性测试等相关能力，均可用于更新风险管理方法和提供鉴证。

- **了解获取人才的不同渠道**——如今，有效管理风险所需的技能十分广泛，尽管“风险管理人员”这一岗位是普遍存在，一个人不大可能拥有全部这些技能。 因此，能获得广泛的技能和迅速增减资源变得越发重要。

- **除了风险管理人员外，还出现了风险导师一职位**——鉴于诸多行业变革的规模和复杂性，我们在调查中发现了“风险导师”这一岗位，该岗位由企业内经验丰富的人员担任，他们向同事就风险管理中易犯的错误及策略提供相关建议。

长期战略——设定企业风险管理目标，不仅仅针对风险职能部门

企业欲建立可持续的运营模式，以在技术团队中长期嵌入正确的风险管理文化和行为方式，因而在过去15年变革中存在一些重大问题需得到解决。事实证明，对于许多企业而言，在保持其各风险团队适当独立性的同时，又相互间跨不同防线地开展良性协作，是面临一项挑战。

许多企业希望拥有既能保护自身又能促进绩效和增加附加值。为此，许多企业制定了风险管理目标，该目标涉及对文化进行变革，以及应用高级分析方法、自动化和人工智能等全新技术来提供实时洞见，从而助力决策制定。

无论实现目标的方法是自建、合作还是购买，企业的成功都可能取决于是否制定了正确的人才战略。仅聘用最优秀的人才是不够的， 肩负实现目标任务的领导层需能在短期内轻松应对不确定性并擅长影响及与企业内其他人员相互协作，以便这些人员能够为其团队提供实现目标的平台。

全球其他地区正开展哪些工作?

图21.受访者提及的人才计划示例

加拿大



开展有关精益原则的正式培训并提出“风险小队”的概念

英国



反向辅导：即由精通数字化相关知识的初级员工对缺乏此类知识的高管进行技术辅导

挪威



风险和技术团队共同参加课程和会议，以形成对风险的共识

日本



与其他组织机构共享知识，旨在综合各专业知识领域

爱尔兰



正式定义了数字化学习途径，以鼓励所有员工保持统一的知识基础

卢森堡



与其他部门定期举行研讨会，以鼓励合作、知识的共享与透明化

意大利



以“学会学习”为原则，着重开展由员工主导的学习

澳大利亚



轮流借调风险管理人员至技术岗位并跨防线

新西兰



多元化——无专门设定从事风险管理的员工

走上正轨后有哪些裨益?

在过去的10年里，技术从根本上重新定义了我们许多人的生活。当前，我们正处于这样一个时刻，即许多从小伴随科技长大的数字原住民开始步入高级管理层的职业阶段。对于企业而言，这将是其制定长远计划的巨大机遇——他们可针对未来二十年建立数字化风险能力、吸引精通数字化技术的人才并向顶尖人才提供职业发展平台。这一领先群雄的契机不可能持续长远，稍纵即逝。

运营环境日趋复杂，能够简化风险管理方法而被广泛理解并融入日常活动的企业，更容易将建立运营团队“自我识别”和管理风险文化，而无需专门设定风险管理人员来应对风险。

数字化风险管理工具

图22.数字化风险管理人员角色的复杂性



创建数字化优势的良机

在一定程度上，企业在风险管理方面最大的人才问题可能并不在风险职能范围之内。与企业其他岗位相比，担任风险管理职务的人员往往存在多对一的情况。因此，我们认为，企业可通过让传统风险管理团队及岗位之外的相关人员从风险和控制的角度思考问题来改善其风险状况。

作者及参与者

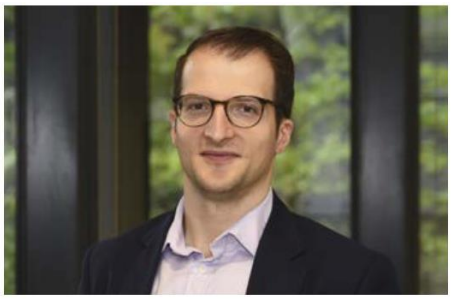
作者



Rob Dighton
总监
科技与数字化风险
rdighton@deloitte.co.uk



Cherry Seaborn
经理
科技与数字化风险
cseaborn@deloitte.co.uk



Dimitar Milanov
高级经理
科技与数字化风险
dmilanov@deloitte.co.uk

其他参与者



Stephen Ley
全球领导合伙人
科技与数字化风险
sley@deloitte.co.uk



Tom Bigham
合伙人
科技与数字化风险
tbigham@deloitte.co.uk



Charlotte Gribben
合伙人
科技与数字化风险
cgribben@deloitte.co.uk

全球联系人

美洲地区		
巴西	Rodrigo Mendes Duarte	rodrigomendes@deloitte.com
加拿大	Nathan Spitse	nspitse@deloitte.ca
加勒比和百慕大国家	Brett Henshilwood	brett.henshilwood@deloitte.com
智利	Oscar Bize	obize@deloitte.com
拉斯科	Jorge Hernandez	jorgehernandez@deloitte.com
墨西哥	Doris Gomes	dorgomes@deloittemx.com
美国	Daniel Soo	dsoo@deloitte.com

亚太地区		
澳大利亚	Jonathan Goldman	jonathangoldman@deloitte.com.au
中国	Tonny Xue	tonxue@deloitte.com.cn
印度	Vishal Jain	jainvishal@deloitte.com
日本	Shoichi Morimoto	shmorimoto@deloitte.com
日本	Yasuhide Onuma	yasuhide.onuma@tohmatsu.co.jp
新西兰	Reenesh Bhana	rbhana@deloitte.co.nz
新加坡	Philip Chong	pchong@deloitte.com
新加坡	Vineet Sinha	vsinha@deloitte.com
台湾	Mike I. Chang	mikeichang@deloitte.com.tw

EMEA		
奥地利	Alexander Ruzicka	aruzicka@deloitte.at
比利时	Johan Van Grieken	jovangrieken@deloitte.com
塞浦路斯	Chrysovalantis Dikomitis	cdikomitis@deloitte.com
芬兰	Tuomo Salmi	tuomo.salmi@deloitte.fi
法国	Gregory Abisror	gabisror@deloitte.fr
德国	Alexander Huffer	ahuffer@deloitte.de
爱尔兰	Colm McDonnell	cmcdonnell@deloitte.ie
以色列	Simeon Zimbalist	szimbalist@deloitte.co.il
意大利	Giuseppe Mazzotta	gimazzotta@deloitte.it
意大利	Andrea Schiavon	aschiavon@deloitte.it
卢森堡	Irina Gabriela Hedea	ighedea@deloitte.lu
马耳他	Ivan Spiteri	ispiteri@deloitte.com.mt
中东	Tariq Ajmal	tajmal@deloitte.com
荷兰	Marko van Zwam	mvanzwam@deloitte.nl
挪威	Erling Pettersen Hessvik	ehessvik@deloitte.no
西班牙	Manel Carpio	macarpio@deloitte.es
瑞士	Michel Simantirakis-Aller	msimantirakisaller@deloitte.ch
土耳其	Cuneyt Kirlar	ckirlar@deloitte.com
英国	Charlotte Gribben	cgribben@deloitte.co.uk
英国	Tom Bigham	tbigham@deloitte.co.uk
俄罗斯	Denis Lipov	dlipov@deloitte.ru
南非	Keshnee Naidoo	kesnaidoo@deloitte.co.za

注释

Deloitte.

本报告所含内容乃一般性信息，我们建议您在根据本报告任何内容采取行动或未采取行动之前获得专业意见。Deloitte LLP不对任何方因本报告中任何材料而采取任何行动或未采取行动所导致的任何损失承担责任。

Deloitte LLP是一家在英格兰和威尔士注册的有限责任合伙企业，注册编号OC303675，注册办公地址1 New Street Square, London EC4A 3HQ, United Kingdom。

Deloitte LLP是Deloitte NSE LLP位于英国的附属公司，为德勤有限公司（一家英国私人担保有限公司）的成员所。德勤有限公司及其每一家成员所均为具有独立法律地位的法律实体。德勤有限公司和Deloitte NSE LLP并不向客户提供服务。请参阅www.deloitte.com/about了解更多有关我们全球成员所网络的信息.

德勤368设计并出版. J18483