# Third Party Risk Management (TPRM)

**Gerenciando o risco de terceiros – Plataforma de *due diligence* efetiva**

## Realidade de hoje

As empresas de todos os setores dependem cada vez mais de uma rede robusta de terceiros, como terceiros intermediários, fornecedores, distribuidores, agentes, joint ventures, alianças, subcontratados, prestadores de serviços, entre outros. Esta rede é fundamental para manter uma presença global, diferencial competitivo e concorrer com eficácia e eficiência no mercado.

Embora os terceiros sejam fundamentais para uma empresa atuar globalmente, os riscos associados a eles não podem ser terceirizados. Há muitos casos em que a falta de supervisão e monitoramento adequado de terceiros gerou graves consequências. As empresas globais foram expostas a riscos significativos, afetando negativamente seu desempenho, imagem e reputação, além do impacto financeiro.

## Compliance regulatório e aderência às boas práticas internacionais

Os órgãos regulatórios em todo o mundo esperam que as empresas tenham uma supervisão e monitoramento efetivo e eficiente de seus terceiros. As empresas tiveram que priorizar e aprimorar seus esforços de *compliance* em consequência de ações de execução e multas notórias em função de casos de suborno e corrupção, lavagem de dinheiro e violações. De fato, a maioria dos casos reportados, envolveu suborno por meio de intermediários externos.

Diversos organismos internacionais publicaram regulamentações e boas práticas quanto ao ciclo de vida de terceiros (identificação, avaliação de riscos, *due diligence*, integração, avaliação e monitoramento contínuo) relacionadas à eficácia dos programas de *compliance*. O Departamento de Justiça (DOJ) e a Comissão de Valores Mobiliários (SEC) dos EUA elaboraram um guia  conjunto que estipulava como a *due diligence* baseada em riscos é particularmente importante com terceiros e será considerada ao avaliar a efetividade do programa de compliance de uma empresa. Além disso, o DOJ forneceu orientações detalhadas recentemente sobre a Avaliação de Programas de Compliance Corporativo .

A supervisão e o monitoramento do ciclo de vida de terceiros evoluíram de uma abordagem reativa para uma de alinhamento aos programas globais de *compliance* corporativo. Para obter essa congruência, os programas de gerenciamento de riscos de terceiros (TPRM) ideais precisam ir além da função de compras e englobar outras partes interessadas e departamentos em toda a empresa. Esses programas também ganharão maturidade via automação — em que a organização tira proveito dos dados e obtém um entendimento dos riscos por meio da tecnologia para aprimorar o gerenciamento de terceiros de maneira sustentável.

1. https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf
2. https://www.justice.gov/criminal-fraud/page/file/937501/download

**Em uma pesquisa recente da KPMG com diretores de Compliance (CCOs), diversos entrevistados disseram que não implementaram as boas práticas para gerenciar seus riscos de *compliance* de terceiros.**

# Principais desafios

Há vários desafios enfrentados pelos executivos e *compliance officers (CCO)* no que tange ao gerenciamento de riscos de terceiros, como:

- Dificuldade em identificar e gerenciar terceiros consistentemente e realizar as avaliações de risco associadas.
- Tempo e experiência necessários para implementar programas de *due diligence* robustos baseados em riscos.
- Falta de capacidade de demonstrar aos reguladores que a supervisão e os controles apropriados estão implementados e funcionando de maneira eficaz.
- Falta de visibilidade das práticas de negócios de terceiros e funções de risco / supervisão.
- Maior risco de perda de dados e violações de privacidade.
- Ausência de um sistema robusto para assessorar na avaliação e monitoramento dos terceiros.

Os reguladores e as boas práticas não defendem um único programa para todas as situações. A abordagem e a implementação do programa de TPRM precisam estar alinhadas às necessidades de negócios de uma empresa, como tamanho, complexidade e perfil e apetite de risco, entre outros fatores. Ao mesmo tempo, querem ver como a estrutura de gerenciamento de terceiros de uma empresa integra um foco preventivo e detectivo, permitindo também que as três linhas de defesa  atuem holisticamente por meio da adoção de elementos de governança importantes em todo o ciclo de vida do TPRM.

# A perspectiva do CCO

Na terceira edição da Pesquisa Maturidade do Compliance no Brasil, a KPMG obteve informações de profissionais de compliance (CCOs) em todos os setores. Esses CCOs discutiram desafios fundamentais, incluindo o entendimento de onde e como os dados relacionados a terceiros são coletados, como devem ser realizadas as avaliações de risco e como as informações devem ser utilizadas — tudo isso conseguindo gerenciar o processo de uma maneira eficaz, consistente e eficiente. Como parte dessas discussões, surgiram necessidades específicas de negócios:

- **Identificação e gerenciamento de terceiros por meio de uma abordagem baseada em riscos.** Um dos principais desafios para o processo de *due diligence* de terceiros é classificar os tipos de terceiros e realizar um exercício de estratificação de riscos, seguido pelo monitoramento e auditorias regulares dos relacionamentos. Os CCOs observaram que a realização do mesmo nível de *due diligence* para todos os terceiros não seria viável e/ou eficaz e eficiente do ponto de vista de gestão de riscos. Portanto, ao classificar os terceiros com base em critérios definidos (ou seja, o valor do relacionamento, o risco-país e o tipo de terceiro), a empresa pode identificar um nível de risco que determinaria o nível de *due diligence* exigido.
- **Integração de processos de terceiros entre as funções de negócios e de *compliance* e definição clara de funções e responsabilidades.** Algumas empresas optaram por ter um modelo descentralizado para integrar e gerenciar seus terceiros. No entanto, isso levou ao desenvolvimento de muitos processos incongruentes, afastando-se de uma abordagem consistente que uma função de conformidade central instituiria. Os CCOs observaram que a aplicação prática de processos de tomada de decisões envolvendo o negócio, *compliance*, área jurídica e ética pode ser difícil.
- **Processos de gerenciamento de riscos de terceiros unificados, impulsionados por sólidas soluções de tecnologia e automação.** Alguns CCOs expressaram um desafio com processos manualmente intensivos e falta de automação. Métodos mais antigos de avaliação de terceiros, incluindo direitos de auditoria de terceiros, não são baratos ou efetivos se aplicados isoladamente sem suporte de uma tecnologia adequada.

# As armadilhas de *due diligence*

As funções de *compliance* e gerenciamento de riscos podem ficar sobrecarregadas com a manutenção da supervisão dentro da própria organização e talvez não tenham o tempo, as habilidades e/ou os recursos para manter a visibilidade sobre a rede de terceiros da empresa. Como resultado, níveis inadequados de *due diligence* são realizados. A simples realização de sanções e verificações de pessoas politicamente expostas (PEP), ou a realização de pesquisas básicas na Internet, geralmente não gera *insights* úteis. Em alguns casos, as empresas quase não realizam verificações, além de obterem informações autorreportadas de terceiros por meio de questionários ou relatórios de crédito.

3. As três linhas de defesa são definidas como 1ª: a empresa, 2ª: compliance e gestão de riscos e 3ª: auditoria interna

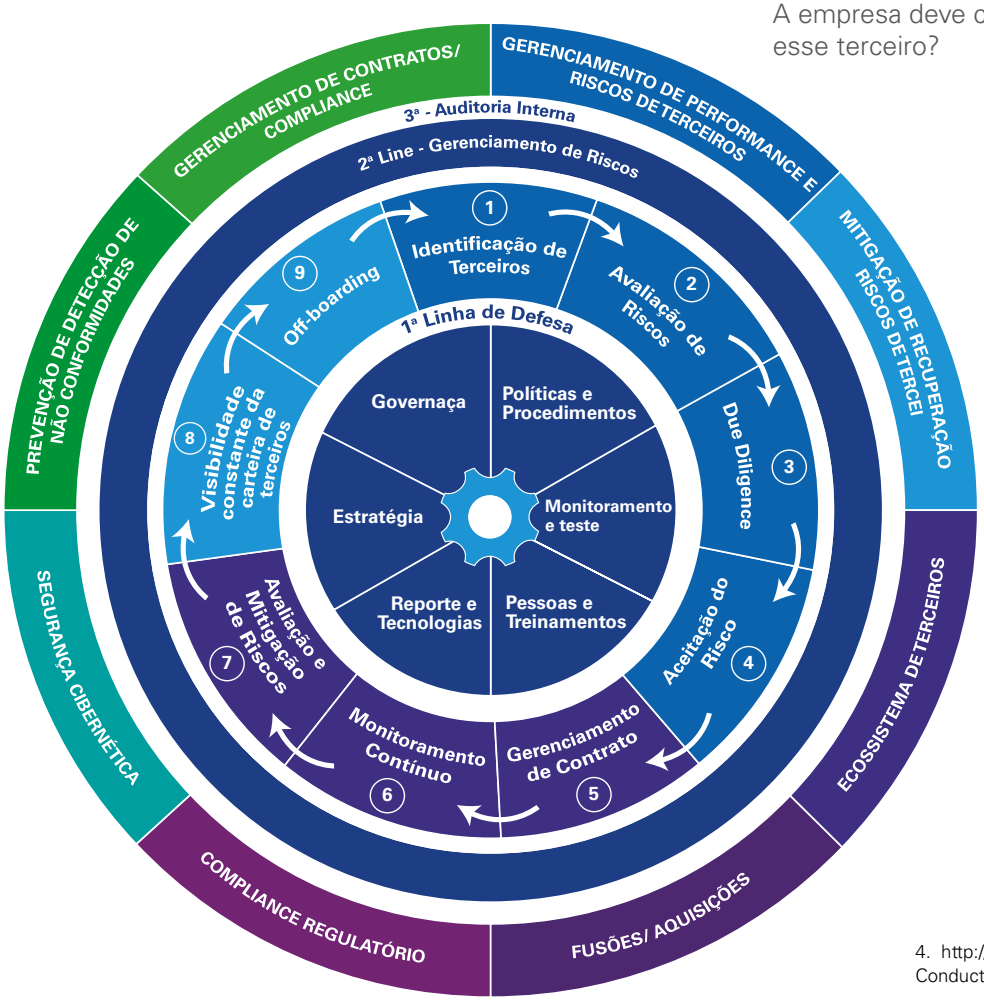
**A Iniciativa de Parceria Contra a Corrupção (PACI) do Fórum Econômico Mundial [4] divide o processo de pré-integração em três etapas essenciais nas suas orientações oficiais para uma *due diligence* apropriada: (1) entender o escopo do universo de terceiros, (2) realizar avaliações de risco em entidades individuais para determinar o nível de *due diligence* necessário e (3) realizar procedimentos de *due diligence*. Além disso, o guia do Departamento de Justiça Americano (DOJ) e da Comissão de Valores Mobiliários dos EUA (SEC) para a FCPA estipula que as empresas devem entender "as qualificações e associações de [seus] parceiros terceirizados, incluindo [sua] reputação de negócios".**

Sem uma visão inteligente e contínua da rede de terceiros de uma empresa nas fases de pré-integração, avaliação de riscos e pós-desempenho, as organizações ficam vulneráveis a riscos significativos de negócio, imagem, reputação e *compliance*. É fundamental que as empresas entendam onde estão os riscos, como identificá-los e quais medidas devem tomar para proteger sua marca e seu resultado final. Esses desafios trazem à luz novos desafios de negócios: a necessidade de avaliar, monitorar e gerenciar proativamente o desempenho de terceiros e implementar processos robustos para assegurar esse comportamento proativo.

# Principais tendências *due diligence*

As boas práticas em relação ao gerenciamento de riscos de terceiros defendem uma abordagem baseada em riscos:

- **Estabelecer o escopo.** Entender o universo de relacionamentos com terceiros e realizar análises de riscos para determinar os terceiros que estariam no escopo para uma análise adicional.
- **Elaborar um processo de avaliação de riscos.** Instituir um processo de avaliação de riscos que seja diferenciado pelo nível do fornecedor e pelo foco no risco, visando a determinar os níveis adequados de análise desses terceiros, nos quais informações adicionais são necessárias.
- **Realizar uma *due diligence* baseada nos riscos.** A partir da avaliação, realizar a *due diligence* baseada nos riscos apropriada para obter informações fundamentais para gerenciar os riscos de negócio.
- **Monitorar e gerenciar ativamente.** Monitorar continuamente e gerenciar terceiros ativamente, o que ajudará a responder às principais questões de negócio: a empresa deve fazer negócios com esse terceiro? Como esse terceiro está gerindo seus riscos que possam impactar seus clientes? A empresa deve continuar fazendo negócios com esse terceiro?




4. http://www3.weforum.org/docs/WEF_ PACI_ ConductingThirdPartyDueDiligence_Guidelines_2013.pdf

# Integrar tecnologia e Data & Analytics

Com a utilização de um maior número de fontes de dados on-line, a aplicação da tecnologia por meio de técnicas de aprendizado de máquina e análises avançadas para pesquisa, as avaliações iniciais de riscos podem ser realizadas com um maior volume de relacionamentos de maneira mais inteligente, rápida e barata. A análise humana pode ser aplicada para a *due diligence* em terceiros mais arriscados, onde os resultados iniciais precisam ser interpretados, e pesquisas adicionais podem ser ampliadas e analisadas conforme necessário. Quando a automação e os processos manuais são integrados, as empresas têm a capacidade de escalar a *due diligence* para uma rede maior, se não completa, de terceiros.

Essas soluções também podem ser integradas a outras plataformas corporativas, fornecendo uma melhor visão do universo de terceiros e clareza sobre as funções e responsabilidades nas linhas de defesa e funções de supervisão de riscos.

Há outros benefícios transformadores envolvidos como consequência da implementação da tecnologia e análise de dados:

- Alinhamento das políticas e práticas de TPRM às atividades de compras e contratações
- Obtenção de um maior entendimento sobre a dependência da organização em relação a terceiros e seus subcontratados
- Redução na redundância de atividades para avaliar terceiros
- Desenvolvimento de um maior uso da automação para gerenciar terceiros
- Implementação de processos consistentes em toda a organização em relação ao tratamento de terceiros
- Esclarecimento da análise de custo-benefício, considerando o custo real da supervisão dos serviços
- Melhoria da prestação de contas para o Conselho, com uma visão abrangente de terceiros, estratégias, tendências e problemas críticos.

# Seguindo em frente

Embora as empresas continuem enfrentando riscos complexos em ambientes de negócios dinâmicos e os reguladores permaneçam pressionando as empresas para que elas estejam conformes, continuará sendo essencial que os negócios mantenham uma abordagem sustentável para que qualquer programa de gerenciamento de riscos de terceiros seja bem-sucedido.

TPRM é a plataforma tecnológica, desenvolvida pela KPMG no Brasil, que permite diversos acessos simultâneos de fontes individuais de informação públicas e privadas e também possibilita uma avaliação completa, eficiente e de alto valor agregado de seus terceiros.

# Fale com o nosso time


**Emerson Melo**
**Sócio-líder de Compliance da KPMG no Brasil**
(11) 3940-4526
emersonmelo@kpmg.com.br

**Ricardo Santana**
**Sócio, KPMG Lighthouse**
santana@kpmg.com.br
(11) 3940-3816

**Carolina Paulino**
**Sócia-diretora Strategic & Compliance Risk da KPMG no Brasil**
CPaulino@Kpmg.com.br
(11) 3940-4096

**Dino Almeida**
**Gerente Sênior Strategic & Compliance Risk da KPMG no Brasil**
dinoalmeida@kpmg.com.br
(11) 3940-4545

**Enio Lourenço**
**Gerente KPMG Lighthouse**
elourenco@kpmg.com.br
(11) 3940-4031

**Sheila Valdevino**
**Gerente de Strategic & Compliance Risk da KPMG no Brasil**
SValdevino@kpmg.com.br
(11) 3940-1702


Baixe o APP
**KPMG Brasil**

**kpmg.com.br**
/kpmgbrasil




Projeto Gráfico e diagramação: Gaudí Creative Thinking.