Construindo confiança com seus terceiros num mundo tecnológico e disruptivo

Pesquisa Global EY de Gestão de Risco de Terceiros 2019-20

Resultados gerais da pesquisa

EY
Building a better working world

Disclaimer

- Nenhuma parte deste documento pode ser reproduzida, transmitida ou distribuída de qualquer forma ou por qualquer meio, eletrônico ou mecânico, inclusive por fotocópia, transmissão por fax, gravação, reutilização ou uso de qualquer sistema de armazenamento e recuperação de informações, sem permissão por escrito da EY. Qualquer reprodução, transmissão ou distribuição deste formulário ou de qualquer material aqui contido é proibida.
- Esses slides são apenas para fins educacionais e não se destinam, nem devem ser considerados, como consultoria contábil.
- As porcentagens são apresentados como números inteiros. Como resultado, algumas porcentagens podem não totalizar 100%.

Table of contents

03 Resultados Globais

05 Dados demográficos dos entrevistados

08 Programa de gestão de risco de terceiros organização, governança e oversight

14 Distribuição das população de terceiros/classificação de riscos

18 Asessments

25 Gestão de incidentes / tratamento de riscos

28 Gestão de quarteirizados

31 Tecnologia

34 Reportes

36 Cybersecurity e resposta a ameaças

39 Solicitações de entrada

42 Regulações de privacidade

44 Inspeções regulatórios e de auditoria interna

46 Terceiros não tradicionais

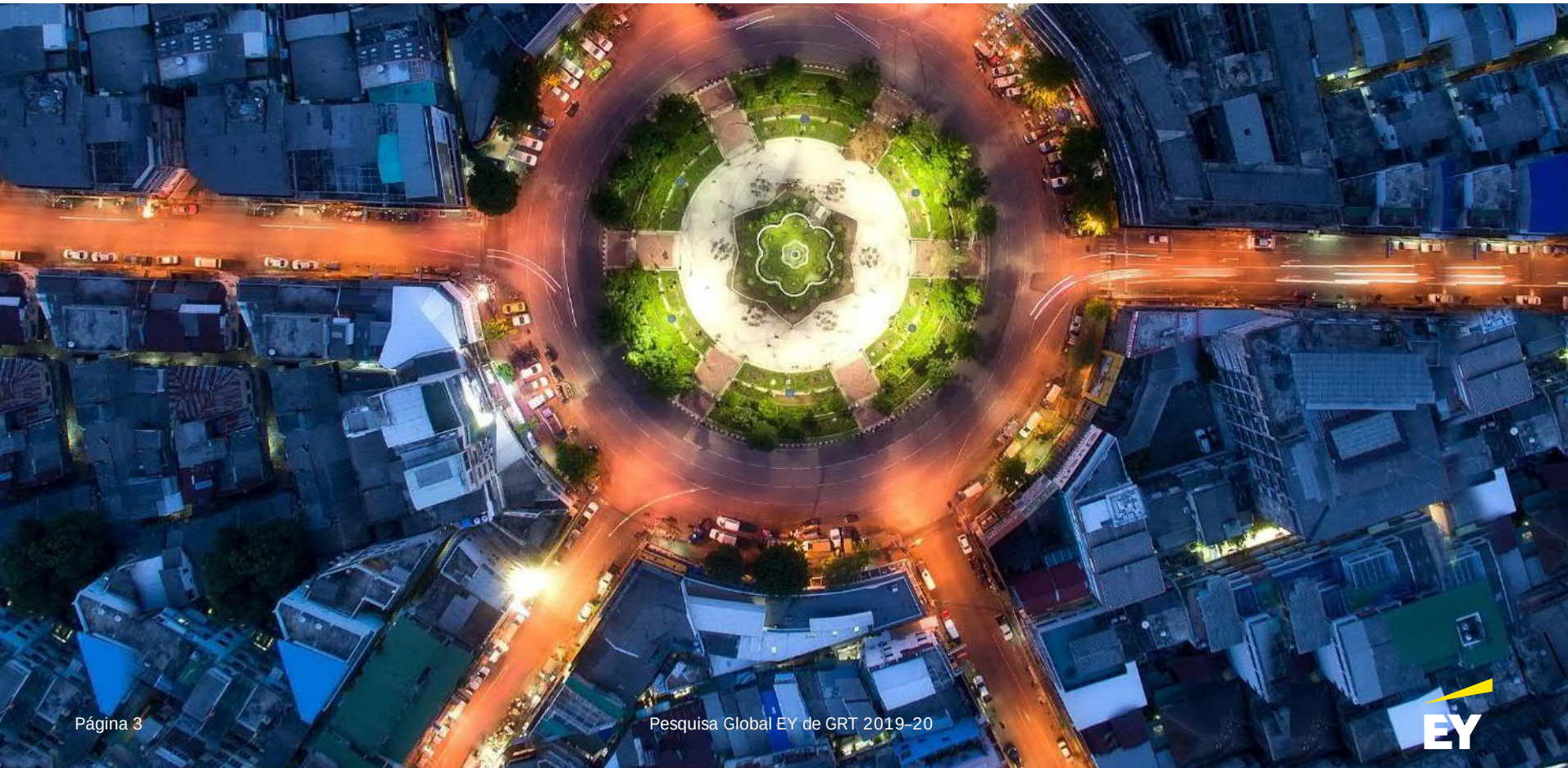
48 Concentração de riscos (somente para serviços financeiros)

50 Gerenciamento de afiliados (somente para serviços financeiros)

54 Inovação

56 Áreas de Investimento

Resultados Globais



Contexto

De Julho a Setembro de 2019, os profissionais da EY conduziram em vários países, uma pesquisa com 246 organizações de diversos portes, níveis de maturidade e setores. Ainda que os executivos que responderam à pesquisa desempenhem funções diferentes dentro de cada organização, todas essas funções lidavam com gestão de risco de terceiros. Esses papéis incluíram, mas não se limitaram a, gerenciamento de riscos corporativos, procurement, cybersegurança, auditoria interna e finanças. O objetivo da pesquisa foi endereçar as diferentes especificações de risco de terceiros em setores distintos.

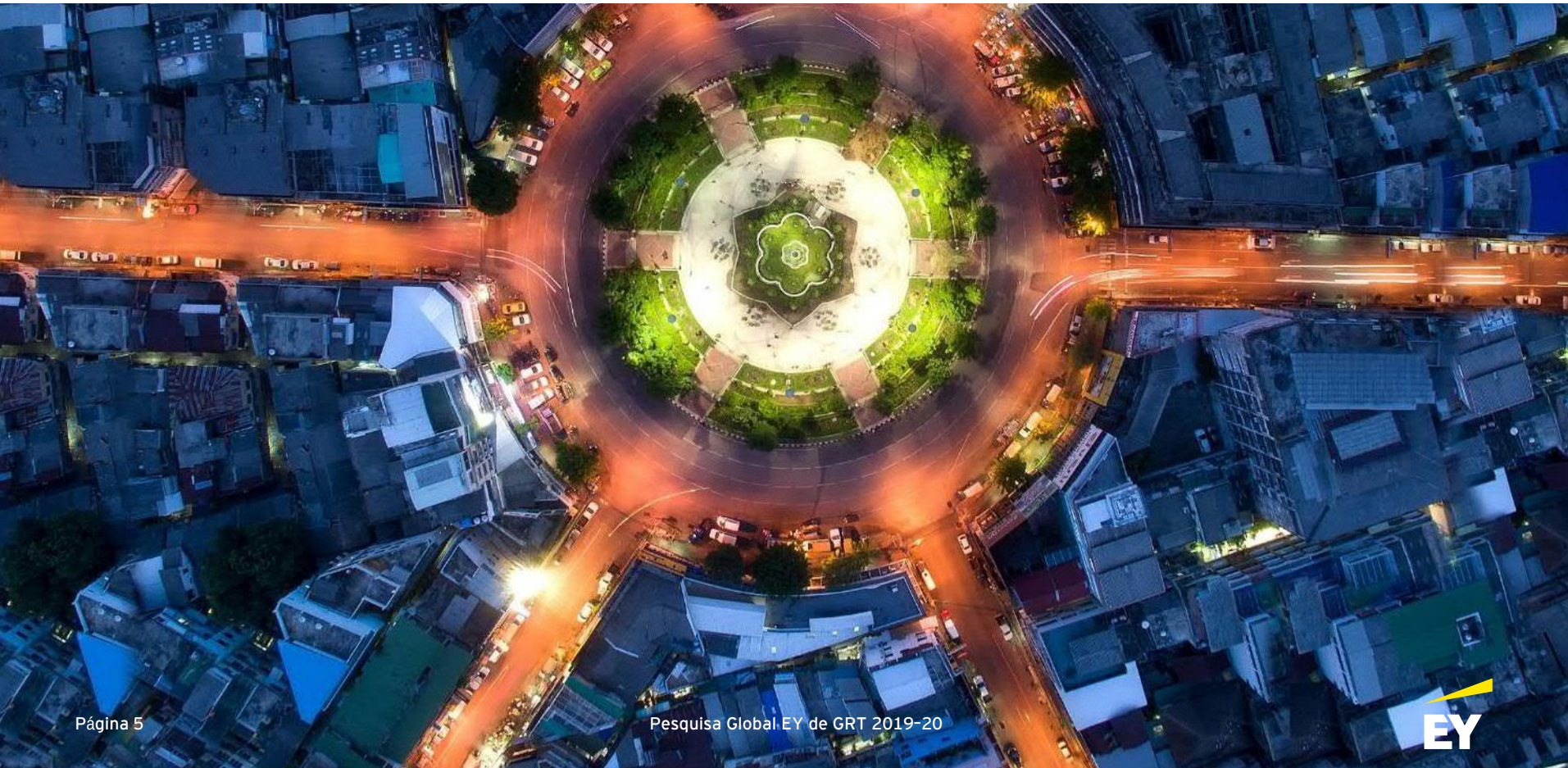
Setores na pesquisa incluíram, mas não se limitaram a bens de consumo e varejo, serviços de saúde, ciências biológicas, mídia e entretenimento, tecnologia, energia e serviços.

Nessa pesquisa, pedimos aos participantes que respondessem questões-chave sobre seus respectivos programas de gestão de risco de terceiros (GRT). Incluindo tópicos como:

- Programa de gestão de risco de terceiros/ Funções na organização, governança e oversight
- Distribuição da população de terceiros/ Classificação de riscos
- Impostos
- Gestão de incidentes/ Tratamento de riscos
- Gestão de quarteirizados
- Apresentação de relatórios
- Tecnologia
- Cybersecurity e resposta a ameaças
- Solicitações de entrada
- Regulações de privacidade
- Inspeções regulatórias e de auditoria interna
- Terceiros não tradicionais
- Concentração de riscos (somente para serviços financeiros)
- Gerenciamento de afiliados (somente para serviços financeiros)
- Inovação

Esse documento inclui os resultados agregados para cada questão em todos os setores.
Para quaisquer questões, suporte para a interpretação de dados ou demandas de dados específicos, contatar GRT@ey.com.

Dados demográficos dos entrevistados



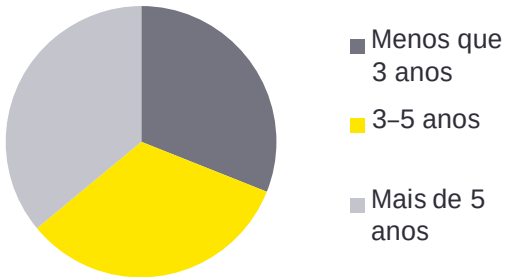
Dos 246 participantes na pesquisa, o maior número de pesquisados foi do setor bancário e de capitais, como resultado de pressões regulatórias. Logo após tivemos os setores de seguros; tecnologia, mídia e entretenimento e telecomunicações; manufatura avançada e mobilidade; e bens de consumo.

Perfil de respondentes (Q1) número de respondentes

Quase dois terços das companhias pesquisadas são americanas, mais de um quarto são europeias, e as remanescentes são da Ásia-Pacífico. As companhias se dividiram quase igualmente entre aquelas que tinham programas de gestão de risco terceirizados ativos há mais de 5 anos, de 3 à 5 anos e menos de 3 anos.

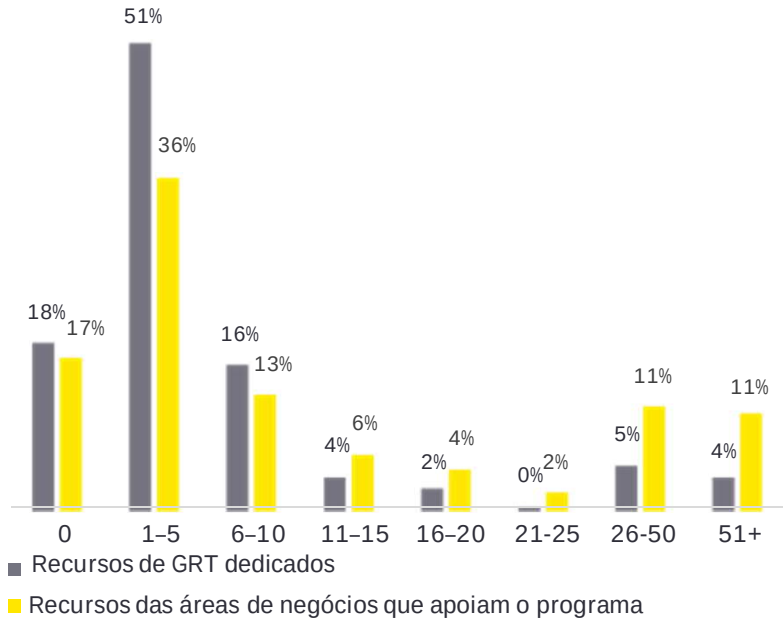
Perfis dos respondentes (Q2, Q3 e Q4)	Participantes	
Por região	#	%
Américas	155	63%
Europa	75	30%
Ásia-Pacífico	16	7%
Por Tamanho (headcount)		
Menos de 5,000	88	36%
5,001 a 15,000	52	21%
15,001 a 25,000	27	11%
25,001 a 50,000	25	10%
50,001 a 100,000	28	11%
Mais do que 100,000	26	11%

Tempo de vida do programa de GRT

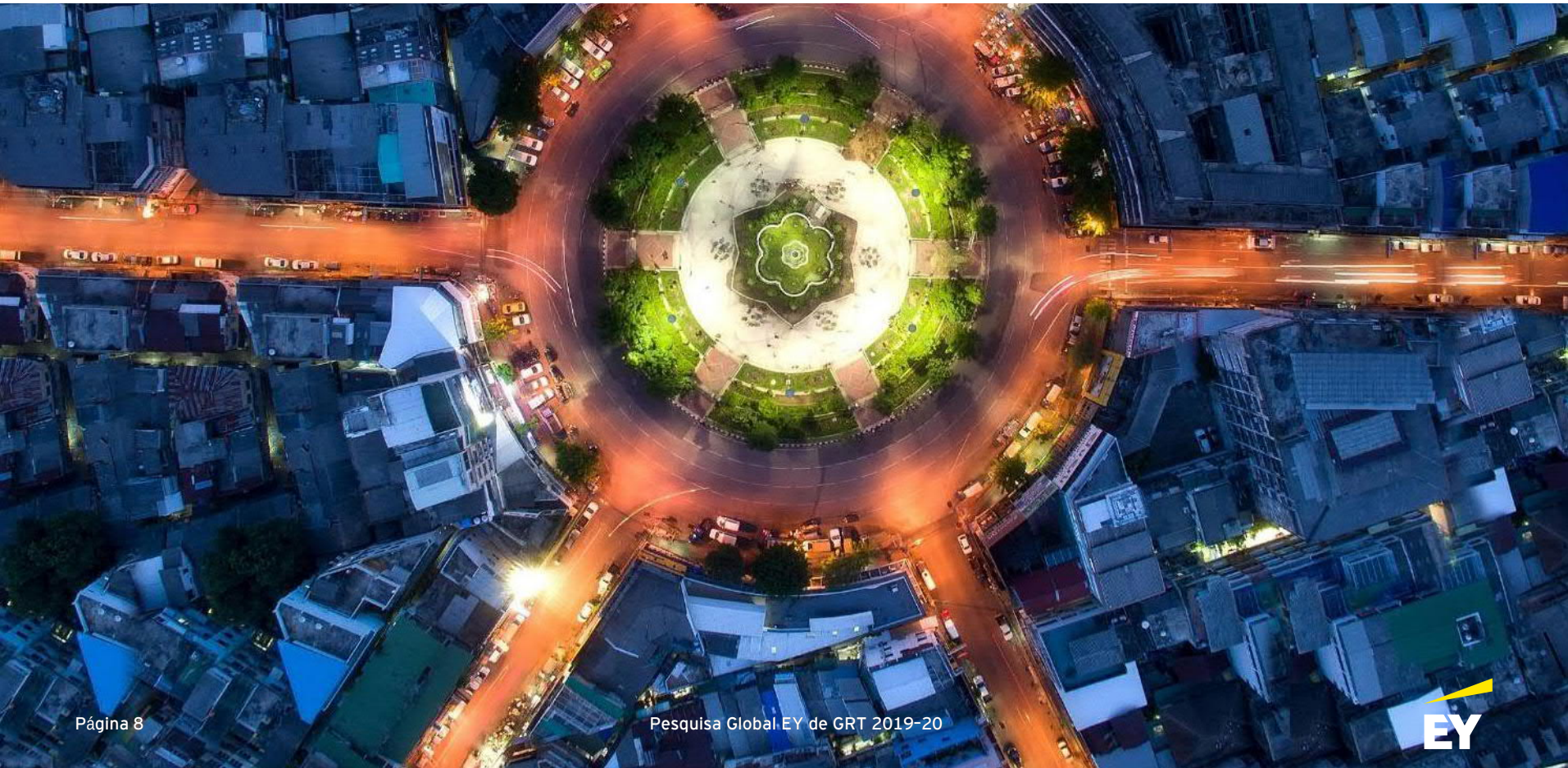


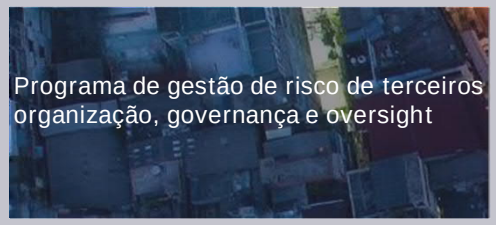
Recursos dos Programas GRT

Q8. Quantos recursos suportam o seu programa de gestão de risco de terceiros nas seguintes categorias?



Programa de gestão de risco de terceiros organização, governança e oversight





Programa de gestão de risco de terceiros organização, governança e oversight

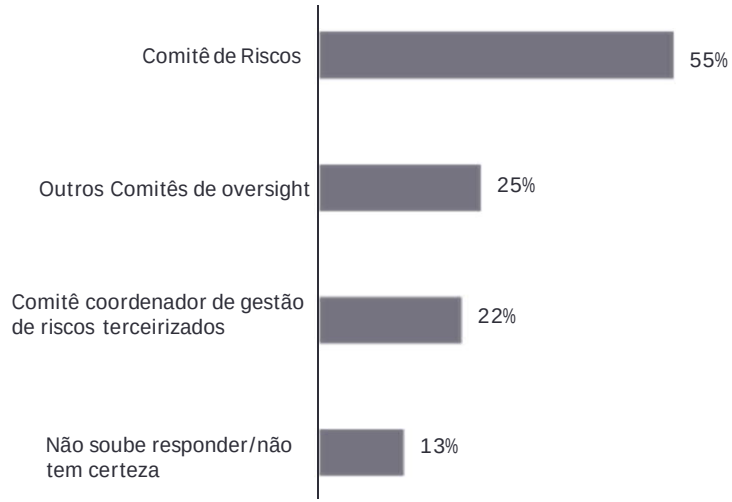
Modelos centralizados e híbridos continuam sendo a estrutura mais comum em programas GRT, traduzindo a importância de uma consistente, e ainda assim flexível, função de GRT em toda a organização.

Estrutura do programa de GRT

Q5. Como é estruturado seu programa de gestão de riscos terceirizado?

Supervisão do programa de GRT

Q6. Qual dos seguintes comitês é responsável por monitorar as atividades do seu programa de gestão de riscos de terceiros?

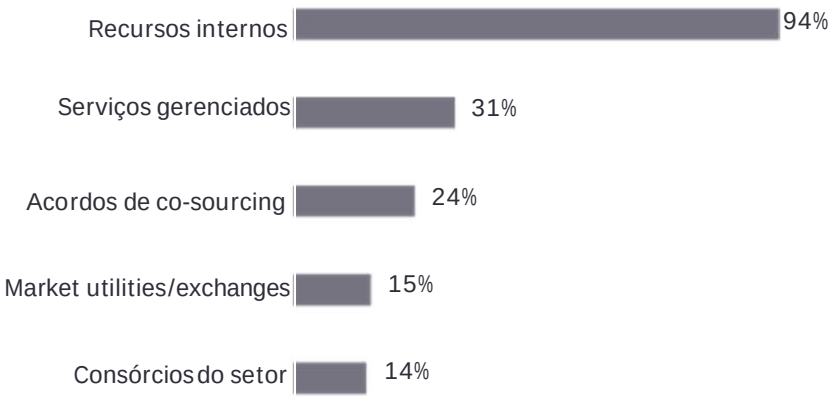


Programa de gestão de risco de terceiros organização, governança e oversight

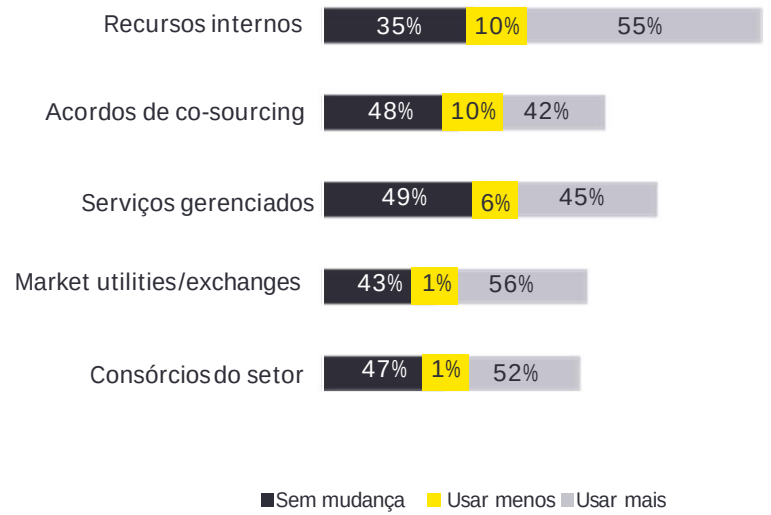
Num horizonte de 2 a 3 anos, existe um claro desejo entre as organizações entrevistadas de alavancar soluções externas mais ativamente. Mais de 40% delas esperam usar mais frequentemente prestadores de serviços para gerenciamento ou co-sourcings para executar sua função de gestão de riscos de terceiros; essa porcentagem salta para mais de 50% para Consórcios do setor e market utilities.

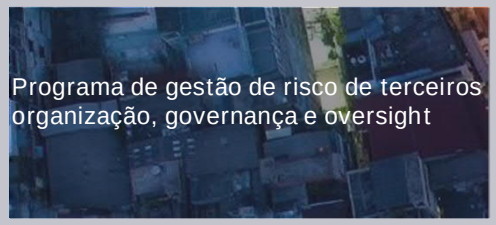
Execução de GRT

Q7A. A sua organização usa atualmente alguma das opções a seguir para execução do seu programa de gestão de riscos de terceiros?



Q7B. Como você espera que isso esteja nos próximos dois ou três anos?

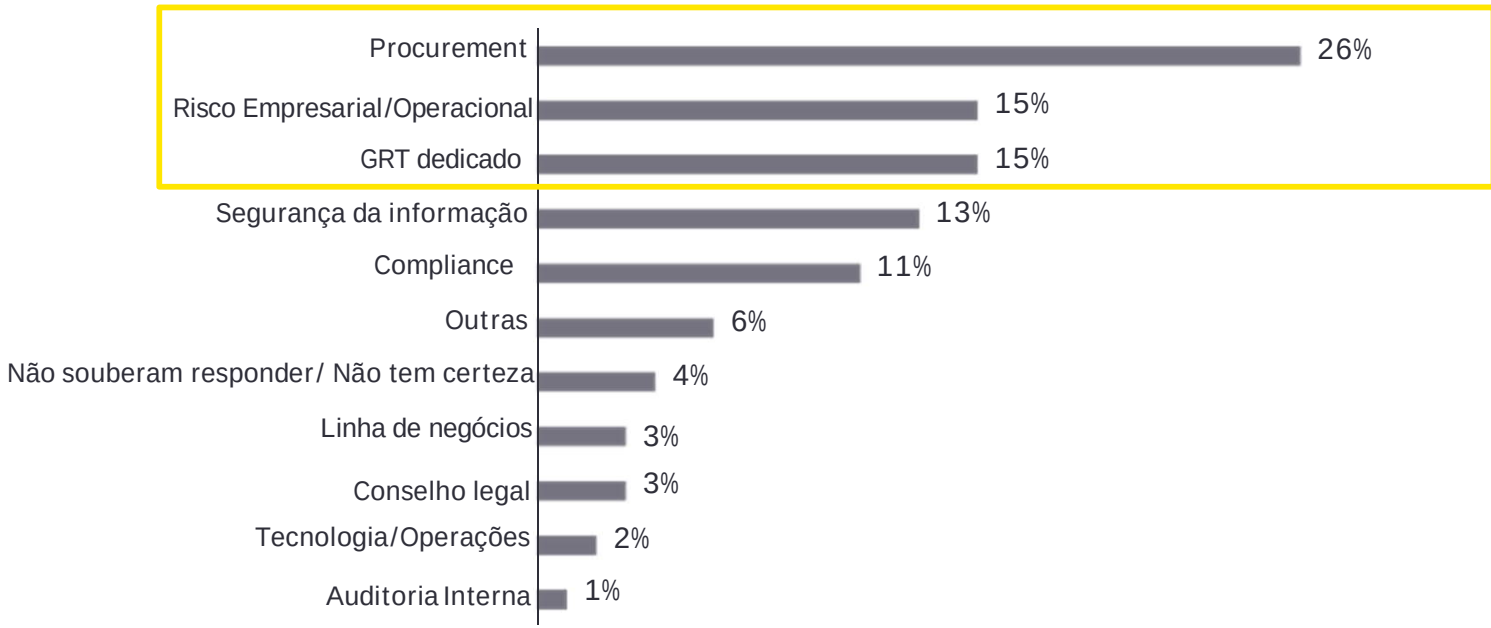




Não há um consenso entre as organizações respondentes sobre quem efetivamente é responsável pela função de GRT; 26% dos respondentes indicam que o Procurement tem responsabilidade primária, enquanto 15% indicam que risco empresarial/operacional tem a responsabilidade. Outros 15% indicam ter um grupo dedicado Responsável pela GRT.

Integração com o programa de GRT

Q9.Qual área tem responsabilidade primária do programa/função de GRT?

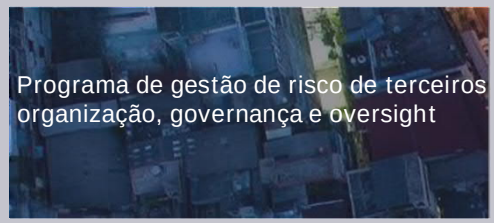


Com o ciclo de vida de GRT envolvendo tantas áreas de uma organização, não é nenhuma surpresa que as organizações pesquisas tenham abordagens diferentes. Enquanto existe certo consenso na responsabilidade de procurement na gestão de inventário de terceiros e no encerramento e vencimento de contratos, há pouco consenso na responsabilidade nas atividades relacionadas a riscos.

Área responsável por GRT

Q10. Qual área tem responsabilidade primária na execução dos componentes a seguir no programa de gestão de risco de terceiros da sua organização?

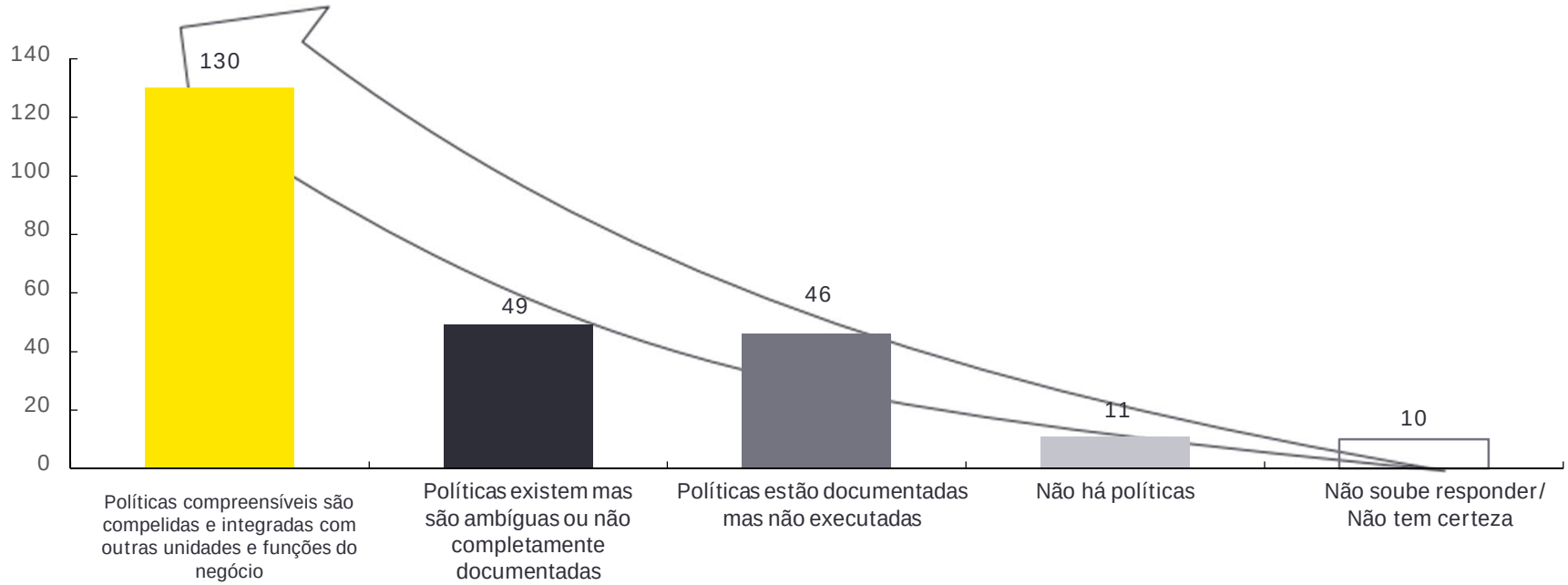
Componente	Procurement	Gestão de Riscos de Terceiros	Conselho Legal/Geral	Segurança da Informação	Risco Operacional/ Empresarial	Compliance	Linha de Negócios	Tecnologia/ Operações	Auditoria Interna	Outros	Ainda não conduzida
Gestão de inventário de terceiros	40%	20%	2%	6%	6%	6%	11%	2%	1%	1%	5%
Desenho e facilitação de risk assessment/ framework	12%	24%	5%	16%	17%	11%	4%	3%	2%	2%	3%
Revisão e atualização de termos de contratos como parte do monitoramento contínuo	27%	5%	35%	7%	1%	5%	15%	1%	1%	1%	3%
Identificação de contratos expirados	48%	4%	17%	2%	1%	2%	21%	1%	1%	1%	3%
encerramento de contratos	38%	4%	24%	2%	1%	1%	25%	1%	0%	1%	1%
Gestão de problemas/ Tratamento de riscos	8%	15%	6%	12%	14%	11%	24%	4%	3%	2%	2%



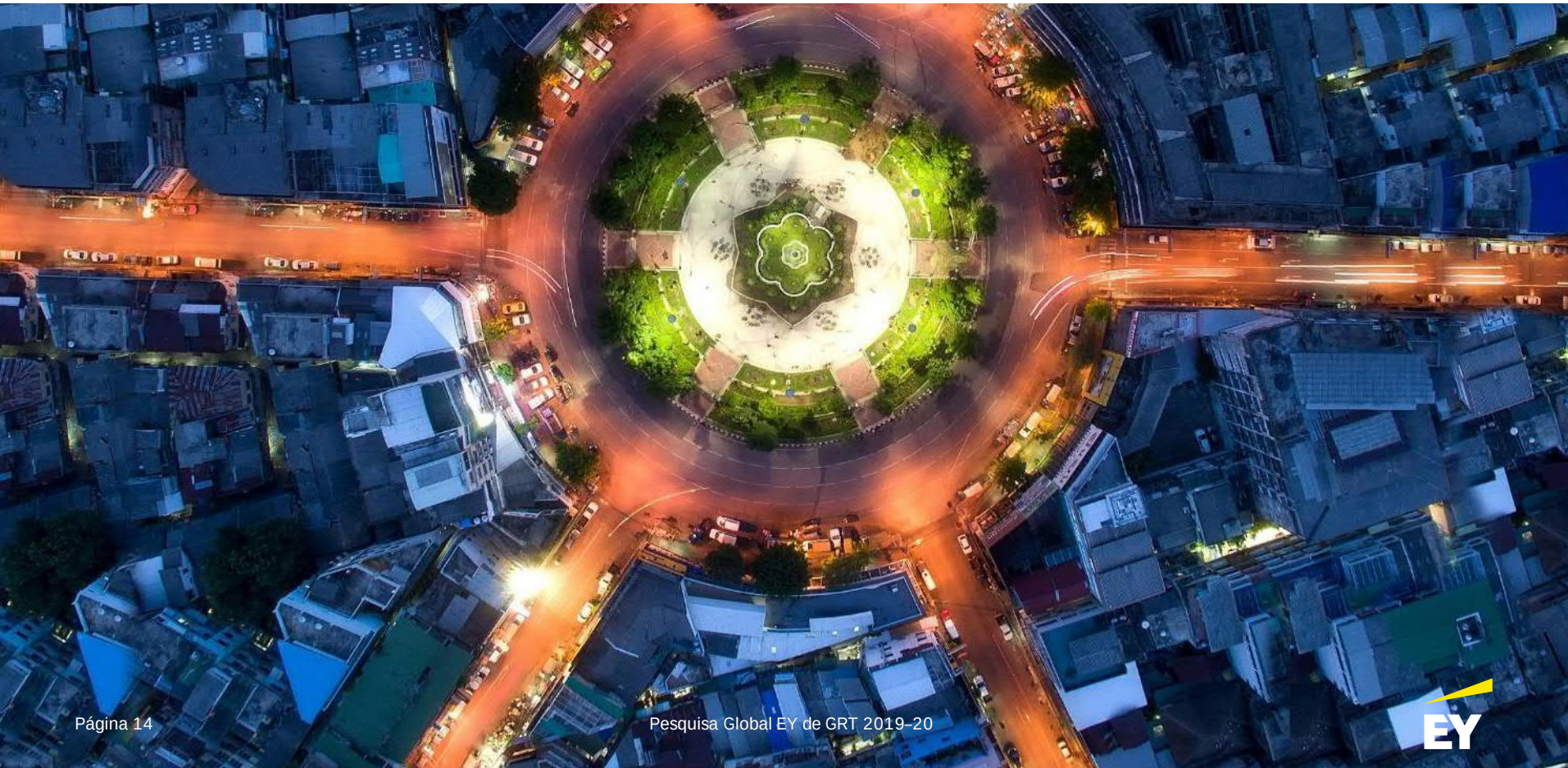
Mais da metade das organizações respondentes indicaram ter políticas compreensivas, compelidas e integradas; porém, 39% indicaram ter políticas documentadas mas que não são efetivamente executadas, ou são executadas mas não completamente documentadas, o que indica que ainda há uma longa curva de maturidade para diversas organizações.

Tipos de políticas de GRT

Q11. Qual das seguintes opções melhor descreve as políticas que sua organização utiliza atualmente para sustentar o programa/função de GRT?



Distribuição da população de terceiros/classificação de riscos



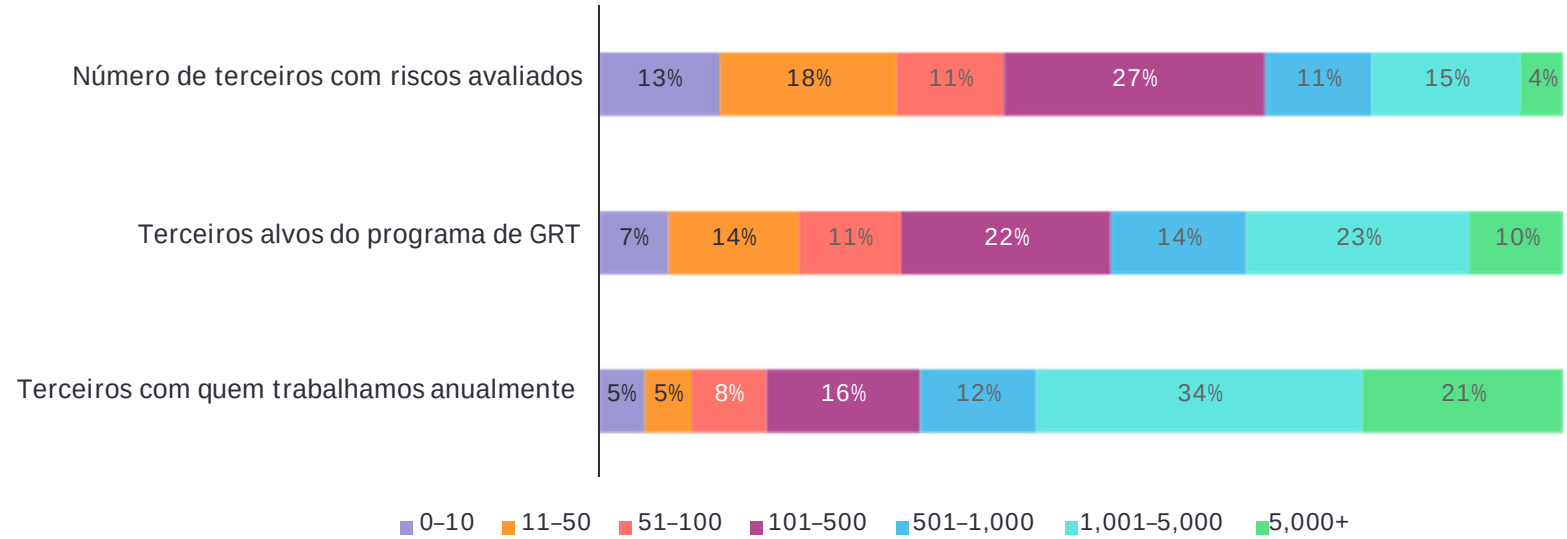
De maneira análoga aos anos anteriores, onde havia um consenso geral sob a porcentagem de terceiros sujeito ao programa de GRT ou à avaliação de risco, observa-se hoje em dia mais variabilidade nos terceiros considerados do inventário. Isso provavelmente se deu aos desafios contínuos na totalidade de inventários e nas mudanças dos ambientes de riscos relevantes.

Volume de Terceiros

Q12. Sua organização trabalha aproximadamente com quantos terceiros anualmente?

Do número total de terceiros, aproximadamente quantos são alvos de seu programa de gestão de risco de terceiros?

Do total de terceiros no seu programa, quantos tiveram seus riscos avaliados?

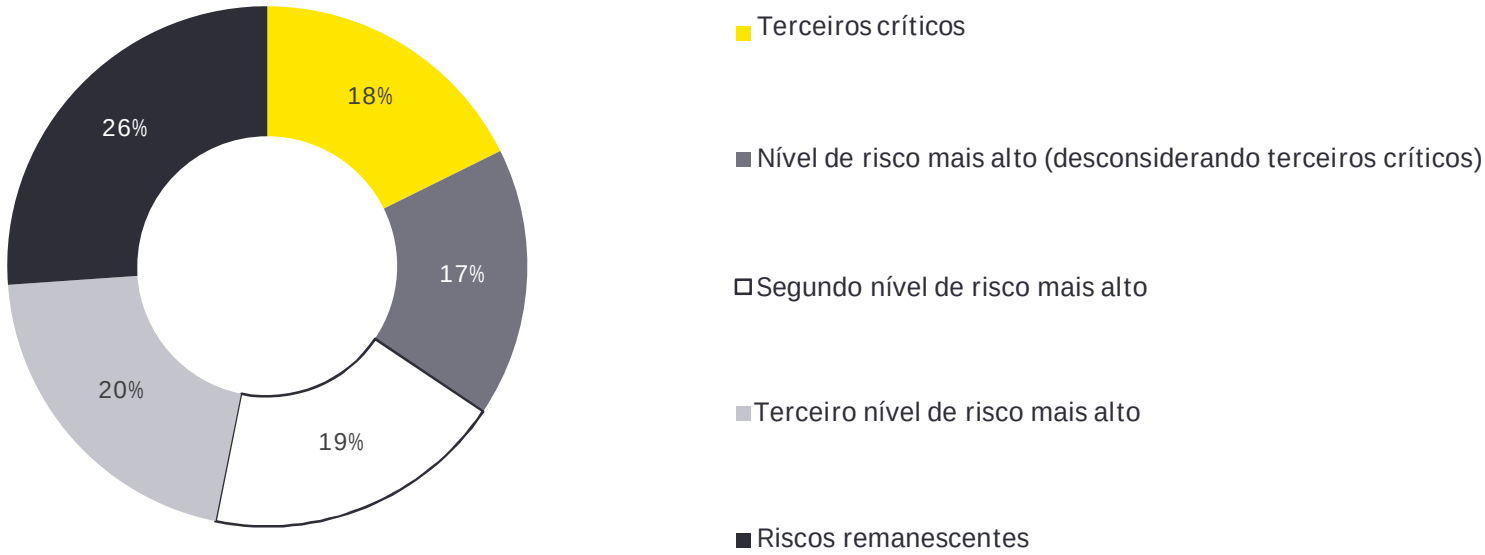


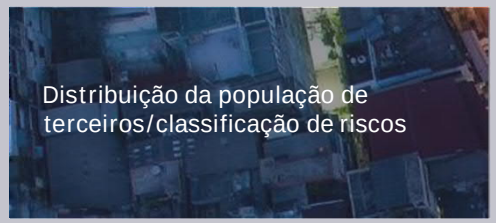
Distribuição da população de terceiros/classificação de riscos

Em comparação com anos anteriores, a natureza dos terceiros críticos é altamente dependente de diferenças de maturidade nos setores.

Escala de risco de terceiros

Q13. Qual porcentagem dos terceiros está no escopo de GRT da sua organização em cada um dos seguintes níveis de risco?
O total deve ser igual a 100%





Em linha com o slide anterior, os critérios para crítico dependem do setor, reduzindo o valor dos dados consolidados em nível global.

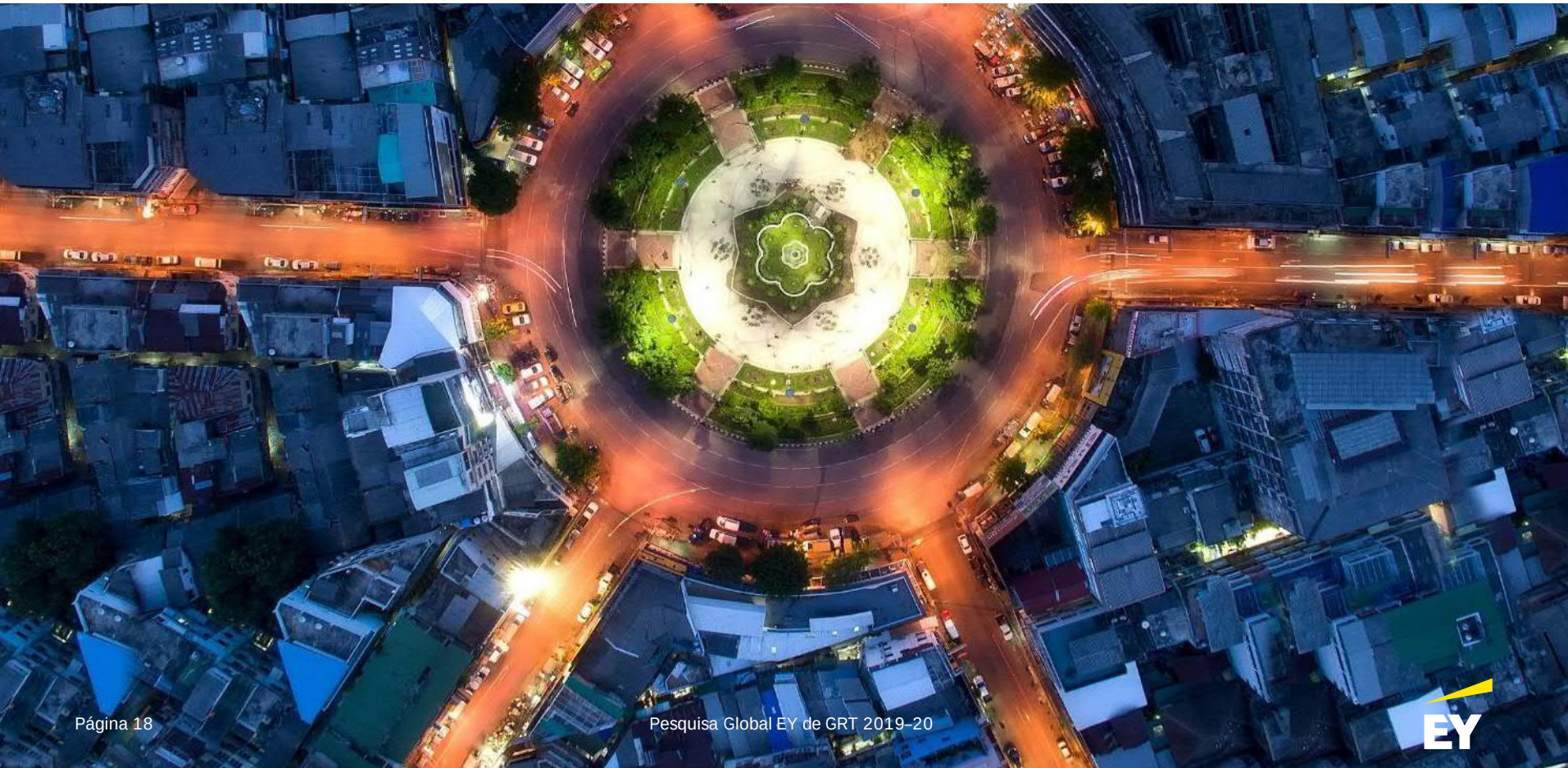
Informação mantida

Q14. Quais tipos de informação você mantém em relação a terceiros?

Critérios para terceiros considerados críticos

Q15. Quais são os 3 critérios mais importantes utilizados por sua organização para definir terceiros críticos?

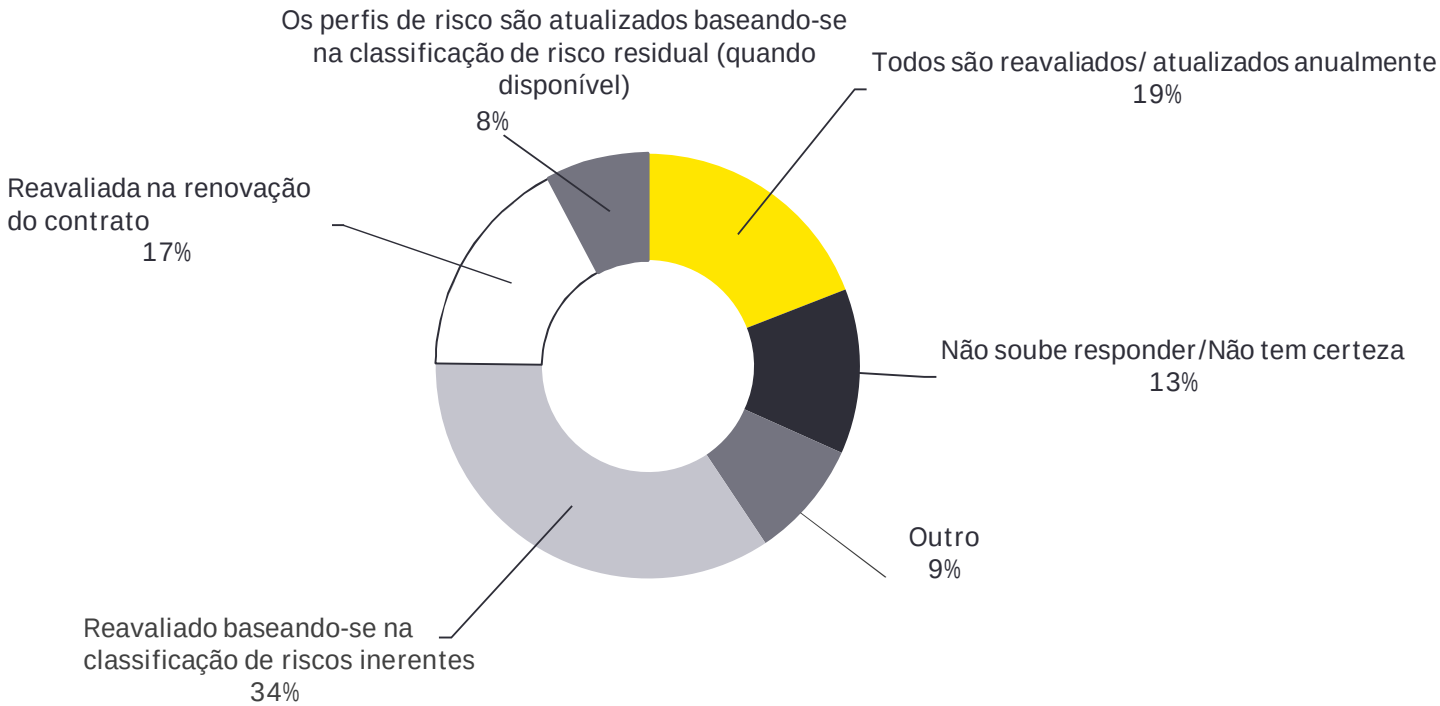
Avaliações



Para aproximadamente 2 entre 3 das organizações pesquisadas, o perfil de risco inerente do terceiro é reavaliado com base em sua própria classificação (e.g., somente reavaliar terceiros de alto risco) ou é realizada periodicamente (e.g., anualmente) demostrando que essas atualizações não dependem somente de eventos contratuais.

Avaliando o risco inerente de terceiros

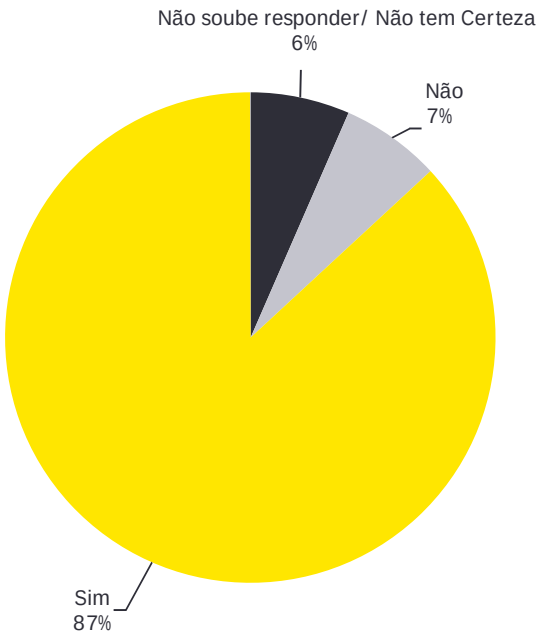
Q16. Qual a abordagem da sua organização ao reavaliar/atualizar os perfis de risco inerente de terceiros?



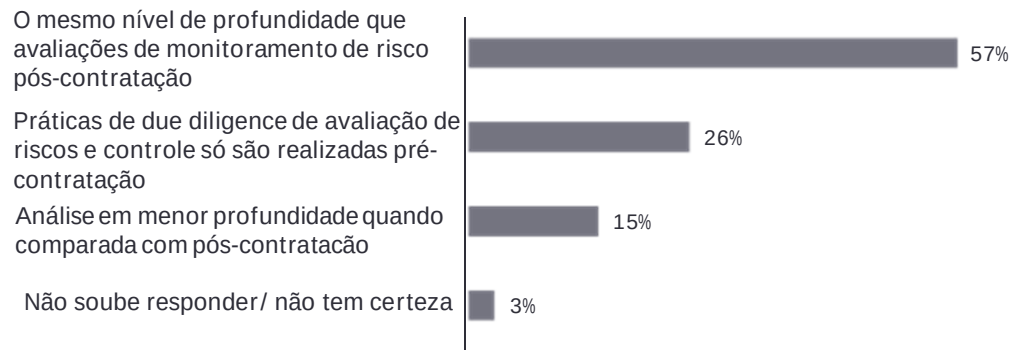
A maioria das organizações respondentes (81%) conduziu alguma forma de due diligence pré-contratação de avaliação de risco. Para a maior parte das organizações, estas avaliações são feitas no mesmo nível de profundidade que o monitoramento pós-contratação, levantando a questão de se estar fazendo demais antes da assinatura de um contrato.

Avaliações de risco pré-contratuais

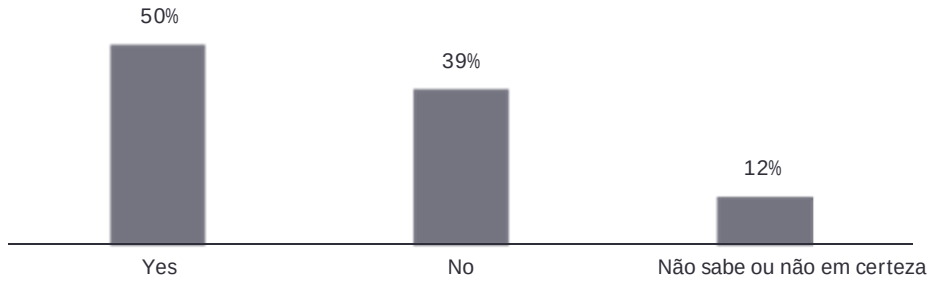
Q17.A sua organização conduz algum due diligence pré-contratação de avaliação de risco?



Q18. [Se sim para a Q17] Qual o nível de profundidade desta avaliação?



Q19. [Se sim para a Q17] A sua organização tem um processo acelerado para Avaliações de risco de pré-contratações para solicitações urgentes?



Baseado nas respostas da pesquisa, o típico questionário de avaliação de risco pré e pós-contratação tipicamente tem menos de 200 questões. Cybersegurança e risco de privacidade representam quase metade de todas as questões, esses resultados estão condizentes com as respostas anteriores sobre o critério mais importante de sensibilidade de dados (Q15)

Questionário de avaliação de risco

Q20. Quantas perguntas no questionário de avaliação de riscos da sua empresa são utilizadas para avaliar terceiros em cada uma das áreas de risco a seguir?

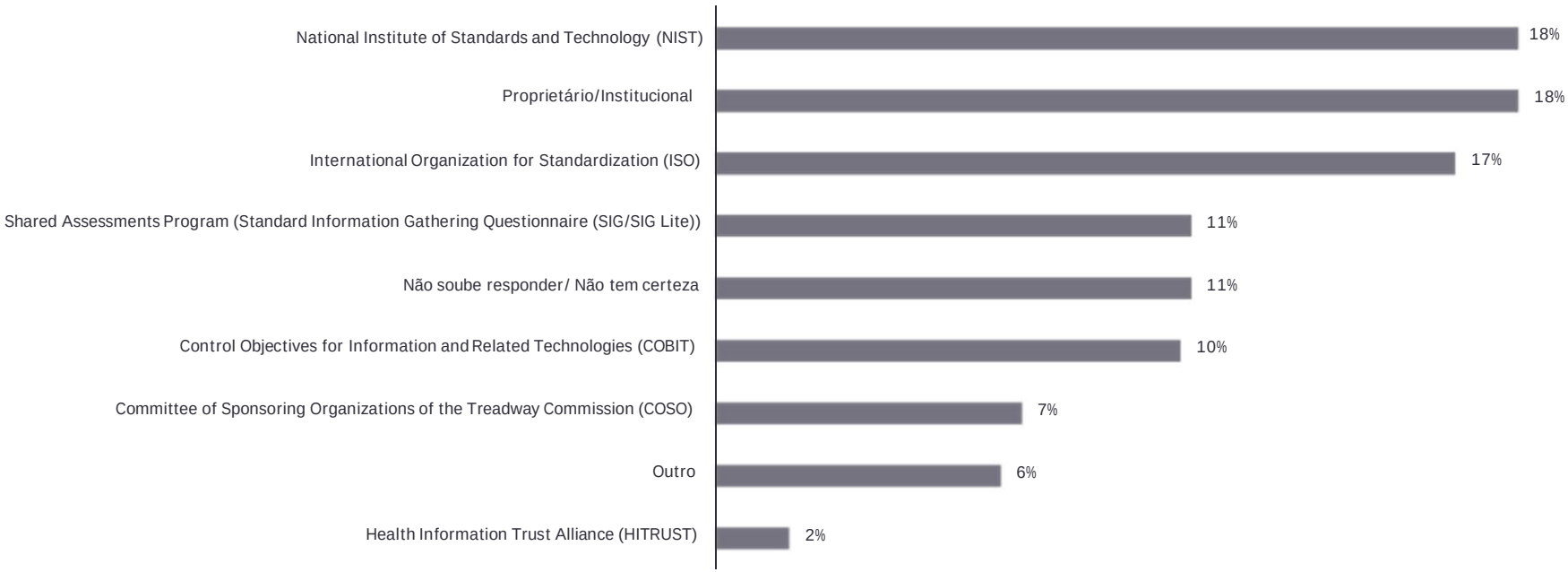
Volume médio de questões

	Questionário de avaliação de riscos inerentes	Questionário de avaliação de riscos pré-contratual	Questionário de avaliação de riscos pós-contratual
Regulação e Compliance	6.1	17.3	23.1
Risco Estratégico	1.7	1.9	5.1
Cybersegurança e risco de privacidade	26.8	57.9	72.5
Risco financeiro	2.6	4.0	15.9
Continuidade dos negócios e resiliência	5.5	12.5	12.9
Risco geopolítico	1.0	1.1	1.8
Risco digital	1.6	4.2	16.4
Risco operacional	3.2	6.5	27.1
Risco reputacional	1.9	2.0	3.0
Risco de sustentabilidade	0.7	1.3	13.2
Total	51.1	108.7	191.0

Nos últimos 2 a 3 anos, tem havido uma significante expansão na proporção de firmas utilizando o NIST (National Institute of Standards and Technology), ainda que o ISO e COBIT também tenham apresentado crescimento na utilização pelas organizações. Ao se utilizar frameworks confiáveis como o NIST, as organizações avaliadas sentiram que possuíam uma base estrutural confortável para seus próprios questionários.

Framework do questionário de avaliação de risco

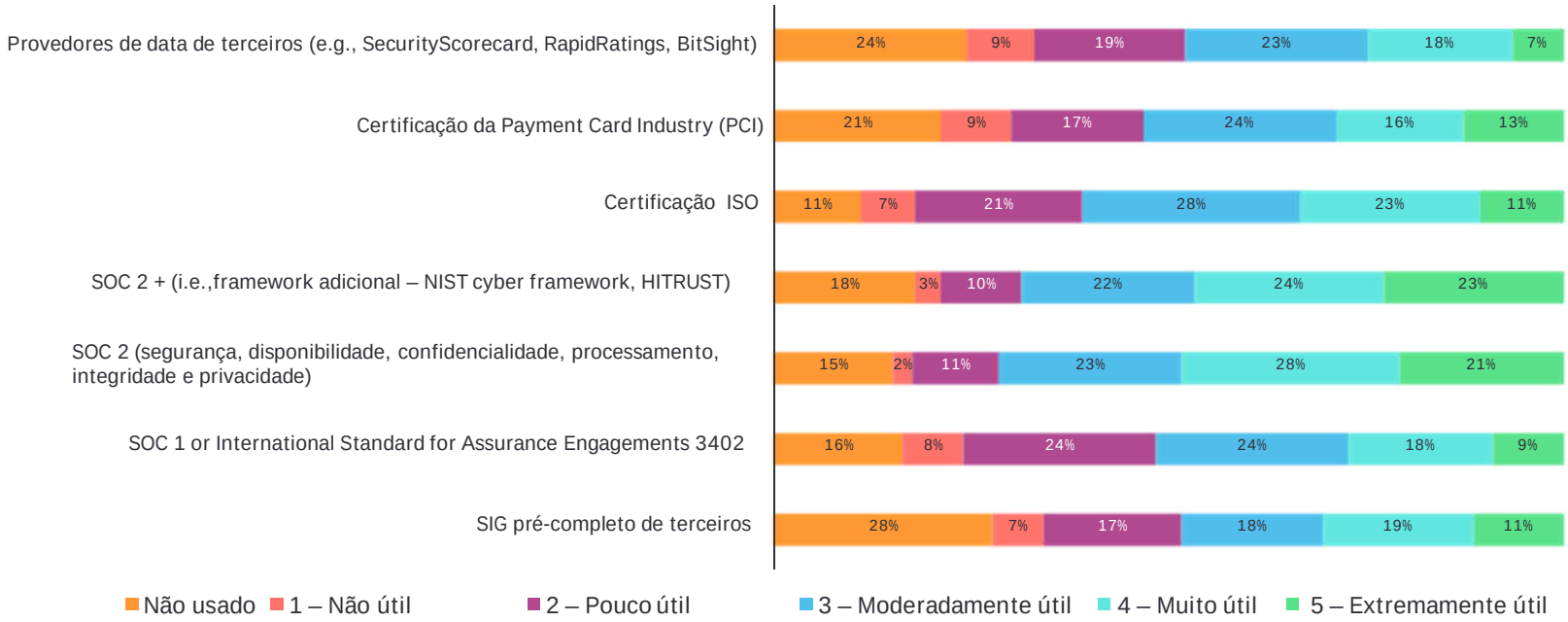
Q21.Qual framework foi usado como base para o questionário de avaliação de risco?



Cerca de metade das organizações pesquisadas classificaram o System and Organizaton Controls (SOC) 2 ou 2+ como frameworks adicionais úteis, consistente com resultados anteriores. Outros frameworks (ISO, PCI, etc.) são moderadamente menos úteis; porém, as organizações ainda não encontraram um framework que obteve sucesso completo em reduzir ou eliminar a necessidade de se realizar avaliações de risco/controle.

Utilidade das ferramentas/documentação em reduzir/remover o risco

Q22.Em uma escala de 5 pontos, sendo 1 nenhum pouco útil e 5 extremamente útil, o quão útil é cada uma das opções a seguir em reduzir/ remover a necessidade de realizar avaliações de risco/controle de terceiros?



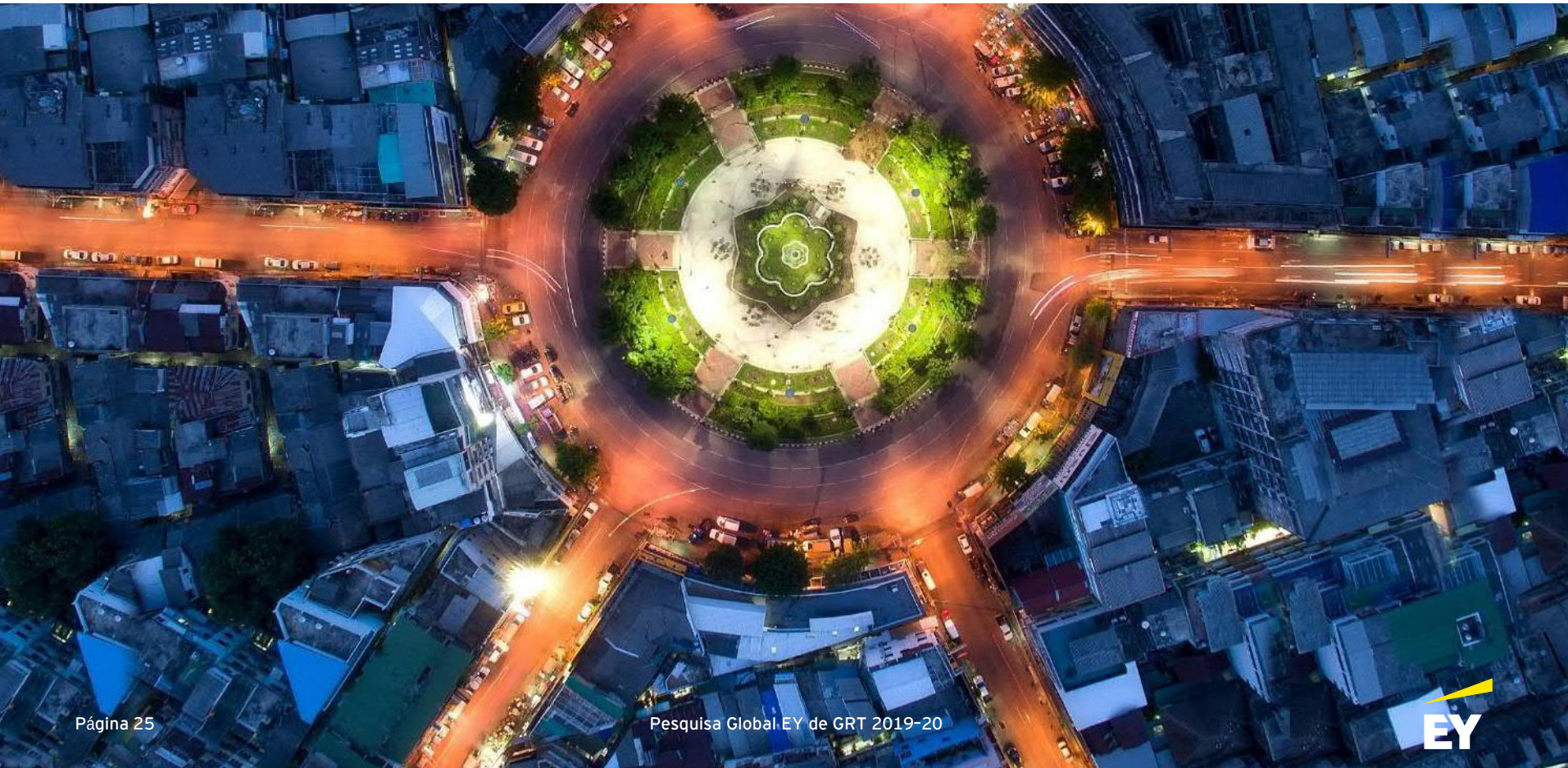
Para terceiros com classificação mais alta de risco, reavaliações são tipicamente realizadas todos os anos, enquanto para terceiros com classificações de baixo risco são menos frequentes, ocorrendo a cada 3 anos ou mais.

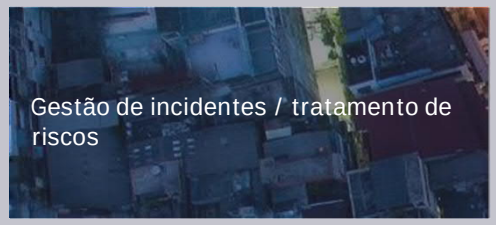
Frequência de realização da avaliação de risco de terceiros

Q23. O quão frequentemente sua organização reavalia (avaliação de riscos/controles) seus terceiros baseado no risco que eles representam para a organização?

Tipo de Risco	A cada 6 meses	Uma vez por ano	Uma vez a cada 2 anos	Uma vez a cada 3 anos ou mais	Não avalia	Não sabe/ Não tem certeza
Riscos críticos	10%	76%	5%	6%	3%	0%
Nível mais alto de risco	3%	52%	18%	7%	5%	14%
Segundo nível mais alto de risco	1%	22%	28%	19%	10%	20%
Terceiro nível mais alto de risco	1%	15%	13%	30%	20%	22%
Risco remanescente	1%	11%	6%	24%	35%	23%

Gestão de incidentes / tratamento de riscos

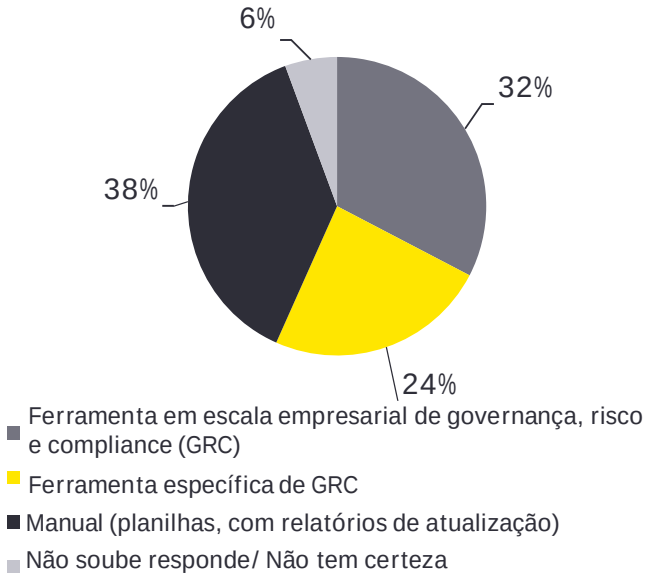




Para problemas identificados em terceiros de classificação crítica, rescisão e mudanças contratuais não são consequências incomuns, o que revela que as organizações utilizam mais frequentemente a rescisão contratual com terceiros na classificação de risco fundamental do que em outras classificações, independentemente da significância dos terceiros para a organização. A severidade da ação adotada apresenta correlação direta com o risco inerente.

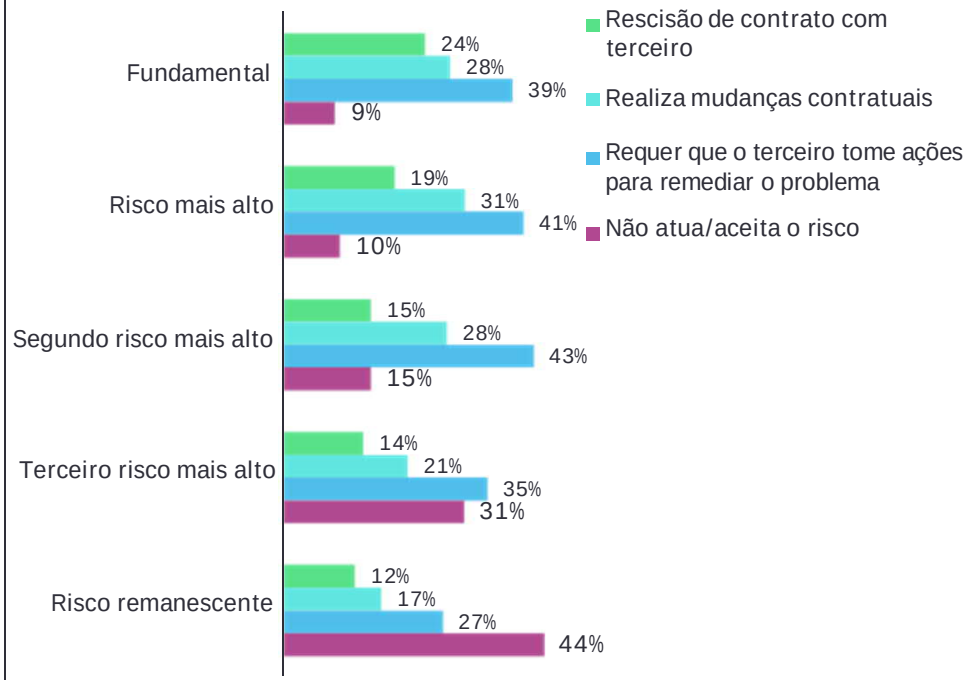
Identificação de riscos

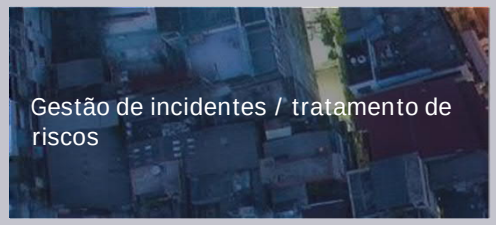
Q24.Como problemas e exceções são identificados e aprovisionados?



Ações em resposta a problemas

Q25.Para problemas identificados em terceiros de cada uma das classificações de risco a seguir, quais ações são tomadas?

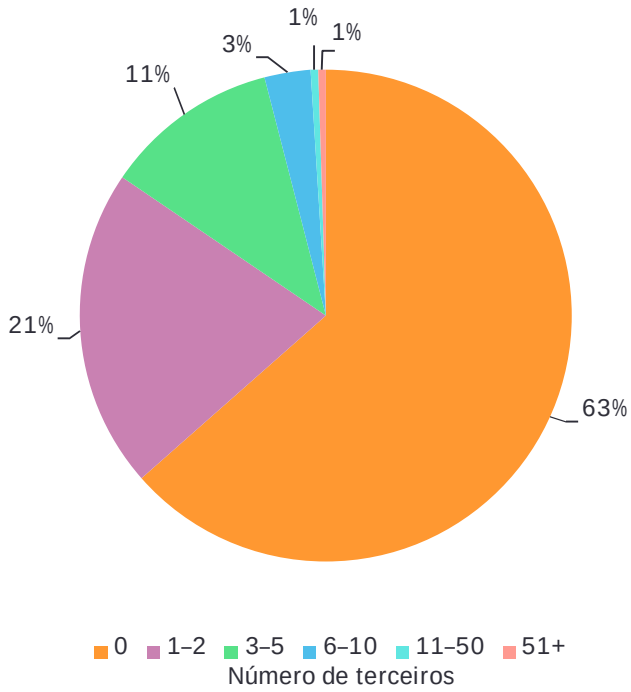




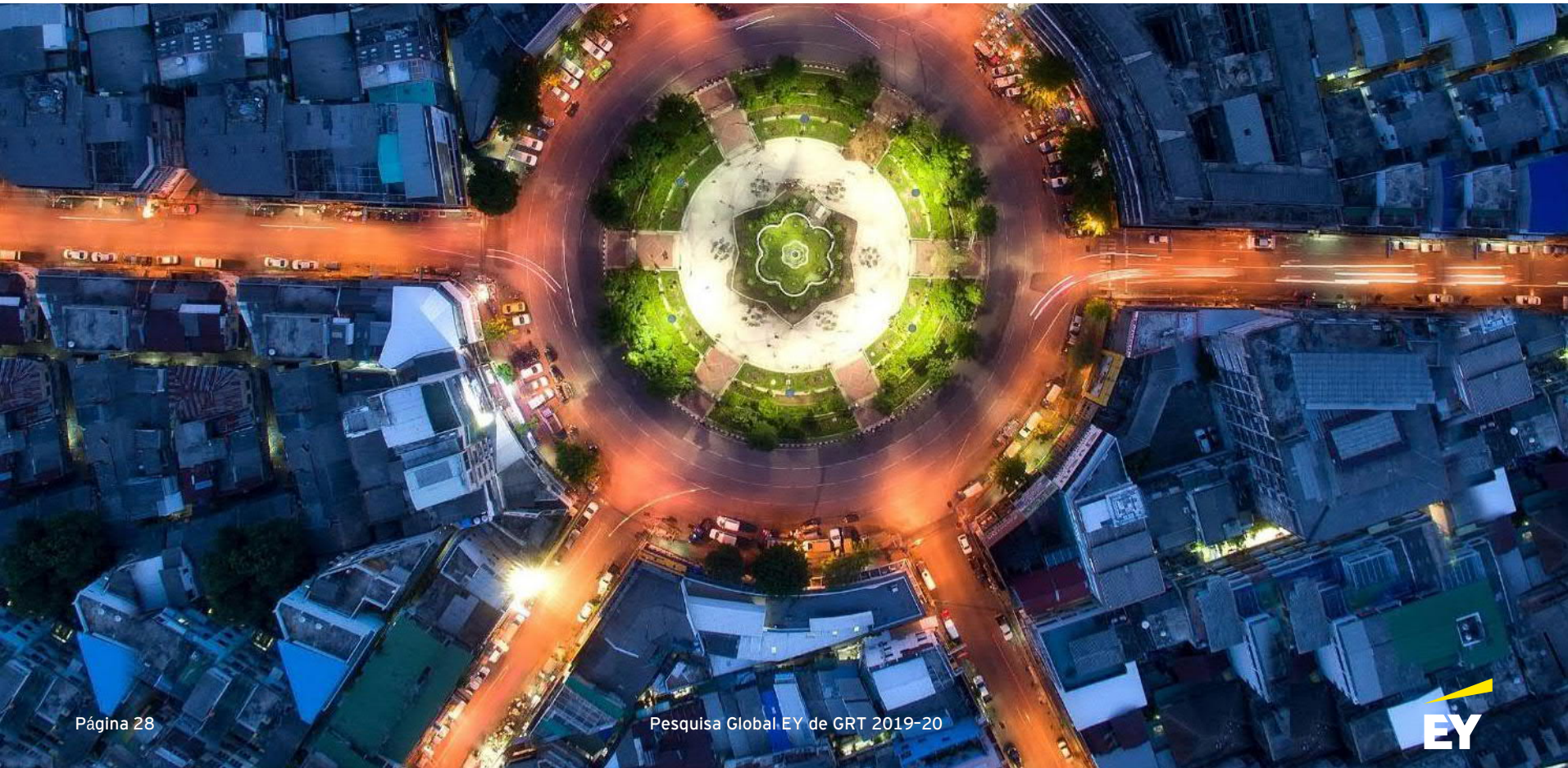
Correlacionando com os dados de ações tomadas após a identificação de problemas (Q25), as ações mais comuns ‘são remediação ou mudanças contratuais, e a maioria das organizações indica que terceiros não são rescindidos devido a problemas identificados. O restante de aproximadamente 1/3 das organizações rescindiram somente de 1 até 5 terceiros, o que é uma porcentagem pequena levando-se em conta que 50% das organizações pesquisadas tem mais de 100 terceiros em seus programas de GRT (Q12)

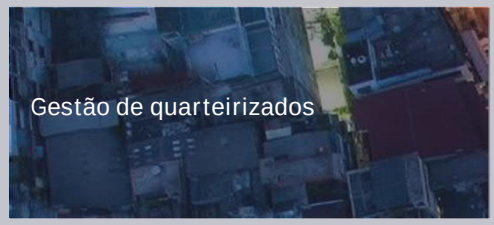
Rescisão de terceiros devido a problemas

Q26.Nos últimos 12 meses quantos terceiros foram rescindidos devido a problemas identificados?



Gestão de quarteirizados

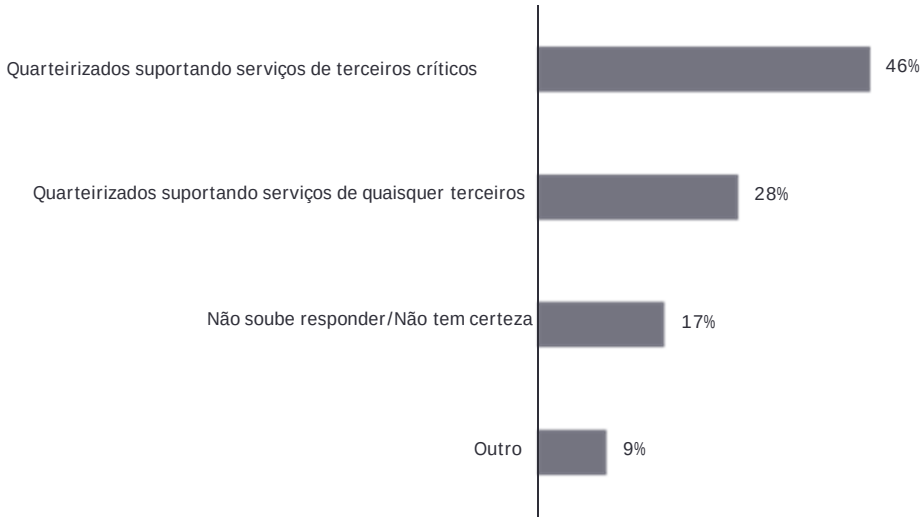




A maioria dos respondentes da pesquisa (26%) somente coletam informações de quarteirizados que suportam os serviços de terceiros críticos. Somente 1 em 3 das organizações coletam informações sobre todas os quarteirizados. Tipicamente, informações de quarteirizados são coletadas durante o processo de avaliação de riscos/controle. É provável que as expectativas de privacidade e inventário global aumentem a necessidade de coletar informações de quarteirizados nos anos por vir.

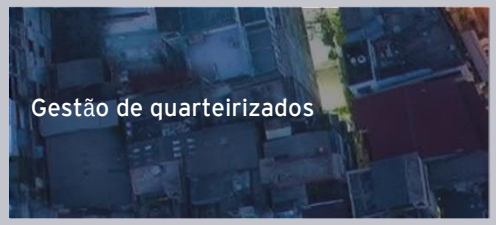
Coleta de dados de quarteirizados

Q27. A sua organização coleta informação sobre quais quarteirizados/ subcontratados?



Métodos de coleta de dados de quarteirizados

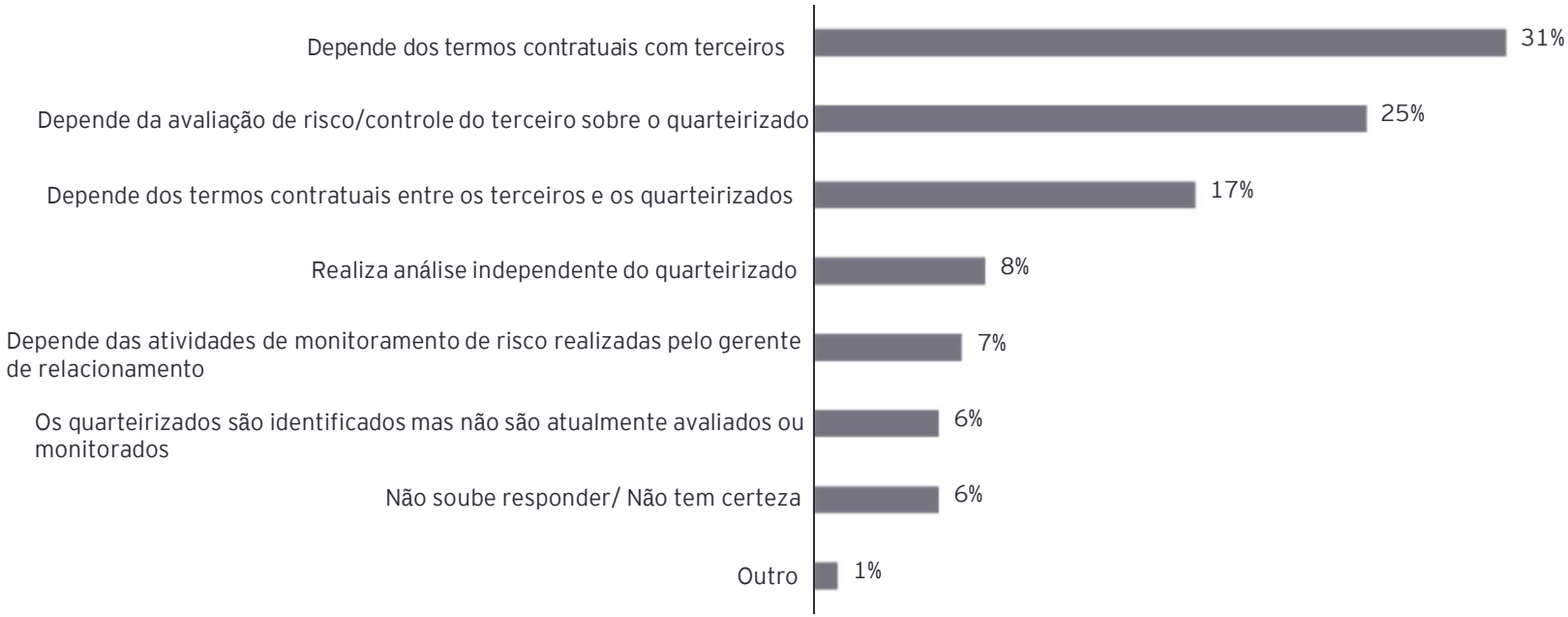
Q28. \Como as informações de quarteirizados são identificadas e coletadas (e.g., nome, localização, serviços prestados)?



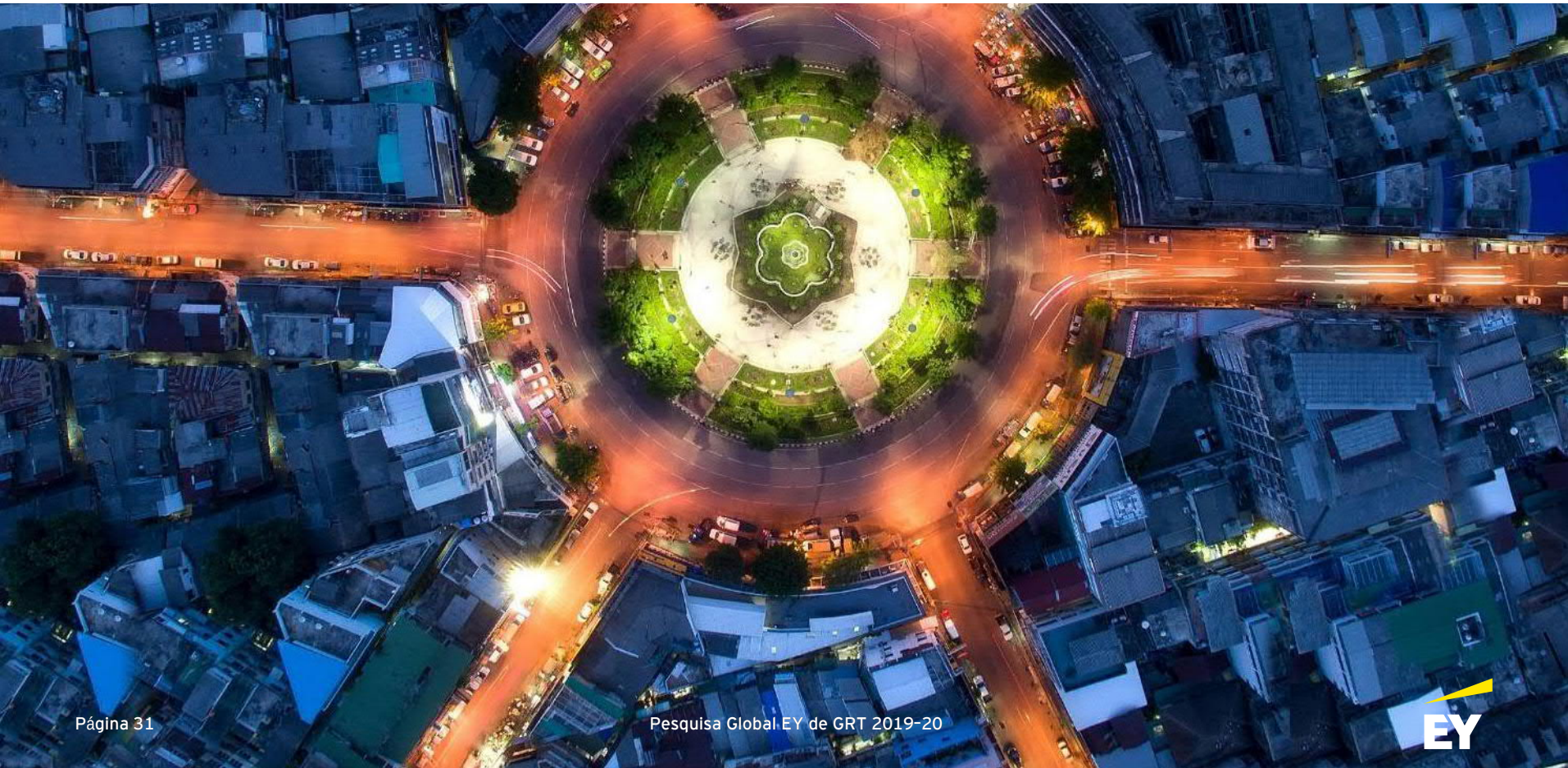
Uma proporção significativa das organizações pesquisadas depende de termos contratuais com terceiros para monitorar quarteirizados. Ainda mais, as organizações também dependem dos termos contratuais entre os terceiros e os quarteirizados. Relativamente poucas das organizações pesquisadas (menos de 20%) realizam sua própria análise de quarteirizados.

Monitoramento de quarteirizados

Q29.Como a sua organização avalia/monitora quarteirizados?



Tecnologia



As organizações pesquisadas indicaram que aproximadamente 1/3 de todas as funções de gestão de riscos são realizadas sem nenhuma ferramenta para gerenciar riscos. Archer, SAP, Ariba e outros métodos são usados frequentemente. Respondentes indicaram que outras ferramentas também são usadas, revelando que as organizações estão possivelmente usando ferramentas de fornecedores menores ou pouco conhecidos.

Ferramentas tecnológicas para gerenciar risco

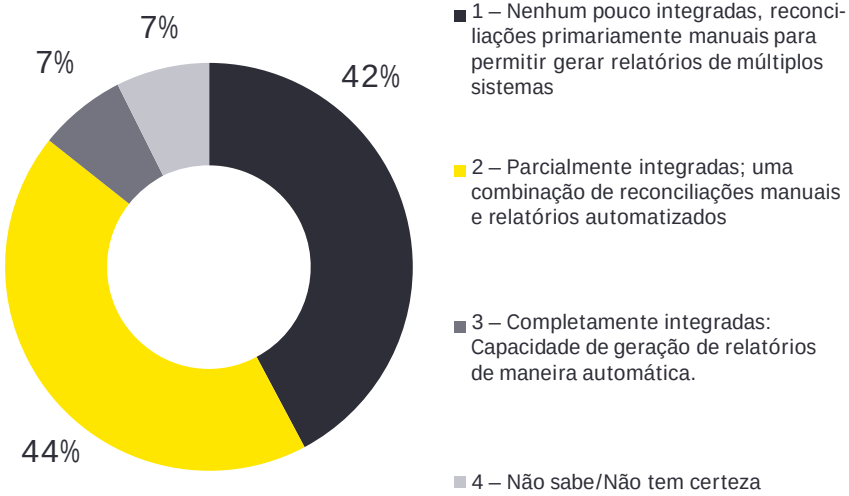
Q30. Que tecnologia / ferramentas sua organização usa para cada uma das seguintes funções para gerenciar riscos?

Função	Nenhuma ferramenta (manual)	Archer®	Bwise®	Metric-Stream	SAP Ariba®	Hiperos®	Process Unity®	Prevalent®	Aravo	Service-Now	OneTrust	Lockpath	Proprietary	Outro
Sourcing	34%	3%	0%	0%	29%	2%	1%	0%	0%	3%	0%	0%	8%	19%
Avaliação de risco inerente	31%	19%	0%	0%	2%	5%	6%	0%	2%	4%	1%	1%	14%	14%
Gestão contratual	33%	5%	0%	1%	22%	2%	3%	0%	0%	2%	0%	1%	12%	22%
Inventário de terceiros primários	32%	15%	0%	0%	12%	3%	3%	0%	1%	4%	1%	0%	11%	17%
Facilitação da avaliação de risco/controle	29%	17%	1%	1%	3%	5%	7%	0%	2%	5%	2%	1%	11%	18%
Gerenciamento de problemas	28%	20%	1%	1%	2%	2%	5%	0%	2%	8%	0%	1%	9%	18%

Dentre as organizações pesquisadas que usam ferramentas/tecnologias como parte de seus programas de GRT, poucas tem uma plataforma tecnológica totalmente integrada. Das organizações que tem uma plataforma integrada, elas estão ativamente incorporando dados externos dentro de seus sistemas utilizando Interfaces de Programação (APIs). Há oportunidades de integração tecnológica e adoção de plataformas para melhorar os processos de GRT, que são predominantemente manuais como visto em questões anteriores (Q30)

Integração tecnológica

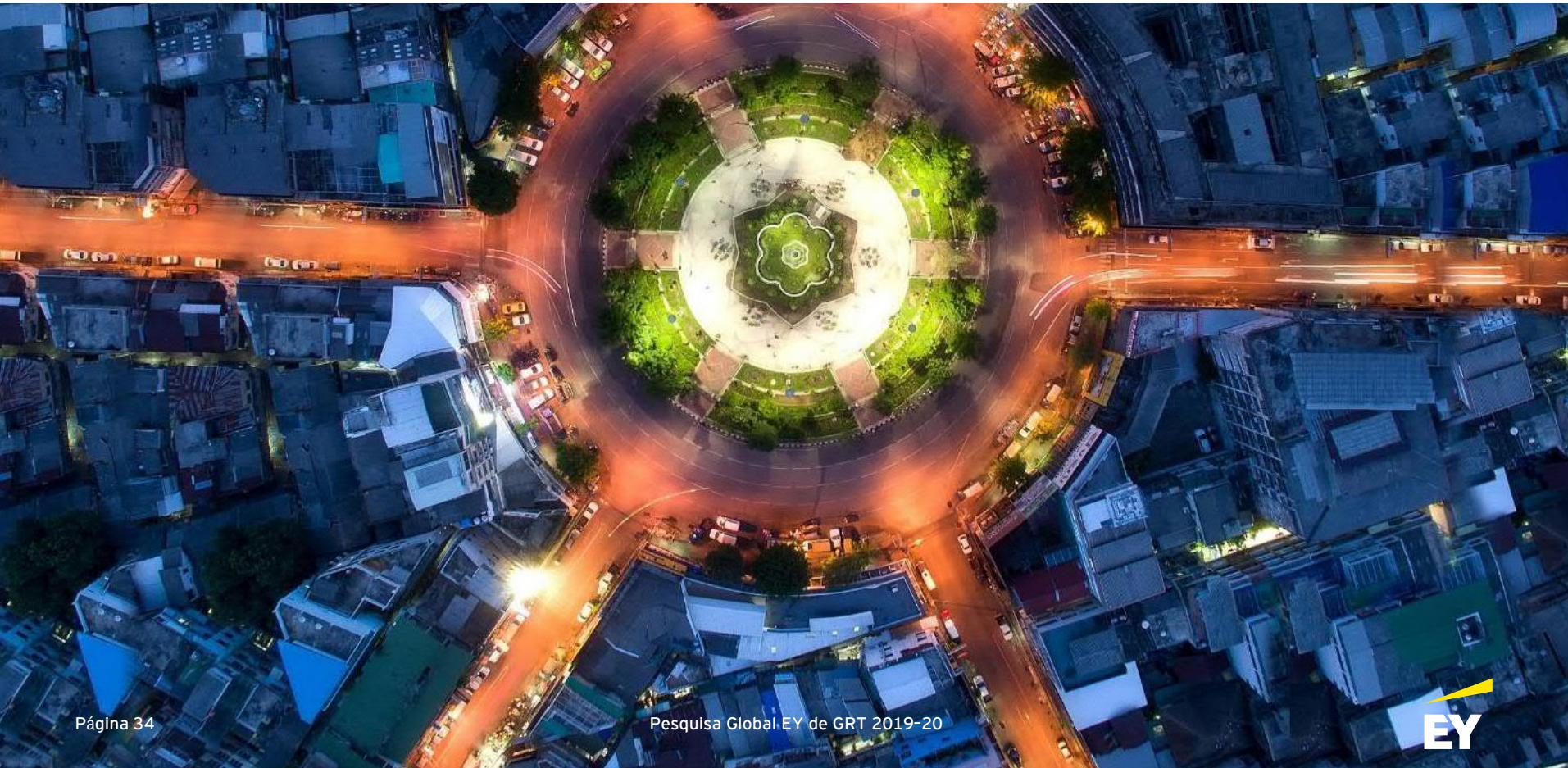
Q31. Quão bem integradas são as ferramentas que sua organização utiliza como parte do seu programa de GRT?



Integração tecnológica

Q32. Caso você tenha uma plataforma de GRT, quais APIs estão configuradas para alimentar esta plataforma e suportar as atuais atividades de monitoramento?

Reportes



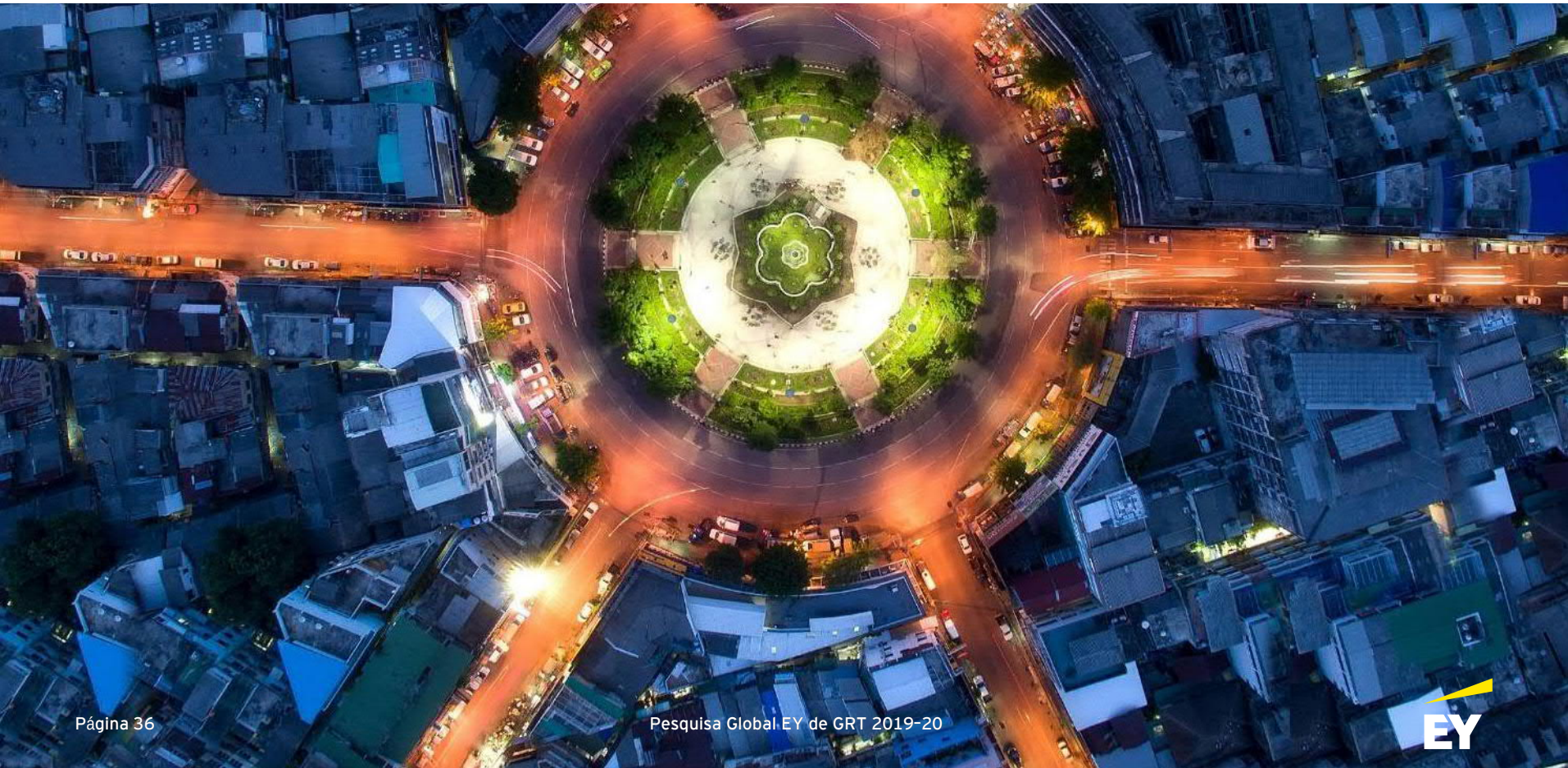
O número de organizações que exige que os programas de GRT reportem a seus comitês é preocupantemente baixo. Tipicamente, a gerência sênior é o maior nível dentro de uma organização para os quais os programas de GRT são reportados regularmente, e se tratando de terceiros críticos, suas situações somente são reportadas para a gerência sênior ou para a liderança em metade das organizações. Um número considerável das organizações respondentes (um pouco mais de 20%) não reportam nada sobre diversos aspectos de seus programas de GRT.

Reportando GRT

Q33. Para quais grupos são reportados os seguintes componentes dos programas de GRT?

Componente GRT	Conselho de Diretores	Gerência Sênior	Gestão de Negócios	Gerência de relacionamento com terceiros	Não são reportados
Métricas operacionais dos programas	24%	48%	44%	36%	15%
KPIs/KRIs	22%	48%	43%	32%	15%
Ambiente dos terceiros	21%	43%	35%	28%	18%
Terceiros críticos	29%	54%	48%	33%	12%
Terceiros com brechas ou incidentes	33%	60%	56%	40%	8%
Terceiros com problemas significativos	24%	58%	58%	42%	9%
Terceiros rescindidos antes da data de fim do contrato	11%	32%	40%	30%	20%

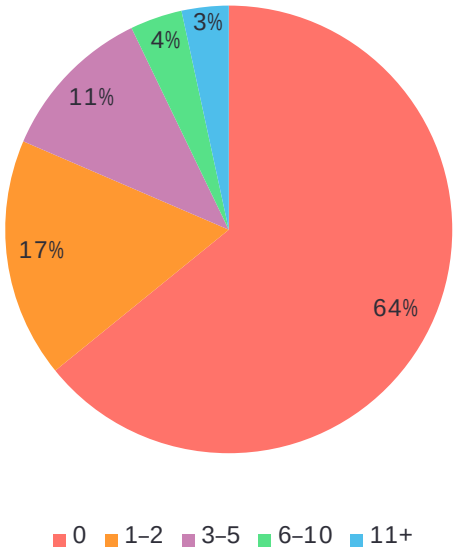
Cybersegurança e resposta a ameaças



Um número significativo das organizações participantes enfrentou violações ou interrupções em seus sistemas causadas por terceiros. Quase uma em cada cinco organizações relataram ter pelo menos três violações, enquanto aproximadamente uma em três relataram pelo menos três interrupções de seus sistemas.

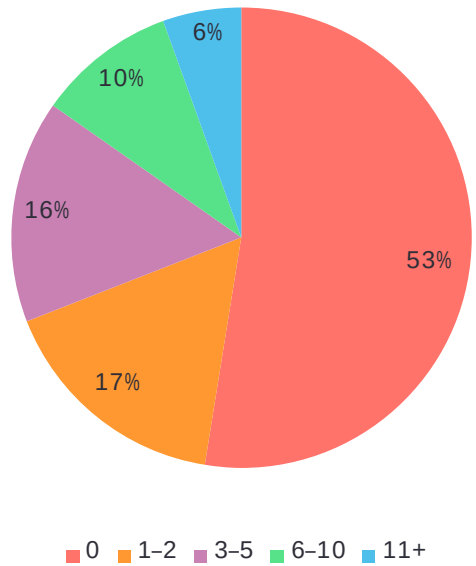
Violações de dados causadas por terceiros

Q34. Nos últimos dois anos, quantas violações ou perdas de dados foram causadas por terceiros?



Interrupções causadas por terceiros

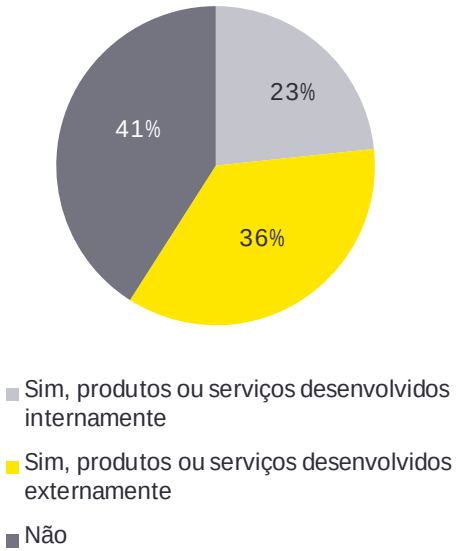
Q35.Nos últimos dois anos, quantas interrupções foram causadas por terceiros?



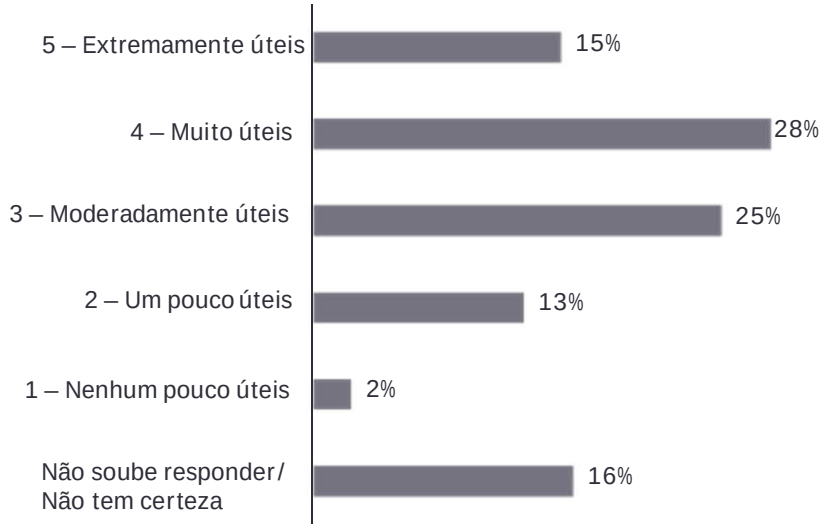
Apesar de um número significativo das organizações pesquisadas ter sofrido brechas, aproximadamente metade delas não utilizam ferramentas de inteligência de ameaças. Isso pode ser motivado pelo fato de somente metade delas classificarem ferramentas de inteligência de ameaças como muito úteis para supervisionar falhas em atividades de risco, mostrando um baixo grau de integração com este tipo de ferramenta.

Inteligência de ameaças

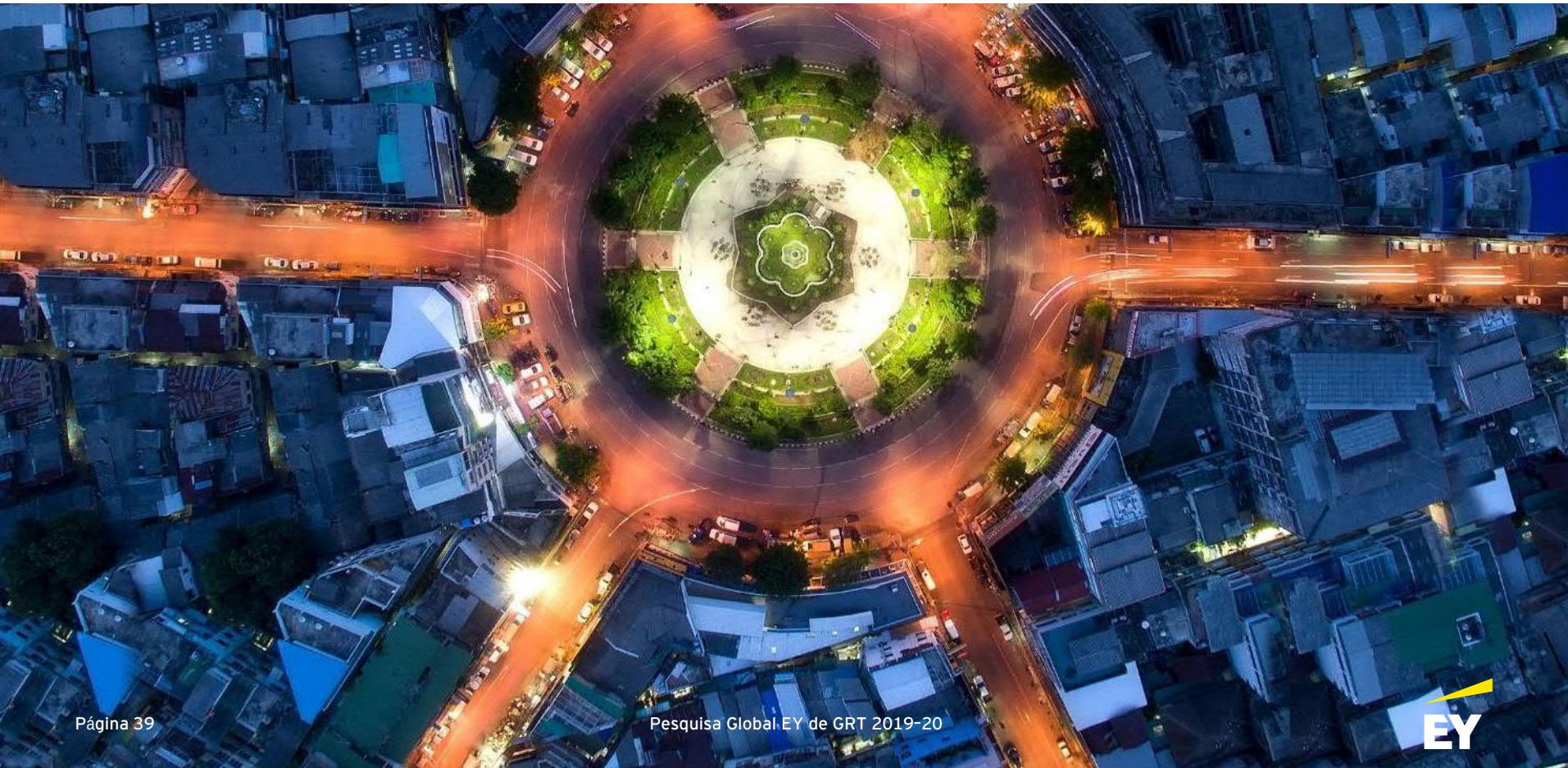
Q36. A sua organização utiliza produtos de inteligência de ameaças ou serviços para continuamente monitorar o ambiente de cybersegurança dos seus fornecedores terceiros?



Q37. [Para aqueles que responderam Sim] Numa escala de 1 até 5, sendo 1 nenhum pouco útil e 5 extremamente útil, o quão útil são ferramentas de inteligência de ameaças para supervisionar falhas em atividades de risco?



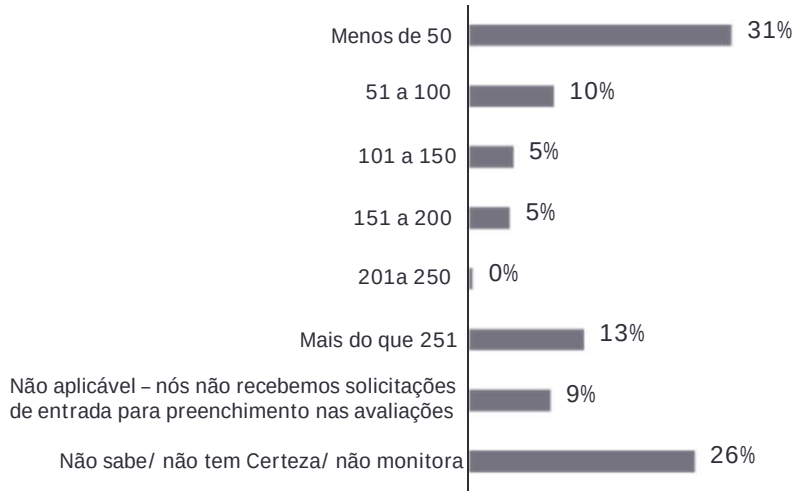
Solicitações de entrada



1/3 das organizações participantes facilitaram mais de 50 avaliações de solicitações de entrada por ano, adicionalmente outros um quarto dos participantes nem mesmo sabem que estão sendo avaliados, mostrando um desencontro entre solicitações de entrada e as funções de gestão de risco internas.

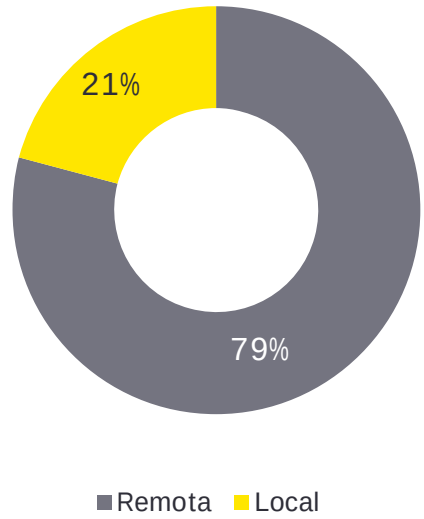
Solicitações de entrada para GRT

Q38. Aproximadamente quantas solicitações de entrada para preenchimento dos questionários de avaliação de risco de terceiros a sua organização recebe anualmente?



Análises locais vs. remotas

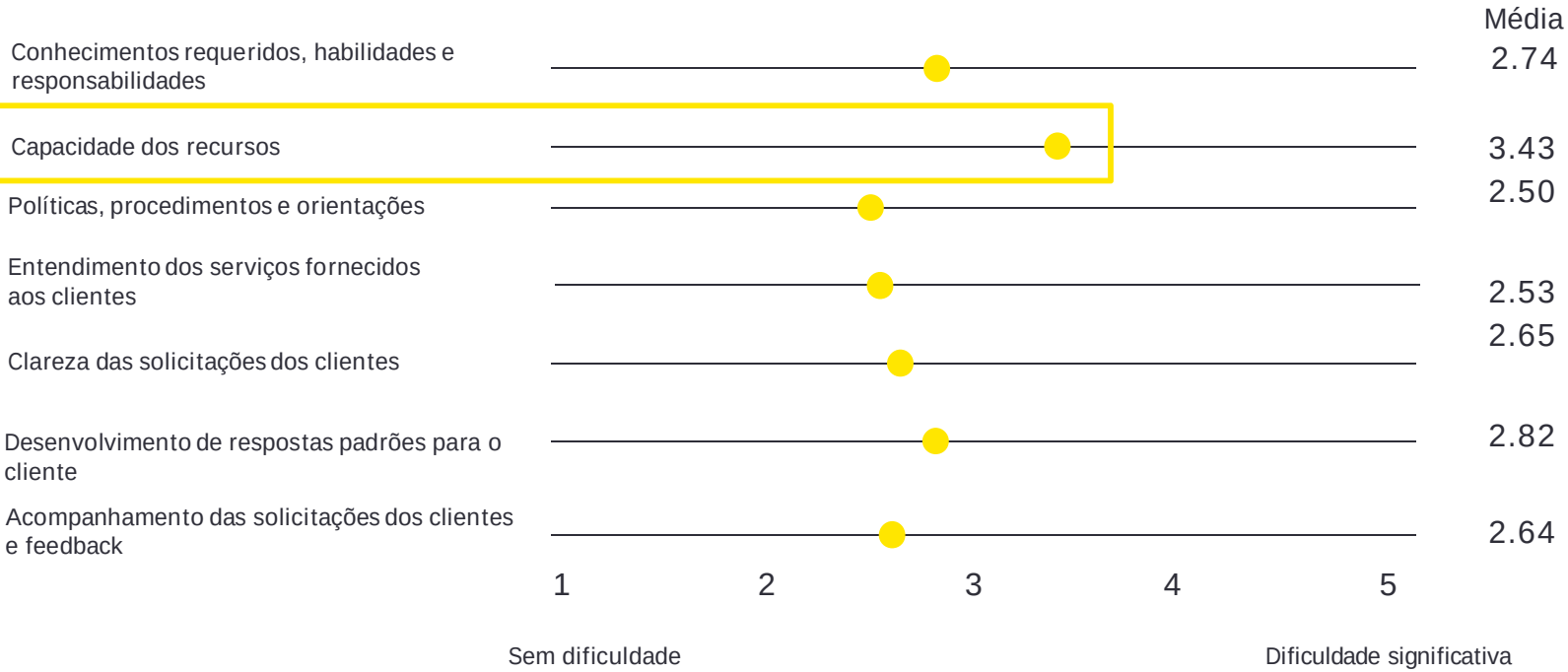
Q39. Qual porcentagem das solicitações de entrada são analisadas localmente vs. remotamente? Por favor forneça porcentagens para cada; o total deve ser igual a 100%.



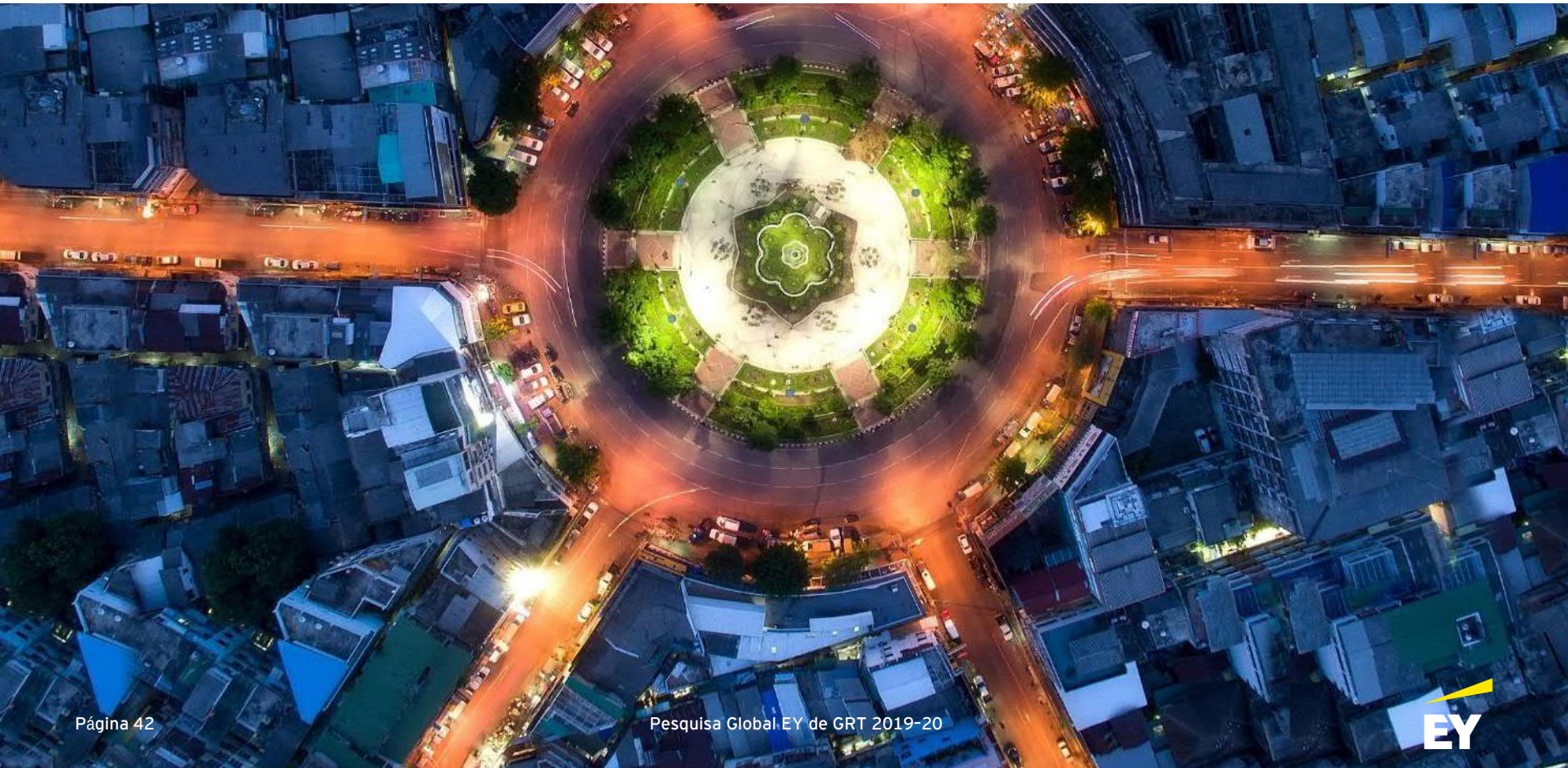
Se tratando de solicitações de entrada, mais da metade das organizações pesquisadas apontou que a limitação de recursos representou um desafio significativo. Esse resultado está alinhado com as respostas anteriores, indicando que as organizações pretendem usar mais recursos internos para execução de GRT nos próximos 2 a 3 anos (Q7).

Dificuldades relacionadas a entrada em GRT

Q40. Em uma escala de 1 a 5, sendo 1 sem dificuldade e 5 dificuldade significativa, qual o grau de dificuldade que a sua organização enfrenta na gestão de risco de terceiros relacionado a entradas, para cada um dos seguintes tópicos?



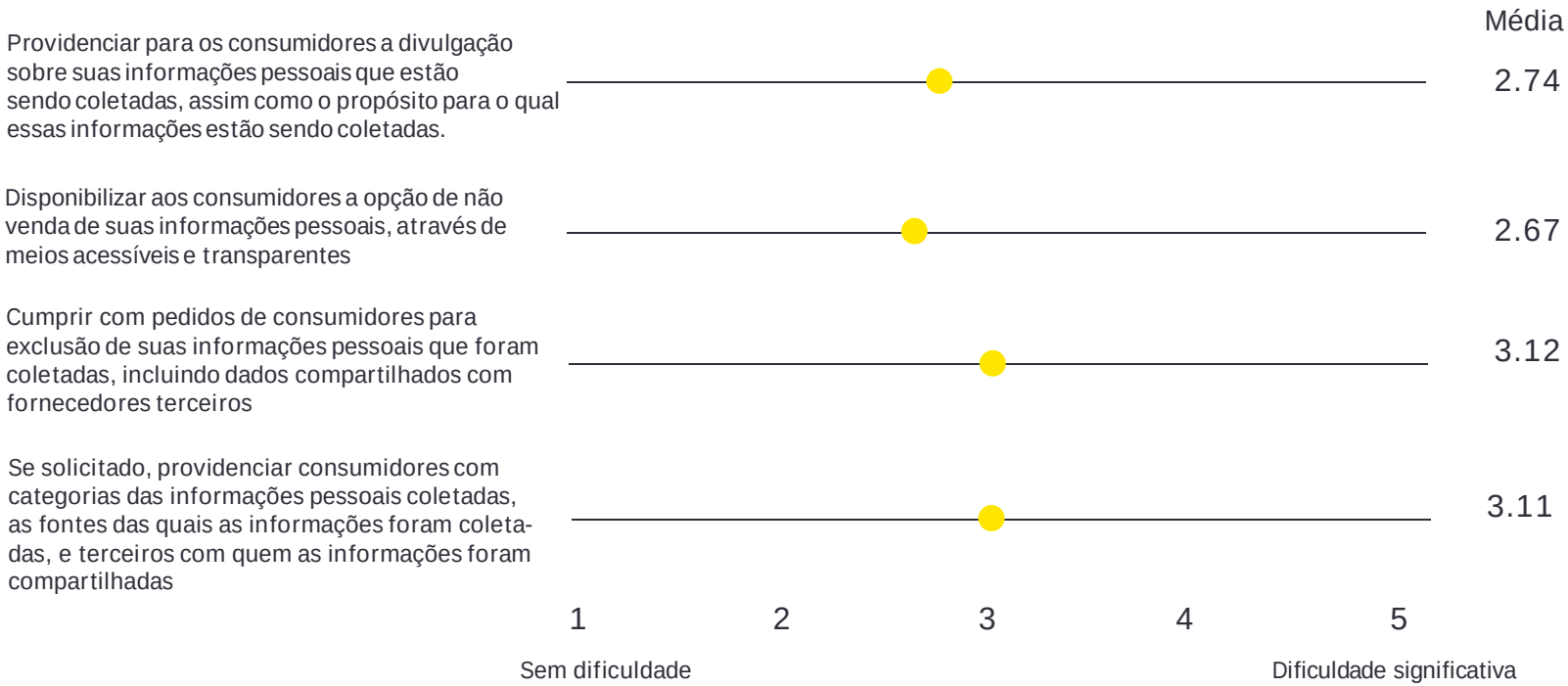
Regulações de privacidade



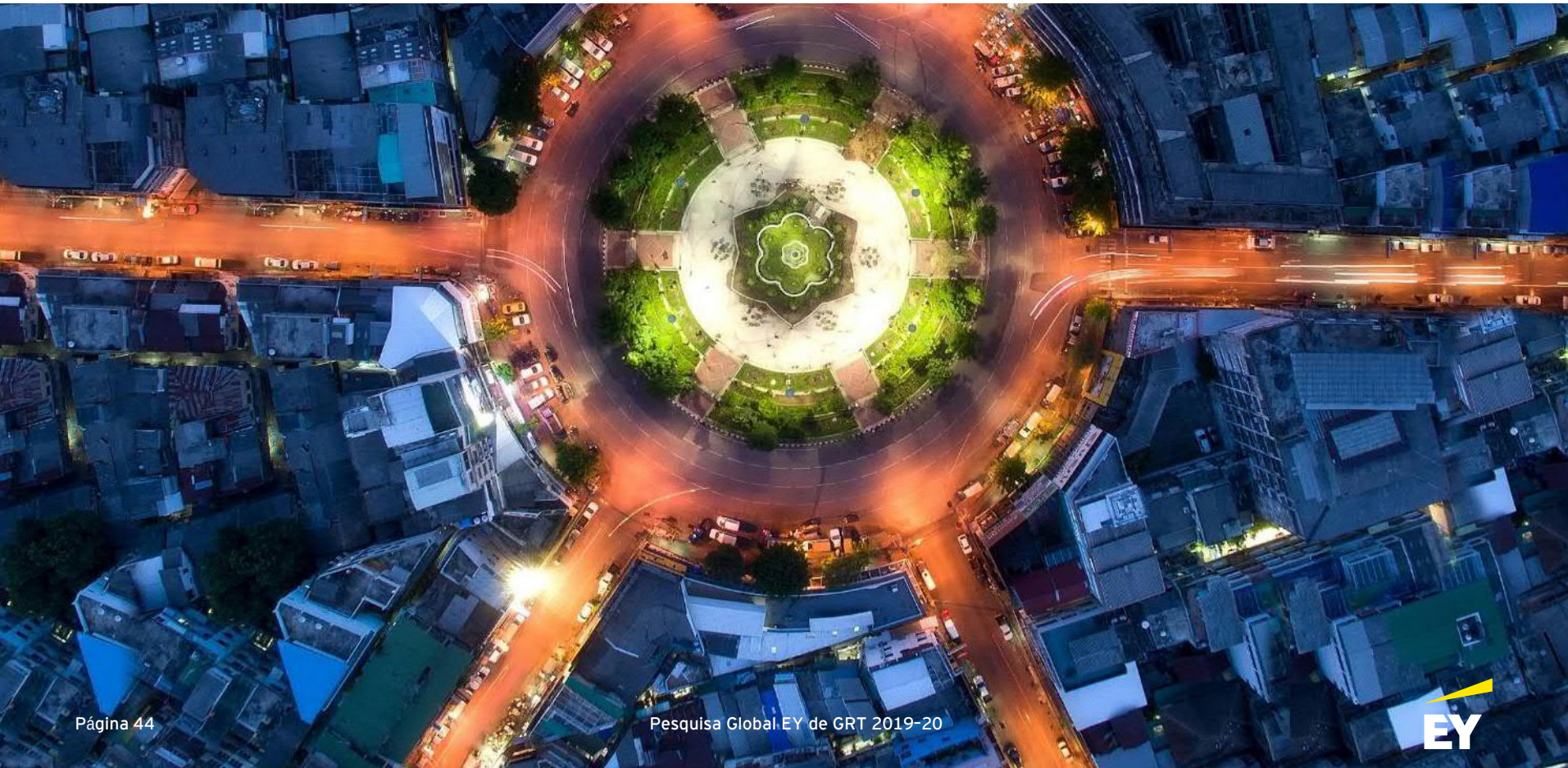
As organizações ainda não estão completamente preparadas para abordar todos os aspectos de regulamentações de privacidade (CCPA, GDPR, etc.). Em particular, as organizações pesquisadas sentem que será um desafio disponibilizar aos clientes a opção de não venda de suas informações pessoais, assim como divulgar efetivamente como as informações estão sendo coletadas e como elas serão utilizadas.

Regulações de privacidade em GRT

Q41. Numa escala de 1 a 5, em relação ao seu universo de terceiros, o quão difícil é abordar as exigências das orientações específicas de privacidade (e.g. GDPR,CCPA) ?



Inspeções regulatórias e de auditoria interna



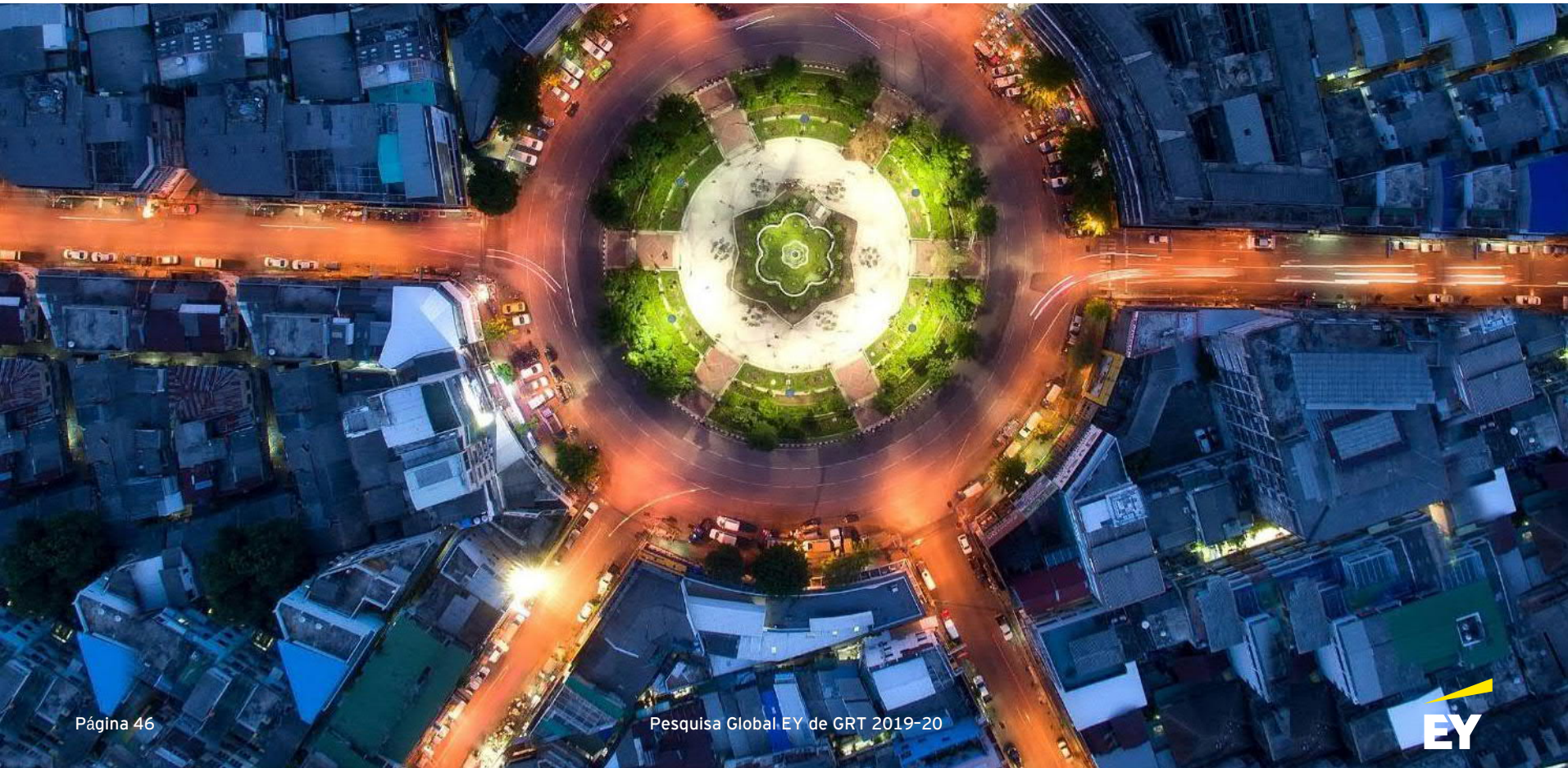
Assim como em anos anteriores, oversight e governança e cybersegurança foram as áreas de foco das companhias pesquisadas, sendo seguidas por gestão e terceiros críticos para reguladores e onboarding de terceiros para a auditoria interna.

Áreas de foco durante supervisão de órgãos reguladores e auditoria interna

Q42. Durante a supervisão mais recente do seu programa de GRT, pelos órgãos reguladores e pela auditoria interna, quais foram as 2 ou 3 mais importantes áreas de foco? Por favor não selecione mais do que 3.

Importantes áreas de foco	Órgãos reguladores	Auditoria Interna
Oversight e governança	72	94
Cybersegurança	45	56
Terceiros críticos para a empresa	33	27
Avaliações de terceiros – segurança da informação e continuidade dos negócios	29	36
Avaliação de riscos inerentes	25	39
Oversight e falhas de quarteirizados	16	7
Privacidade/confidencialidade	16	23
Gerenciamento de problemas e/ou aceitação de riscos	15	29
Atividades de onboarding	14	45
Avaliação de terceiros - compliance	13	25
Modelos operacionais	12	19
Manutenção do inventário de terceiros	10	23
Terceiros do exterior	8	6
Terceiros não tradicionais (i.e., corretores, agentes, intermediários financeiros)	7	3
Avaliação de terceiros - performance	4	12
Compliance/ Proteção ao consumidor	4	3
Modelo de risco residual	3	10
Outro	3	4
Não aplicável	52	39

Terceiros não tradicionais

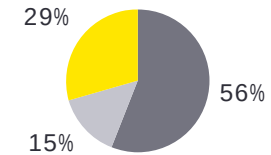
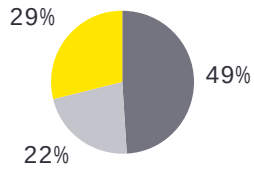
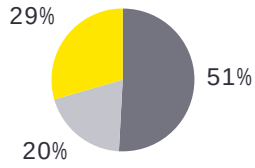
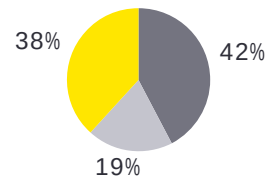
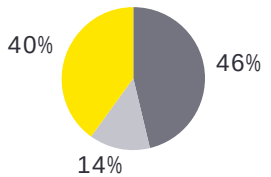
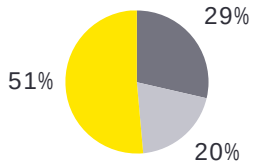
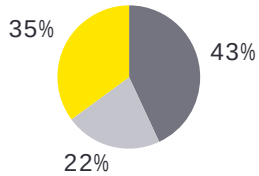
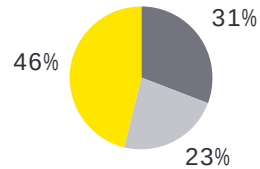


Das organizações pesquisadas, os terceiros não tradicionais mais comumente cobertos em GRT são parcerias estratégicas, operadoras de seguro e escritórios de advocacia prestando consultoria legal externa. Os mais prováveis de não serem cobertas em GRT são locações arrendadas, organizações de caridade e fundos de pensão.

Terceiros não tradicionais

Q43. Para cada um dos tipos de terceiros não tradicionais a seguir, há a cobertura em seu programa de gestão de risco de terceiros?

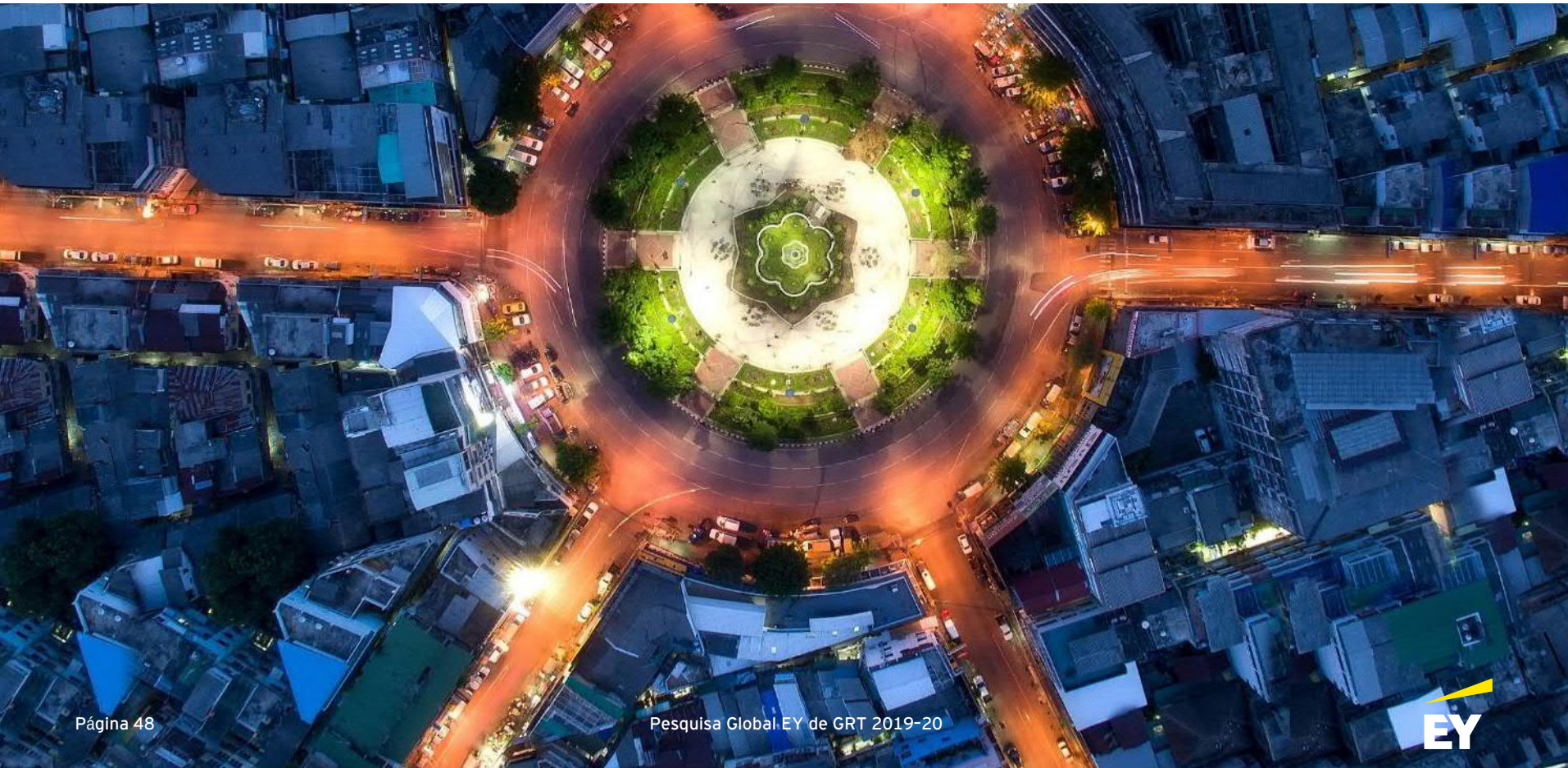
Terceiros não tradicionais*

Parcerias estratégicas	Escritórios de advocacia prestando consultoria legal externa (litígios)	Operadores de seguro	Joint ventures
			
Planos de pensão	**Locações arrendadas**	**Corretores**	**Organizações de caridade**
			

Cobertas em GRT | Cobertas por programa específico | Não cobertas

*Resultados refletem os terceiros não tradicionais mais comuns com base nos resultados da pesquisa.

Riscos de concentração (somente para serviços financeiros)

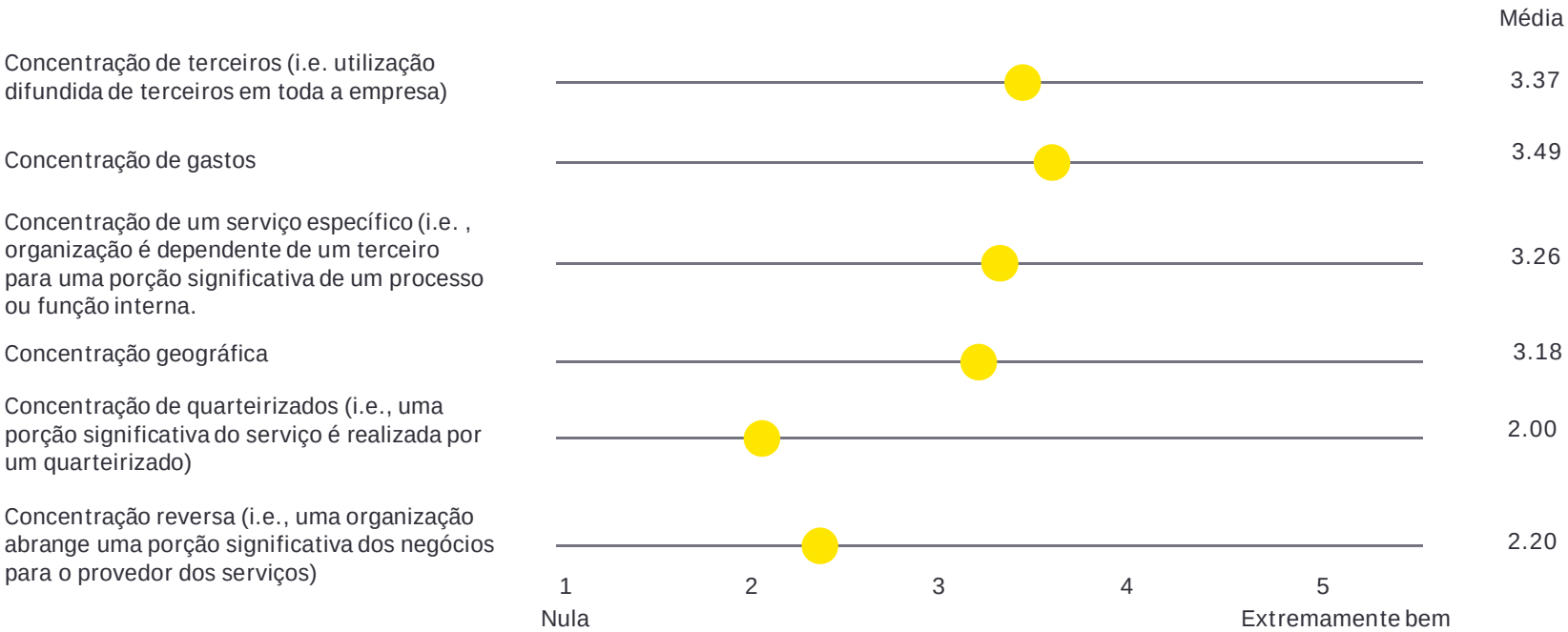


Riscos de concentração (somente para serviços financeiros)

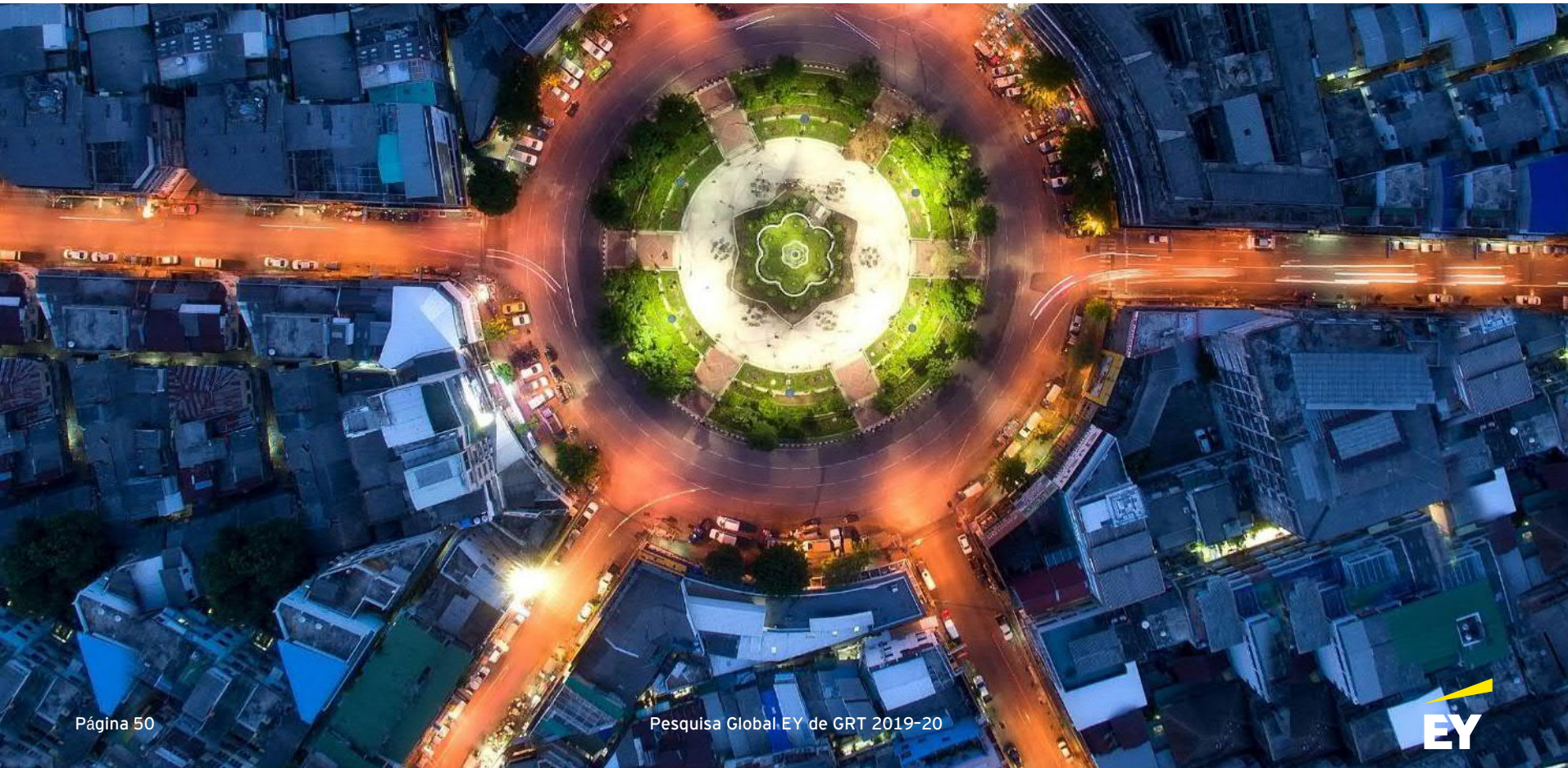
Cerca de metade das organizações pesquisadas acham relativamente fácil reportar concentrações de gastos e concentração de terceiros, mas bem menos julgam fácil reportar a respeito de quarteirizações ou concentração reversa.

Risco de concentração de serviços financeiros

Q45. [Somente para serviços financeiros] Numa escala de 1 a 5, qual a capacidade da sua organização de reportar cada um dos seguintes tipos de risco de concentração, sendo 1 nula e 5 extremamente bem?



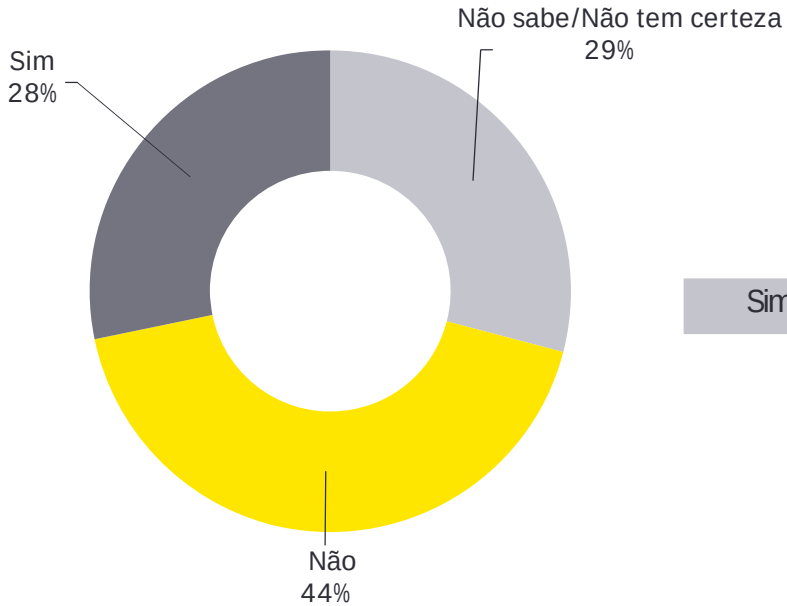
Gerenciamento de afiliados (somente para serviços financeiros)



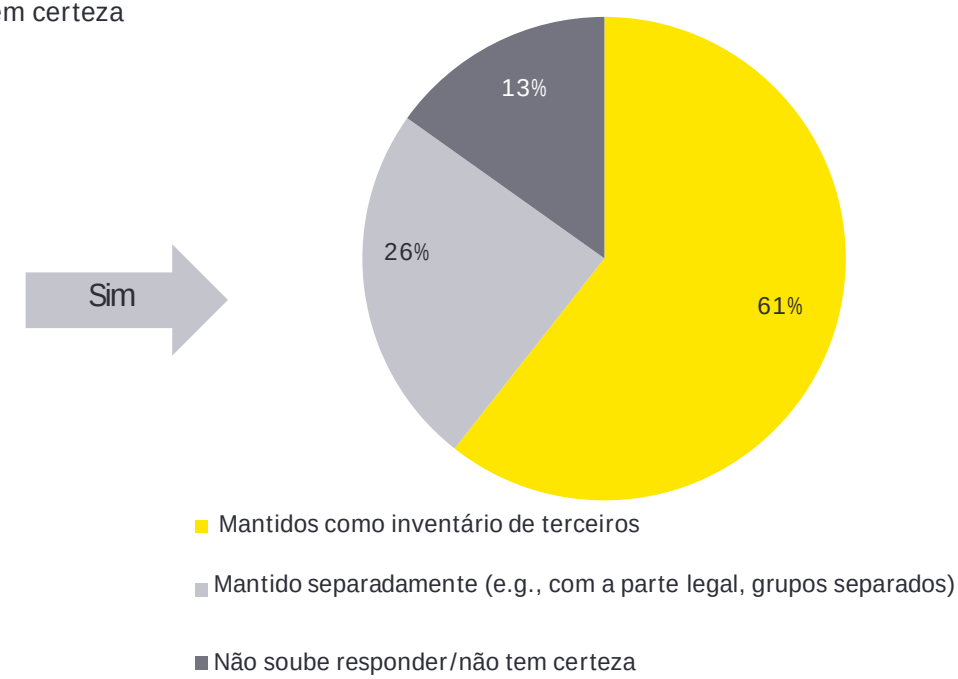
Das organizações pesquisadas, 18% tem afiliados que são alvos do programa de GRT. Dessas, 61% mantém esses afiliados como parte de seus inventários de terceiros.

Afiliados fornecendo bens/serviços para GRT

Q46. Afiliados fornecendo bens/serviços para a unidade de operação nos EUA da sua organização são alvos do programa de GRT?



Q47. [Se sim] Afiliados são mantidos no inventário de terceiros ou são mantidos separadamente?

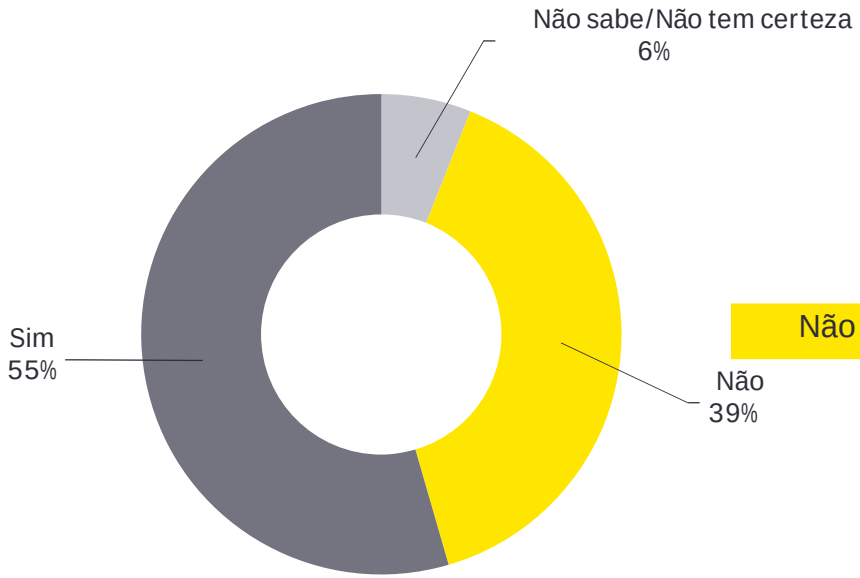


Gerenciamento de afiliados (somente para serviços financeiros)

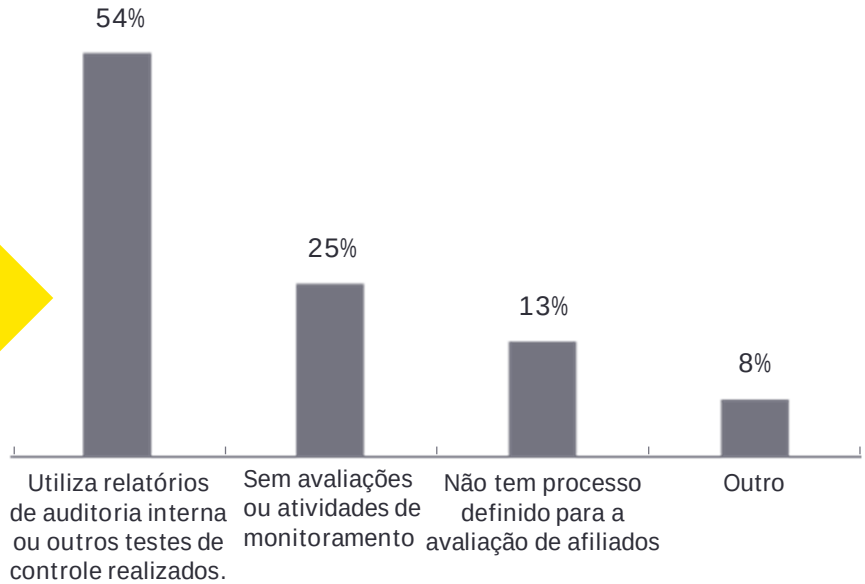
Dessas companhias pesquisadas que tem afiliados como alvo de seus programas de GRT, 55% dizem que o processo é o mesmo para avaliá-los. Das organizações que possuem processos diferenciados, a maioria utiliza relatórios de auditoria interna ou outros testes de controle, o que sugere que é possível mensurar corretamente o gerenciamento necessário de afiliados sem esforços adicionais de avaliação.

Processo de avaliação de afiliados

Q48. O seu processo de avaliação de afiliados internos é o mesmo que o processo de gestão de risco de terceiros?



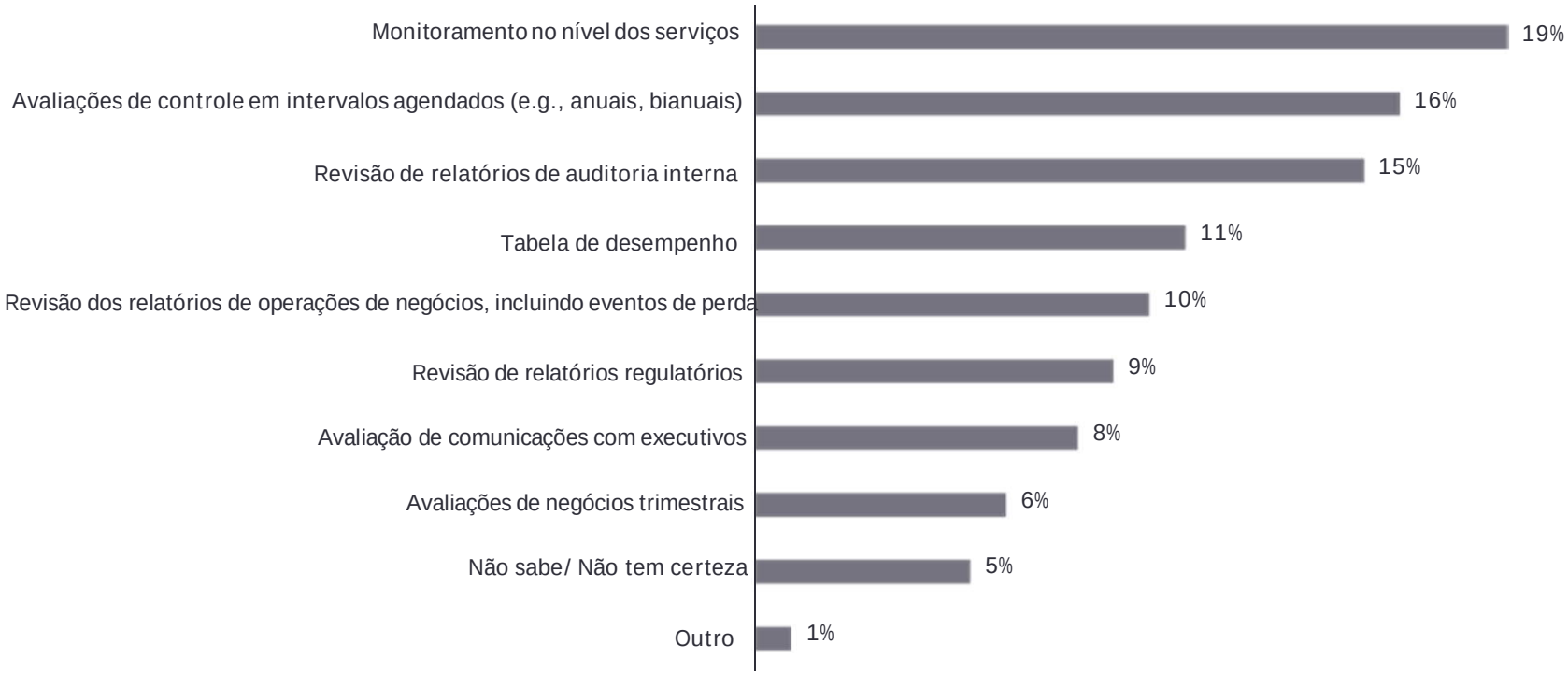
Q49. [Se não] Como o processo se diferencia de outras companhias?



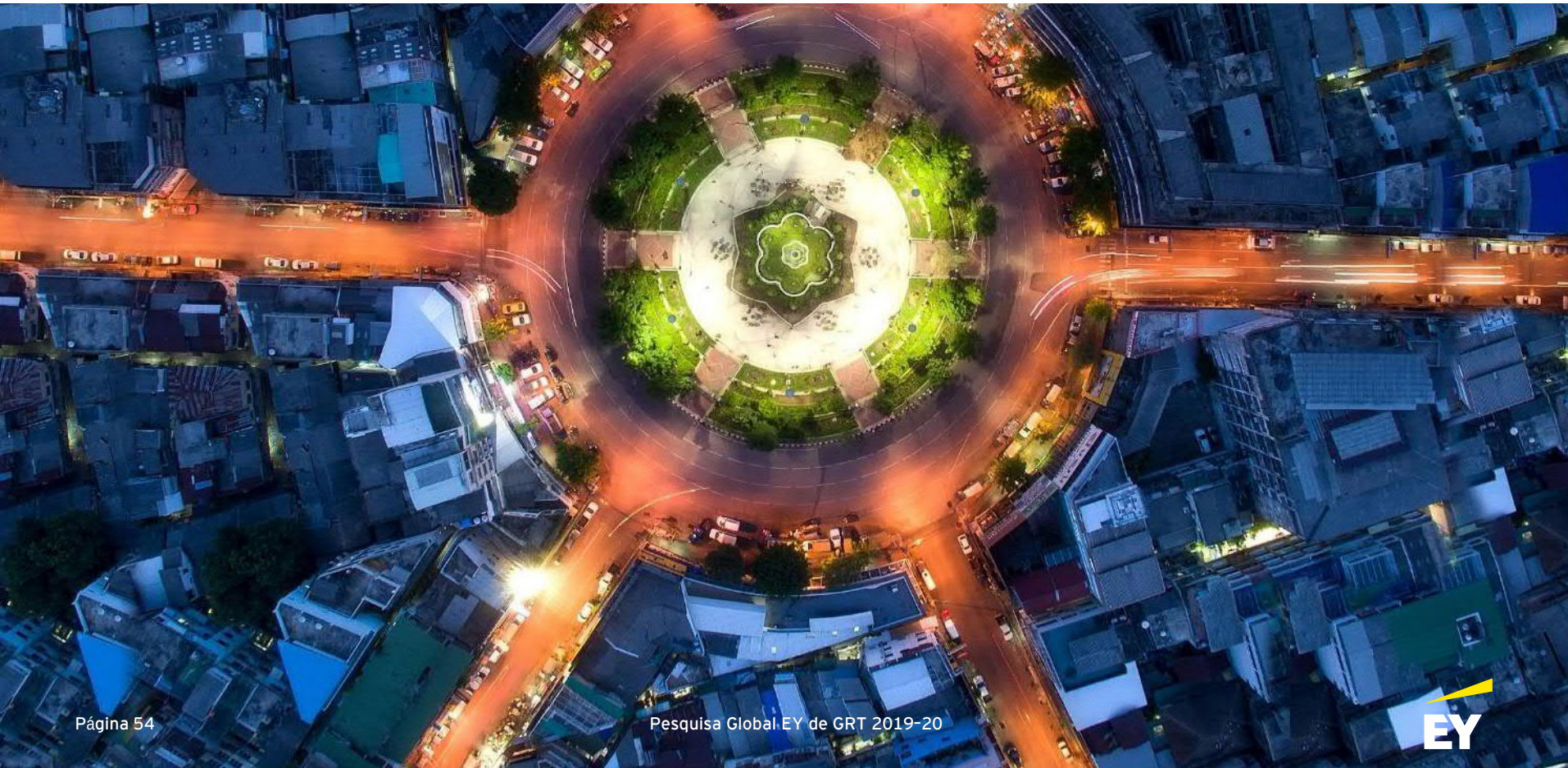
Monitoramento de afiliados tende a variar bastante, sem nenhum consenso mesmo em atividades básicas como monitoramento no nível dos serviços.

Requerimentos de monitoramento intercompany

Q50. Qual dos seguintes requerimentos de monitoramento se aplicam aos afiliados provedores de bens/serviços para a sua organização?



Inovação

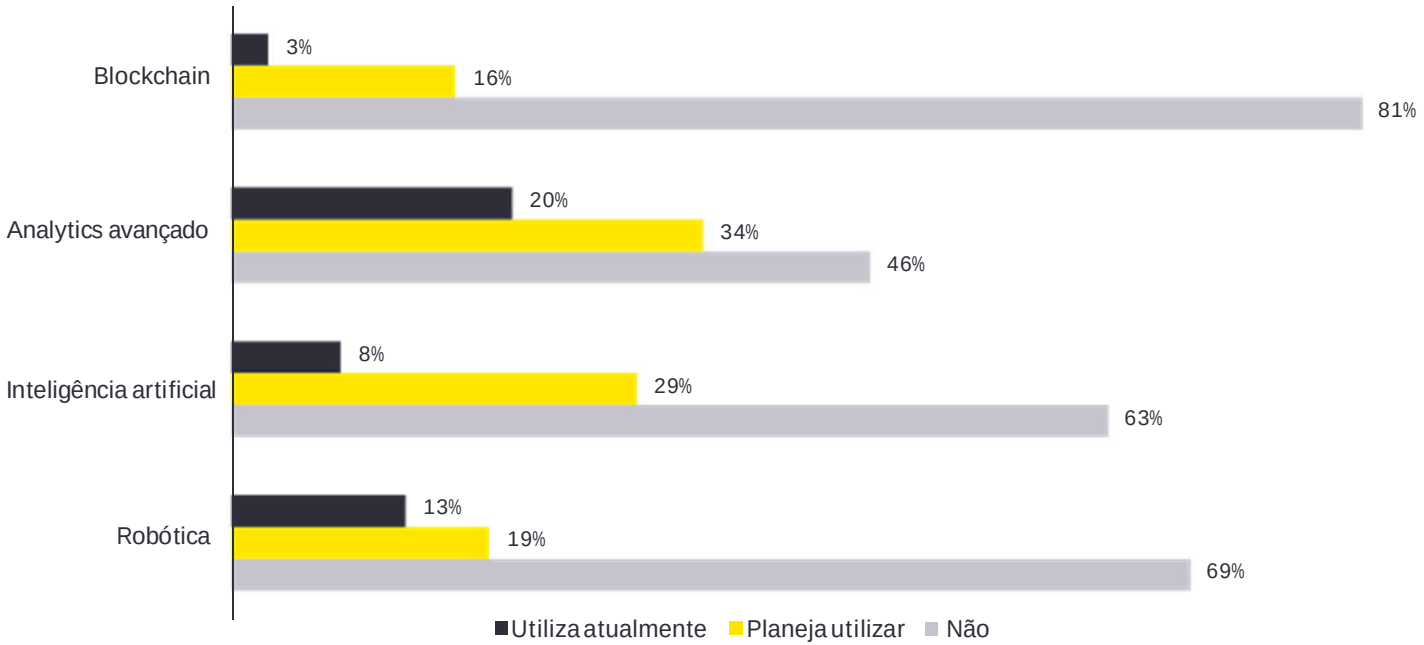


Somente uma em cada cinco das organizações pesquisadas está utilizando analytics avançado, e ainda menos utilizam inteligência artificial, robótica ou blockchain. Contudo, muito mais organizações reconhecem os benefícios que tais tecnologias podem trazer. Mais de uma em três espera começar a utilizar analytics avançado em dois a três anos, e quase uma em três planeja utilizar inteligência artificial.

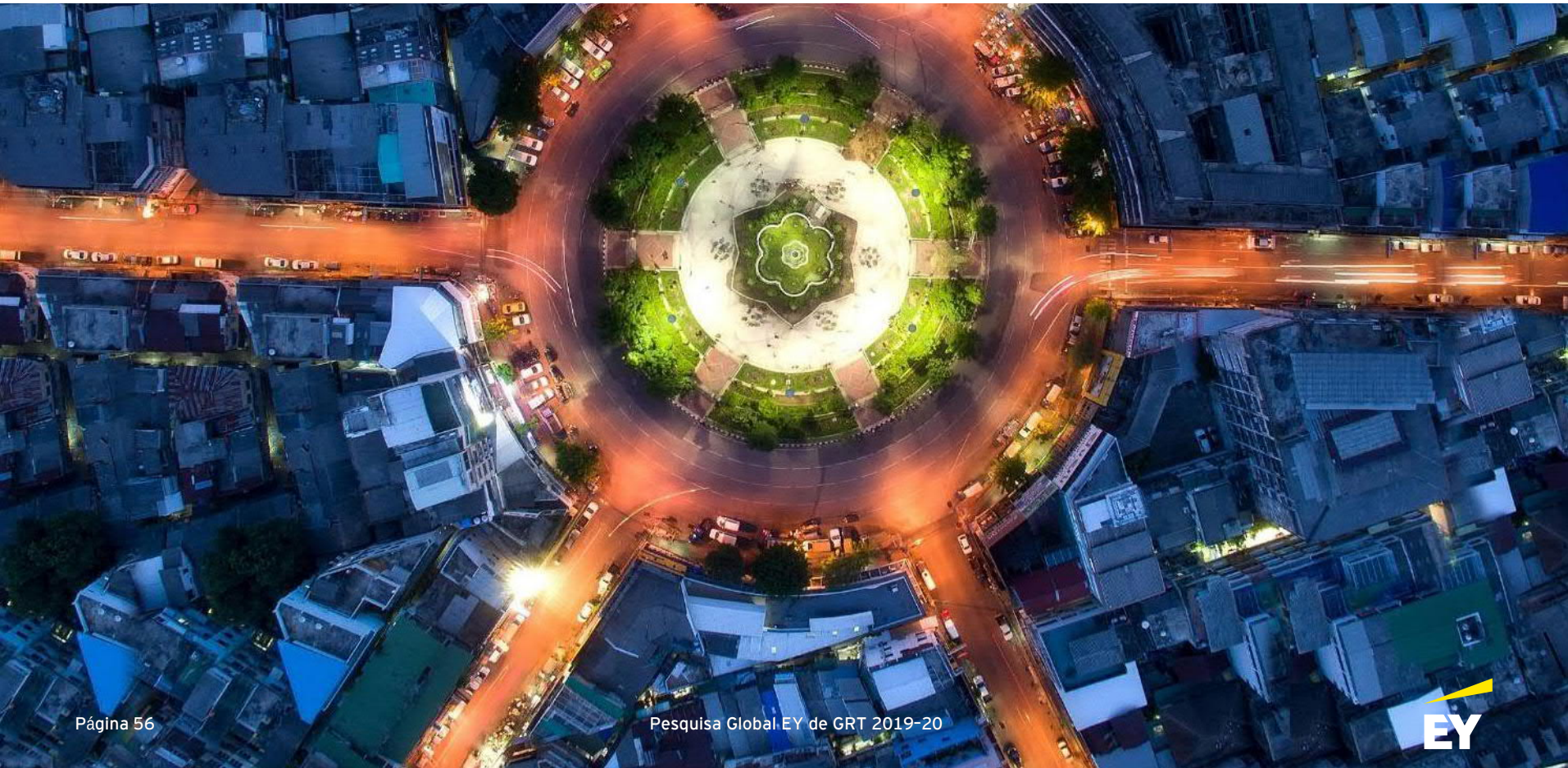
Tecnologias emergentes para GRT

Q51. A. A sua organização utiliza atualmente alguma das seguintes tecnologias emergentes como suporte para seus programas de gestão de riscos de terceiros?

B. Se não, a sua organização planeja começar a utilizar alguma das seguintes tecnologias nos próximos 2 a 3 anos ?



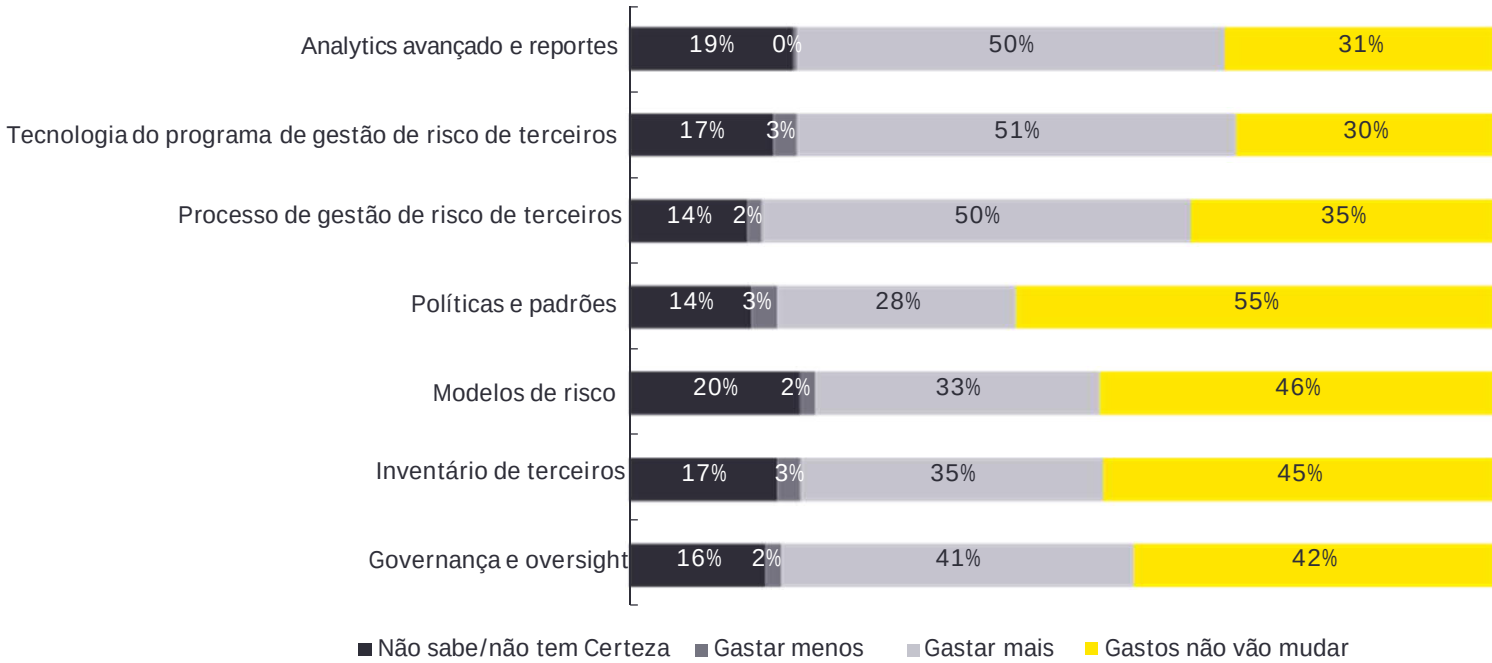
Áreas de investimento



De modo a melhor alavancar as tecnologias possuídas, e permanecer na vanguarda quanto ao uso de tecnologias emergentes, a maioria das organizações pesquisadas planeja aumentar seus gastos com tecnologia, suportando seus programas de GRT e analytics avançado. Analytics avançado é atualmente a tecnologia emergente mais comumente utilizada (Q51), e 50% das organizações planejam aumentar seus gastos com ela no futuro. Das organizações pesquisadas, 85% irão manter ou aumentar seus gastos com processos de gestão de risco de terceiros.

Tempo investido em atividades

Q52. Em comparação com o ano atual, a sua organização pretende gastar mais, menos ou o mesmo montante para as seguintes atividades?



EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2020 EYGM Limited
All Rights Reserved.

002185-20Gbl
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com

Contacts

GLOBAL

Amy Brachio
EY Global Advisory Risk and Performance Improvement Leader
amy.brachio@ey.com
Tel: +1 612 371 8537

Nitin Bhatt
EY Global Advisory Risk Transformation Leader
Email: nitin.bhatt@in.ey.com
Tel: +91 80 6727 5127

AMERICAS

Matthew Moog
EY Global Financial Services GRT Leader
matthew.moog@ey.com
+1 201 551 5030

Vignesh Veerasamy
EY Global and Americas GRT Leader
vignesh.veerasamy@ey.com
+1 415 425 3993

Michael Giarrusso
Americas GRT Financial Services Leader
michael.giarrusso@ey.com
+1 617 585 0395

ASIA-PACIFIC

Chris Lim
APAC Financial Services GRT Leader
chris.lim@sg.ey.com
+65 6309 6320

Steven Xiong
APAC Risk Transformation Leader
steven.xiong@cn.ey.com
+862122282688

OCEANIA

Hanny Hassan
Oceania Financial Services GRT Leader
hanny.hassan@au.ey.com
+61 2 9248 4141

Heidi Riddell
APAC and Oceania Risk Leader
heidi.riddell@au.ey.com
+61 2 9248 4569

EUROPE, MIDDLE EAST, INDIA AND AFRICA (EMEIA)

Kanika Seth
EMEIA Financial Services GRT Leader
kseth@uk.ey.com
+44 20 7951 7469

Netta Nyholm
EMEIA GRT Leader
netta.nyholm@de.ey.com
+49 221 2779 16427