KPMG

Third Party Risk Management outlook 2020

Ser criativo transforma negócios

KPMG International

home.kpmg/thirdpartyrisk

Conteúdo

Introdução

As organizações dependem cada vez mais de fornecedores terceirizados para oferecer produtos e serviços essenciais aos seus clientes. Elas também estão descobrindo que falhas de terceiros podem manchar rapidamente suas reputações e ter implicações operacionais e de custos significativas. À medida que as organizações tratam de suas preocupações em torno dessas questões, fica evidente que elas precisam de uma estratégia clara para a seleção, aprovação e gerenciamento de terceiros. Como há diversas partes envolvidas, desde o negócio, bem como as funções de aquisição e supervisão de risco, desenvolver e implementar esta estratégia continua a ser altamente desafiador.

De forma simples, o Third Party Risk Management (TPRM) é o programa que uma organização usa para avaliar e gerenciar seus riscos apresentados por produtos e serviços de terceiros. Por exemplo, com relação a um contrato em que os dados de uma organização estão sendo armazenados nas instalações de terceiros, a organização precisa avaliar o risco da segurança dos dados. Um programa TPRM funcionando adequadamente envolveria o diretor de Segurança da Informação da organização - como gerente de risco de segurança de dados - no processo de aquisição antes da contratação. Ao fazer isso, é possível determinar:

- Como o terceiro irá acessar, armazenar ou transmitir os dados da organização
- Que se tenha um ambiente de controle que atenda às expectativas da organização ou precise ser aprimorado
- Se requisitos específicos devem ser negociados no contrato.

As partes interessadas da função de risco podem incluir o departamento de Compliance, que determinaria se o provedor de serviços terceirizado apresenta ou não risco de crimes financeiros ou de violações de sanções.

Após a assinatura do contrato, o programa de TPRM da organização deve se concentrar na gestão contínua do relacionamento, no desempenho do terceiro e na validação contínua da conformidade do terceiro com as expectativas do ambiente de controle.

Considerando a importância atribuída a tais atividades, bem como a diversidade de serviços prestados por terceiros na maioria das organizações, como as empresas podem garantir que seu programa TPRM tenha a estrutura de governança, funções e modelo de entrega de serviço corretos? Como as organizações podem, efetivamente, gerenciar o risco de seus terceiros e, ao mesmo tempo, atender às necessidades dos proprietários de relacionamento e de outras partes da empresa para que estes terceiros sejam envolvidos em tempo hábil?

Além disso, como pode o programa TPRM fazer melhor uso da inovação e das novas tecnologias para avaliar continuamente a eficácia dos controles críticos em uma abordagem otimizada?

Foi com perguntas como essas que a KPMG International embarcou em uma pesquisa com 1.100 executivos seniores para observar as estratégias de TPRM de grandes empresas em 14 países e jurisdições e em vários setores da macroindústria em todo o mundo.

Neste material, apresentamos nossas principais descobertas, reconhecendo que os princípios do TPRM são amplamente comuns em todos os setores e regiões. Para apoiar as organizações em sua busca pela otimização do programa TPRM, também apresentamos os principais elementos de nossa estrutura e metodologia TPRM, que desenvolvemos por meio de uma ampla experiência do cliente.

À medida que os negócios se ajustam às novas condições operacionais, na esteira da interrupção causada por eventos globais e da incerteza econômica, muitos irão reavaliar o perfil de risco de seus terceiros e reavaliar sua própria resiliência. À medida que as empresas fazem isso, a necessidade de um programa TPRM robusto e sustentável será mais importante do que nunca.

Definindo o conceito de terceiros

Antes de discutirmos nossas descobertas em detalhes, vale a pena esclarecer o que queremos dizer com certos termos usados ao longo deste material. Primeiro, como definimos terceiros?

Apenas uma minoria (41%) dos entrevistados em nossa pesquisa está totalmente confiante de que seu negócio possui uma definição clara de 'terceiros'. Dentro da KPMG International e de firmas-membro da KPMG, incluímos as seguintes partes externas em nossa definição de terceiros: vendedores, fornecedores, prestadores de serviços, agentes, distribuidores, corretores, joint ventures e revendedores. Entre terceiros internos, incluímos afiliadas, serviços compartilhados e empresas / entidades matrizes dentro do mesmo grupo. Não incluímos clientes em nossa definição, porque

as empresas não envolvem clientes em um programa de terceiros antes de entrar em uma transação. Firmas de serviços financeiros, por exemplo, incorporam clientes por meio de um processo separado de Know Your Customer (KYC).

Riscos que são cobertos por um programa TPRM

Em segundo lugar, quando falamos sobre riscos de terceiros, a quais riscos específicos nos referimos? Na figura 1, destacamos as principais categorias de risco a que todas as empresas estão expostas, bem como algumas das ameaças individuais que se enquadram nessas categorias.

Dependendo da natureza do produto ou serviço de terceiros fornecido, cada um desses riscos (e, de forma mais geral, uma combinação de vários deles) pode estar presente no relacionamento com terceiros. Os programas TPRM devem esclarecer as funções e responsabilidades pela identificação e avaliação de cada tipo de risco no nível de serviço ou produto, de modo que os especialistas em risco necessários dentro da organização determinem se o terceiro pode gerenciar o risco de acordo com as expectativas do negócio. Afinal, existem muitos exemplos de empresas sendo atingidas por penalidades severas, bem como danos à reputação, quando um risco não foi identificado e mitigado, seja por meio do ambiente de controle de terceiros ou dos controles de compensação internos da empresa.

O fator de sucesso nº 1 para programas TPRM é o foco de tempo, esforço e experiência nos serviços terceirizados de maior risco. Em nossa pesquisa, descobrimos uma incompatibilidade entre as áreas de risco que são consideradas de missão crítica para as empresas e os riscos que são priorizados pelo Programa TPRM. Por exemplo, nossa pesquisa descobriu que os dados

Figura 1. Riscos potenciais para um programa TPRM cobrir

Risco regulatório e compliance	— Requisitos regulamentares — Risco de roubo / crime / disputa	— Fraude, antissuborno e corrupção / sanções — Conformidade com procedimentos e padrões internos
Risco estratégico	— Risco de entrega de serviço — Risco de expansão / implantação — Fusões e aquisições	— Alinhamento à estratégia de terceirização — Risco de propriedade intelectual
Risco de subcontratado	— Aplicável em todas as áreas de risco	
Risco de concentração	— Concentração de fornecedores em serviços críticos — Concentração da indústria (incluindo subcontratante) — Concentração de habilidades críticas	— Concentração geográfica — Concentração reversa
Tecnologia/risco cibernético	— Segurança da informação — Cybersecurity — Privacidade de dados / proteção de dados	
Risco do país	— Risco geopolítico — Sustentabilidade climática	
Viabilidade financeira	— Risco financeiro de empréstimos a terceiros — Risco de liquidez	
Risco operacional e cadeia de abastecimento	— Continuidade de negócios — Recuperação de desastre — Segurança física — Resiliência operacional	— Gestão de desempenho (incluindo SLAs) — Risco de modelo — Riscos de recursos humanos (risco de conduta etc.)
Risco reputacional	— Mídia adversa — Ações judiciais (passadas e pendentes) — Marca/reputação do terceiro	— Principais diretores / proprietários de terceiros — Segurança no trabalho
Risco legal / jurídico	— Jurisdição legal — Termos e condições do contrato	

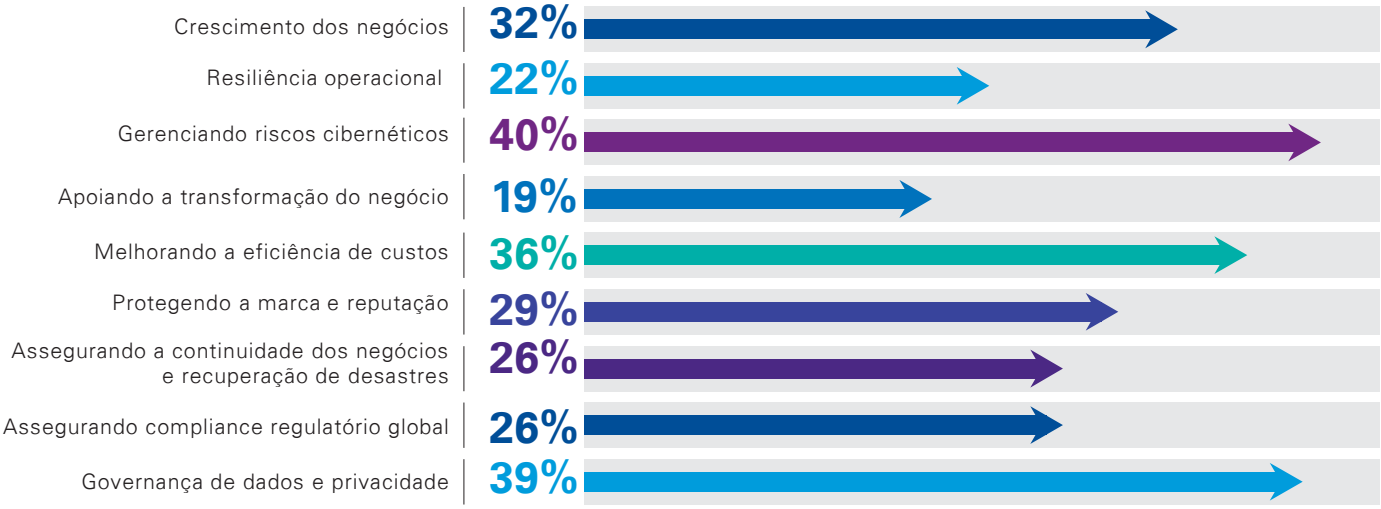
Source: Third Party Risk Management outlook 2020, KPMG International 2020

de governança e privacidade - junto com o risco cibernético - são o motor mais importante da atividade de terceiros em todos os setores e geografias (consulte a figura 2). Não obstante, quando examinamos os riscos que as empresas cobrem em seus programas de TPRM, na figura 3, apenas 54% dos entrevistados priorizam dados / privacidade.

Ao falar com David Hicks, sócio da KPMG no Reino Unido, sobre essa observação, ele alertou que "os programas TPRM devem ter uma estratégia bem definida e bem pensada, apoiada por um apetite de risco claramente articulado. Dessa forma, os programas têm limites definidos para gerenciar e reportar ao conselho e à alta administração."

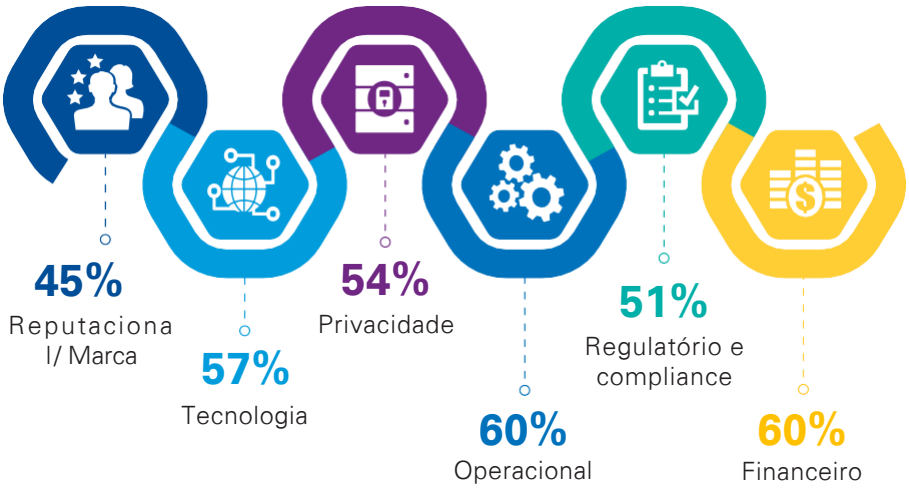
Ao reexaminar estes dados, no contexto da nova realidade colocada pelos eventos globais e incertezas econômicas, refletimos sobre o baixo percentual (22%) atribuído à Resiliência Operacional como um impulsionador da atividade de TPRM. Como Gavin Rosettenstein, diretor da KPMG Austrália, observa: "Discussões recentes com clientes demonstraram que as equipes de TPRM e Cadeia de suprimentos estão fortemente investidas e cientes do papel que terceiros desempenham na entrega de serviços de negócios críticos para clientes. Esperamos que a resiliência operacional continue a motivar o investimento em TPRM nos próximos anos.

Figura 2. Quais são os motivadores mais importantes da atividade de TPRM em sua empresa hoje?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Figura 3. Quais dos riscos a seguir são monitorados como parte de sua atividade de TPRM?



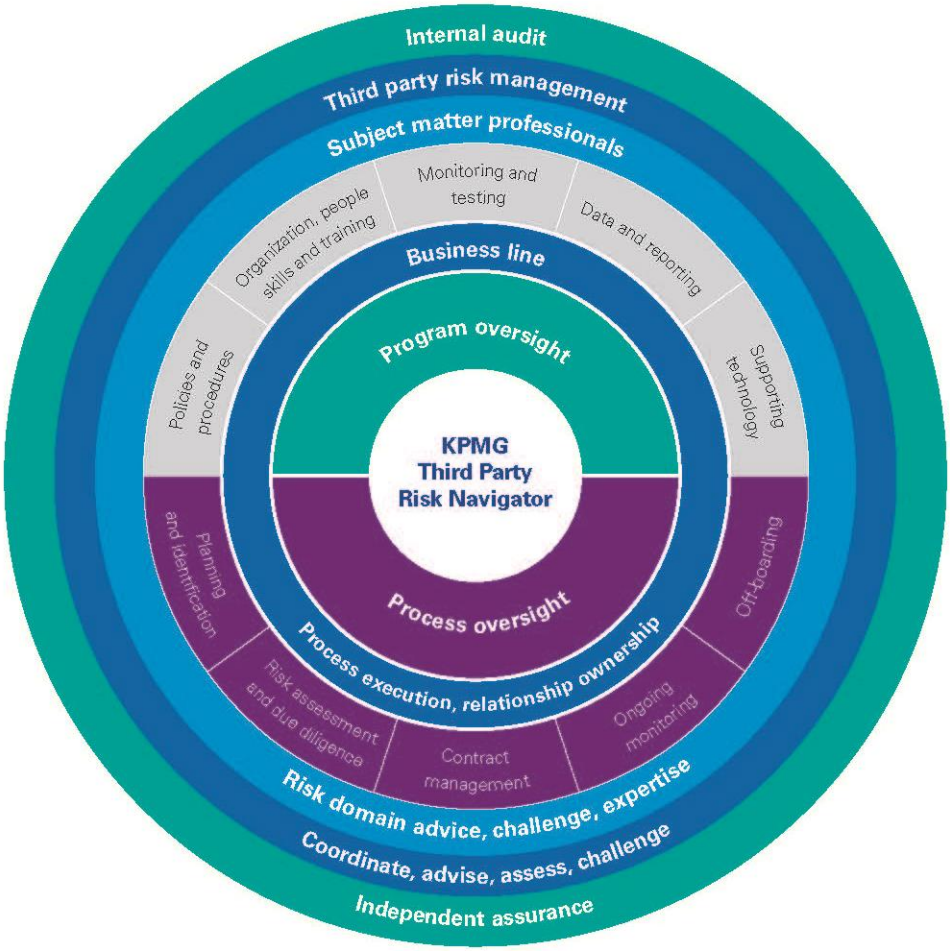
Source: Third Party Risk Management outlook 2020, KPMG International 2020

> TPRM programs must have a well-defined and thought-through strategy, supported by a clearly articulated risk appetite. That way, programs have defined thresholds to manage against and report up to the board and senior management.
>
> — David Hicks
> Partner, KPMG in the UK

Distinguir entre o programa TPRM e o processo

É importante notar desde o início que não acreditamos que exista um programa TPRM "padrão". Dito isso, os programas TPRM bem-sucedidos em todos os setores seguem um processo definido para identificar, monitorar e gerenciar o risco de terceiros, sob a liderança da governança do programa definido. A Figura 4 descreve as principais áreas do programa TPRM e como essas áreas se aplicam ao ciclo de vida TPRM de ponta a ponta.

Figura 4. Principais áreas de um programa TPRM e ciclo de vida TPRM de ponta a ponta



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Na próxima seção, discutiremos nossas principais observações da pesquisa. Na seção 2, delineamos a estrutura desenvolvida pela KPMG para construir um modelo operacional TPRM eficaz. Por fim, na seção 3, definimos as etapas que as empresas devem seguir para impulsionar uma mudança positiva e atingir a maturidade.

Esperamos que esta visão geral seja útil e ficaremos felizes em conversar com você para apresentar mais detalhes.

> Recent discussions with clients have demonstrated that TPRM and Supply Chain teams are keenly invested in and cognizant of the role that third parties play in delivering critical business services to customers and clients.
>
> — **Gavin Rosettenstein,** Director, KPMG Australia

Seção 1:

Sumário executivo

TPRM é uma prioridade estratégica

Mais de três em cada quatro entrevistados em nossa pesquisa (77%) dizem que o TPRM é uma prioridade estratégica para seus negócios. Além disso, seis em cada dez entrevistados disseram que os riscos mais graves para a reputação de sua organização vêm do fracasso de terceiros no cumprimento de suas metas. Essas observações destacam o quão dependentes a maioria das empresas estão em relação aos terceiros para fornecer produtos e serviços essenciais aos seus clientes e consumidores. Ao mesmo tempo, a crescente pressão regulatória - especialmente em relação a violações de privacidade e perda de dados do cliente ou à resiliência operacional - está colocando os relacionamentos com terceiros sob escrutínio adicional. Seis em cada dez (59%) entrevistados afirmaram que suas organizações foram recentemente sujeitas a sanções e observações regulatórias em relação ao TPRM.

Os eventos globais e as incertezas econômicas enfatizaram quão necessários são os terceiros para as operações comerciais. A KPMG definiu quatro fases a serem consideradas pelas empresas na sequência de uma pandemia ou evento global e incerteza econômica: Reação, Resiliência, Recuperação e Nova Realidade. Especificamente, no que diz respeito ao TPRM, as duas primeiras dessas fases lidam com a mudança de emergência para modelos de trabalho remoto e a reconfiguração de modelos de prestação de serviços de terceiros para garantir que os serviços sejam mantidos para clientes e consumidores. As duas segundas fases cobrem a preparação de como as empresas irão operar na Nova Realidade, em que os ambientes de controle são distribuídos ainda para as casas de trabalhadores contingentes remotos e no qual o distanciamento social é necessário para prevenir subsequentes ameaças do vírus. Os programas TPRM também terão que considerar quais novas regulamentações governamentais podem surgir e atualizações para o programa TPRM podem ser necessárias devido à incerteza geral em torno da resiliência do ecossistema de terceiros, conforme os impactos financeiros da crise se manifestam.

As empresas são inconsistentes em sua abordagem ao TPRM

As empresas trabalham com uma ampla variedade de terceiros em todo o mundo, e cada terceiro gerencia um subconjunto de riscos em nome da empresa. Por um bom motivo, as empresas precisam entender a capacidade de cada terceiro de gerenciar riscos de acordo com as expectativas antes de decidir se contrata esse terceiro. É preocupante, porém, que nossa pesquisa sugira que muitas organizações não estão preparadas para a complexidade que acompanha a avaliação de vários riscos de maneira coesa em todas as linhas de negócios e regiões. A identificação e avaliação holística do risco antecipadamente no processo de integração, bem como durante o ciclo de vida do contrato, é crucial para que as organizações tenham uma visão geral do perfil de risco de todo o portfólio de terceiros. Três quartos (74%) dos entrevistados admitem que suas organizações precisam urgentemente tornar o TPRM mais consistente em toda a empresa
.

Uma abordagem baseada em risco é a prioridade número 1 para programas TPRM

Gerenciar o risco de terceiros no ambiente de negócios atual está longe de ser simples, e o escopo do programa, junto com a quantidade de coordenação envolvida, faz com que alguns se sintam oprimidos. A situação é agravada por limitações de recursos organizacionais e orçamento. Metade das empresas não têm recursos internos suficientes para gerenciar todos os riscos de terceiros que enfrentam. Em nossa opinião, as organizações podem alcançar eficiência e

eficácia ao adotar uma abordagem baseada em riscos para avaliar e monitorar produtos e serviços de terceiros que apresentam o maior risco para a organização.

Dados e tecnologia estão melhorando o desempenho das equipes de TPRM

Em todos os setores e regiões, os entrevistados indicaram que o grande volume de atividades de avaliação de terceiros aumentou nos últimos anos. No início, os programas TPRM simplesmente aumentaram seu número de funcionários para concluir um número maior de avaliações de risco. Hoje, as organizações têm potencial para inovar sua abordagem em três áreas:

— Maior automação do fluxo de trabalho interno do processo TPRM

— Aproveitamento de provedores de serviços compartilhados para *due diligence*

— Mudança de avaliações de risco pontuais para monitoramento de controles contínuos.

Atualmente, vemos apenas cerca de um quarto das empresas usando tecnologias para melhorar a automação do fluxo de trabalho ou o monitoramento de terceiros. A tecnologia é, no entanto, o investimento mais favorecido (61%) que os entrevistados fazem quando um financiamento adicional é disponibilizado para eles.

"É um momento empolgante para trabalhar no TPRM", diz Jon Dowie, sócio da KPMG no Reino Unido, "uma vez que a indústria finalmente chegou a um consenso de que nossa abordagem para avaliações de risco pontuais precisa evoluir. Empresas de todos os setores estão colaborando em padrões comuns para questionários e avaliações, para que suas equipes possam se concentrar no tratamento de riscos de terceiros, em vez de perseguir respostas a questionários ou viajar para avaliações in-loco."

É hora de dimensionar o programa de forma sustentável

As organizações estão amadurecendo seus programas de TPRM para entender melhor onde está o risco de interrupções de serviço resultantes do não desempenho de terceiros. Além disso, as organizações estão expandindo a identificação de riscos, avaliação e gestão de subcontratados de materiais. Conforme exploraremos na próxima seção deste relatório, muitas organizações têm espaço para melhorias em todo o seu modelo operacional, incluindo governança, processo, infraestrutura e dados. Com isso em mente, nossa análise nos ajudou a refinar as etapas que as organizações devem seguir para atualizar seus programas TPRM. Essas etapas - que descrevemos na seção 3 deste relatório - se concentram em ajudar as equipes a elevar seus programas, otimizar processos e aproveitar as novas tecnologias para obter melhores resultados com os recursos limitados disponíveis.

> "Companies across industries are collaborating on common standards for questionnaires and shared assessments, so that their teams can focus on treating third-party risks, rather than chasing down questionnaire responses or traveling for on-site assessments."
>
> — **Jon Dowie**
> Partner, KPMG in the UK

Seção 2:

Metodologia TPRM

Greg Matthews, sócio da KPMG nos EUA, diz que os principais programas TPRM estão experimentando novos modelos operacionais para identificar, monitorar e gerenciar riscos de terceiros de forma mais eficiente - sem comprometer a eficácia. "Alcançar a transformação do TPRM exigirá programas para superar os obstáculos que afetaram esses programas durante sua construção inicial e iterações subsequentes, como suporte executivo inadequado, responsabilidade insuficiente e resistência de terceiros em cooperar com o processo de TPRM", explica ele.

A estrutura da KPMG para um modelo operacional de TPRM eficaz é baseada em quatro pilares: governança, processo, infraestrutura e dados. Cada um desses pilares possui requisitos específicos, que definimos a seguir. Um ponto preocupante é que muitas empresas ainda têm um longo caminho a percorrer antes de atingir a maturidade, conforme ilustram os dados de nossa pesquisa.

> "Achieving TPRM transformation will require programs to overcome the roadblocks that have plagued these programs throughout their initial build and subsequent iterations."
>
> — **Greg Matthews**
> Sócio, KPMG in the US

Governança

O que é requerido?

- Um único líder do programa
- Uma estrutura de subordinação à alta administração e ao Conselho
- Uma estratégia de terceirização para a organização, bem como um apetite de risco definido
- Funções e responsabilidades claras em todo o programa TPRM e no ciclo de vida TPRM de ponta a ponta
- Políticas, padrões e apetite pelo risco que estabelecem o escopo e o foco do programa
- Um inventário de serviços de terceiros aos quais o programa se aplica, com base nas definições acordadas de serviços de terceiros.

Por que as empresas precisam agir:

- 74% dos entrevistados disseram que sua organização precisa urgentemente tornar o TPRM mais consistente em toda a empresa
- 57% dos entrevistados disseram que sua organização está muito longe de ter um contrato de toda a empresa para serviços que podem ou não podem ser terceirizados.

Processo

O que é requerido?

- Consistência de execução em todo o programa TPRM para conduzir dados de qualidade para análise
- Equipes de avaliação que têm a combinação certa de habilidades, experiência e largura de banda
- Uma abordagem baseada em risco para avaliar serviços de terceiros que está ligada ao apetite de risco do programa
- Uma avaliação de risco que ocorre antes da execução do contrato e auxilia na tomada de decisão

— Análise e mitigação de risco contínua, em vez de um foco míope na coleta de dados e na coleta de respostas ao questionário
— Monitoramento contínuo ao longo da vida dos contratos
— Procedimentos e modelos que esclarecem os processos e geram consistência
— Cobertura de risco de terceiros e subcontratados materiais, além de terceiros.

Por que as empresas precisam agir:

— 52% dos entrevistados acreditam que o programa de TPRM de sua organização é sobrecarregado e impede sua capacidade de fazer negócios

— A escassez de habilidades é o desafio número um dos entrevistados ao tentar transformar sua atividade de TPRM

— 67% dos entrevistados dizem que as avaliações de risco de terceiros de sua organização são realizadas por vários recursos em toda a organização, ao invés de uma pessoa ou equipe

— Apenas 32% dos entrevistados disseram que suas organizações são altamente proficientes no desenvolvimento de uma compreensão abrangente dos riscos apresentados por terceiros

— Apenas 36% dos entrevistados disseram que suas organizações têm uma abordagem baseada em riscos para monitoramento contínuo

— 40% dos entrevistados dizem que suas organizações não realizam monitoramento de terceiros após a contratação, muitas vezes porque eles permitiram que essa atividade de monitoramento caducasse com o tempo

— 72% dos entrevistados disseram que suas organizações precisam urgentemente melhorar a forma como avaliam terceiros.

Infraestrutura

O que é requerido?

— Uma arquitetura de tecnologia TPRM que suporta fluxo de trabalho eficiente, automação de tarefas e relatórios
— Uma trilha de auditoria documentada e bem compreendida
— Um modelo de entrega de serviço que está alinhado ao estilo operacional da empresa (seja centralizado ou distribuído) e permite o gerenciamento consistente de risco em todas as linhas de negócios e regiões
— A integração de atividades e tecnologia de TPRM nos processos existentes em toda a empresa, como Aquisições, Jurídico e Financeiro, e nas funções e atividades de supervisão de risco existentes.

Por que as empresas precisam agir:

— Há pouca consistência, entre as empresas, em qual modelo operacional usar, com a responsabilidade final pelo TPRM diferindo visivelmente entre as empresas (ver figura 5)

— Apenas 24% dos entrevistados disseram que suas organizações estão usando a automação para aumentar a eficiência do programa TPRM, realizando tarefas de rotina.

Dados

O que é requerido?

— A coleta de dados em tempo real em torno da capacidade do programa TPRM de gerenciar as atividades de avaliação, integração e monitoramento de terceiros e sua capacidade de gerenciar o desempenho específico de cada serviço de terceiros e os ambientes de controle em que operam

— Um modelo de dados abrangente para a coleta de informações de terceiros, incluindo detalhes do serviço, pontuação de risco, informações de contrato e monitoramento de desempenho

— Feeds de dados internos que monitoram e registram eventos e incidentes específicos atribuíveis a terceiros, e feeds de dados externos que monitoram informações em tempo real sobre terceiros, como mídia adversa, mudanças na propriedade do negócio, ações corporativas, vulnerabilidade cibernética, pontuações e classificações de viabilidade financeira

— Um processo para atualizar os perfis de risco de terceiros quando há alterações na pontuação de risco, de preferência em tempo real conforme surgem problemas ou motivadores externos, ou quando há mudanças no ambiente de controle do terceiro

— Acompanhamento em tempo real do desempenho em relação aos acordos de nível de serviço (SLAs)

— Rastreamento em tempo real de riscos em relação aos principais indicadores de risco (KRIs)

— Tomada de decisão baseada em dados, na qual as avaliações de risco e monitoramento de desempenho influenciam os termos do contrato e a tomada de decisão durante a recontratação ou a continuação do relacionamento com terceiros.

Por que as empresas precisam agir:

— 37% dos entrevistados disseram que, em sua organização, as barreiras técnicas, como sistemas incompatíveis, são o principal obstáculo ao compartilhamento de dados de terceiros em toda a empresa

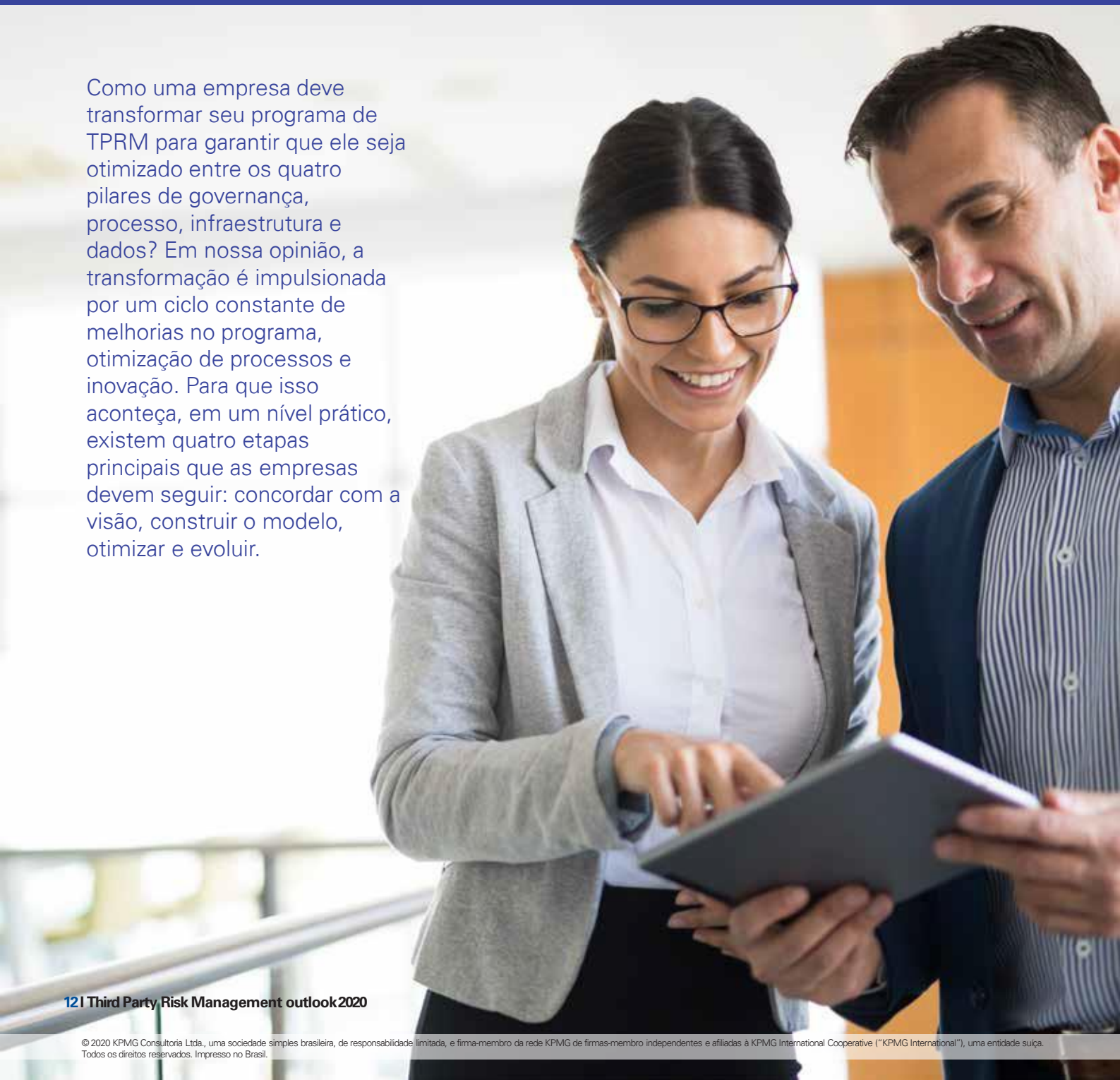
— Menos da metade dos entrevistados estão muito confiantes nos inventários eletrônicos de suas organizações de contratos de terceiros, monitoramento e relatórios de risco e estoques de terceiros

— Apenas um em cada quatro (26%) entrevistados acredita fortemente que sua organização possui todos os dados necessários para realizar as avaliações.

Seção 3:

Jornada para a maturidade do TPRM

Como uma empresa deve transformar seu programa de TPRM para garantir que ele seja otimizado entre os quatro pilares de governança, processo, infraestrutura e dados? Em nossa opinião, a transformação é impulsionada por um ciclo constante de melhorias no programa, otimização de processos e inovação. Para que isso aconteça, em um nível prático, existem quatro etapas principais que as empresas devem seguir: concordar com a visão, construir o modelo, otimizar e evoluir.



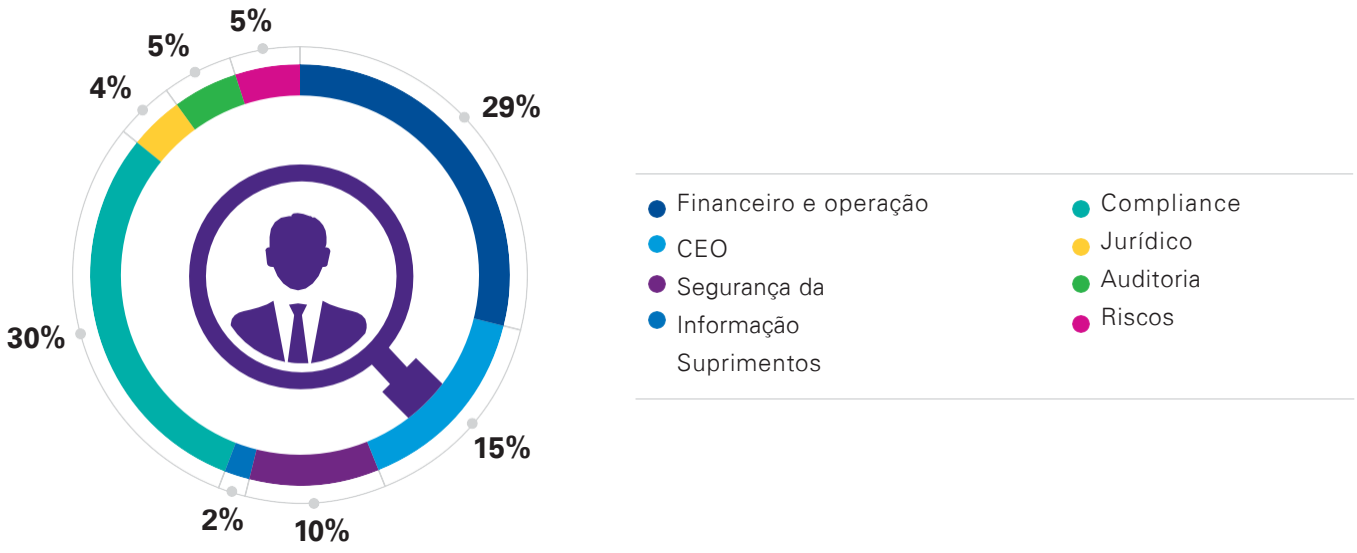
1 Visão

Quase todas as empresas têm algum tipo de programa TPRM em vigor. Embora 51% das organizações dos entrevistados estejam trabalhando com orçamentos limitados, dado o maior foco no uso de terceiros, três em cada quatro (76%) entrevistados indicam que o financiamento está disponível ou crescendo para evoluir e fortalecer o programa TPRM de sua organização.

Uma consideração importante para o programa TPRM em toda a empresa é designar a propriedade do programa e determinar onde o TPRM se encaixa na organização. Em última análise, isso é decidido pela natureza e complexidade de cada negócio, embora nossa pesquisa tenha descoberto que a responsabilidade é mais provável de cair sob Risco e Conformidade (30%) ou Finanças, Administração e Operações (31%) - veja a figura 5. Dentro do último grupo, as organizações estão cada vez mais identificando a função de Procurement para executar as atividades do ciclo de vida do TPRM. "Descobrimos que colocar o TPRM dentro da organização de compras mais ampla pode levar a eficiências operacionais significativas e a uma experiência de usuário aprimorada para proprietários de relacionamento comercial de serviços de terceiros", disse Alexander Geschonneck, sócio da KPMG na Alemanha. "Dito isso, pode haver uma elevação do conjunto de habilidades e uma mudança cultural necessária para preparar a função de aquisição para assumir a execução do TPRM, bem como possíveis complicações da linha de relatórios para relatórios de risco de terceiros aos comitês de risco e ao Conselho. "

> We find that placing TPRM within the broader procurement organization can lead to significant operational efficiencies and an improved user experience for business relationship owners of third-party services. "
>
> — **Alexander Geschonneck, Sócio**, KPMG in Germany

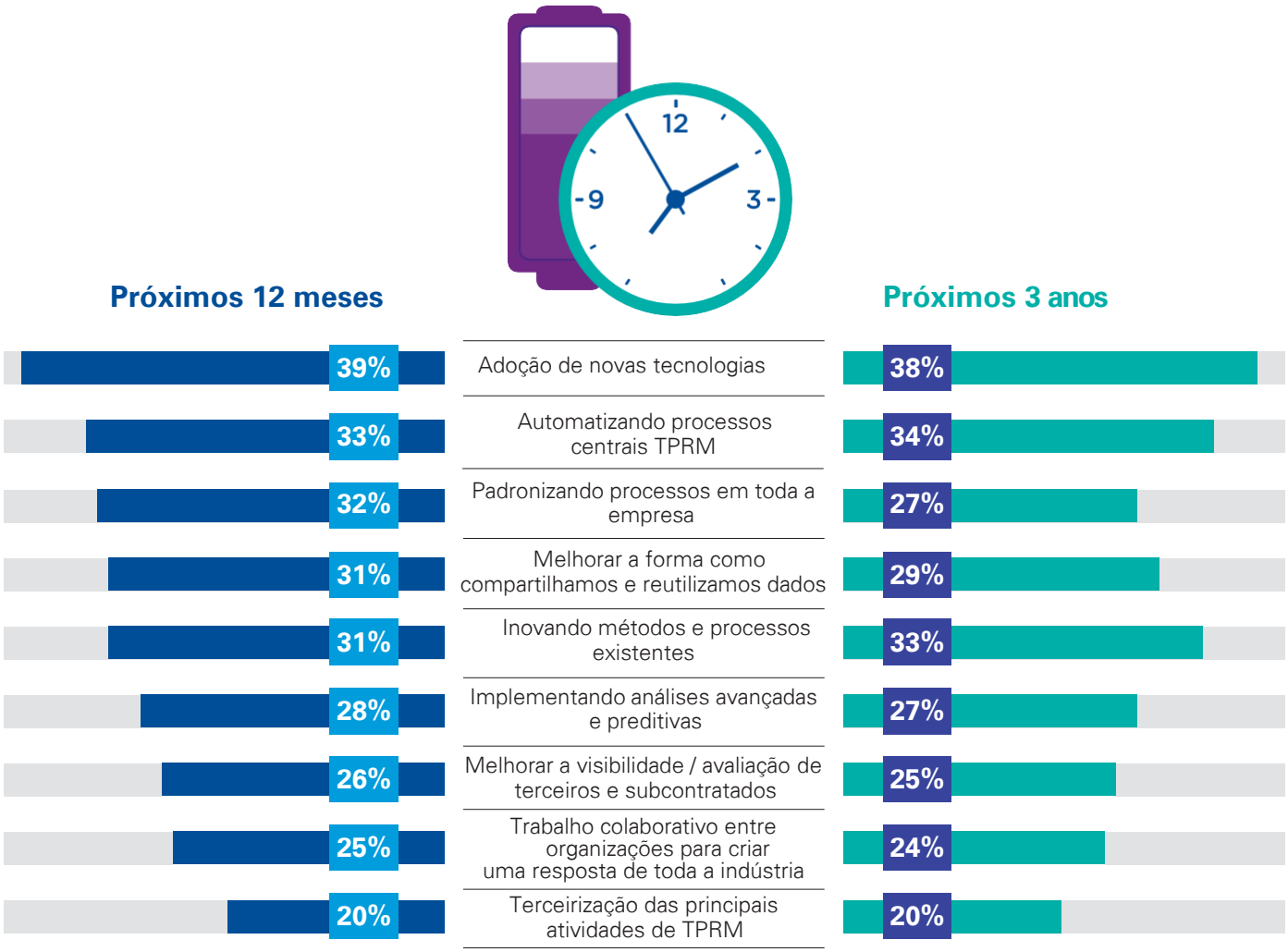
Figura 5. Quem é o responsável final pelo TPRM em sua empresa?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Em segundo lugar, para estabelecer a visão, as proteções e a propriedade do programa, é feita a determinação das aspirações para a capacitação da tecnologia. A este respeito, as empresas devem ter cuidado para não tentar 'correr antes de andar'. Embora muitas organizações reconheçam que a automação do programa como um todo é essencial para dimensionar o TPRM e para ajudar as equipes a processar e analisar grandes volumes de dados - como ilustrado pela figura 6 - a tecnologia deve ser vista como um facilitador e não como um impulsionador do progresso. Automatizar processos fracos não irá aprimorar esses processos magicamente.

Figura 6. Em quais das seguintes iniciativas sua equipe estará concentrando mais tempo e energia nos próximos 12 meses e nos próximos três anos?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

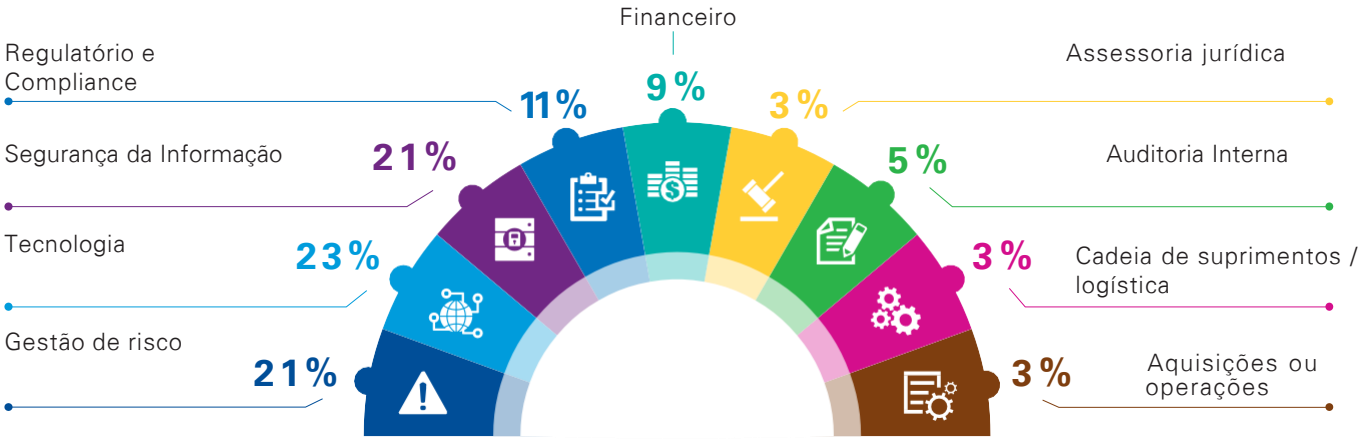
2 Construir o modelo

Os programas TPRM são complexos. Não apenas todas as partes da organização usam terceiros, cada serviço prestado pelo terceiro possui múltiplos riscos e diferentes funções de supervisão precisam ser consultadas sobre avaliações de risco individuais. Como explica Amanda Rigby, sócia da KPMG nos Estados Unidos, "Depois que o programa é estabelecido, as empresas continuam a ajustar e esclarecer como ele funciona à medida que aumentam sua eficácia em toda a empresa. O desenvolvimento do programa TPRM não é um exercício único. A maioria dos clientes passou por três ou mais iterações do programa antes de encontrar o equilíbrio certo para sua organização."

As considerações no estágio de construção do programa incluem decidir exatamente como, quando e onde envolver as partes interessadas de negócios em todo o ciclo de vida do TPRM. Aquisição, por exemplo, geralmente possui a integração e terceiros processo de gerenciamento, enquanto os proprietários de negócios e avaliadores de TPRM centralizados interagem com os especialistas no assunto de risco em pontos críticos, como durante o processo de avaliação de risco inicial e contínuo (ver figura 7 para um resumo de principais grupos envolvidos). Além disso, a equipe do programa TPRM é amplamente encarregada de executar o programa; as funções de supervisão de risco são responsáveis pelos riscos que supervisionam; e a empresa é responsável pela gestão do serviço de terceiros no dia a dia.

> TPRM program development is not a one-time exercise. Most of our global clients have gone through three or more iterations of the program before they strike the right balance for their organization.
>
> — **Amanda Rigby,** Partner, KPMG in the US

Figura 7. Quem fornece a segunda linha de defesa para TPRM?



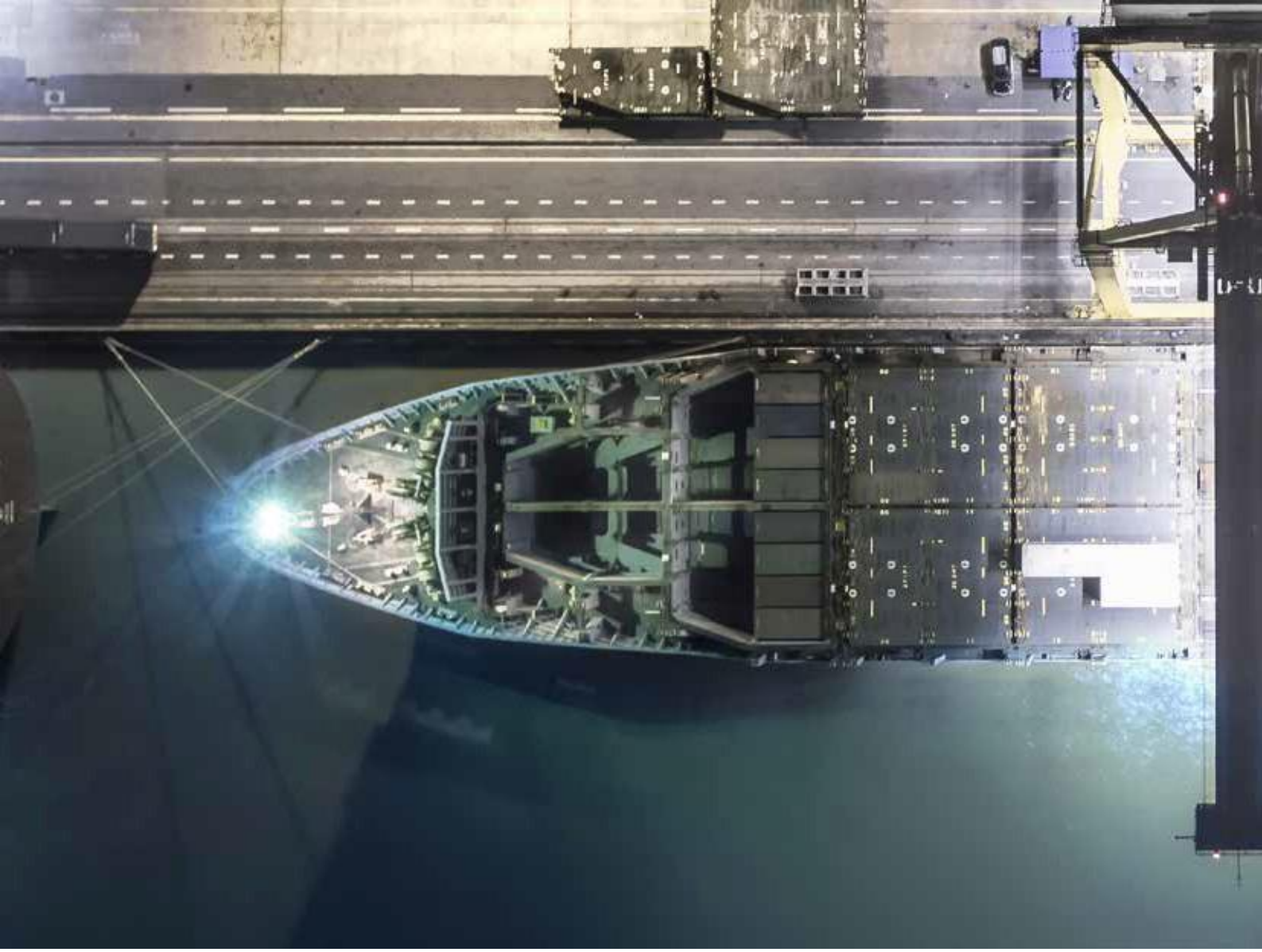
Source: Third Party Risk Management outlook 2020, KPMG International 2020

Outra consideração é em torno de qual modelo usar para concluir as atividades de avaliação de risco. As empresas podem optar por usar um modelo distribuído, por meio do qual o gerente de relacionamento comercial coordena as atividades de avaliação de risco inerentes. Como alternativa, as empresas podem identificar uma equipe centralizada que facilite a avaliação de risco inerente em nome (e com a contribuição) da empresa. Neste modelo, a equipe centralizada ajuda os proprietários de relacionamento de negócios a superar desafios em torno da integração e da escassez de habilidades e leva a um maior grau de consistência, o que é fundamental porque as informações de risco inerentes são a base da análise do programa TPRM.

"Em muitos casos, vemos que há um custo geral mais alto para manter um modelo distribuído por causa do treinamento e supervisão necessários entre os gerentes de fornecedores", diz Lem Chin Kok, sócio da KPMG em Singapura. "Vemos híbridos dos dois modelos, mas na maioria das vezes há uma tendência maior para um modelo centralizado do que para um modelo distribuído, em que a equipe centralizada executa as atividades de avaliação de risco e fornece os resultados para os gerentes de relacionamento de negócios, que finalizam a decisão de prosseguir com o fornecedor terceirizado."

Frequentemente, as organizações têm requisitos específicos que precisam ser desenvolvidos em paralelo; por exemplo, no clima atual, as organizações multinacionais também precisam garantir que atendam aos crescentes requisitos regulatórios globais e às nuances em todas as regiões. Obtendo o suporte certo de Risco de Conformidade e Tecnologia, o gerenciamento é essencial quando se trata de atualizar o programa em uma base contínua para cumprir os requisitos e acompanhar as novas expectativas regulatórias, incluindo a privacidade dos dados do cliente. Outra área de foco para os respondentes da pesquisa é o risco de terceiros e subcontratados materiais. Um exemplo de relacionamento de subcontratado material é aquele em que o terceiro usa um provedor de nuvem para apoiar a entrega de seu serviço.

As empresas precisam estabelecer uma supervisão consistente dessas terceiras partes, o que não é pouca coisa, visto que não há contrato direto entre a organização e suas terceiras partes. Quando se trata de gerenciamento de risco de quarta parte, as organizações geralmente empregam uma ou mais das medidas descritas na figura 8. Compreender o papel do subcontratado na entrega do serviço de terceiros, incluindo dados de como



a quarta parte tem acesso e como sua função influencia os riscos de continuidade de negócios, é vital para obter uma imagem completa dos riscos do serviço em que a organização está entrando. Entender se o terceiro tem um programa em vigor para gerenciar seus terceiros (ou seja, a quarta parte da organização) é uma parte importante da avaliação de permitir ou não que terceiros usem subcontratados.

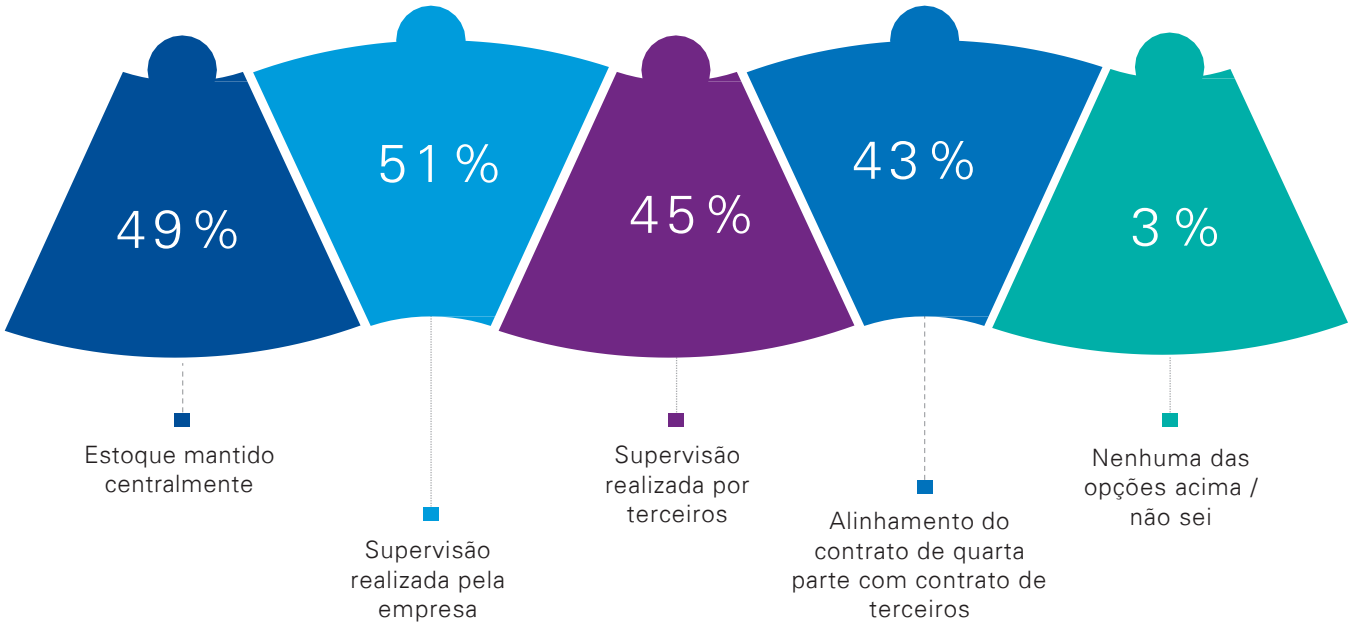
> We see hybrids of the two models, but most often there is a greater leaning toward a centralized model than there is toward a distributed model.
>
> — **Lem Chin Kok**
> Partner, KPMG in Singapore

Resolver essas considerações iniciais é um grande passo à frente, mas é apenas parte do que é necessário antes que a maturidade total do programa TPRM possa ser atingida. As organizações precisam expandir seus programas de TPRM para levar em consideração não apenas a avaliação de risco pré-contrato, mas também o monitoramento contínuo ao longo da vida do contrato.

3 Otimize o processo

A otimização do processo visa a garantir que terceiros que não atendam aos critérios de risco pré-determinados e aos limites de materialidade não sejam apresentados para avaliação pelo programa TPRM. As organizações podem otimizar o processo de estratificação de risco de duas maneiras: segmentação de risco - estabelecendo uma metodologia de pontuação de risco disciplinada em serviços de terceiros - e aprimoramento do modelo de entrega de serviço para reduzir custos e aumentar a responsabilidade. Essas ações ajudarão a lidar com as limitações de orçamento organizacional sinalizadas pelos entrevistados em nossa pesquisa, assim como a apoiar as equipes na tomada de decisões corretas com os dados disponíveis.

Figura 8. Qual dos seguintes processos e práticas você precisa para gerenciar o risco de terceiros indiretos?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

As organizações devem segmentar terceiros em três categorias:

— aqueles que apresentam risco nominal para a organização e não precisam ser avaliados quanto ao risco

— terceiros que são apropriados para o processo TPRM padrão

— terceiros que apresentam um perfil de risco homogêneo e são gerenciados de forma mais eficiente e de maneira centralizada, por meio de um programa de especialidade.

Com relação à segmentação de risco, o objetivo deve ser permitir a customização e adaptação para terceiros que não apresentam o perfil de risco padrão para requisitos de avaliação de risco de terceiros. Por exemplo, um terceiro do qual a organização compra suprimentos de escritório pode não garantir o mesmo grau de avaliação que um terceiro para o qual a organização está terceirizando um centro de contato com o cliente principal.

Praticamente, isso é conseguido através do alinhamento das categorias de serviço de Procurement com risco nominal ou designações de programa de especialidade. Para o padrão Processo TPRM, a primeira etapa é fazer uma série de perguntas de passagem, incluindo:

— O terceiro interage com nossos clientes / clientes?

— O trabalho é realizado no mesmo país que a organização?

— O terceiro terá acesso à propriedade intelectual ou aos dados do cliente / cliente? Em caso afirmativo, os dados serão armazenados na nuvem?

— O serviço de terceiros está relacionado a uma área de análise ou requisitos regulatórios?

— Este serviço de terceiros representa uma terceirização de material ou função crítica?

Uma resposta afirmativa a qualquer uma das perguntas acima pode levar ao envolvimento da função de supervisão de risco associada e ao preenchimento de questionários de risco específicos e avaliações de devida diligência. Por outro lado, respostas negativas a essas questões podem limitar o volume das atividades de avaliação de risco, diminuindo esforços e custos.

Quando se trata de otimizar o modelo de prestação de serviços de TPRM, vemos os principais programas realizando uma revisão de quem na organização deve concluir as atividades de TPRM. O maior desafio de um modelo distribuído, em que o gerente de relacionamento com terceiros está fortemente envolvido, é a falta de habilidades. Durante eventos globais e incertezas econômicas, algumas organizações também foram desafiadas a obter informações precisas e atualizadas sobre serviços de terceiros, reconhecendo que os gerentes de relacionamento de terceiros já estavam sob pressão crescente.

Provavelmente em resposta a tais desafios de talento, os entrevistados indicam que o treinamento e o desenvolvimento de habilidades é uma área de foco principal para os programas TPRM de sua organização (ver figura 9). Reconhecendo que a experiência no domínio de risco é limitada nas organizações, muitos clientes estão centralizando os aspectos da execução do processo TPRM e determinando onde um generalista pode ser capaz de concluir os aspectos dos processos de avaliação de risco e devida diligência. As organizações estão determinando quais controles e áreas de risco requerem o foco dedicado de um especialista no domínio. Embora uma equipe centralizada possa executar avaliações e pontuações de risco, a empresa ainda é responsável por tomar a decisão de prosseguir (ou não) com a contratação do terceiro. Nossa visão é que definir claramente esses componentes estruturais do processo TPRM permite que as organizações automatizem tarefas, estruturem fluxos de trabalho e simplifiquem a coleta e análise de informações por equipes diferentes.

4 Evoluir e inovar

Dado que o maior esforço no programa TPRM gira em torno da coleta de informações e avaliação de informações de controle de terceiros, essas são as áreas onde vemos o maior foco em investimento. Nos próximos anos, prevemos um progresso significativo em dois grandes tópicos:

— O compartilhamento de respostas de due diligence em toda a indústria

— O uso de tecnologia e serviços de pontuação para avaliar ambientes de controle de terceiros de uma maneira mais contínua e consistente.

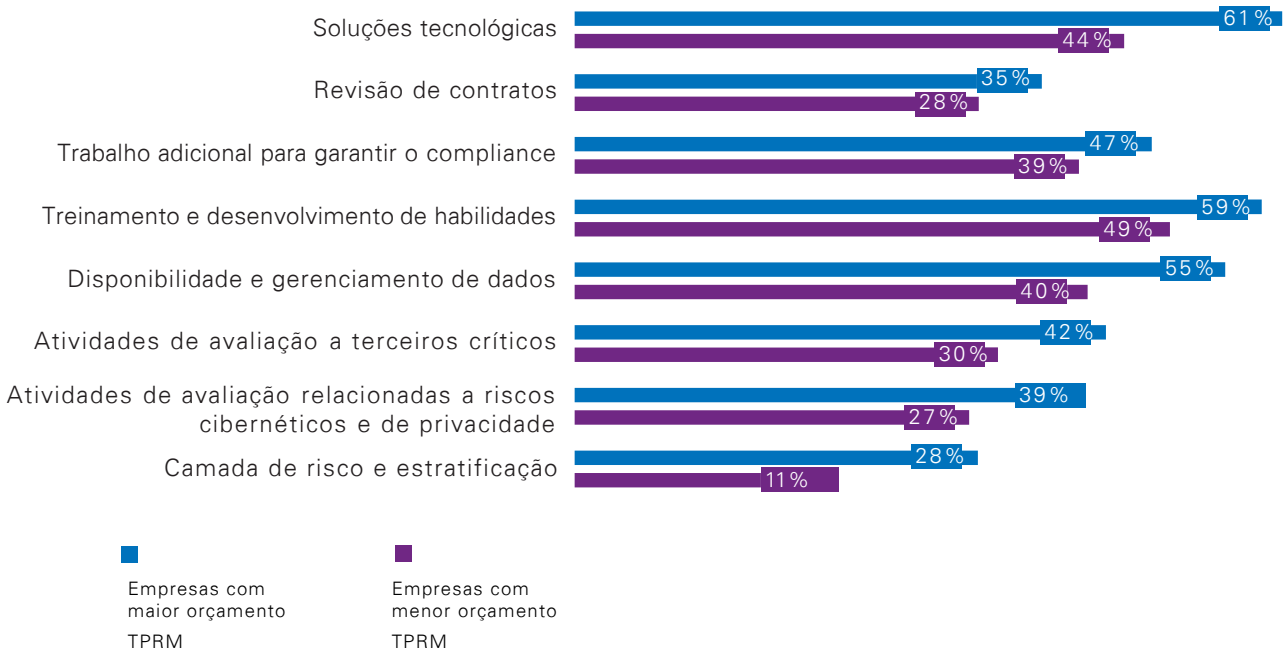
A maioria dos entrevistados está aproveitando ou procurando aproveitar as informações de avaliação compartilhadas para reduzir custos. Há um crescente reconhecimento e aceitação de que as empresas de serviços públicos podem coletar e compartilhar informações entre terceiros e seus clientes. A proposta de valor é clara para terceiros e seus clientes. Para terceiros, a coleta e o compartilhamento de informações podem significar que uma concessionária coleta as informações uma vez, conclui a avaliação uma vez e, em seguida, oferece os resultados da avaliação a todos os seus clientes, em vez de cada cliente realizar uma avaliação de risco separada.

Nesse cenário, a proposta de valor para os clientes viria do recebimento das informações de avaliação necessárias em tempo hábil e do compartilhamento dos custos de avaliação de risco associados em todo o setor.

Com relação à inovação em tecnologia TPRM, nossa pesquisa indica que as empresas estão concentrando seus orçamentos limitados em novas ferramentas (veja a figura 9). Isso está de acordo com nossa experiência, baseada na maturidade dos programas TPRM. No passado, as organizações realizavam um volume maior de atividades de avaliação, aumentando o número de funcionários. Agora, vemos equipes líderes de TPRM usando automação, análise de dados e processamento de linguagem natural, bem como incorporando serviços de pontuação para monitoramento contínuo acessível e escalável em áreas de risco selecionadas, gerenciamento de desempenho e conformidade de contrato. Os programas TPRM estão explorando como podem usar o aprendizado de máquina para avaliar dados internos sobre eventos de risco e identificar os eventos de risco que podem ter sido causados por terceiros. Eles estão automatizando o monitoramento da conformidade de seus terceiros com os termos de SLA, identificando oportunidades para recuperar taxas por compromissos perdidos e adotar uma abordagem mais proativa ao risco de reputação, como automatizar a análise de dados de mídia social.

Algumas dessas inovações estão crescendo em atratividade à medida que as equipes ajustam seus programas para enfrentar os desafios apresentados por eventos globais e pela incerteza econômica e suas consequências. Dada a limitada capacidade que, atualmente, as organizações possuem para conduzir análises no local, elas estão identificando maneiras de atualizar o programa TPRM para lidar com a nova realidade, a exemplo de determinar como o monitoramento contínuo pode atingir certos objetivos do programa TPRM em vez do padrão questionário de risco, avaliação de due diligence e revisão no local. As organizações também estão repensando como o monitoramento de risco proativo baseado em dados - aproveitando a IA e o aprendizado de máquina - pode identificar o alerta precoce de indicadores de resiliência de terceiros e podem ajudar a mitigar o impacto de crises futuras. Finalmente, as organizações estão considerando como precificar com mais precisão o risco de pandemias e outros riscos de cauda.

Figura 9. Onde você está investindo seus fundos para TPRM?



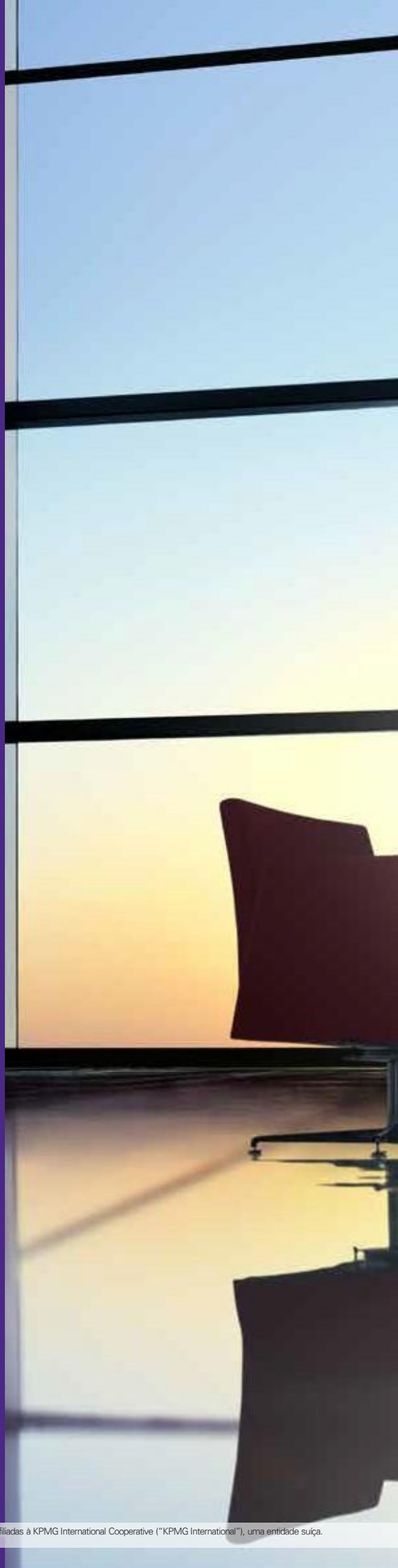
Source: Third Party Risk Management outlook 2020, KPMG International 2020

Conclusões

Nossa pesquisa confirma que as organizações em todos os setores e regiões estão corretamente considerando o TPRM como uma prioridade estratégica. Vemos as empresas adotando uma abordagem proativa em relação ao TPRM e explorando como elas podem refinar e expandir seus processos existentes por meio da capacitação e inovação tecnológica.

Dito isso, nossa pesquisa também deixa claro que, para muitas organizações, o TPRM continua sendo um trabalho em andamento.

À medida que se ajustam aos eventos globais e às incertezas econômicas, as organizações também podem descobrir que suas informações históricas de avaliação de terceiros e análise do ambiente de controle precisam ser atualizadas para levar em conta novos riscos e desafios. Como questão de extrema urgência, as organizações devem melhorar a resiliência dos negócios em serviços críticos ao cliente, entendendo com precisão o papel que terceiros desempenham na entrega desses serviços e no ajuste de políticas e controles de acordo.



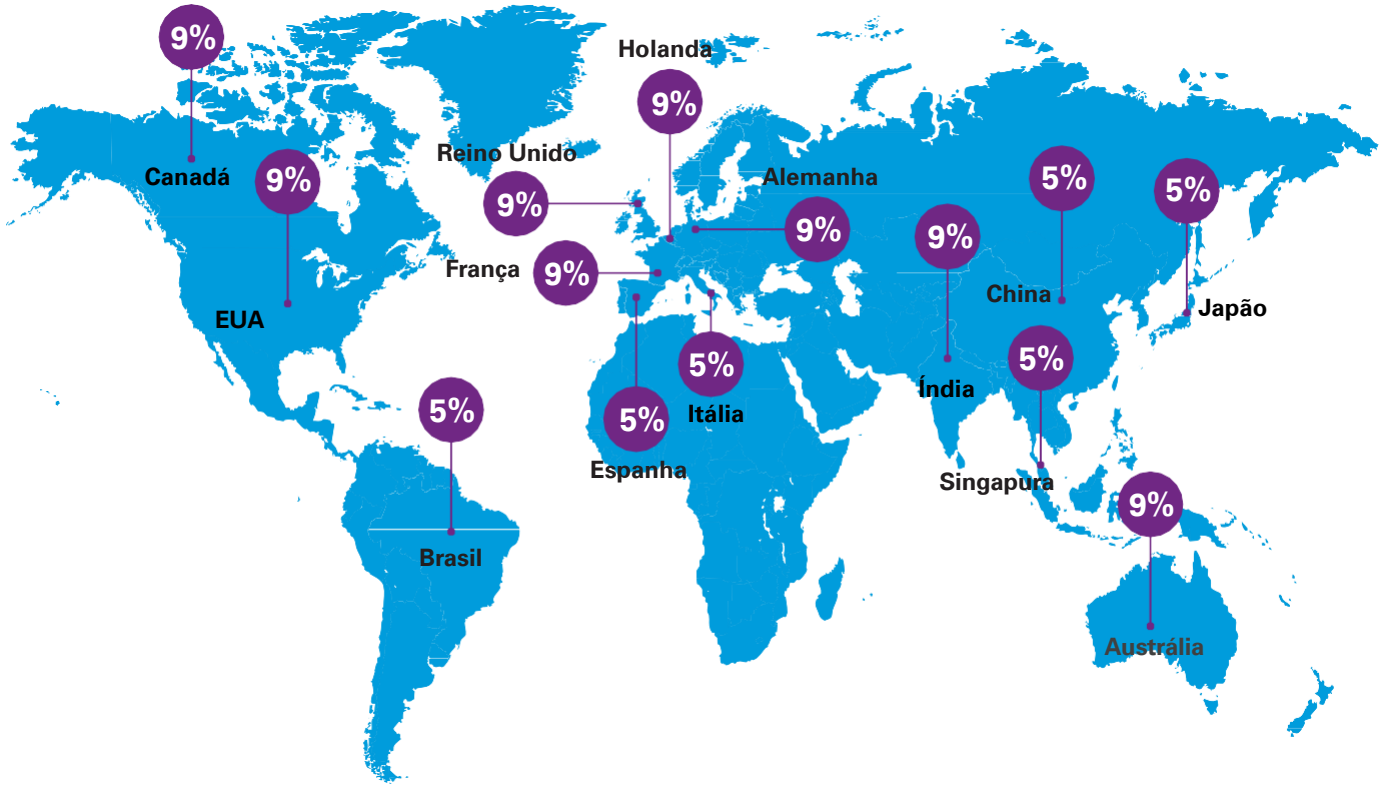
Sobre a pesquisa

No início de 2020, a KPMG conduziu uma pesquisa online com 1.100 executivos seniores que trabalham para grandes empresas em 14 países e jurisdições e seis indústrias em todo o mundo. No decorrer de nossa pesquisa, também realizamos discussões aprofundadas com dez especialistas em TPRM, tanto de firmas-membro da KPMG quanto de empresas.

Figura 10. Em que setor sua empresa atua?

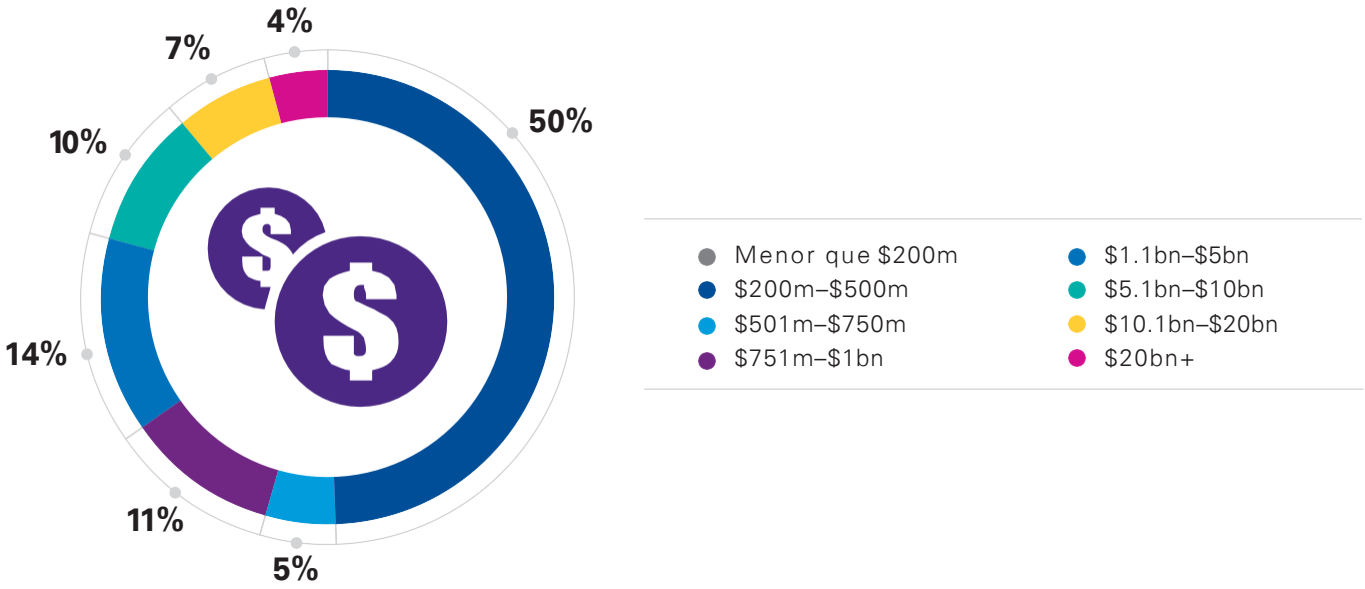
Source: Third Party Risk Management outlook 2020, KPMG International 2020

Figura 11. Em que país / jurisdição sua empresa opera principalmente?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Figura 12. Qual é a receita anual global total da sua organização em dólar?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Fale com o nosso time

David Hicks
Global Forensic Leader
KPMG International
T: +44 207 6942915
E: david.hicks@kpmg.co.uk

Alexander Geschonneck
Partner
KPMG in Germany
T: +49 30 2068 1520
E: ageschonneck@kpmg.com

Greg Matthews
Partner
KPMG in the US
T: +1 212 954 7784
E: gmatthews1@kpmg.com

Lem Chin Kok
Partner
KPMG in Singapore
T: +65 62132495
E: clem@kpmg.com.sg

Emerson Melo
Sócio líder da prática de Forensic da KPMG no Brasil
T: +55 11 3940 4526
E: emersonmelo@kpmg.com.br

Carolina Paulino
Sócia Forensic da KPMG no Brasil
T: +55 11 3940 4096
E: cpaulino@kpmg.com.br

Dino Almeida
Sócio Forensic da KPMG no Brasil
T: +55 11 3940 4545
E: dinoalmeida@kpmg.com.br

Fernanda Flores
Sócia Forensic da KPMG no Brasil
T: +55 11 3940 4891
E: fernandaflores@kpmg.com.br

Marcelo Gomes
Sócio Forensic da KPMG no Brasil
T: +55 11 3940 4829
E: marceloagomes@kpmg.com.br

Raphael Sore
Sócio Forensic da KPMG no Brasil
T: +55 11 3940 5958
E: rsore@kpmg.com.br

Thais Silva
Sócia Forensic da KPMG no Brasil - RJ
T: +55 21 2207 9237
E: thaisasilva@kpmg.com.br

Alessandro Gratão
Sócio-diretor Forensic da KPMG no Brasil
T: +55 11 3940 5740
E: alessandrogratao@kpmg.com.br

Fernando Lage
Sócio líder GRC da KPMG no Brasil
T: +55 19 3198-6745
E: flage@kpmg.com.br

Alexandre Martins,
Sócio Risk Advisory Solution da KPMG no Brasil
T: +554133042737
E: amartins@kpmg.com.br

Patricia Silva
Sócia Risk Advisory Solution da KPMG no Brasil
T: +55 31 2128 5740
E: pssilva@kpmg.com.br

Carlos Tomiato
Sócio Financial Services da KPMG no Brasil
T: +55 11 3940 5493
E: ctomiato@kpmg.com.br

Eduardo Azevedo
Sócio-diretor Auditoria Interna e Compliance da KPMG no Brasil
T: +55 11 3940 5123
C: eduardoazevedo@kpmg.com.br

Ser criativo transforma negócios.

#KPMGTransforma

Baixe o APP KPMG South America

kpmg.com.br /kpmgbrasil