KPMG

サードパーティリスク管理の展望2020

KPMG International

home.kpmg/thirdpartyrisk

目次

はじめに

組織が重要な商品やサービスをクライアントや顧客に届ける上で、第三者（サードパーティ）であるサプライヤーへの依存度が大きくなっています。また、サードパーティの失敗がすぐに自組織の評判を傷つけ、下流行程とコストに多大な影響を及ぼすことに気づきはじめています。これらの問題に関する懸念に組織が対応しようとすれば、サードパーティの選択、承認、管理に明確な戦略が必要となることは明らかです。調達やリスク監視部門など無数の利害関係者が関与しているために、この戦略の策定と実行は引き続き非常に困難なものとなっています。

サードパーティリスク管理（TPRM）を一言で表すと、組織がサードパーティの商品やサービスによりもたらされるリスクを評価・管理するために利用するプログラムのことです。たとえば、契約により当該組織の情報がサードパーティの施設に保存されている場合、組織はデータセキュリティのリスクを評価する必要があります。TPRMプログラムを適切に機能させるために、組織の最高情報セキュリティ責任者がデータセキュリティリスクの管理者として契約前から調達プロセスに関与することになります。その際、最高情報セキュリティ責任者は以下の判断を行うことができます。

- サードパーティは組織のデータにどのようにアクセスし、それを保存し、送信するか
- 組織の期待を満たし、強化ニーズに対応できる統制環境を持っているか
- 契約に特定の要件を盛り込む交渉をするべきか

その他の関係者の例として、たとえばリスク監視機能関連では、コンプライアンス部門が挙げられます。コンプライアンス部門は、サードパーティのサービスプロバイダーが金融犯罪や経済制裁規制違反のリスクがあるかどうかを判断します。

契約締結後、組織のTPRMプログラムは、サードパーティとの継続的関係管理、サードパーティの業績監視、サードパーティが期待される統制環境を遵守していることの継続的検証に集中しなければなりません。

そのような活動の重要性と、多くの組織においてサードパーティが提供するサービスの多様性を考慮した上で、TPRMプログラムに適切なガバナンス構造と役割、サービスデリバリーモデルを確保するために、組織は何ができるでしょうか。サードパーティ全体のリスクを効果的に管理しながらも、組織内の関係担当者やその他の関係者がサードパーティに適時に関与できるようにバランスを取るには、どうすればよいでしょうか。さらには、重要な統制の有効性を最適な方法で継続的に評価するために、TPRMプログラムがイノベーションと新たなテクノロジーを最大限に活用できるようにするにはどうすればよいでしょうか。

このような問いに取り組みたいと考えたKPMGインターナショナルは、世界14ヵ国および法域と複数のマクロ産業セクターにわたる大規模組織を対象に、1,100人のTPRM担当上級幹部の調査を実施しました。

本レポートでは、TPRMの基本的性質には、産業および地理的領域全体にわたり広範な共通性が見られるという認識のもと、主な結果を提示しています。私たちは、TPRMプログラムの最適化を追求する組織を支援するために、さまざまなクライアントとの経験を通じて開発したTPRMフレームワークおよび方法論の主要要素も紹介しています。

グローバル事象や経済的不透明性が引き起こす破壊の結果、組織が新たな経営環境に適応する際、多くの組織はサードパーティのリスク特性と自身のレジリエンスを再評価することになります。組織がそれを行うとき、堅固で持続可能なTPRMプログラムが、以前にも増して求められるようになるでしょう。

サードパーティの明確化

KPMGの結果を詳細に論じる前に、本レポートを通じて使用するいくつかの用語の意味について明確化することが有用でしょう。まず、サードパーティの定義とは何でしょうか。

「サードパーティ」という語の定義について自組織で合意があると完全に確信している組織は、本調査の回答者の中で少数派（41%）にすぎませんでした。KPMGインターナショナルおよびKPMGのメンバーファームでは、以下のような外部者がKPMGのサードパーティの定義に該当すると考えています。ベンダー、サプライヤー、サービスプロバイダー、代理店、販売業者、ブローカー、ジョイントベンチャー、再販店。内部のサードパーティとしては、関連会社、シェアードサービス、同一グループ内の親会社／事業体。私たちの定義では顧客は含まれません。

なぜなら、取引に入る前に、サードパーティプログラムを通じて顧客を吟味したり、受入手続を実施したりすることはないからです。たとえば金融サービス事業者であれば、顧客確認（KYC）という別のプロセスを通じて顧客を受け入れます。

TPRMプログラムが対応するリスク

次に、サードパーティリスクというとき、具体的にどのリスクを指しているのでしょうか。図1では、すべての組織がさらされている主要リスクのカテゴリーを概説するとともに、これらのカテゴリーに該当するいくつかの脅威も示しました。

提供されるサードパーティの商品またはサービスの種類に応じて、これらの各リスク（一般的には、これらの複数リスクの組み合わせであることが多い）がサードパーティとの関係性において提示されます。TPRMプログラムは、各種リスクの特定と評価に関する役割および責任を商品またはサービスのレベルで明確化し、当該サードパーティが組織の期待に即してリスクを管理できるかどうかを組織に不可欠なリスク専門家が判断できるようにしなければなりません。サードパーティの統制環境あるいは組織の内部補完統制を通じてリスクが特定・緩和されなかったために、結局は組織が厳しい処罰を受け、評判を落とすことになった多くの事例があります。

TPRMプログラムに関する第1の成功要因は、もっともリスクの高いサードパーティのサービスに時間、労力、専門性を集中させることです。KPMGの調査では、組織にとって極めて重要と考えられるリスク領域と、TPRMプログラムで優先されるリスクとのミスマッチが発見されました。たとえば調査では、全セクター

図1. TPRMプログラムが対象とすべき潜在的リスク

規制／コンプライアンスリスク	― 規制要件 ― 盗難／犯罪／紛争リスク	― 不正、贈収賄防止、腐敗／経済制裁 ― 社内手続および基準の遵守
戦略リスク	― サービスデリバリーリスク ― 拡大／展開リスク ― 合併および買収リスク	― 外部委託戦略との一致 ― 知的財産リスク
再委託リスク	― 全リスク領域に適用可能	
集中リスク	― 重要サービスにわたるサプライヤーの集中 ― 産業集中（再委託業者を含む） ― 重要スキル（すなわち、技術支援）の集中	― 地理的集中 ― 逆集中
テクノロジー／サイバーリスク	― 情報セキュリティ ― サイバーセキュリティ ― データプライバシー／データ保護	
カントリーリスク	― 地政学的リスク ― 気候の持続可能性	
財務の健全性	― サードパーティへの融資による財務リスク ― 流動性リスク	
オペレーショナル／サプライチェーンリスク	― 事業継続 ― 災害復旧 ― 物理的セキュリティ ― オペレーショナルレジリエンス	― 業績管理（SLAを含む） ― モデルリスク ― 人材リスク（コンダクトリスクなど）
評判リスク	― ネガティブニュース ― 訴訟（決着済みおよび係争中） ― サードパーティのブランド	― サードパーティの重要な理念／所有者 ― 職場の安全性
法的リスク	― 法域 ― 契約条件	

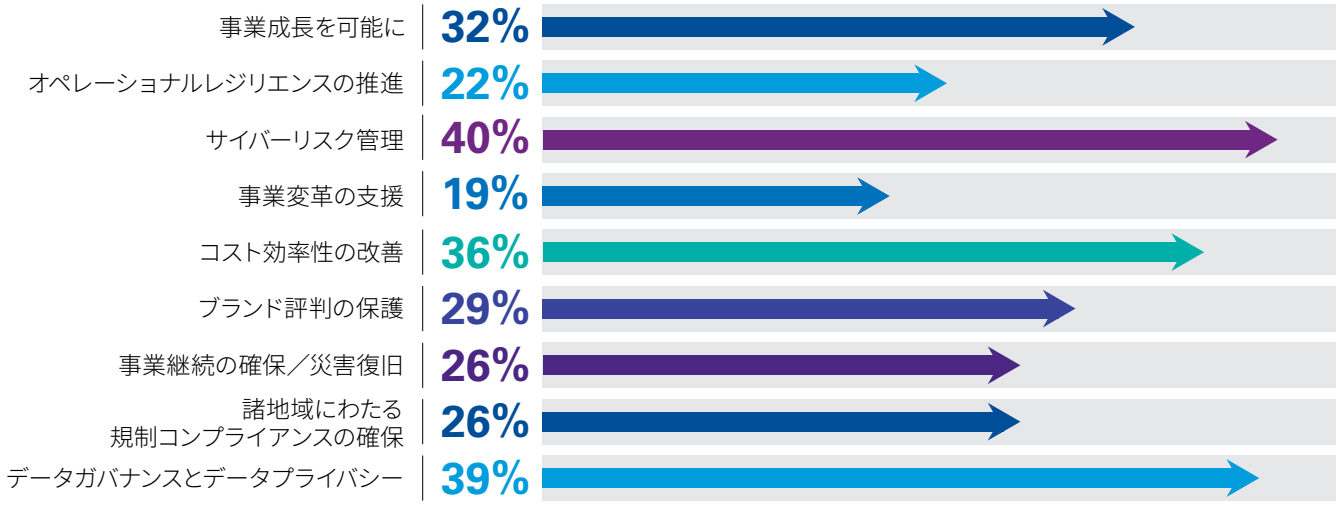
出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

および地理的領域にわたり、データガバナンスとデータプライバシー（サイバーリスクとともに）がサードパーティ活動の最重要ドライバーでした（図2を参照）。それにもかかわらず、組織がTPRMプログラムで対象とするリスクをKPMGが調査したとき（図3を参照）、データ／プライバシーを優先しているのは回答者のわずか54%にすぎませんでした。

KPMG英国のパートナーを務めるデイビッド・ヒックスは、この結果について次のように述べています。「TPRMプログラムは、明確に規定されたリスクアペタイトに基づき、よく定義され考え抜かれた戦略を持たなければなりません。このようにしてプログラムは、対処すべき基準、さらには取締役会や経営上層部に対する報告の基準を設けています。」

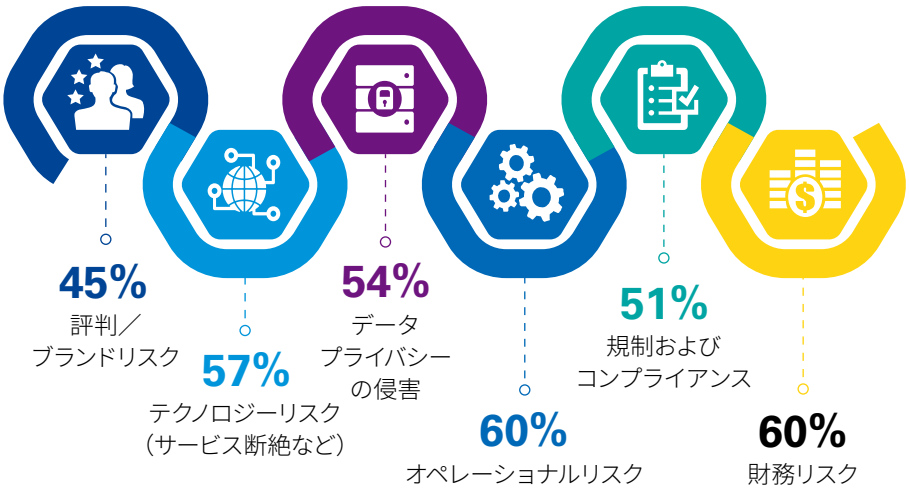
グローバル事象と経済的不透明性によりもたらされた新常態の文脈でこのデータを再吟味するならば、TPRM活動のドライバーとしてオペレーショナルレジリエンスが挙げられる比率（22%）はもっと高くなるはずだと私たちは考えました。KPMGオーストラリアのディレクターを務めるギャビン・ロゼッテンシュタインも、次のように指摘しています。「クライアントとの最近の対話からは、TPRMチームとサプライチェーンチームに盛んに投資が行われ、顧客やクライアントに重要なビジネスサービスを提供する上でサードパーティが果たす役割が認識されていることが分かります。今後数年間においては、引き続き、オペレーショナルレジリエンスがTPRMへの投資の動機となると予想されます。」

図2. 現在、貴組織におけるTPRM活動の最も重要なドライバーは何ですか



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

図3. 貴組織のTPRM活動の一環として、以下のどのリスクを対象としていますか



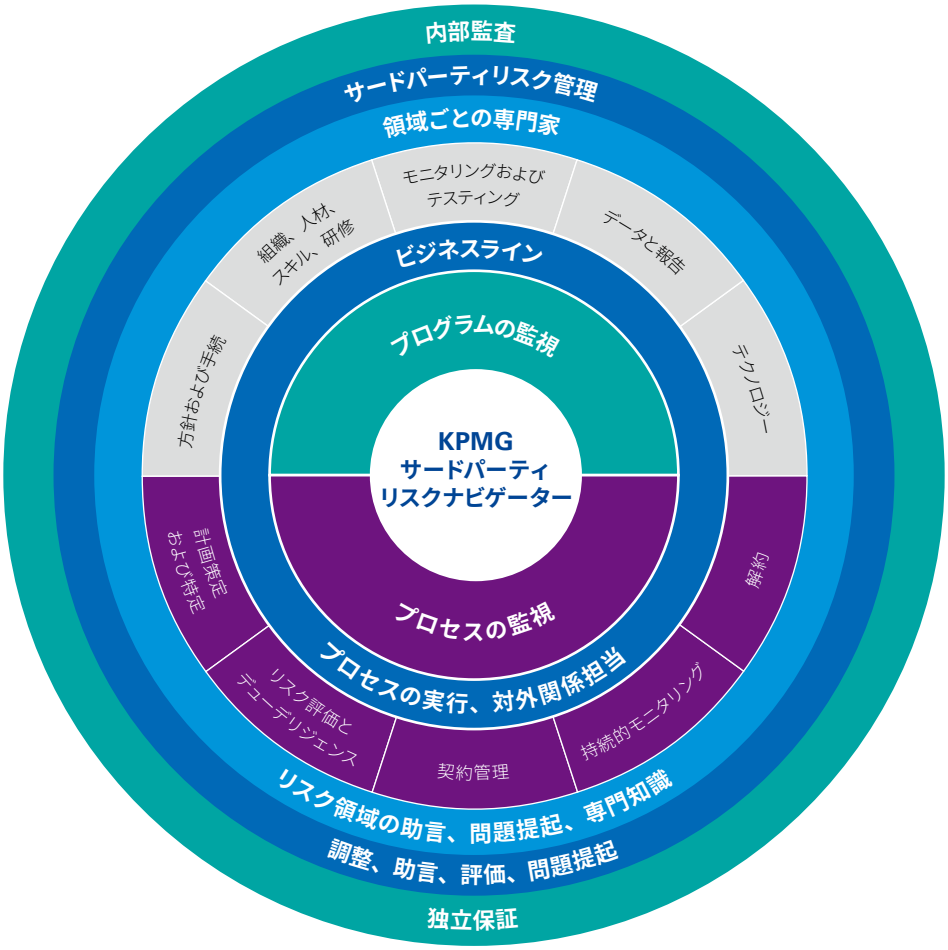
出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

> TPRMプログラムは、明確に規定されたリスクアペタイトに基づき、よく定義され考え抜かれた戦略を持たなければなりません。このようにしてプログラムは、対処すべき基準、さらには取締役会や経営上層部に対する報告の基準を設けています。
>
> ——KPMG英国パートナー
> **デイビッド・ヒックス**

TPRMプログラムとプロセスの区別

「あらゆるケースに対応できる」TPRMプログラムなどは存在しないという私たちの考えについて、まず言及しておくことが有益です。とはいえ、どの産業であれTPRMプログラムが成功を収めるには、明確なプログラムガバナンスのリーダーシップのもと、サードパーティリスクの特定、監視、管理という明確なプロセスに従う必要があります。図4は、TPRMプログラムの主な領域と、これらの領域がTPRMのライフサイクル全体にどのように適用されるか概要を示したものです。

図4. TPRMプログラムの重要領域とTPRMの全ライフサイクル



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

次の第1節では、主な調査結果について論じます。第2節では、有効なTPRMオペレーティングモデルを構築するための、KPMGの専用フレームワークについて概説します。最後に第3節では、プラスの変化を推進し成熟を実現させるために組織が講じるべき手段を提示します。

皆様が本レポートに有用性を見出し、話し合うことでさらに考察を深めていただければ幸いです。

> クライアントとの最近の対話からは、TPRMチームとサプライチェーンチームに盛んに投資が行われ、顧客やクライアントに重要なビジネスサービスを提供する上でサードパーティが果たす役割が認識されていることが分かります。

——KPMGオーストラリア　ディレクター　**ギャビン・ロゼッテンシュタイン**

第1節

主な調査結果

TPRMは戦略的優先事項

本調査の回答者の4分の3（77%）が、TPRMは自身の事業の戦略的優先事項であると述べています。加えて、回答者の10人中6人が、自組織にとって、もっとも深刻な評判リスクはサードパーティの業務遂行の失敗によるものだと述べています。これらの結果は、大半の事業が自身の重要な商品およびサービスをクライアントや顧客に届ける上で、サードパーティにいかに依存しているかを顕著に示しています。同時に、特にプライバシーの侵害および顧客データの喪失やオペレーショナルレジリエンスとの関係で規制圧力が高まっていることから、サードパーティとの関係が一層精査されるようになっています。10人中6人の回答者（59%）が、最近、TPRMとの関連で自組織が経済制裁や規制当局による指摘の対象となったと述べています。

グローバル事象と経済的不透明性が、事業経営にとってサードパーティがいかに必要かを際立たせました。KPMGは、パンデミックやグローバル事象および経済的不透明性の結果として、事業において検討するべき4つの段階（1対処、2レジリエンス、3回復、4新常態）を規定しました。TPRMに関して具体的に述べると、最初の2つの段階で、リモートワークモデルへの緊急シフトと、クライアントや顧客のために確実にサービスが維持されるようにサードパーティのサービスデリバリーモデルの再構築が行われます。後の2つの段階では、ニューリアリティにおいて組織が経営を行うための準備が行われます。リモートで働く臨時雇用者のために統制環境を自宅にまで拡大したり、ウイルスの感染を防ぐために職場にソーシャルディスタンスが要求されたりするのが、ニューリアリティです。TPRMプログラムはまた、政府による新しい規制として何が加わるかについて検討しなければなりません。危機の財務的影響が現れるとき、サードパーティのエコシステムのレジリエンスをめぐる一般的不透明性のために、TPRMプログラムへの更新が必要になるかもしれません。

組織のTPRMへのアプローチにおける一貫性のなさ

組織は世界中のさまざまなサードパーティと広範に協働し、各サードパーティは組織に代わってリスクの一部を管理します。組織がサードパーティとの提携を決定する前に、各サードパーティのリスク管理能力が期待に沿うかどうかを理解する必要があるというのももっともです。しかし困ったことに、KPMGの調査では、多くの組織が準備不足であることが分かっています。複数のリスクをビジネスラインと地域全体で一貫した方法で評価するという複雑性に対応できていないのです。受け入れのプロセスの最初から、また契約の全期間にわたり、全体的リスクを特定し評価することは、自組織の全サードパーティのリスク特性への見通しを組織が獲得する上で欠かせません。回答者の4分の3（74%）が、より一貫性のある全組織的なTPRMを緊急に構築する必要があると認めています。

リスクベース・アプローチは、TPRMプログラムに関して「真っ先に」取り組むべきこと

現在のビジネス環境におけるサードパーティリスクの管理は、単純とは言い難いものです。プログラムの範囲や関連する調整の量を考えると、途方に暮れている人も多いことでしょう。この状況は、組織のリソースと予算が限られていることで一層困難となります。組織の半数は、直面するサードパーティリスクのすべてを管理するだけの十分な能力を組織内に持ってはいません。KPMGの見解では、組織は自身に対してもっとも大きなリスクをもたらす

サードパーティの商品およびサービスを評価し監視するという、リスクベースのアプローチを取ることで、効率性と有効性の両方を達成することができます。

データとテクノロジーがTPRMチームの業績を改善

あらゆる産業と地域にわたり、近年、サードパーティの評価活動が大幅に増加したという回答が見られました。まず、TPRMプログラムは一層多くのリスク評価を遂行するために端的に人員を増やしました。現在、組織は次の3領域において、アプローチを革新させる余地があります。

- TPRMプロセスの内部ワークフローの一層の自動化
- デューデリジェンスの質問表および回答に関するシェアードサービスの活用
- 特定時点でのリスク評価から継続的な統制監視への移行

現在、テクノロジーを使用して、ワークフローの自動化あるいはサードパーティの監視のいずれかを改善している組織は、約4分の1しかありません。しかし、追加資金が利用可能になった場合、回答者がもっとも好んで行う投資はテクノロジーへの投資（61%）です。

「ようやく業界が、特定時点でのリスク評価アプローチを進化させる必要があるという合意に達したため、TPRMへの取組みは刺激的な仕事となっています」と、KPMG英国のパートナーを務めるジョン・ダウィーは述べます。「自社チームが質問表の回答を苦労して回収したり現場での評価に出向いたりせず、サードパーティリスクへの対処に集中できるようにと、あらゆる産業の企業が協働し、質問表とシェアード評価の共通基準を策定しています」

今こそプログラムの持続可能な拡大を

組織は、サードパーティが役割を果たせないことによるサービス断絶リスクがどこにあるかをよりよく理解するために、TPRMプログラムの成熟度を高めています。さらに、重要な再委託業者に対しても、リスクの特定、評価、管理を拡大しつつあります。本レポートの次節で考察するように、多くの組織は自身のオペレーティングモデル全体、ガバナンスの包摂性、プロセス、インフラ、データにわたり改善の余地があります。今回の調査によって、TPRMプログラムのアップグレードのために組織が講じるべき手段がより明確になったと思われます。これらの手段（本レポートの第3節で概説）は、チームがプログラムを向上させ、プロセスを最適化し、新たなテクノロジーを活用して利用可能なリソースの範囲内でよりよい結果を達成できるよう支援することに重点をおいています。

> 自社チームが質問表の回答を苦労して回収したり現場での評価に出向いたりせず、サードパーティリスクへの対処に集中できるようにと、あらゆる産業の企業が協働し、質問表とシェアード評価の共通基準を策定しています。
>
> ——KPMG英国　パートナー
> **ジョン・ダウィー**

第2節

効果的なサードパーティリスク管理（TPRM）のフレームワーク

KPMG米国のパートナーを務めるグレッグ・マシューズによると、先進的TPRMプログラムは、サードパーティリスクをより効率的に（効果を損なうことなく）特定、監視、管理するために、新たなオペレーティングモデルを実験しています。「TPRMの変革を達成するには、プログラムがいくつかの障害を克服する必要があります。幹部による支援が足りなかったり、説明責任が不十分であったり、TPRMプロセスへの協力にサードパーティが抵抗を示すなどといった最初の構築時からこれらのプログラムを苦しめ、その後も繰り返し問題を起こしてきた障害です」と、彼は説明します。

効果的なTPRMのためのオペレーティングモデルに関するKPMGのフレームワークは、ガバナンス、プロセス、インフラ、データという4つの柱を基盤とします。各柱は、以下に示す特定の要件を持っています。懸念事項の1つは、KPMGの調査データが示すとおり、多くの組織が依然として成熟への到達からほど遠いという点です。

> TPRMの変革を達成するには、プログラムがいくつかの障害を克服する必要があります。最初の構築時からこれらのプログラムを苦しめ、その後も繰り返し問題を起こしてきた障害です。
>
> ――KPMG米国　パートナー
> **グレッグ・マシューズ**

ガバナンス

必要なことは何か

- プログラムには単一のリーダーを
- 経営上層部および取締役会に対する報告構造
- 組織の外部委託・サードパーティ戦略、および明確に規定されたリスクアペタイト
- TPRMプログラム全体とTPRMの全ライフサイクルにわたる明確な役割、責任、説明責任
- プログラムの範囲と重点領域を確立するための方針、基準、リスクアペタイト
- サードパーティと合意されたサービス契約に基づき、プログラムが適用されるべきサードパーティのサービスの在庫管理

組織が行動を起こさなければならない理由

- 回答者の74%が、自組織のTPRMプログラムについて、全組織にわたる一層の一貫性を持たせることが喫緊の課題であると答えている
- 回答者の57%が、外部委託できるサービスとできないサービスの峻別について、全組織的な合意からはほど遠いと答えている

プロセス

必要なことは何か

- 分析用データの質の向上のために、TPRMプログラム全体にわたる実行の一貫性
- スキルと専門性、処理能力を適切なバランスで備えた評価チーム

— プログラムのリスクアペタイトに基づいたサードパーティのサービスを評価するためのリスクベース・アプローチ

— 契約実行に先立つリスク評価と意思決定の支援

— データ収集と質問表の回答の回収に近視眼的に集中するのではなく、リスク分析と低減を継続的に実施

— 継続的監視を含む、契約の全期間にわたる持続的監視

— プロセスを明確化し一貫性を高める手順およびテンプレート

— サードパーティに加え、フォースパーティおよび重要な再委託業者のリスクも対象に

組織が行動を起こさなければならない理由

— 回答者の52%が、組織のTPRMプログラムは過剰性能であり、事業遂行能力を阻害していると考えている

— TPRM活動の変革を試みるにあたり、回答者が挙げた第1の課題はスキル不足

— 回答者の67%は、自組織のサードパーティリスク評価は1人の担当者または1つの担当チームによってではなく、組織横断的な多くの人員によって遂行されていると回答

— サードパーティがもたらすリスクの包括的理解を形成することに関して、非常に熟達していると答えた回答者は、わずか32%

— 持続的監視のためのリスクベース・アプローチを有していると答えた回答者は、わずか36%

— 時間の経過とともに監視活動が立ち消えとなり、契約後のサードパーティの監視を行わなくなることがあると答えた回答者は40%

— フォースパーティの評価方法を緊急に改善する必要があると答えたのは、回答者の72%

インフラ

必要なことは何か

— 効率的なワークフロー、タスクの自動化、報告を支援するTPRMのテクノロジーアーキテクチャ

— 文書化され、よく理解された監査証跡

— ビジネスラインと地域全体にわたり一貫性あるリスク管理を可能にする、組織の経営スタイルに沿った（一元型または分散型）サービスデリバリーモデル

— TPRM活動およびテクノロジーを既存の全組織的プロセス（調達、法務、財務など）に、そして、既存のリスク監視機能と活動に統合すること

組織が行動を起こさなければならない理由

— TPRMの最終的責任の所在が組織によって顕著に異なっており、どのオペレーティングモデルを使用するかに関して、統一見解がない（図5を参照）

— TPRMプログラムにおけるルーチンタスクの実行を自動化によって効率性を高めていると答えた回答者は、わずか24%

データ

必要なことは何か

— サードパーティの評価、研修、活動の監視を管理するTPRMプログラムの能力と、各サードパーティのサービスの具体的成果およびサードパーティが事業を行う統制環境を管理するTPRMプログラムの能力に関するリアルタイムのデータ収集

— サービスの詳細、リスクスコアリング、契約情報、業績監視を含む、サードパーティの情報を収集する包括的データモデル

— サードパーティに起因する特定事象および事件を監視し記録する組織内データフィードと、サードパーティに関するリアルタイムの情報を監視する外部データフィード（アドバースメディア、事業所有権の変更、法人活動、サイバーセキュリティ脆弱性スコア、財務的実行可能性評価など）

— 問題や外部要因が発生したり、サードパーティの統制環境に変化が生じたりするなど、リスクスコアの変更が生じた場合に、サードパーティのリスク特性を可能な限りリアルタイムで更新するプロセス

— サービスレベル合意書（SLA）に照らしたリアルタイムの業績追跡

— 重要リスク指標（KRI）に照らしたリアルタイムのリスク追跡

— サードパーティとの再契約または関係継続において、リスク評価および業績監視が契約条件や意思決定に影響する場合の、データドリブンの意思決定

組織が行動を起こさなければならない理由

— サードパーティのデータを組織内で共有する際、互換性のないシステムなどの技術的障壁が主な障害となっていると述べた回答者は37%

— サードパーティとの契約における自組織の在庫の電子記録、リスク監視、報告、サードパーティの在庫の管理に関して大いに自信があると答えたのは、回答者の半分未満

— 評価の実施に必要な全データを自組織が持っていると確信しているのは、回答者のわずか4分の1（26%）

第3節

TPRMの高度化に向けて

ガバナンス、プロセス、インフラ、データの4つの柱にわたり確実な最適化を達成するには、組織はいかにTPRMプログラムを変革するべきでしょうか。KPMGの見解では、変革は常にプログラムの向上、プロセスの最適化、イノベーションというサイクルで進みます。実践的レベルでこのサイクルを引き起こすために、組織が講じるべき重要な手段があります。それは、ビジョンへの合意、モデルの構築、最適化、進化の4つです。

1 ビジョンへの合意

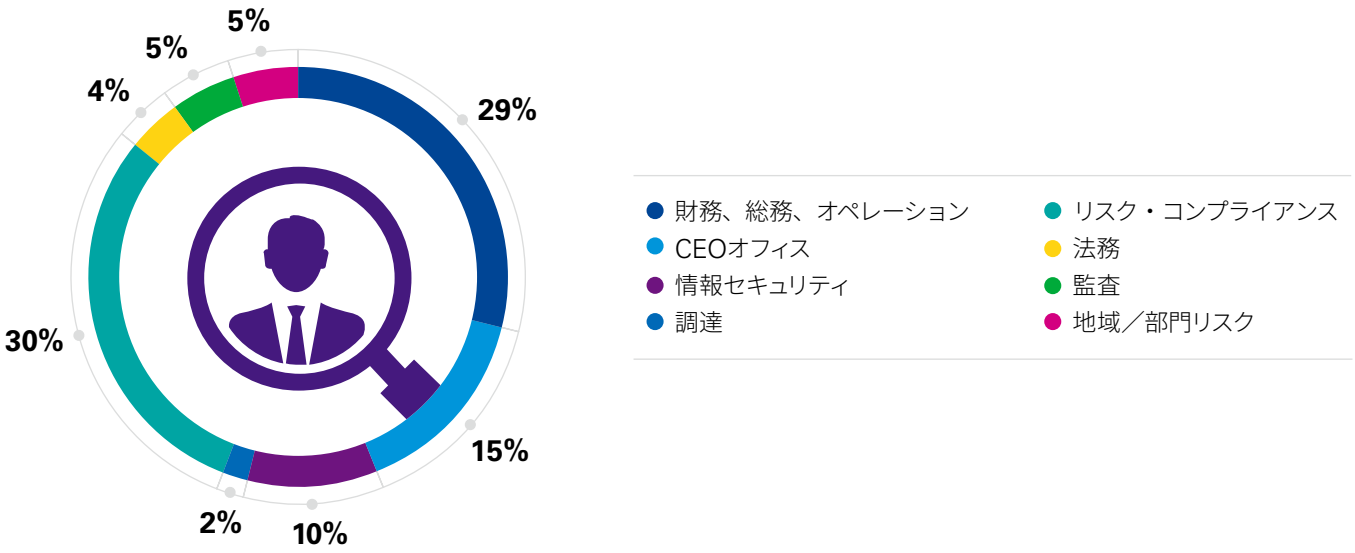
大半の組織が何らかのTPRMプログラムを導入しています。回答者の51%は限られた予算内で取り組んでいますが、サードパーティの利用がますます重要となる中、自組織のTPRMプログラムを進化および強化するために資金を利用できる、または資金は増えていると述べた回答者は4分の3（76%）に上ります。

全組織的TPRMプログラムについて主な検討事項は、プログラムに担当責任者を指名し、組織内のどこにTPRMを任せるかを決めることです。これは結局のところ、各組織の特質と複雑性によりますが、KPMGの調査では、リスクおよびコンプライアンス（30%）か、あるいは財務、総務、オペレーション（29%）が責任を負う可能性がもっとも高くなっています（図5を参照）。後者のグループでは、調達部門にTPRMのライフサイクル活動を実行させる組織が増えています。

「広義の調達部門内にTPRMをおくことで、オペレーションの効率性を大幅に高め、サードパーティのサービスに関する事業提携担当者のユーザー体験を改善できることが分かりました」と、KPMGドイツのパートナーを務めるアレクサンダー・ゲショネックは述べます。「とはいえ、調達部門がTPRMを実行するための準備として、一連のスキルの向上や文化的改革が必要となるかもしれません。また、サードパーティリスクをリスク委員会や取締役会に報告するために、報告ラインが複雑になるということもあるかもしれません。」

> 広義の調達部門内にTPRMをおくことで、オペレーションの効率性を大幅に高め、サードパーティのサービスに関する事業提携担当者のユーザー体験を改善できることが分かりました。
>
> ——KPMGドイツ　パートナー　**アレクサンダー・ゲショネック**

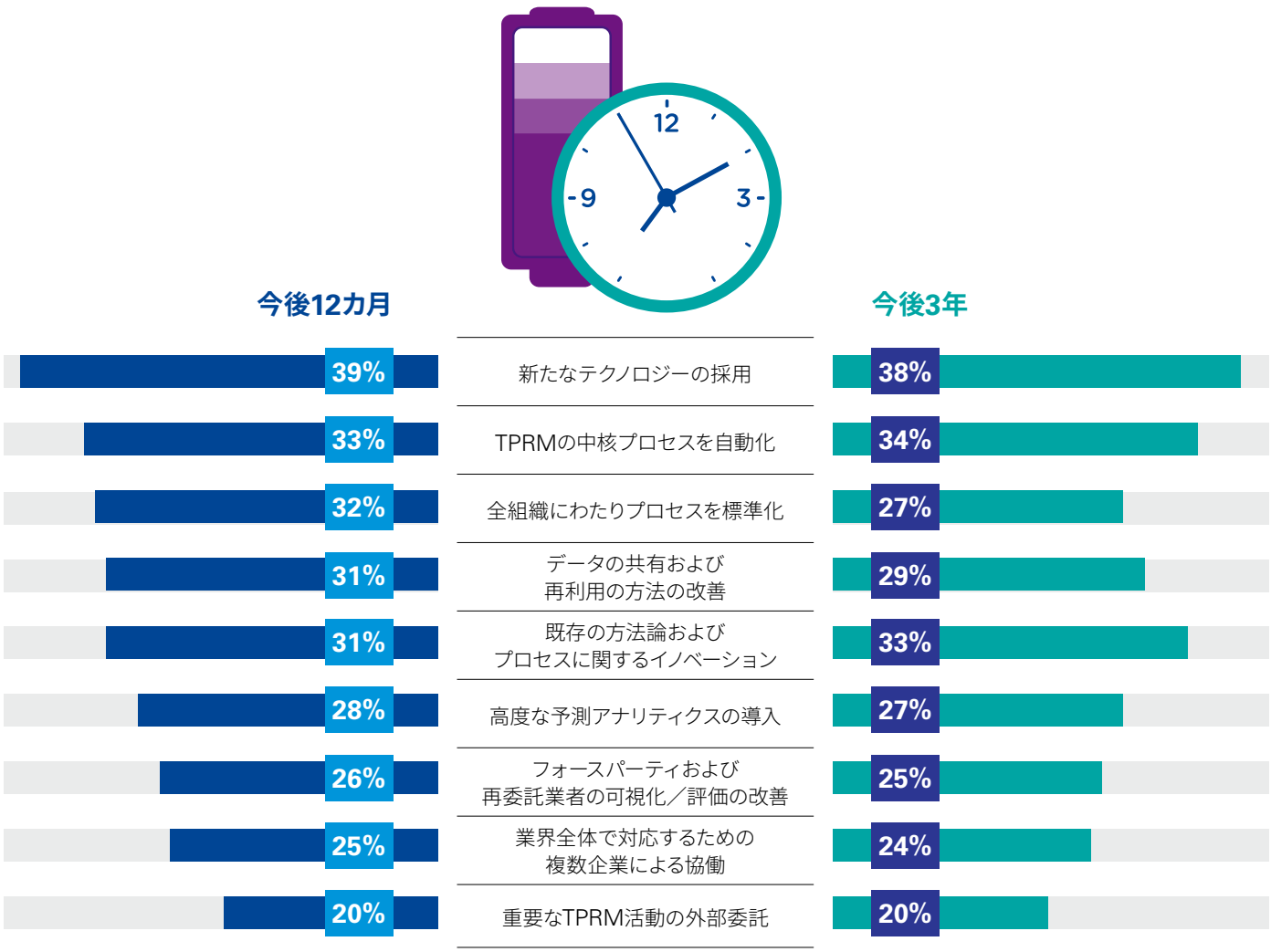
図5. 貴組織におけるTPRMの最終的責任はどこにありますか



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

プログラムのビジョンの確立とガードレールおよび責任者の設定の次は、テクノロジーを可能にする野心を抱くことです。この点に関しては、組織は「走ろうとするのならその前にまず歩けなければならない」ということを忘れてはなりません。TPRMの拡大とチームが大量のデータを処理し分析するのを支援する上で、TPRMプログラム全体の自動化が欠かせないことは、多くの組織が認識しています（図6を参照）が、テクノロジーは進歩のドライバーというよりは、進歩を可能にするものと見なすべきです。脆弱なプロセスを自動化しても、これらのプロセスが魔法のように強化されることはありません。

図6. 次の中で、今後12ヵ月および今後3年において、
貴組織のチームが最も時間と労力を集中させる取組みはどれですか



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

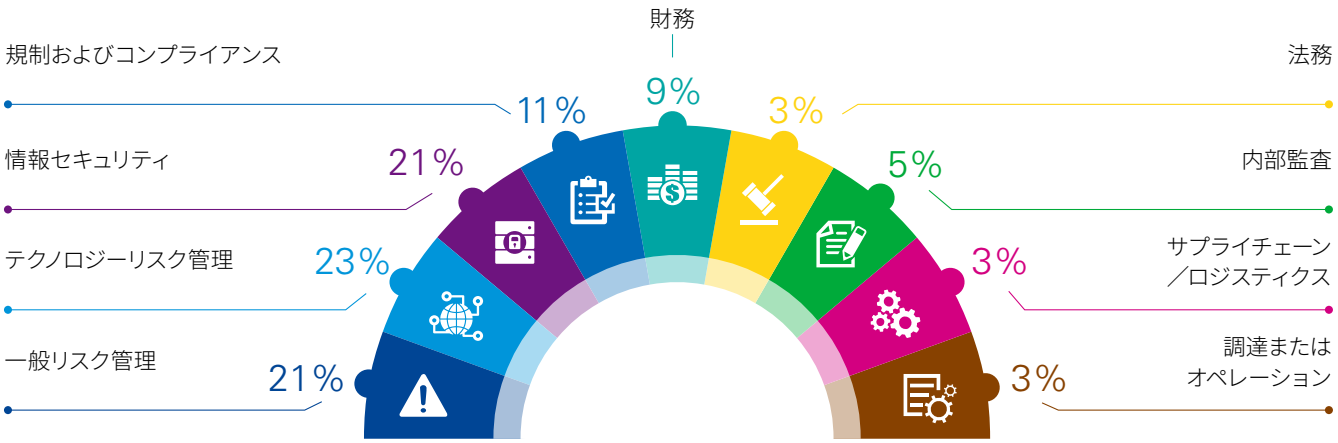
2 モデルの構築

TPRMプログラムは複雑です。組織のどの部署もサードパーティを利用しているというだけではなく、サードパーティの各サービスが複数のリスクを持っており、個々のリスク評価についてさまざまな監視機能に助言を求める必要があります。KPMG米国のパートナーを務めるアマンダ・リグビーが説明するとおり、「プログラムを構築した後、組織は横断的にその有効性を高めるために、プログラムの機能の仕方を調整し明確化することを続けます。TPRMプログラムの開発は、一度きりの実践ではありません。大半のクライアントは、自組織に適切なバランスを突き止めるのに、プログラムを3回もしくはそれ以上繰り返しています。」

プログラム構築の段階で検討することには、TPRMの全ライフサイクルを通じて事業関係者がいつ、どのように、どこで関与するかを厳密に決めることも含まれます。たとえば調達部門は、一般的にサードパーティの導入および管理プロセスに責任を負いますが、事業責任者と中央のTPRM評価者は、リスク評価プロセスの最初および継続プロセスなどの重要ポイントで、リスク管理の専門家との橋渡しをします（主な関与グループをまとめた図7を参照）。これ以外では、一般にTPRMプログラムのチームがプログラムの実行に責任を負い、リスク監視機能が監視するリスクに責任を負い、事業部門は日々、サードパーティのサービス管理に説明責任を負います。

> TPRMプログラムの開発は、一度きりの実践ではありません。大半のクライアントは、組織に適切なバランスを突き止めるのに、プログラムを3回もしくはそれ以上繰り返しています。”
>
> ——KPMG米国　パートナー　**アマンダ・リグビー**

図7. TPRMの第2の防衛線はどこが担いますか



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

もう1つの検討事項は、リスク評価活動の遂行にどのモデルを使用するかということです。組織は、事業部門ごとに固有のリスク評価活動を調整する際に使う分散モデルの使用を選択するかもしれません。あるいは、事業部門は、固有のリスク評価を推進する一元管理チームに任せるかもしれません。このモデルでは、事業部門がプログラムの実践やスキル不足にかかわる課題を克服するのを一元管理チームが支援し、一貫性を強化していきます。固有のリスク情報はTPRMプログラムのアナリティクスの基盤であるため、一貫性の強化は重要です。

「ベンダーのマネジャー全体に研修と監視が必要となるため、多くの事例で、拡散モデルの維持コストが全般的に高くなることが分かりました」と、KPMGシンガポールのパートナーを務めるレム・チン・コックは述べます。「2つのモデルの混合型、ただし、多くの場合拡散型よりもかなり一元管理型よりのモデル（一元管理チームがリスク評価活動を実施し、サードパーティのプロバイダーとの関係継続について最終的意思決定を行う事業関係マネジャーに結果を提供するモデル）も見られます。」

組織は並行して構築しなければならない特定要件を持っていることが珍しくありません。たとえば、現在の環境では、多国籍企業もまた、増加するグローバルな規制要件と諸地域間の差異に確実に対応しなければなりません。規制要件を遵守し、顧客やクライアントのデータプライバシーも含め規制当局の新たな期待に沿い続けるために、継続的にプログラムを更新していくことに関しては、コンプライアンスおよびテクノロジーリスク管理から適切な支援を受けることが欠かせません。

調査の回答者が重視するもう1つの領域は、フォースパーティおよび重要な再委託業者のリスク管理です。重要な再委託業者との関係の一事例は、サードパーティが自組織のサービスデリバリーの支援にクラウドのプロバイダーを利用している場合です。組織はこれらのフォースパーティへの一貫性ある監視態勢を確立する必要があります。これは、組織とフォースパーティとの間に直接的契約関係がないことを考えると、簡単なことではありません。フォースパーティのリスク管理については、組織は一般的に、図8に示された1つあるいはそれ以上の手段を用います。フォースパーティがアクセスできるデータやその役割が事業継続

リスクにどのような影響を及ぼすかを含め、サードパーティのサービスデリバリーにおける再委託業者の役割を理解することは、組織が利用するサービスの完全なリスク像を獲得するのに欠かせません。サードパーティが自らのサードパーティ（すなわち、組織から見たフォースパーティ）のリスク管理にプログラムを導入しているかを明らかにすることは、当該サードパーティに再委託業者の利用を許可するかどうかの評価の重要な部分をなします。

> 2つのモデルの混合型、ただし、多くの場合拡散型よりもかなり一元管理型よりのモデルも見られます。”
>
> ——KPMGシンガポール
> パートナー
> **レム・チン・コック**

これらの最初の検討事項を解決することは大きな一歩とはなりますが、これはTPRMプログラムが完全な成熟に達するのに必要な一部にすぎません。組織は契約前のリスク評価だけではなく、全契約期間中にわたる持続的監視も考慮に入れるよう、TPRMプログラムを拡大する必要があります。

3 プロセスの最適化

プロセスの最適化は、既定のリスク基準と重要性基準値を満たさないサードパーティが、TPRMプログラムによる評価へと進むことがないようにすることを目的とします。組織はリスク峻別プロセスを2つの方法で最適化できます。1点目はサードパーティのサービス全体に規律あるリスクスコアリングメソッドを確立すること、つまりリスクのセグメント化であり、2点目はコスト削減と説明責任の徹底のためのサービスデリバリーモデルの強化です。これらの活動は、KPMGの調査で回答者が示した予算的制約への対処に役立つとともに、チームが、利用できるデータを用いて適切な決定を下す助けとなります。

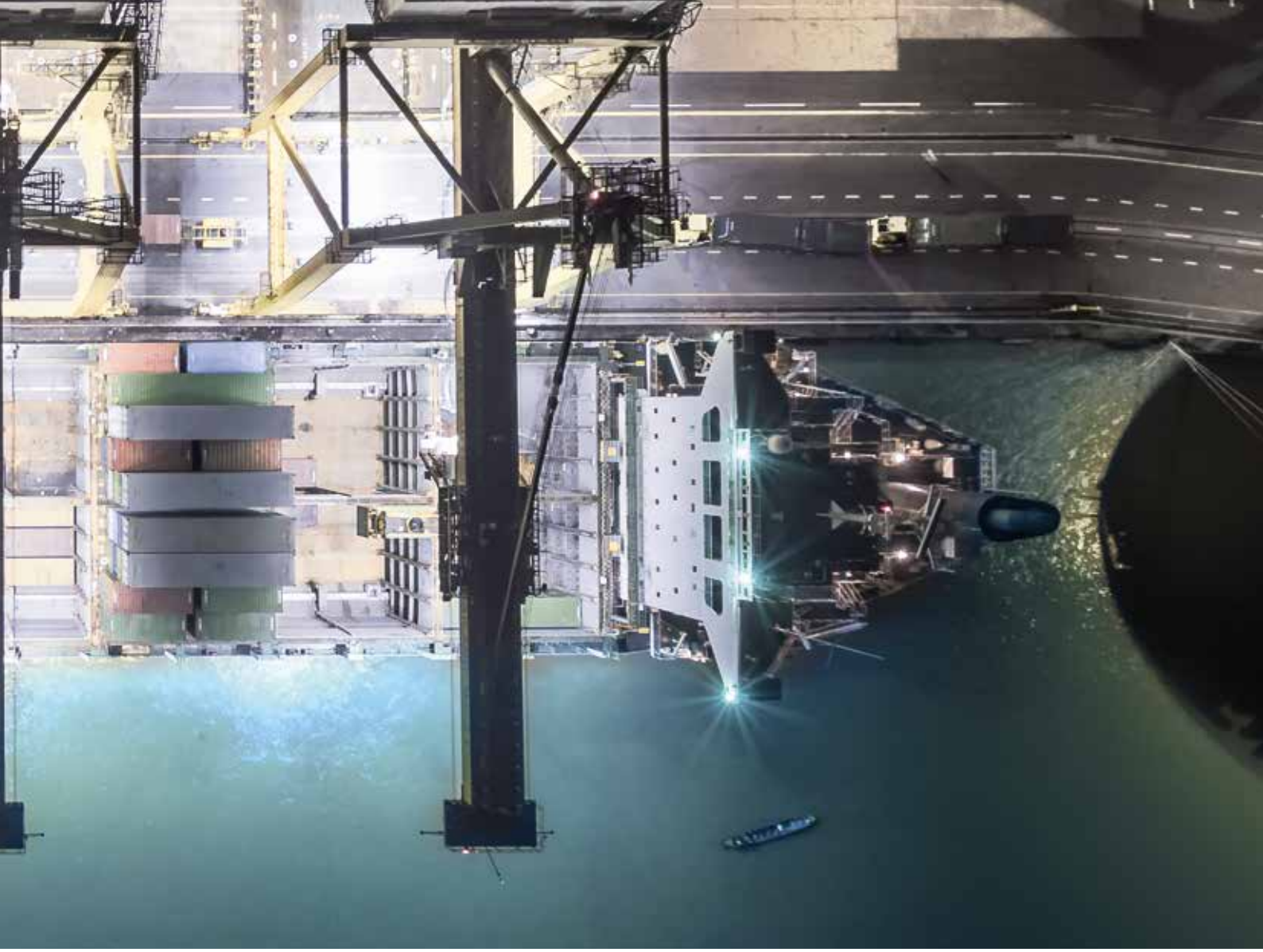
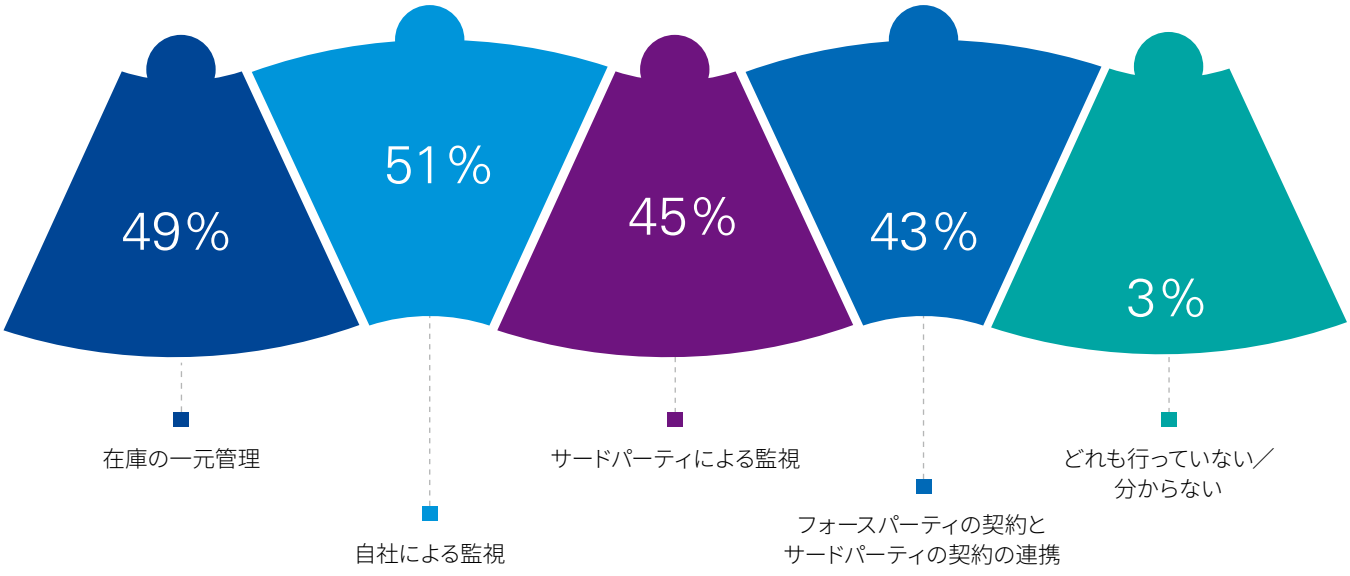


図8. 貴組織のフォースパーティのリスク管理のために、以下のどのプロセス・実務を行っていますか



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

組織はサードパーティを以下の3つのカテゴリーにセグメント化するべきです。

- 組織に対して通常のリスクをもたらし、リスク評価の必要はないサードパーティ
- TPRMプロセス基準に照らして適切なサードパーティ
- 異質のリスク特性を有するため、特別プログラムによってより効率的に一元管理されるべきサードパーティ

リスクセグメント化では、サードパーティリスク評価の要件に関して標準的リスク特性を提示しないサードパーティのために、カスタマイゼーションと特別な取扱を可能にすることを目的とするべきです。たとえば、組織が事務用品を購入するサードパーティは、中核顧客のお客様窓口を外部委託するサードパーティと同程度の評価は必要ないかもしれません。

これは実務的には、調達サービスごとに、形式上のリスク、特別プログラム指定のいずれに分別するかによって達成されます。TPRMプロセス基準に関しては、第1ステップは事前に以下のような一連の質問をすることです。

- そのサードパーティは、自組織のクライアント／顧客と接触するか
- 業務は自組織と同一国内で行われるか
- そのサードパーティは、知的財産または顧客／クライアントのデータにアクセスすることになるか。アクセスする場合、そのデータはクラウドに保存されるか
- そのサードパーティのサービスは、規制当局が精査する領域または規制要件と関連するか
- そのサードパーティのサービスは、重要な外部委託または重要な機能であるか

上記質問の答えが1つでもイエスの場合、関連するリスク監視機能の関与と、特定のリスク質問表への記入、そしてデューデリジェンスの評価を行うことになるかもしれません。一方、これらの質問への答えがノーである場合、リスク評価活動量を限定し、労力とコストを削減してもよいでしょう。

TPRMサービスデリバリーモデルの最適化に関しては、組織内の誰がTPRM活動を遂行するべきかのレビューを実施しているという先進事例があります。それぞれの外部委託担当マネジャーが大きく関与する分散モデルの最大の課題はスキル不足です。グローバル事象と経済的不透明性の中、サードパーティのサービスに関して正確な最新情報を得ること、外部委託担当マネジャーがすでに高まっている圧力にさらされていることを認識することが課題となっている組織もあります。

そのような人材課題への対応として、回答者は研修とスキル開発が自組織のTPRMプログラムの重要な注力領域であると述べています（図9を参照）。組織全体にわたりリスク分野の専門知識が限られているという認識のもと、多くの回答者はTPRMプロセス実行の諸側面を一元管理し、どこでジェネラリストがリスク評価の諸側面とデューデリジェンスプロセスを遂行できる可能性があるかを決めています。組織はどの統制およびどのリスク領域に専任の専門家を充てる必要があるかを決めています。一元管理チームがリスク評価とスコアリングを実施する一方、事業部門が依然としてサードパーティとの契約継続（または終了）の決定に説明責任を負うかもしれません。KPMGの見解では、TPRMプロセスのこれらの構成要素を明確に定義することで、組織はタスクを自動化し、ワークフローを構造化し、さまざまなチームによる情報の収集および分析を単純化することができます。

4 進化と革新

TPRMプログラムにおいて、情報収集とサードパーティの統制情報の評価に、もっとも多くの努力が費やされていることを考えると、これらはもっとも投資対象として関心が高まっている領域です。今後数年では、次の2つの広範なトピックにわたり大幅な進歩が予想されます。

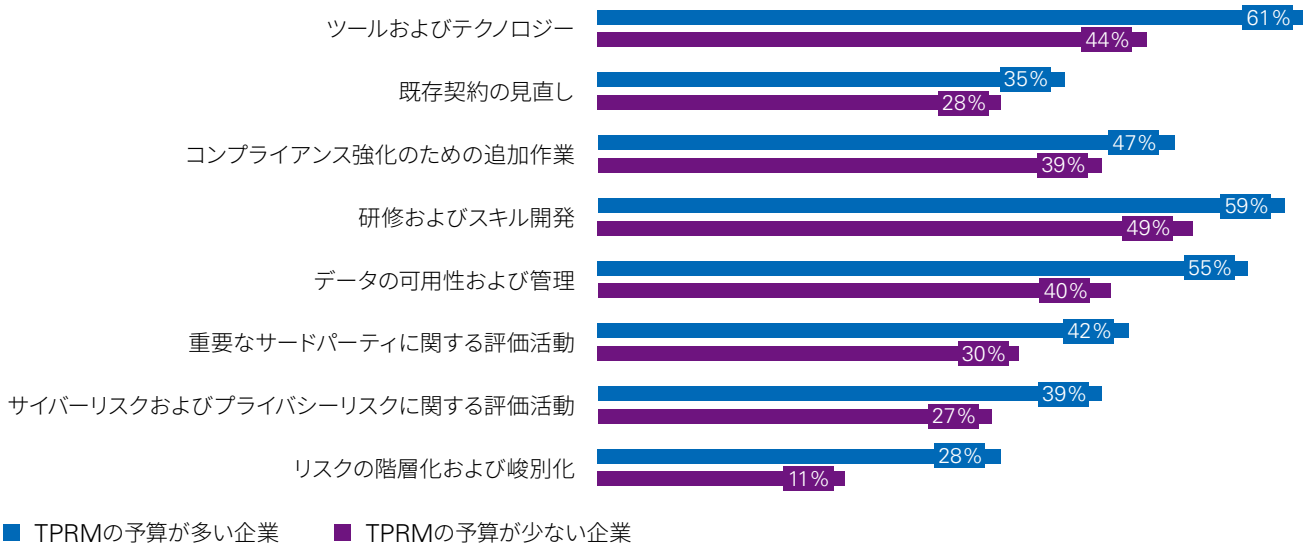
- デューデリジェンスの共有に業界全体で対応
- サードパーティの統制環境をより継続的かつ一貫性ある仕方で評価するために、テクノロジーとスコアリングサービスを使用

調査回答者の過半数は、コスト削減のために共有の評価情報を活用しているか、あるいは今後活用したいと考えています。業界が共同でサードパーティとその顧客の間の情報を収集かつ共有するユーティリティサービスについては、承認と受容が進みつつあります。ユーティリティがサードパーティとユーティリティの利用顧客に与えるメリットは明確です。サードパーティにとって、情報の収集および共有は、各顧客が別々にリスク評価を行うのではなく、ユーティリティが一度情報を収集し、評価を終えた後、その顧客すべてに評価結果を提供するということを意味します。このシナリオでは、顧客へのメリットは、適時に必要な評価情報を獲得でき、関連するリスク評価コストを業界全体で分担できるということになるでしょう。

TPRMテクノロジーのイノベーションに関しては、組織は限られた予算を新たなツールに集中させているということがKPMGの調査で示されています（図9を参照）。これはTPRMプログラムの成熟度に基づく、私たちの経験とも一致します。過去には、組織は評価活動の増加を人員を増やすことで対処してきました。現在では、先進的TPRMチームが自動化、データアナリティクス、自然言語処理を使用するとともに、選択したリスク領域全体にわたる、手頃でスケーラブルな継続的監視、業績管理、契約のコンプライアンスにスコアリングサービスを導入している状況が見られます。TPRMプログラムは、リスク事象関連の組織内データを評価し、サードパーティにより引き起こされた可能性のあるこれらのリスク事象を特定するために、機械学習をどのように利用できるかを研究しています。サードパーティのSLA条項遵守の監視を自動化し、契約不履行への補償を受け取る機会を特定し、ソーシャルメディアデータの自動分析などにより評判リスクに一層積極的なアプローチを取るということを行っています。

これらのイノベーションのいくつかは、グローバル事象および経済的不透明性とその余波によりもたらされた課題に対処するために、チームが自組織のプログラムを調整する際、一層魅力を増しています。現在、組織の現場レビューを行う能力が制限されていることを踏まえ、標準的リスク質問表やデューデリジェンス評価、現場レビューの代わりに、継続的監視によりTPRMプログラムの特定目標をいかに達成できるかの判断など、新常態への対処にTPRMプログラムを更新する方法を特定しています。組織はまた、データドリブンの積極的リスク監視（人工知能と機械学習を活用して）がサードパーティのレジリエンスに関する早期警告指標をいかに特定できるか、そして、将来の危機の影響緩和にいかに役立ちうるかを再考しています。最後に、組織はパンデミックとその他のテールリスクにおいて損害をより正確に見積もる方法を検討しています。

図9. TPRMのどこに資金を投資していますか



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

結論

KPMGの調査では、あらゆるセクターと地理的領域にわたる組織が、TPRMを戦略的優先事項にするべく適切に検討していることが確認されました。組織はTPRMに積極的アプローチを取り、テクノロジーの強化とイノベーションを通じて既存プロセスをいかに洗練させ拡大できるかを探究していることが分かりました。

とはいえ、調査ではまた、多くの組織にとってTPRMはまだ完成途上にあることがはっきりしました。また、グローバル事象と経済的不透明性に順応する際、組織はこれまでのサードパーティ評価情報と統制環境分析を、新たなリスクと課題を考慮するよう更新する必要があると気づく可能性もあります。もっとも急を要することとして、組織はサードパーティが重要な顧客／クライアントに対するサービスデリバリーで果たす役割を正確に理解し、それに応じて方針と統制を調整することで、重要な顧客／クライアントのサービス全体にわたり事業のレジリエンスを改善しなければなりません。

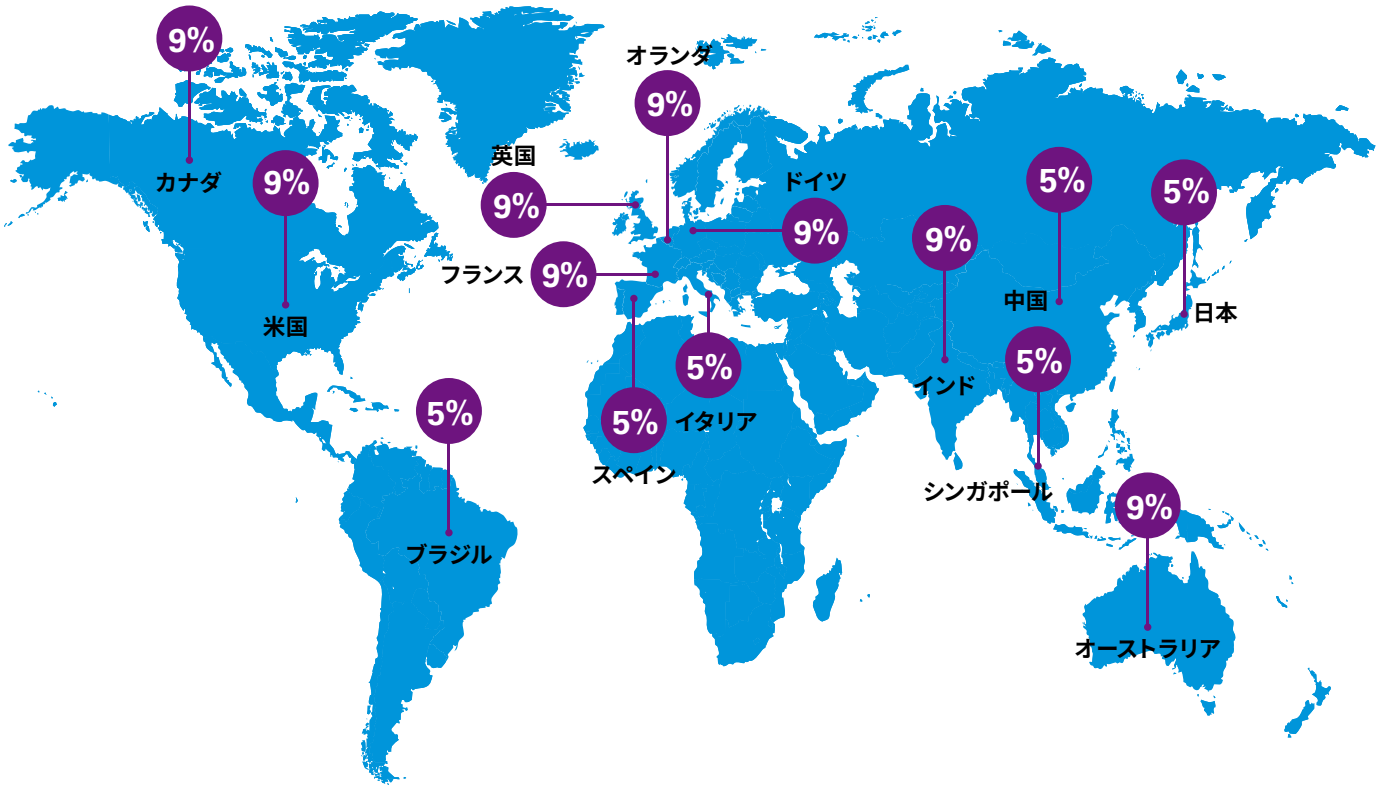
調査について

2020年の初め、KPMGは世界14ヵ国および法域と6つの業界において、大規模組織でTPRMを担当する1,100人の上級幹部を対象にオンライン調査を実施しました。調査の過程で私たちは、KPMGのメンバーファームおよびクライアント企業から10人のTPRM専門家を集め、徹底的な討論も行いました。

図10. 貴組織が属するセクターはどれですか

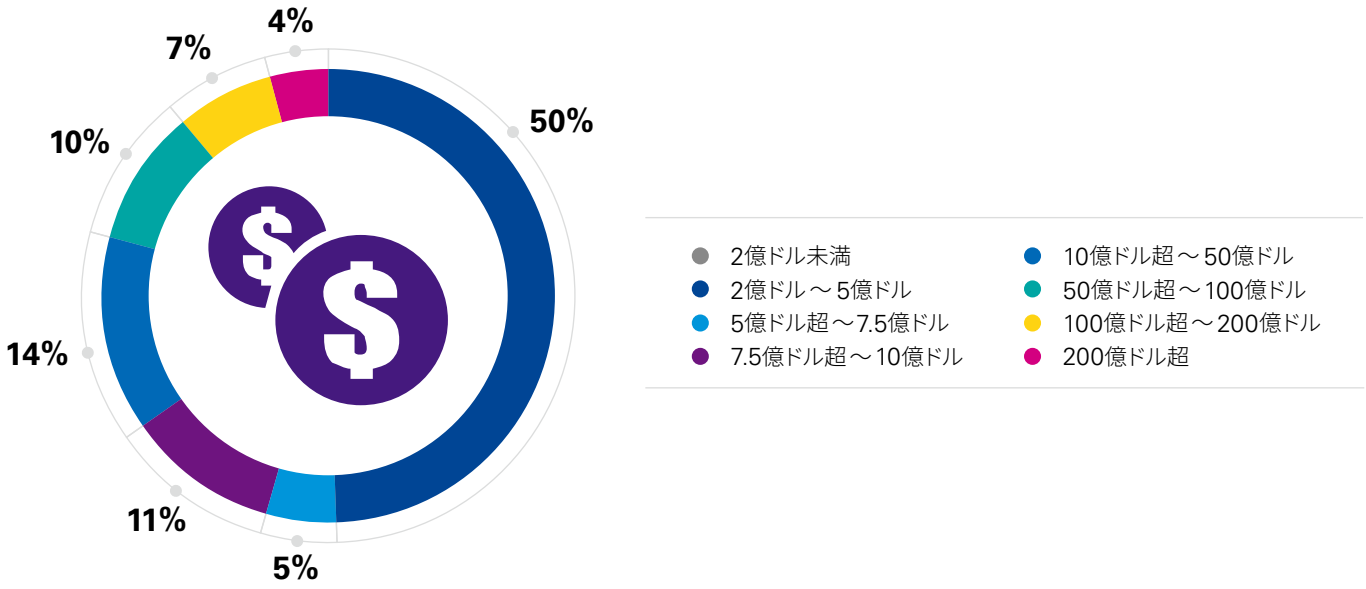
出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

図11. 貴社が主に事業活動を行っている国／法域はどこですか



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

図12. 貴組織のグローバルな年間総収益を米ドルでお答えください



出所：サードパーティリスク管理の展望2020、KPMGインターナショナル2020

Contacts

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: +6562132495
E: clem@kpmg.com.sg

山﨑 千春
あずさ監査法人
マネージング・ディレクター
E: chiharu.yamazaki@jp.kpmg.com

東海林 正賢
KPMGコンサルティング
フィンテック・イノベーション部 部長
パートナー
E: masayori.shoji@jp.kpmg.com

津田 圭司
KPMGコンサルティング
ディレクター
E: keiji.tsuda@jp.kpmg.com

大塚 卓美
あずさ監査法人
シニアマネジャー
E: takumi.otsuka@jp.kpmg.com

KPMGジャパン

home.kpmg/jp/regtech
regtech@jp.kpmg.com

KPMGコンサルティング株式会社

home.kpmg/jp/kc
kc@jp.kpmg.com

本冊子で紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはあずさ監査法人までお問い合わせください。

home.kpmg/jp/socialmedia

Designed by Evalueserve.

Publication name: Third Party Risk Management outlook 2020

Publication number: 137087-G

Publication date: July 2020