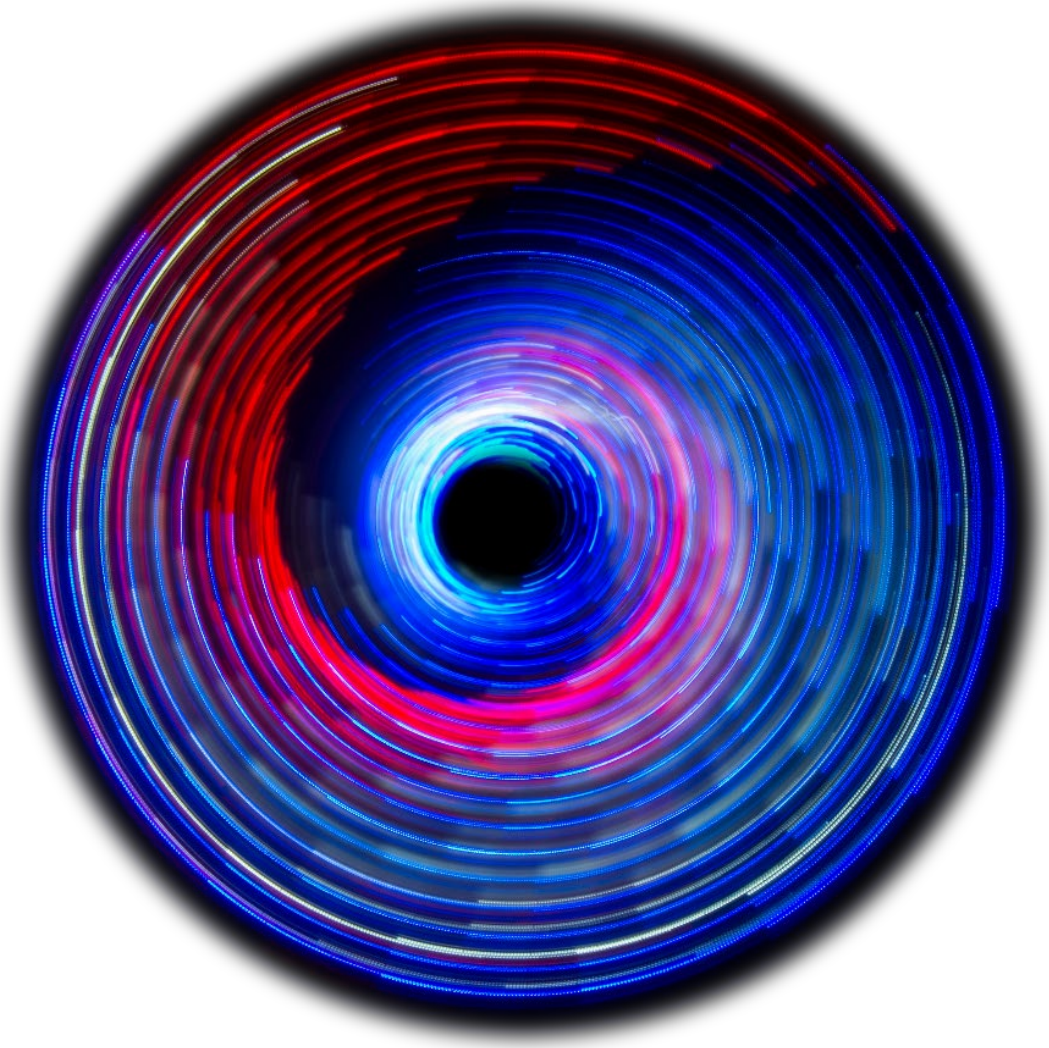
Deloitte.
デロイト トーマツ

トーマツ



金融機関におけるサードパーティリスク管理態勢の高度化支援サービス

有限責任監査法人トーマツ

金融機関のサードパーティリスク管理を
リスクベースで全社的に連携した実効性の
高いプロセスとガバナンス体制へと進化させ、
ビジネスの競争力強化に貢献します。

金融機関を取り巻く サードパーティリスクの変化

金融機関にとって、外部委託先を含むサードパーティとの取引は業務効率化や競争力強化の観点で不可欠です。近年では、クラウドサービスの活用やAPI連携を通じたフィンテック企業等、異業種との協業も進み、顧客への新たな商品・サービス提供や迅速化等を目的に、サードパーティの関与は年々拡大しています。
一方で、サードパーティに起因する情報漏洩、業務停止、コンプライアンス違反等のリスクは、社会的信用の失墜や法令違反につながる可能性があり、これらのリスクを可視化し、適切に管理していくことは重要な経営課題となっています。

サードパーティリスク管理の典型的な課題

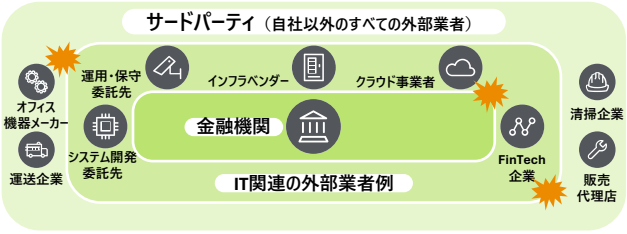
サプライチェーンの多様化やサイバー脅威の高まりを背景に、従来の一律的な外部委託先管理では実効性が担保できず、リスクの多様化・変化に十分対応できない状況です。
サードパーティとの取引や業務が拡大するにつれ、リスク評価やモニタリングの負荷も高まり、金融機関において管理上の課題も顕在化しています。

銀行の事例

委託先が**パブリッククラウド上に構築した開発サーバー**が不正アクセスされ**ランサムウェアに感染**
リモートアクセスするための認証方法が脆弱（ID・パスワードのみ）であり、総当たりの解析で特定されたことが原因

保険会社の事例

委託先が利用するサーバに対して不正アクセスされ提供していた**個人情報の一部情報漏洩サイトに掲載**
委託元が求める**セキュリティ管理ルールに基づいた情報管理の不徹底**が原因



金融業界の動向

■金融機関においても、外部委託先を含むサードパーティの広がりは多岐にわたる

現状・課題

■弱点のある取引先等を起点に、攻撃経路として狙われる事例が発生している

想定されるリスク

■重要業務を担うサードパーティでサイバー攻撃が発生すると、サービスや自社業務が停止し、顧客に影響が及ぶ可能性がある

複雑化するビジネスの中で拡大するサードパーティに対して金融機関はどのように向き合うべきでしょうか？

サードパーティリスクの実効的な管理は経営層が組むべき経営課題の一つです

外部委託先やクラウド、ASP等を自社システムで一元管理しているものの、登録項目が多く、所管部門の負荷が高い事例が見受けられる。
また、各社の情報更新や現状把握に多大な時間を要している。

管理負荷の増大

システムの業務内容や重要度が異なる情報を委託しているものの、評価する基準や管理レベルが一律でリスク対応が漏れるケースがある。

画一的な管理

サードパーティに対するリスク評価を毎年実施している一方、リスク評価後の分析・深掘りが不十分で、グループ会社間で評価基準が統一されておらず、グループ全体でのリスク可視化に課題が残っている。

リスク評価の形骸化

サードパーティリスク管理態勢高度化のアプローチ

サードパーティリスク管理態勢の高度化には、管理対象の多様性と拡大に対応したリスクベースアプローチが不可欠です。
サードパーティごとのリスクプロファイル作成や、関与形態（外部委託、業務提携、サービス利用等）に応じたリスク評価方法の導入、重要なサードパーティについては実地調査による重点的なモニタリングの実施などが求められます。
これにより、従来の画一的な管理から脱却し、実効性の高い態勢の構築を目指します。

プロセス	現状把握・分析	設計・再構築	定着化
考慮ポイント	■サードパーティの網羅的な把握 ■現行プロセスの課題抽出	■リスクレベル別の評価プロセス設計 ■評価基準等の強化・見直し	■プロセスの周知・理解促進 ■PDCA体制の構築
主な実施内容	■サードパーティの管理実態の棚卸し ■委託先管理プロセス（選定、評価、モニタリング、契約終了）の実態把握 ■チェックリスト・運用フローの把握と分析	■リスク分類（例：重要・通常・簡易）に応じた評価プロセス設計 ■セキュリティ・サイバー対策等を含む評価基準・チェックリスト項目の再設計 ■評価体制・管理フロー案の検討・策定	■新プロセス・基準・規程等の説明会や教育・研修の実施 ■初期運用サポート（コンソーシング、QA対応等） ■全社的なサードパーティリスク評価結果の収集・分析の実施
成果物例	■課題整理・ギャップ分析一覧	■リスク管理体制案 ■リスク評価基準・チェックリスト ■規程・ガイドライン案	■教育・研修資料、FAQ集案 ■一元的なサードパーティリスク分析レポート案

サードパーティリスク管理態勢高度化支援サービスの概要

当社のサードパーティリスク管理態勢高度化支援サービスは、金融機関における多様なサードパーティとの関与形態や拡大する管理範囲に対応し、実効性の高い管理態勢の構築を支援します。
具体的には、現状分析、リスク評価プロセスの構築、最新規制動向への対応支援、グループ横断のガバナンス態勢の強化などをワンストップで提供します。
各金融機関の業務特性やリスク環境に合わせたサービスを提供することで、金融機関の持続的な成長に伴走します。

リスクレベルに応じた管理プロセスの整備・助言

委託業務の重要度や取扱情報の機密性など、リスクレベルに応じた最適な管理プロセスの設計・構築を支援します。
高リスク委託先には、定期的な現地調査や継続的モニタリングなど、実効性の高い統制を導入し、低リスク委託先には、効率的な簡易評価を組み合わせることで、ガバナンス強化と業務効率化の両立を実現します。

組織間・グループ間の統一評価基準・プロセス策定支援

グループ内外の組織間で評価基準や管理プロセスが異なる課題に対し、全社・グループ横断で統一された評価基準および管理プロセスの策定を支援します。
これにより、グループ全体でのリスク可視化と情報の一元管理を実現し、経営層による迅速かつ的確な意思決定を後押しします。

リスク対応への実行支援・コンソーシング

サードパーティリスク評価の運用立ち上げや評価プロセスの見直しなどに際し、リスク評価所管部署の実務担当者と一体となって、リスク評価プロセスの再設計から実際の評価・モニタリング（現地調査含む）・改善活動まで、現場に寄り添いながら伴走型で支援します。

トーマツの強み・実績

トーマツでは、金融機関に対する規制動向を踏まえたサードパーティに係るガバナンスとリスク管理に関する豊富な知見・実績を有しています。
トーマツによる態勢高度化の支援は、リスクベースアプローチを基本とし、当局からの要請や昨今のトピックを加味した実効性のあるメソドロジーを有しています。
これまでの豊富な経験を活かして高品質なサードパティリスク管理態勢の高度化支援サービスを提供します。

1

サードパーティリスク管理に関する多数の支援実績

金融機関に対する規制動向を踏まえたサードパーティリスクに係るガバナンスとリスク管理態勢の構築、リスク評価プロセスの整備、規程策定などの豊富な支援実績を有しています

2

規制当局との連携と理解に基づいた助言の実施

金融庁をはじめとする国内当局との人材交流やコミュニケーションにより、最新動向や背景となる規制環境をタイムリーに把握しており、お客様の組織や環境に適したアドバイスが可能です

3

金融機関に対する理解・環境知見を活用

数多くの金融機関に対する組織・環境の知見を活かし、効率的にお客様の現状を把握・分析します
また、お客様の状況応じたレベルアップを考えた深度ある助言を実施します

※貴社および貴社との関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容が提供できない可能性があります。詳細はお問合わせください。

Deloitte. トーマツ.
デロイト トーマツ

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
https://www.bsigroup.com/clientDirectory