KPMG

サードパーティリスクマネジメントにおけるレジリエンスの実現

2026年
グローバルサードパーティリスクマネジメント（TPRM）サーベイ

kpmg.com

KPMGによる最新のグローバルサードパーティリスクマネジメント（以降、TPRM）サーベイの結果をご報告できることを、大変嬉しく思います。

組織が重要な業務を支えるために、ベンダー、サプライヤー、サービスプロバイダー、テクノロジーパートナーなどのサードパーティへの依存をますます高める中で、サードパーティリスクの管理は戦略的な最重要課題となっています。
急速なデジタルトランスフォーメーションの進展、グローバル・サプライチェーンの拡大、規制当局の要求水準の高まり、そしてサイバーセキュリティ脅威の増大により、TPRMを取り巻く環境は大きく変化しています。

近年、組織にはリスクを特定・評価するだけでなく、サードパーティのライフサイクル全体を通じて、新たに生じる課題を継続的にモニタリングし、対応していくことが求められています。しかしながら、多くのクライアントからは、実際には必ずしもそれが十分にできていないという声が聞かれます。その理由として、真に重大なリスクをもたらすサードパーティに注力すべきところ、リスクの低いサードパーティの評価にリソースが割かれてしまっているケースが多いことが挙げられます。

こうした背景を踏まえ、本サーベイではTPRMにおける最新の動向、実務、課題を探っています。調査結果からは、組織がどのようにTPRMフレームワークを高度化させ、新たなテクノロジーを導入し、外部プロバイダーを活用し、リスク管理機能を統合するとともに、規制上および業務上のプレッシャーに対応しているのかに関する示唆を得られます。また、レジリエンスの強化と価値創出を見据えたTPRMのための戦略的な提言も提示しています。

Alexander Geschonneck
Global Lead, Forensic

Roy Waligora
Global Lead, Third Party Risk Management

エグゼクティブサマリー

効果的かつ効率的なTPRMは、今日の複雑なビジネス環境においてますます重要である一方、その実現はより困難になっています。本グローバルTPRMサーベイは、従来の受動的なアプローチから脱却し、レジリエンスを備えた将来対応型のTPRMプログラムを構築するための青写真を示しています。本サーベイの結果を通じて、ガバナンスおよびプログラム統合、テクノロジーとデータの活用、ならびにサービスデリバリーにおける将来対応型のアプローチをご紹介します。

TPRMは、いま大きな転換点を迎えています。長年にわたり、経営層はサードパーティエコシステムの重要性が高まっていることを認識してきましたが、近年ではその「認識」と「行動」との間にあるギャップを、最新の機能によって埋める機会が生まれています。
業種や地域を横断して851名の企業内有識者から知見を集めたKPMGのグローバルTPRMサーベイでは、経営層はリスクの大きさを理解している一方で、実行面にはなお改善の余地があるということを示しています。実際、過去3年間だけでも、回答した組織の3分の1がサードパーティに起因して金銭的損失または評判の低下を被っており、28%がサプライチェーンの混乱を経験しています。こうしたことからも、先を見据えた能動的な対策がもたらす効果は非常に大きいといえます。
絶え間ない混乱が常態化する世界においては、チェックリストに依存する対応を超え、真に能動的なレジリエンスを構築することが今後の進むべき道です。
本調査データは、現在の取組みをさらに改善・高度化するための機会を示しています。以下は主な調査結果の一部です：

TPRMの主な推進ドライバーは規制遵守とサイバーリスク

規制遵守とサイバーリスクという、いずれも重要かつ差し迫った課題が関心の中心を占めており、TPRMプログラムには、目先の課題にとどまらず、次に到来するリスクを事前に見通し、顕在化する前に管理できる能力を強化する余地があることが示唆されています。

TRRMとERMの統合に向けた改善余地

TPRMプログラムのうち、全社的リスク管理（ERM）と「概ね統合」されている割合は53%にとどまり、「完全に統合」されている割合はわずか18%です。この結果は、全社横断的なリスクの可視化を実現するために、大きな改善の余地があることを示しています。

スケーラブルで戦略的なモデルへの移行の重要性

真にスケーラブルで戦略的なTPRMのオペレーティングモデルが新たな潮流として浮上しています。多くの組織では、高頻度かつ大量に発生する個別業務を外部委託しており、エンドツーエンドのマネージドサービスへと移行する道筋が見えつつあります。しかし、こうした体制をすでに導入している組織は、全体のわずか5%にとどまっています。

AIの活用による価値創出機会の拡大

組織の半数以上が人工知能（AI）の活用を検討しており、そのうち22%は「非常に効果的である」と評価しています。この結果から、テクノロジーへの投資をより具体的で実質的な価値へと結び付けていく余地が明確に示されています。

データ品質向上による信頼の向上機会

TPRMプログラムを支えるデータに対して高い信頼を寄せているリーダーはわずか15%にとどまっており、データ品質の向上は、TPRMの有効性を高めるための重要な機会であるといえます。

これらの調査結果は、TPRMプログラムの高度化に向けた取組みをより大胆に前進させることの価値を明確に示しています。レジリエンスは、一度達成して終わる目標ではなく、継続的に鍛え上げていく「筋肉」のようなものです。レジリエンスの実現には、統合されたシステム、スマートなテクノロジー、そしてビジネス横断的に共有されたオーナーシップを通じて、リスク管理を戦略・業務・企業文化の中核に織り込んでいくことが求められます。

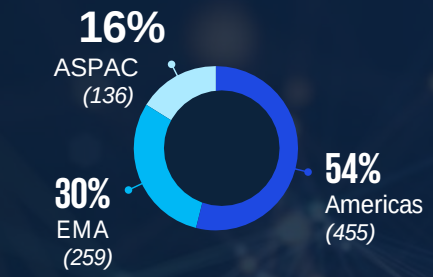
本レポートでは、数多くの情報の中から要点を整理し、サーベイから得られた知見を5つの主要テーマに集約するとともに、リスク、コンプライアンス、テクノロジーの各リーダーが将来対応型のTPRMプログラムを構築するために必要な実践的な指針を提供しています。

調査方法

KPMGは、アメリカ地域、欧州、アジア太平洋地域といった多様な地域、様々な企業規模、ヘルスケア、テクノロジー、金融サービス、製造、小売、エネルギーなどの業種を対象に、851名からウェブベースのアンケート調査を2025年に実施しました。回答者には、取締役、バイスプレジデント、部門責任者、Cレベルの経営幹部、TPRMに直接または間接的に関与するマネージャーが含まれています。本調査では、TPRMプログラムの成熟度、システム／ツールの利用状況、リスク評価、ライフサイクル管理、レジリエンス、データ品質、テクノロジーの導入状況などを対象にしました。また、売上規模、業種、機能別、規制レベル、地域別に結果を分析しています。

回答者概要

組織の所在地域



主要セクター

- 21% ヘルスケアおよびライフサイエンス（178）
- 19% テクノロジー、メディア、通信（164）
- 19% 金融サービス（165）
- 16% 産業用製造（139）
- 12% 消費財・小売（103）
- 11% エネルギー、天然資源、化学（96）

現在の役職

- 32% ディレクター/シニアディレクター (273)
- 26% バイスプレジデント/シニアバイスプレジデント (218)
- 22% 部門長 (187)
- 17% Cレベル (144)
- 3% マネージャー/シニアマネージャー (29)

サードパーティへの年間支出額

(81)	<US$0.1 億	10%
(122)	US$0.1–0.49 億	14%
(151)	US$0.5–0.99 億	18%
(255)	US$1–4.9 億	30%
(242)	>US$5 億	28%

回答企業の年間売上

(232)	<US$50 億	27%
(179)	US$51–100 億	21%
(194)	US$101–200 億	23%
(242)	>US$200 億	29%

担当領域

- 39% 全社的リスク管理（ERM）(331)
- 20% 情報セキュリティリスク(171)
- 20% コンプライアンス・リーガル(173)
- 14% オペレーション・ロジスティクス(55)
- 6% 財務・監査(121)

TPRMへの関与レベル

- 56% TPRMの管理または監督業務に直接関与（474）
- 44% 直接的な責任は持たないが、助言や支援を提供している(377)

調査結果に基づき抽出された主要テーマ

コンプライアンスとサイバーセキュリティ: TPRM戦略を支える二つの柱

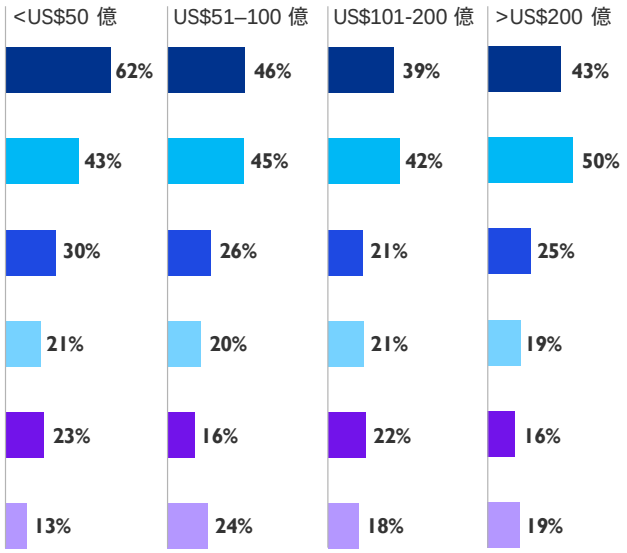
規制遵守およびサイバーリスクは、引き続きTPRM戦略の中核を占めています。調査回答者の48%がサイバーリスクを最大の推進要因として挙げ、45%が規制遵守としています。多くの組織において、TPRM戦略はいまだ「防御」を起点として策定されているのが実情です。これは、サードパーティにおける単一の脆弱性が、事業全体に瞬時に波及し、業務を停止に追い込む可能性があることを踏まえれば、合理的な対応といえます。こうした優先順位は、サードパーティの脆弱性が全社的な脅威へと急速に拡大し得るという認識が高まっていることを反映しています。また、企業に対してサードパーティとの関係性を厳格に精査することを求める世界各国の規制要件やフレームワーク主導の義務付けが、この切迫感を一層強めています。

支出の優先順位も、これらの懸念を色濃く反映しています。ただし、投資が必ずしも包括的なリスク管理の実現に結び付いていない点は課題として残ります。TPRMにおける支出項目としては、リスク評価およびデューデリジェンス（52%）が最も多く、次いでTPRM向けのテクノロジー／ツール（51%）が続いています。さらに、サイバーセキュリティ／データ保護（49%）、規制監査（45%）が僅差で続く結果となっています。

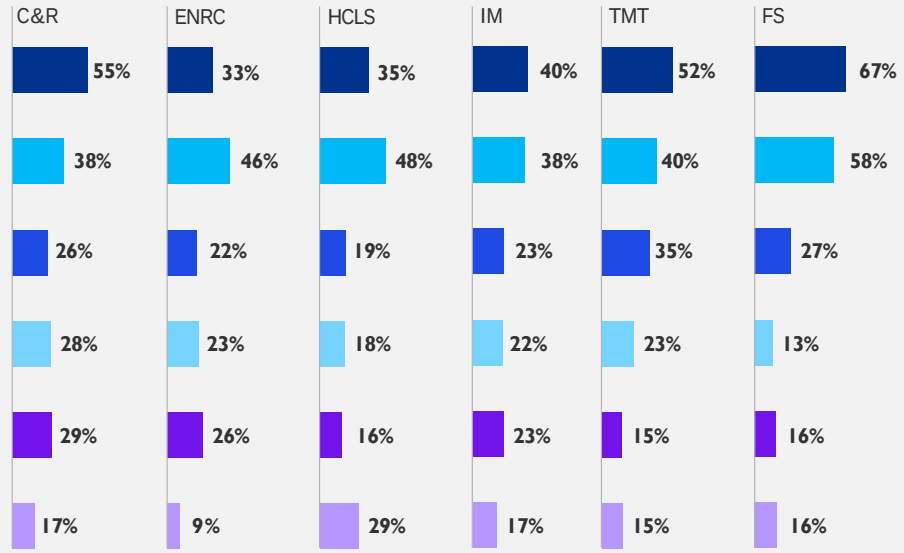
図表1：サイバーリスクおよび規制リスクがTPRM戦略の中核を占める

過去数年間で、TPRMにおいて重要性が高まったリスクは何ですか。

回答企業の売上規模別：



回答企業のセクター別：



- サイバーリスク／情報セキュリティリスク
- 規制およびコンプライアンスリスク
- レピュテーション（ブランド）リスク
- テクノロジー・イノベーションリスク
- 事業継続リスク
- リーガルリスク

C&R(消費財・小売)
ENCR (エネルギー、天然資源、化学)
HCLS (ヘルスケアおよびライフサイエンス)
TMT(テクノロジー、メディア、通信)
FS(金融サービス)

Source: Global TPRM Survey, 2025
Note:回答は複数選択のため、合計が100%にならない場合があります。

本調査によれば、サイバーリスクは特に中小規模の組織において重要性が高まっています。リソースが限られている中小企業では、サイバー対策がサイバー脅威に対する主要な防御手段となっている場合が多いと考えられます。一方で、十分な資金力を有する大規模組織では、全社横断的なリスク管理能力を拡充し、より包括的にリスクを管理することで、全体的なリスクエクスポージャーを低減することが可能です。

また、業種特有の要因も、TPRM戦略の推進ドライバーや支出の優先順位に影響を与えています。例えば、金融業界では厳格な規制要件が主な推進力となっている一方、ライフサイエンス分野では、多様なサードパーティとの関係性に起因する複雑なコンプライアンス対応が課題となっています。さらに製造業では、環境・社会・ガバナンス（ESG）要素、人権、サステナビリティといった複数の観点をTPRMフレームワークに組み込む動きが進んでいます。多くの業界において、部品や原材料の原産地を把握することは、関税や貿易コンプライアンスの対応に加え、調達基準の遵守を求める規制への対応においても極めて重要です。

企業が直面するサードパーティリスクの範囲の広さと、TPRMプログラムにおける多種多様な優先事項は、規模および複雑性の課題を浮き彫りにしています。業界を問わず、サードパーティエコシステムの相互接続性が高まるにつれて、サードパーティリスクは著しく増加しており、リスクレベルに応じた適切なアプローチの必要性は一層高まっています。現代の企業は、価値創出やイノベーション推進のためにサードパーティとのパートナーシップへの依存度が高まっていますが、その拡大スピードは、組織がリスクを十分に管理できる能力を上回っています。

本調査によると、経営幹部の83%が今後1～3年の間にパートナーネットワークを拡大する計画を立てている一方で、71%はパートナーとの間でゴールの合意形成を図ることに課題を感じていると認めています[1]。

KPMGがクライアント向けにTPRMプログラムの設計・運用を支援してきた豊富な経験に照らすと、数万社に及ぶベンダーを抱える企業が、すべてのサードパーティを同一レベルでスクリーニングしようとしているケースも少なくありません。しかし実際には、より深度のある調査を要する高リスクのサードパーティは、そのうちのごく一部（例えば10～20%程度）である場合が大半です。これは、最も重要な領域にリソースを再配分するための極めて大きな機会と言えます。

もう一つの重要な注力分野は、「Nthパーティ」に対する認識を高めること、すなわち、直接のサードパーティにとどまらず、そのサードパーティが依存している取引先まで視野を広げることです。Nthパーティの可視性は、特定の地域におけるサードパーティへの過度な依存リスクを把握・管理するために不可欠です。多くの企業はこうした可視性を十分に確保できていませんが、当該ベンダーとの取引を継続するのか、代替的な対応策や緊急の対応策を策定するのか、といったリスク許容度に関わる意思決定を行う上で、「Nthパーティ」に関する情報は不可欠です。

拡大するサードパーティリスクの領域をレジリエンスをもって管理するための戦略的提言：

リスクベースのデューデリジェンスを採用する：地理的要因のみに着目するのではなく、提供されるサービスの内容やサードパーティへの依存度に基づいてリスクを評価し、最もリスクの高い領域にリソースを集中させる。

ESGを統合する：進化する規制要件やステークホルダーの期待に対応するため、オンボーディングおよびモニタリングのプロセスに、ESGおよび人権の観点を組み込む。

AIおよび自動化を活用して人材の価値を高める：プロセスの効率化、重複作業の削減、評価の迅速化を通じて業務効率を向上させ、戦略的なリスク管理にリソースを集中させる。

データガバナンスを強化する：データ品質およびシステム統合を高度化し、信頼性の高いデータに基づく意思決定を可能にするリスク管理を実現する。

グローバル基準との整合を図る：過度に複雑で、効率性や有効性を損なうプロセスを回避しつつ、グローバルな規制要件および標準に適合させる。

[1] "Accelerate growth and innovation with the right partner ecosystem," KPMG 米国, 2025.

規制要件および監督・審査の強化が進んでいる

米国

- 通信（Telecom）：FCC（米連邦通信委員会）によるサプライチェーン・セキュリティ要件
- 大統領令：EO 14028「ソフトウェア・サプライチェーン・セキュリティの強化」
- 金融サービス：TPRMに関する監督当局合同ガイダンス
- ライフサイエンス：米国食品医薬品局（FDA）による規制・監督
- プライバシー：中央消費者保護庁（Central Consumer Protection Authority）による規制
- ヘルスケア：医療情報技術の経済性および臨床的有用性に関する法律（HITECH法）
- 全業種共通：米司法省（DOJ）による「企業コンプライアンス・プログラム」に関するガイダンス改訂

カナダ

- プライバシー：個人情報保護および電子文書法（PIPEDA）
- 金融サービス：OSFIガイドラインB-10（TPRMに関する指針）

欧州

- 通信：5Gセキュリティ・ツールボックス（Toolbox for 5G Security）
- 金融サービス：DORA（デジタル・オペレーショナル・レジリエンス法）、EBAアウトソーシング・ガイドライン
- 重要情報インフラ（CII）：NIS2指令
- ヘルスケア：TPRM（TPRM）に関する欧州医薬品庁（EMA）の要件
- プライバシー：一般データ保護規則（GDPR）

インド

- TPRMに関するインド準備銀行（RBI）のガイダンス

シンガポール

- 金融サービス：シンガポール金融管理局（MAS）によるアウトソーシング通知
- 重要情報インフラ（CII）：サイバーセキュリティ法

日本

- プライバシー：個人情報保護法

英国

- 通信：通信セキュリティ法（Telecommunication Security Act）
- 金融サービス：PRA、FCA、イングランド銀行（BoE） — オペレーショナル・レジリエンスに関する監督声明 SS1/21/SS2/21

オーストラリア

- 重要情報インフラ（CII）：重要インフラのセキュリティ
- 金融サービス：オーストラリア健全性規制庁（APRA） — CPS 230、CPS 231、CPS 234
- 通信：通信セクター・セキュリティ改革

統合の課題：TPRMとERMは未だ異なる「言語」で語られている

全社的リスク管理（ERM）は、主として経営戦略に影響を及ぼし得るハイレベルな脅威に焦点を当てる一方で、TPRMは日々のベンダー管理やサードパーティデータの取扱いといった、より実務的な領域を担うことが多く、この点が両者の乖離を生んでいます。包括的なリスク管理の必要性が広く認識されているにもかかわらず、TPRMとERMの統合は依然として断片的な状況にとどまっています。調査では、53%の組織が「概ね統合されている」と回答し、18%が「完全に統合されている」としていますが、戦略面とオペレーション面の双方で一貫性のある形でTPRMをリスク管理機能と整合させることは、依然として大きな課題となっています。

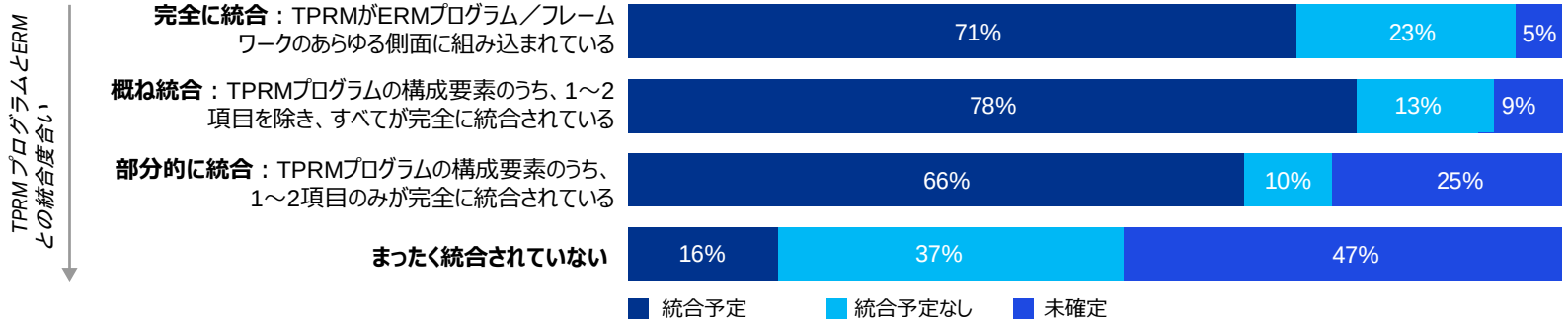
実務上、「概ね統合されている」とは、TPRMのデータがERMのダッシュボードや報告フレームワークに反映されているものの、システム、プロセス、意思決定において深いレベルでの連携が十分に確立されていない状態を指す場合が少なくありません。ERMは経営戦略の遂行を阻害しかねない「全社レベルのリスク」に注力する一方で、TPRMは多数のサードパーティを対象とした取引・業務レベルの対応に偏りがちです。さらに、TPRMの所管は組織内で分散しているケースが多く、委員会形式で運営されていたり、調達、サプライチェーン、サイバーセキュリティといった複数の所管部門がそれぞれ一部を担っていたりすることが一般的です。その結果、統一されたリスク管理の枠組みの下に集約されることなく、異なる言語、優先順位、視点が併存し、全社的に一貫したリスク認識の欠如につながっています。

「成熟した組織にとって、統合とは本質的に“集中”と“優先順位付け”に他なりません。適切なリソースを確保し、適切な人材を採用し、適切なテクノロジーを導入し、戦略を策定した上で、それを着実に実行していくことが重要です。」

-Srijit Menon
Partner, KPMG India
Global Lead, Third Party Security

図表2：TPRMとERMプログラムの統合には、なお改善の余地がある

TPRM／ERMプログラムの統合度合いおよび今後の統合計画



Notes: (a) TPRMプログラムとERMとの統合度合いの回答者の回答に応じて直近3年における統合計画の有無を確認しています。
(b) 四捨五入の関係により、合計が100%にならない場合があります。
Source: Global TPRM Survey, 2025

TPRMとERMの分断は、考え方の違いにも起因しています。TPRMはしばしば二つの視点から捉えられます。一つは、金融犯罪、サイバー脅威、贈収賄、コンプライアンス違反といった「被害リスク」に焦点を当てるコンプライアンスの視点です。もう一つは、取引をより迅速に、より高品質に、より低コストで実行することを重視する調達／サプライチェーン／財務の視点です。これらの領域間でリスクに対する共通理解が欠如している場合、統合は進みにくくなります。

このギャップを埋めるために、先進的な組織では、TPRMをソース・トゥ・ペイ（調達から支払まで）といった業務プロセスに組み込み、全社戦略やリスクプログラムの設計と整合させる取組みを進めています。この変革には、方針やポリシーの整合にとどまらず、テクノロジーの統合、共通のリスク分類（タクソノミー）、部門横断的なガバナンスが不可欠です。例えば、KPMGのTPRMフレームワークは、組織が現在の成熟度を評価し、最適な統合に向けた道筋を描くことを可能にするとともに、サイバーセキュリティ、コンプライアンス、財務、オペレーションといった関係者を結び付ける自動化およびデリバリーモデルによって、その実行を支援します。

また、テクノロジーは極めて重要な役割を果たします。今後3年間でさらなる統合を計画している組織は71%に上る一方で、TPRMデータを「完全に信頼できる」と評価している組織はわずか17%にとどまっています。このデータ品質のギャップは、報告の集約化や統合的なリスク評価の実施、さらには他部門の成果を活用する取組みを阻害する要因となっています。

TPRMとERMを統合するための戦略的提言

統合の目標を明確化する：ダッシュボードへの反映にとどまらず、共通の統制、統一されたリスク評価、共同での意思決定を含む「完全な統合」の姿を定義する。

サイロ化を解消する：TPRMを、ERM、コンプライアンス、サイバーセキュリティ、調達、サプライチェーン、オペレーション、ITと整合させる部門横断的なガバナンス体制を構築する。

データ品質への投資を強化する：信頼性の高いリスク報告および分析を支えるため、データの完全性と正確性を最優先事項とする。

テクノロジーを戦略的に活用する：自動化やAIを活用して業務を効率化しつつ、それらのツールを全社的なリスクフレームワークの中に適切に組み込む。

TPRMを業務プロセスと整合させる：調達や財務プロセスにTPRMを組み込み、受動的な対応にとどまらない、戦略的なリスク管理を実現する。

> 「サードパーティリスクに関して、企業は有効性、効率性、そして体験価値を同時に追求しています。単にコンプライアンスのチェック項目を満たすだけにとどまらず、自社とベンダーやパートナー双方にとって真の価値をもたらす、レジリエンスがありスケーラブルなプロセスを構築できるかが重要です。」

– Joey Gyengo
Principal, US Third Party Risk Management Lead, KPMG US

マネージドサービスおよびアウトソーシング：外部支援を活用したTPRMのスケール拡大

調査によると、80%を超える組織が、デューデリジェンスやオンボーディングから、モニタリング、是正対応に至るまで、TPRMの中核的な活動の遂行において、マネージドサービス、アウトソーシング、またはその両方を活用しています。こうした活用は、従来のプロフェッショナルサービスにとどまらず、リスク管理テクノロジーやインテリジェンスツールにも及んでいます。一方で、その導入は必ずしも包括的ではなく、エンドツーエンドのマネージドサービスを採用している組織は全体の約5%に過ぎません。多くの組織は、ライフサイクル全体を外部委託するのではなく、評価件数が多いフェーズに限定して外部支援を活用する部分的なモデルを選択しています。例えば、回答者の44%が継続的モニタリングにマネージドサービスを利用しており、27%がデューデリジェンスをアウトソーシングしています。これにより、多数のサードパーティをより効果的かつ効率的に管理し、リスク管理の実効性と効率性の向上を図っています。

統制を失うことへの懸念や、機密性の高い自社データを共有することへの不安は、アウトソーシング、コソーシング、マネージドサービスの活用をより広く進める上での大きな障壁となっています。中には、自社のサードパーティエコシステムを競争優位の源泉と捉え、その情報を外部と共有することに慎重な組織も少なくありません。

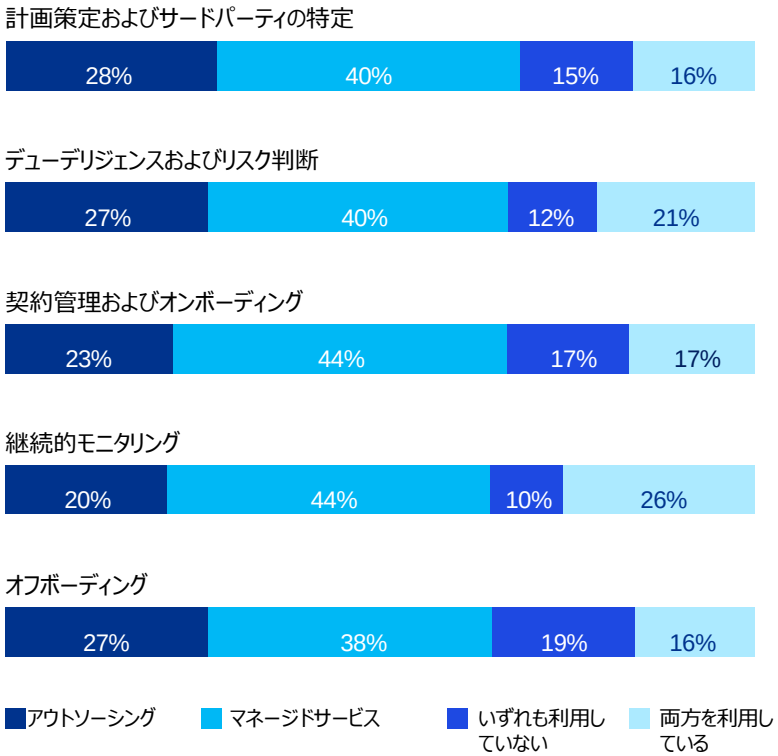
リスク管理をサービスとして活用するという考え方が浸透するにつれて、外部委託を受容する度合いは徐々に高まりつつありますが、それでもなお、企業は自社の中核的な業務と位置付ける機能については、引き続き慎重な姿勢を保っています。

エンドツーエンドのマネージドサービスは依然として限定的であるものの、プロセスの複雑性を管理し、アウトソーシングやコソーシングを通じてコスト削減を図ろうとする組織を中心に、関心が高まりつつあります。これは、TPRMそのものの複雑性や、組織が直面するリソースの制約を反映しているだけでなく、より広範な市場動向を示すシグナルでもあります。

その一つが、AIの成熟によって、TPRMにおいてパートナー主導のサービス提供モデルへと移行する企業が増えている点です。組織は、個々のTPRM業務を迅速化する目的でAIの組み込みを進めていますが、多くの場合、全体最適の視点を欠いたまま導入が進められており、その結果、エンドツーエンドの効率性を損なう断片的な「ツールの寄せ集め」となってしまっています。マネージドサービス・プロバイダーを活用することで、組織はこうした断片的なツール群を、TPRMライフサイクル全体に最適化された、単一の統合型プラットフォームへと置き換えることが可能です。

図表3：TPRMプログラムは、特に契約管理およびオンボーディングにおいて、マネージドサービスへの依存度が高い

TPRMプログラムのうち、どの業務においてアウトソーシングまたはマネージドサービスを活用していますか。



Notes: (a) 回答数が少ないため、「その他」カテゴリは図表には含めていません。
(b) 四捨五入の関係により、合計が100%にならない場合があります。
Source: Global TPRM Survey, 2025

AIの進展にも後押しされ、TPRMの提供モデルは、より成果志向になっています。マネージドサービス提供者はこの進化の最前線に立ち、テクノロジーを活用した拡張性のあるモデルを通じて、単なる工数削減にとどまらず、業務効率の向上やリスク低減といった測定可能な成果の実現を目指しています。

最終的には、TPRMにおけるフルスケールのマネージドサービス活用は現時点では主流ではないものの、TPRMプロセスの成熟が進み、拡張性がありコスト効率に優れ、かつ信頼できるパートナーを求める組織の増加に伴い、その活用は今後拡大していくと見込まれています。

組織がアウトソーシング、コソーシング、マネージドサービスを導入するにあたり、効果的な監督体制は不可欠です。成功のためには、プロバイダーとの関係を管理できる十分なスキルを持つ人材を配置し、自社のニーズに合致したプログラムを設計するとともに、成果を継続的にレビューし、適切に検証・改善していく必要があります。強固なプロジェクト管理およびガバナンスは、コントロールを維持し、マネージドサービスがその価値を確実に発揮するために重要です。

もちろん、新たなサービス提供モデルへ移行するための準備状況は、業種によって異なるのが一般的です。例えば、金融業界では、大規模な顧客確認プログラム（KYC)や成熟したリスク管理機能を有していることから、サードパーティプロバイダーによる補完を目的として、主要プロセスの一部をアウトソーシングすることに比較的慣れています。一方、他業種の企業では、マネージドサービスを十分に活用するための内部成熟度やリソースが不足している場合もあります。

多くの組織は、マネージドサービスを活用する前提として、TPRMプロセスの定義や標準化に引き続き取り組んでいます。

組織は、外部プロバイダーが自社のリスクアペタイトやレジリエンス目標と整合していることを確保する必要があります。先進的な取組みとしては、サービスレベル合意（SLA）や主要業績評価指標（KPI）を含む明確な契約フレームワークを構築するとともに、技術的な専門性と高い顧客志向を兼ね備えたプロバイダーを選定することが挙げられます。効果的なプロバイダーは、組織のリスクプロファイルに即した対応を行い、高リスク領域に重点を置きつつ、組織に過度な負担をかけることなく、評価プロセスの効率化を支援します。

先進的なマネージドサービスの提供モデルは、テクノロジー活用が一層進んでおり、AIを用いた大量スクリーニングや、チャットボットによる低リスクの問い合わせ対応の迅速化を実現しています。これらのツールは、一貫性と効率性の高いサービス提供を支えるとともに、顧客体験の向上にも寄与しています。このような提供モデルは、成熟度が許す範囲において、オンショアおよびオフショアの高度な専門知識を有する人材チームによってさらに強化されており、これらのチームはエンドツーエンドの支援提供において重要な役割を果たしています。

マネージドサービスおよびアウトソーシングを活用した、TPRMの運用規模拡大に向けた戦略的提言

アウトソーシング前に内部プロセスを定義・成熟させる：マネージドサービス導入に備え、TPRMの業務フローを標準化し、文書化することで、円滑な移行と運用を可能にします。

強固なガバナンス体制を確立する：サービスレベル合意（SLA）および主要業績評価指標（KPI）を活用し、適切な監督を維持するとともに、社内のリスクアペタイトおよびレジリエンス目標との整合性を確保します。ガバナンスを契約に組み込み、定期的に見直すことが重要です。

専門性と顧客志向を兼ね備えたプロバイダーを選定する：規制当局の期待を理解し、自社のリスクプロファイルに即応でき、高リスク領域に重点を置いたサービス提供が可能なパートナーを選定することが望まれます。

文化的受容性および変革管理に留意する：外部プロバイダーやアウトソーシングモデルに対する信頼を醸成するため、変革管理への継続的な投資が求められます。

スケーラビリティを見据えた設計を行う： TPRMのニーズが進化する中で、統制や品質を損なうことなく、より広範または複雑なリスク領域にも対応できるよう、マネージドサービスモデルの拡張性を確保する。

「TPRMにおいてマネージドサービスを活用していると回答する組織は数多く見られますが、その多くはエンドツーエンドでの活用には至っておらず、部分的なアウトソーシングにとどまっています。
真の機会は、このギャップを埋めることにあります。すなわち、スケールを図る前にプロセスを定義・簡素化し、基礎を確実に整えることで、より迅速かつ効率的なTPRMの実現が可能となります。」

– Roy Waligora
Partner and Global Lead, TPRM
KPMG UK

テクノロジーとAI: TPRMの成熟度を高め、価値を創造する

テクノロジーは、TPRMを再構築しつつあり、AIや自動化は、特にリスク評価、デューデリジェンス、リスク格付けの効率化において大きな可能性をもたらしています。しかしながら、現場の実態は必ずしも整理されているとはいえません。AIの導入状況にはばらつきがあり、多くの場合、分断された形で進められています。多くの組織では、TPRMを支援するために1～5種類のシステムを使用しており、他のプラットフォームとの統合が最大の課題となっています。自動化は、デューデリジェンスやリスク評価といった限定的な業務に適用されることが一般的であり、ライフサイクル全体には及んでいません。その結果、複雑性を低減するどころか、相互に連携しないシステムの寄せ集めとなり、かえって複雑になっています。

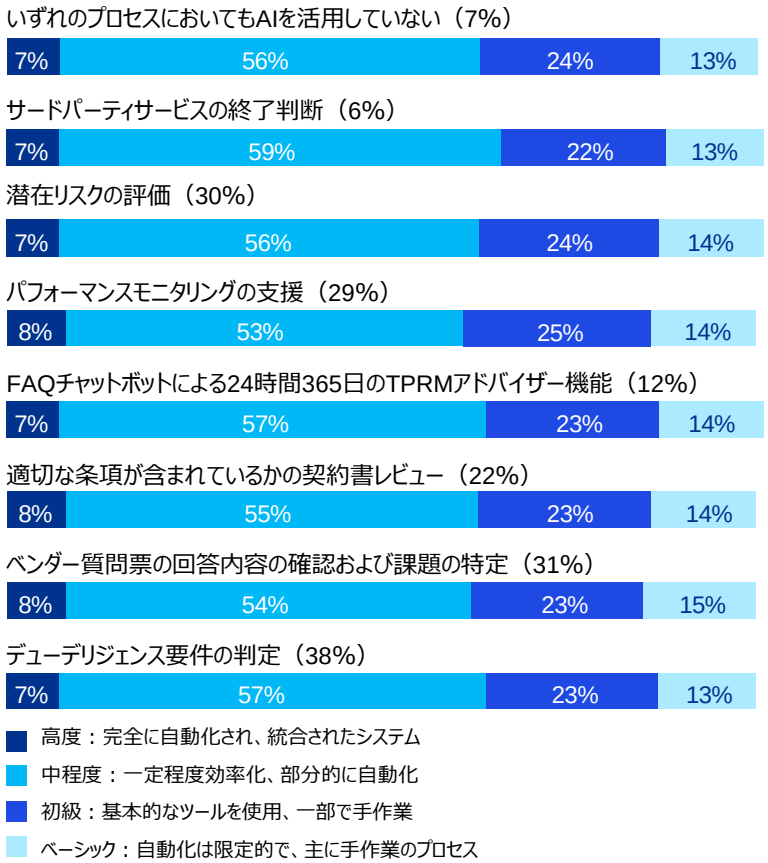
AIの導入は、特にレポーティングやデータの可視化の領域で進展していますが、その有効性については評価が分かれています。回答者の約5割がAIを利用していると回答している一方で、「非常に効果的である」と評価しているのは22%にとどまり、40%は「ある程度効果的である」と回答しています。この有効性のギャップは、多くの場合、信頼性の確保やオーケストレーションに起因しています。AIの高い効果を実現している組織は、分断されたプロセスを連携させ、エンドツーエンドのワークフロー全体に対する明確なオーナーシップを有しています。個別に動作する単機能のエージェントは、統合されオーケストレーションされたプロセスと比較すると、効果が限定的です。

最も強力なAIの活用事例では、ディープリサーチやデータベースから取得した知見にサードパーティから直接収集したデータを組み合わせることで、リスクをより包括的に把握しています。これにより、組織は現時点の事象を評価するだけでなく、シナリオ分析を行い、「現在」と「次に起こり得る事態」の双方に備えることが可能となります。TPRMの将来は、エンドツーエンドのオーケストレーションにあります。これにより、より高度なベンダー評価が可能となり、企業は現在の事象に対応するだけでなく、将来の変化を先取りする力を得ることができます。

今後を見据えると、今後3年間で約4～5割の組織が、TPRMの中核業務においてAIを中程度に活用すると見込んでいます。この分野には大きな機会が存在しています。AIは、エンドツーエンドの業務を加速し、リスク検知能力を高め、より高度でリアルタイムな意思決定を可能にします。こうした可能性を実現するためには、計画的な投資、部門横断での連携、そしてパイロット段階から全社展開へとスケールさせるための明確なロードマップが不可欠です。

図表4：多くのTPRMプログラムでは、自動化は中程度の水準にとどまっており、高度な自動化の恩恵を受けているケースは限られている

自動化が活用されているTPRMプログラムの領域および各TPRMプログラムにおける自動化度合

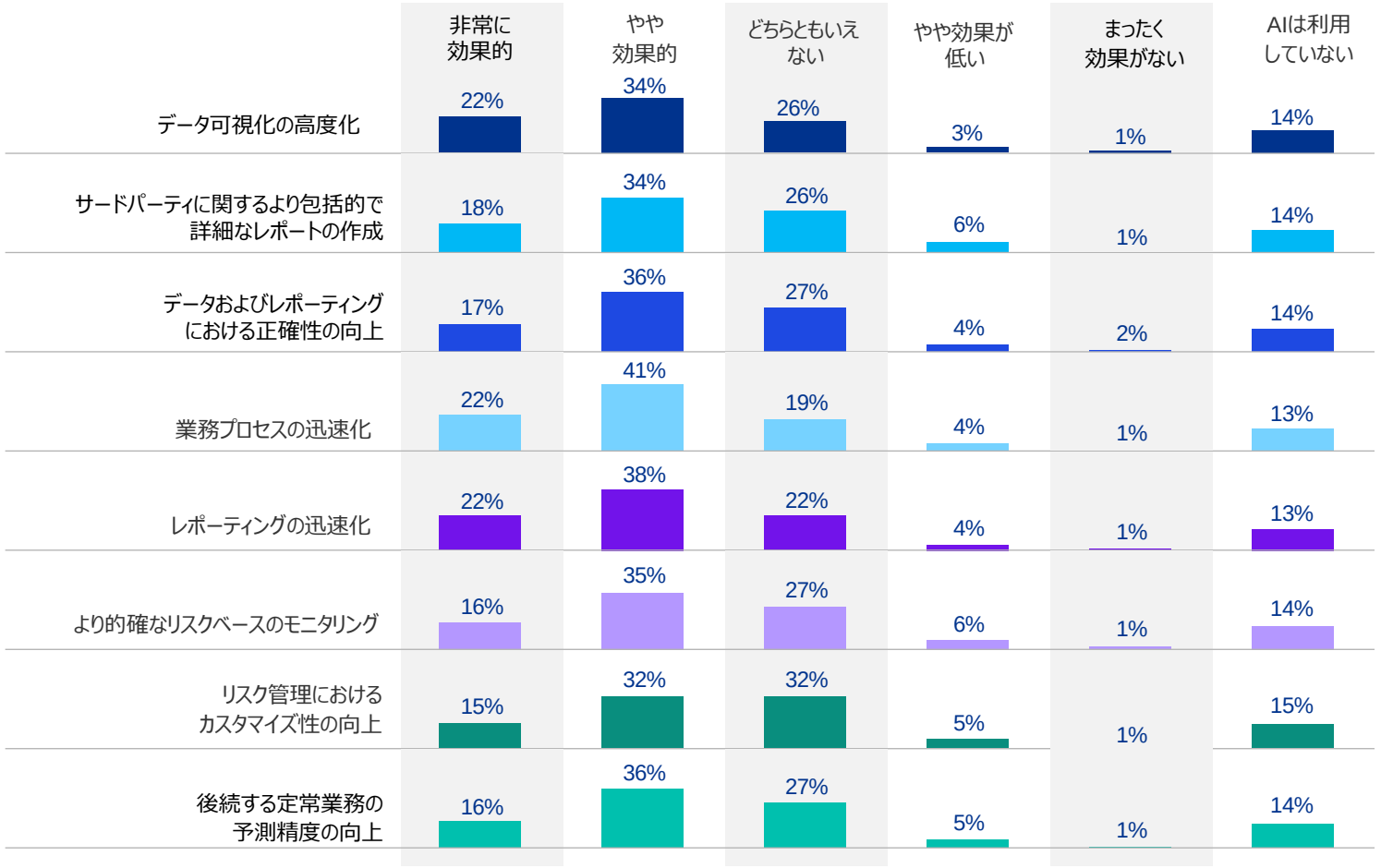


Notes: (a) ()内は当該TPRMプログラムにおいて自動化が活用されいていると回答（複数回答）した割合を示します。表現上の都合により、上位8項目が掲載されています。 (b) 四捨五入の関係により、合計が100%にならない場合があります。

Source: Global TPRM Survey, 2025

図表5：TPRMプロセスの改善におけるAIの有効性にはばらつきがある

AIは、TPRMプロセスの改善においてどの程度効果的ですか。



Notes: (a)「その他」カテゴリーは、図表には含まれていません。 (b) 四捨五入の関係により、合計が100%にならない場合があります。

Source: Global TPRM Survey, 2025

TPRMにおけるAI・自動化を高度化するための戦略的提言：

エンドツーエンドのワークフローにAIを組み込む:個別のユースケースにとどまらず、オンボーディングからオフボーディングに至るTPRMライフサイクル全体にわたってAIを統合することが求められます。

自動化と人の専門性を組み合わせる: AIツールとマネージドサービスチームを組み合わせることで、リスク判断が十分な情報に基づき、状況に即した形で行われ、かつ事業目標と整合するようにします。

システム統合を優先的に進める:プラットフォームの分断を解消し、シームレスなデータ連携を実現することで、AIおよび自動化の価値を最大化します。

効果の高いユースケースに注力する:大量スクリーニング、リスクスコアリング、チャットボットによる問い合わせ対応などの領域から着手し、短期間で成果を示すことが有効です。

AI導入に向けた準備への投資が不可欠:データ品質、ガバナンス、プロセスの成熟度を確保し、AIを効果的に展開できる基盤を整える必要があります。

データ品質と信頼:
信頼できるTPRMの基盤

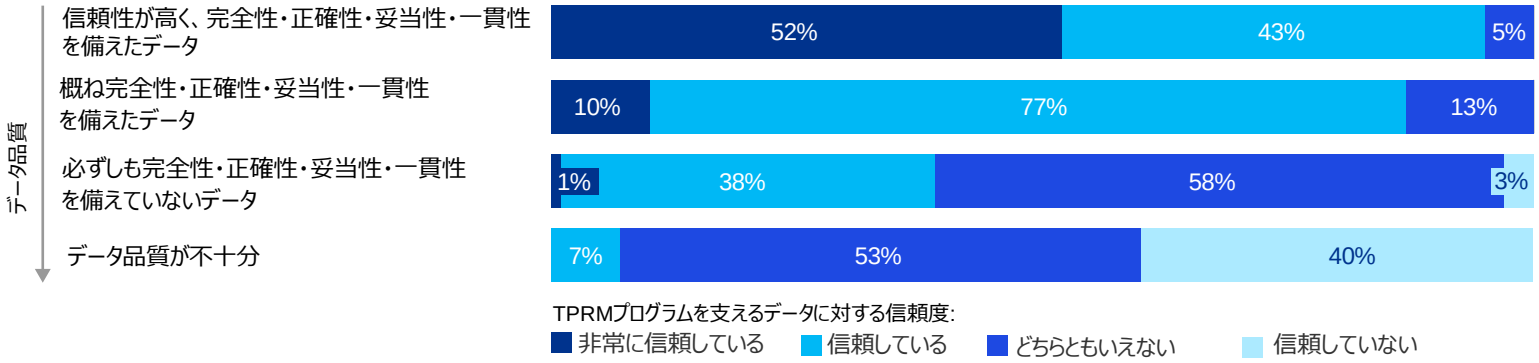
TPRMの有効性に対する信頼は、信頼性の高いデータに依存しています。本調査では、その点が明確に示されています。高品質なデータを有する責任者は、自社のリスク管理に対して高い信頼を寄せている一方で、データ品質が低い責任者は十分な信頼を置いていません。極めて明快な結果です。具体的には、高品質なデータを有していると回答した回答者のうち、52%がTPRMに関する意思決定について「非常に信頼している」と回答しているのに対し、データ品質が不十分であると回答した回答者のうち、40%が「信頼していない」と回答しています。

データ品質の向上は、TPRMプログラムにとって極めて重要な改善機会として位置付けられます。回答者の59%が、自社のデータは概ね完全性・正確性・一貫性を備えていると回答している一方で、最高水準のデータ品質を有していると回答したのは17%にとどまっています。データ品質は企業規模が大きくなるにつれて向上する傾向が見られますが、それでもなお、大企業であっても分断されたシステムの統合やデータの完全性確保に課題を抱えています。

こうした分断は、多くの場合、システムの断片化や一貫性のないデータ運用に起因しています。例えば、国ごとに異なる調達システムが導入されている場合、グローバルで統合された可視化が実現できず、地域を横断したサードパーティリスクの評価が困難になります。統合が不十分であることは、サプライチェーンにおける高リスク領域の可視性を制約します。サードパーティを統合的に把握できなければ、リスクを統合的に把握することはできません。

図表6：TPRMプロセスにおける信頼度はデータ品質に支えられています

TPRMレポーティングで使用されるデータの品質と、TPRMプログラム全体を支えるデータに対する信頼度



Note: 四捨五入の関係により、合計が100%にならない場合があります。
Source: Global TPRM Survey, 2025

データ品質が低いことは、不確実性を生むだけでなく、戦略的な投資を損なう要因ともなります。データ品質は、AIやマネージドサービスを効果的に導入・活用する上での大きな障壁です。実際、本調査におけるデータ品質に関する結果は、AIやマネージドサービスを活用しているとする回答者の広範な認識とは乖離しており、多くの組織が、これらのツールをTPRMライフサイクル全体ではなく、限定的なプロセスにのみ適用している可能性を示唆しています。信頼できるデータがなければ、いかに高度なツールであっても、有意義なインサイトの提供や自動化を実現することはできません。

組織は、データガバナンスの強化、標準化されたレポーティング、継続的な検証への投資を行う必要があります。しかし、関与するシステムや機能部門が多岐にわたることから、この課題は非常に困難に感じられる場合も少なくありません。どこから着手すべきか判断できずにいる組織も多く見受けられます。実務的なアプローチとしては、まず対象を絞り、特に重要性の高い一部のベンダー（例えば、重要なサードパーティや特定の地域）に焦点を当てて、データのクレンジングおよび検証から着手することが有効です。このように構造化された段階的な改善は、費用対効果を定量的に示す成果を生み出し、より広範なデータガバナンス施策を推進するためのモメンタムを生み出すことにつながります。

TPRMにおけるデータ品質及び信頼を向上させるための戦略的提言:

重要なサードパーティから着手する：初期段階のデータクレンジングは、最も重要なサードパーティに重点的に取り組むことで、早期に成果を創出し、その価値を示すことができます。

データの是正に段階的なアプローチを採用する：データ品質向上の取組みを一度に全面的に実施しようとするのではなく、各段階で費用対効果を確認できるよう、管理可能なステップに分解して進めることが求められます。

データガバナンスおよび標準化への投資が不可欠：事業部門や地域を横断して、明確なオーナーシップ、一貫した定義、標準化されたレポーティングを確立する必要があります。

調達システムとリスク管理システムの統合を進める：グローバルな業務全体を通じてサードパーティデータを統合的に把握できるようにすることで、可視性を高め、リスク評価の高度化につなげます。

データ品質向上の取組みをAIおよびマネージドサービスの目標と整合させる：基盤となるデータの改善が、より広範な自動化やアウトソーシング戦略を確実に支えるようにする必要があります。

「信頼できるデータの基盤を構築することは、TPRMに対する信頼を高め、その潜在能力を最大限に引き出すための最も効果的な方法です。高品質なデータを有していると回答したリーダーが17%にとどまっているという事実は、今後取り組むべき明確な方向性を示しています。データの完全性に注力することで、組織はAIをはじめとするテクノロジー投資からより大きな価値を引き出し、より迅速で的確な意思決定を可能にする、真にレジリエントなTPRMプログラムを構築することができます。」

– Gavin Rosettenstein
Partner, KPMG Australia

提言の総括: レジリエントかつ将来に対応したTPRMプログラムの構築

将来に対応できるTPRMプログラムへの道筋は、段階的な小規模改善にとどまるものではなく、より大胆で戦略的な取組みを必要とします。受動的でコンプライアンス起因の機能から、価値を創出する能動的なレジリエンスの中核へと進化するためには、新たな発想への転換が不可欠です。以下のアクションは、本調査から得られた主要な示唆を整理したものであり、組織を守るだけでなく、競争優位性を高めるための明確なロードマップを示しています。

重点領域への絞り込み

広範で非効率なスクリーニングから脱却し、リスクベースで的を絞ったアプローチへ移行する必要があります。真に脅威となる少数のベンダーにリソースを集中させることで、重要な領域における洞察を深め、低リスクのベンダーに過度な労力を費やすことを防ぐことができます。

サイロ化の解消

リスク管理が分断された状態では、真のレジリエンスを実現することはできません。TPRMとERMの機能を統合し、全社横断で統一されたリスクの全体像を構築することで、単なるコンプライアンス対応にとどまらない、戦略的な意思決定を支える基盤を整えることが重要です。

戦略的資産としてのデータの活用

TPRMプログラムの有効性は、それを支えるデータの質に大きく依存します。単一の信頼できる情報源を確立するため、データガバナンスへの投資が不可欠です。正確で信頼性の高いデータは、効果的なAI活用、信頼性の高いレポーティング、そして自信を持った意思決定のための重要な基盤となります。

AIの実行的活用への移行

単にAIを活用するということでなく、明確な目的を持って展開する必要があります。TPRMライフサイクル全体にわたって自動化と高度なワークフローを組み込み、プロセスの迅速化、潜在的なリスクの発見、そしてより戦略的な業務に人材を振り向けられる環境を整えることが求められます。

N^{th}パーティを含めた広範囲のリスク検討

リスクエクスポージャーは、一次取引先だけで完結するものではありません。サプライチェーンのより深層に潜むリスクを把握するためには「N^{th}パーティ」まで可視性を確保し、集中リスクの管理や予期せぬ混乱の未然防止につなげることが重要です。

オーナーシップではなく成果のアウトソース

マネージドサービスを活用することで、ボリュームの大きい業務における効率性と対応力を拡大することが可能です。一方で、ガバナンスおよび戦略に対する統制は自社で堅持し、外部パートナーが自社のリスクアペタイトを補完する存在として機能するよう管理する必要があります。外部委託は、リスク管理の代替ではなく、その延長線上にあるべきものです。

KPMGによる支援

本サーベイ結果は、TPRMを単なる防御的対応から脱却させ、戦略的な価値創出へと進化させるためのプレイブックを示しています。KPMGは、プレイブックを確実に実行し成果に繋げるために必要な経験、テクノロジー、グローバルな体制を提供しています。私たちは、お客様とともにレジリエンスを強化し、業務効率を高め、サードパーティとの関係から戦略的な価値を引き出すことを支援します。KPMGのグローバルTPRMチームは、深い専門知識、先進的なテクノロジー、そして堅牢なマネージドサービスモデルを組み合わせた幅広い支援を提供できる体制を整えており、市場において明確な差別化を実現しています。

グローバル体制

KPMGのTPRMプロフェッショナルは、グローバルに展開するデリバリーセンターのネットワークを通じて業務を行っており、主要なグローバル拠点において24時間365日対応可能な高度な専門人材を擁しています。この体制により、お客様のニーズに応じてチームを柔軟に編成・拡張することが可能であり、複数のタイムゾーンおよび言語への対応を実現するとともに、国・地域をまたいだ一貫性のある高品質なサービス提供を可能にしています。

分野横断型アプローチ

KPMGは、分野横断型アプローチを採用し、リスク管理、調達、コンプライアンス、テクノロジー、サイバーセキュリティ、ESGといった各分野の専門家を結集することで、TPRMプログラムの設計、導入、継続的な高度化を支援しています。このような分野横断的な体制により、TPRMプログラムのあらゆる要素が網羅され、明確なオーナーシップと説明責任のもとで、効果的な運用が確保されます。

次世代型のマネージドサービス

KPMGのTPRM向けマネージドサービスは、自動化、AI、専門知識を必要に応じて組み合わせることで、継続的な変革を推進するエンジンとして機能します。モジュール型かつサブスクリプションベースで提供されるマネージドサービスは、最先端のテクノロジー、自動化、オフショアのケイパビリティを活用することにより、業務効率の向上を実現するよう設計されています。従来型のアウトソーシングとは異なり、KPMGの包括的なマネージドサービスは、オンボーディングおよびデューデリジェンスから、継続的モニタリング、課題管理、オフボーディングに至るまで、TPRMライフサイクル全体を網羅しています。

私たちのTPRMソリューションは測定可能な価値を提供します

業務効率の向上：自動化およびプロセスの標準化・高度化により、サードパーティ管理に伴う事務負荷を大幅に削減し、オンボーディングの迅速化を実現します。

リスク低減: KPMGのマネージドサービスを通じて、ベンダー／サードパーティのライフサイクル全体にわたり、リスクをプロアクティブに特定し、評価し、低減します。また、セキュリティ態勢およびコンプライアンス水準の向上にも寄与します。

戦略的インサイトの提供：高度なアナリティクスおよびレポーティングにより、意思決定に直結する示唆を提供し、TPRMの継続的な高度化・改善を支援します。

レジリエンス強化:TPRMをERMと統合し、KPMGのグローバルリソースを活用することで、事業中断リスクや規制環境の変化に強い組織基盤の構築を支援します。

執筆者：

For more information, contact us:

Alexander Geschonneck

Partner, Global Forensic Leader
KPMG Germany
ageschonneck@kpmg.com

Alexander is the Global Lead for KPMG Forensic. Alexander advises companies, banks, and public organizations on investigations, anti-money laundering, and anti-fraud and anti-corruption measures. In addition, he coordinates KPMG's global Forensic practices to support clients in responding to the threat of financial crime.

Joey Gyengo

Principal, US Third Party Risk Management Lead,
KPMG US
jgyengo@kpmg.com

Joey is an Atlanta-based principal in KPMG's Consulting practice and the US Enterprise Risk Management (ERM) and Third Party Risk Management (TPRM) leader. His 20-plus years of experience include a deep background in enterprise risk and resilience; governance, risk, and compliance (GRC); internal audit; and internal controls. Joey advises boards and senior leadership on risk strategy, risk governance, and risk management.

Roy Waligora

Partner and Global Lead, TPRM
KPMG UK
roy.waligora@kpmg.co.uk

Roy is a Forensic partner based in London. He leads on Global Third Party Risk Management, supporting our global teams and clients to respond to the challenge of managing third parties effectively enabled by technology. Roy also has over 25 years of cross-border due diligence and investigations experience.

執筆協力者:

Laura Bubeck, Jilane Khakkhar, Lauren J. Polana, Matthew P. Miller, Rohit Nag, Tara Nelson, Kathleen Nichols, Rama Ramaswami, Rishab Sengupta, Chandra Shekhar, Constance Thaete, and Anshita Tripathi.

グローバルのワーキンググループの連絡先：

UK and Global

Roy Waligora
Partner and Global Lead, TPRM
KPMG UK
roy.waligora@kpmg.co.uk

Helena Bartles
Director, Forensic
helena.bartles@kpmg.co.uk

US

Joey Gyengo
Principal, US Third Party Risk Management Lead
jgyengo@kpmg.com

Daniel W. Click
Partner, Advisory
dclick@kpmg.com

Diana Keele
Managing Director,
Risk Services
dkeele@kpmg.com

Canada

Sonu Sikand
Partner, Info Tech Risk Services
sonusikand@kpmg.ca

Peter W. Armstrong
Partner, Forensic
pearmstrong@kpmg.ca

India

Vipul Jain
Partner, India Lead, Non-Cyber Third-Party Risk Management
vipuljain@kpmg.com

Srijit Menon
Partner, KPMG India Global Lead, Third Party Security
srijitmenon@kpmg.com

Maneesha Garg
Partner and Head,
Managed Services
maneesha@kpmg.com

Netherlands

Hokkie Blogg
Partner, Cyber Strategy & Risk
blogg.hokkie@kpmg.nl

Belgium

Jens Moerman
Director, Forensic
jensmoerman@kpmg.com

Germany

Verena Hinze
Audit – Regulatory Advisory
vhinze@kpmg.com

France

Caroline Albarel
Partner, Advisory
calbarel@kpmg.fr

Italy

Valerio Falcicchio
Partner, Advisory
valeriofalcicchio@kpmg.it

Daniele Ianniello
Partner, Advisory
dianniello@kpmg.it

Japan and ASPAC

Mariko Yamada
Director, Forensic
mariko.yamada@jp.kpmg.com

Australia and South ASPAC

Gavin Rosettenstein
Partner, KPMG Australia
gavin1@kpmg.com.au

Middle East

Nicholas Cameron
Partner, KPMG United Arab Emirates
nicholascameron@kpmg.com

Related insights

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: | kpmg.com | Subscribe

お問合せ先：

西嶌 宏之
代表取締役パートナー
KPMGジャパンおよびASPAC
フォレンジックサービス統括
KPMG Forensic & Risk Advisory
E: Hiroyuki.nishjima@jp.kpmg.com

萩原 卓見
執行役員パートナー
金融セクター
KPMG Forensic & Risk Advisory
E: Takumi.Hagiwara@jp.kpmg.com

山田 茉莉子
ディレクター
グローバルネットワークASPAC・日本TPRM担当
KPMG Forensic & Risk Advisory
E: Mariko.Yamada@jp.kpmg.com

塩野 祐輝
シニアマネージャー
KPMG Forensic & Risk Advisory
E: Yuki.Shiono@jp.kpmg.com

KPMG Forensic & Risk Advisory
T: 03-3548-5773
E: FRA-Contact@jp.kpmg.com
kpmg.com/jp/fra

本リーフレット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。
詳しくは株式会社 KPMG Forensic & Risk Advisoryまでお問い合わせください。

本冊子は、KPMGインターナショナルが2026年2月に発行した「The 2026 KPMG Global Third-Party Risk Management Survey」を、KPMGインターナショナルの許可を得て翻訳したものです。翻訳と英語原文間に齟語がある場合は、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。