KPMG
cutting through complexity

あずさ監査法人

April 2014

新たな第三者委託先監督の枠組み

信頼せよ、されど検証せよ

金融機関が国内外の第三者と委託関係を結び、その関係が複雑化していく中、米国やその他の法域において第三者のリスク管理に対する金融当局の注目度が高まっています。米通貨監督庁（OCC）および米連邦準備制度理事会の最近の文書では、この分野での銀行および銀行持株会社による調査の強化に関するガイダンスに重点が置かれており、金融機関による第三者委託先監視（TPO）プロセスの管理方法に関する規制当局の見方の変化を反映しています。

第三者委託関係のリスク管理に関するOCCの最新ガイダンス（OCC公示2013-29、「第三者委託関係：リスク管理ガイダンス」、2013年10月30日付）には、金融機関による第三者委託関係の評価手法の抜本的変更が示唆されています[1]。このガイダンスは第三者委託関係、とりわけ金融機関を深刻なリスクにさらす可能性のある「重要活動」に含まれる第三者委託関係に関して、十分なリスク評価・監視プロセスの採用を求めています[2]。さらにガイダンスは、第三者委託関係に関する十分なリスク報告を取締役会が必ず受けるよう指示しており、第三者委託先が実質的に金融機関の既存の全社レベルリスク管理（ERM）およびコンプライアンスの枠組みに完全に統合されることを求めています。

---

1 ガイダンスは「第三者委託関係」を、契約または他の方法による銀行およびその他の組織との事業上の合意事項と定義。第三者委託関係には、外部委託された商品およびサービス、独立性を持ったコンサルタントの使用、ネットワーク利用協定、小規模事業決済業務サービス、関連会社および子会社から提供されるサービス、合弁事業、銀行が継続的関係を持つ、または関連する業績に責任を有する可能性のあるその他の事業上の合意事項などが含まれる。関連会社との関係は、規制 W（12 CFR 223）で実施される連邦準備法（12 USC 371c および 12 USC 371c-1）のセクション 23A および 23B への準拠が求められる。通常、顧客との関係は第三者委託関係には含まれない。

2 ガイダンスは、「重要活動」を、「重要な銀行機能（支払、精算、決済、保管等）もしくは重要な共有サービス（情報技術等）、または下記の性格のその他の活動」と定義している。

- 第三者委託先が期待通りに動かなければ銀行が深刻なリスクに直面する可能性がある。
- 顧客に深刻な影響を及ぼす可能性がある。
- 第三者委託関係の実施とリスク管理には大規模な投資が必要である。
- 銀行が代わりの第三者委託先を見つけなければならないか、外部委託された活動を社内に移管しなければならない場合、銀行業務に深刻な影響を与える可能性がある。

従来、金融機関は多くの場合、調達・サプライヤー管理プロセスを伴うサイロ化された（タテ割りの）リスク領域の監督を通して、第三者委託先リスクを管理してきました。OCCは、消費者コンプライアンス・リスク、情報セキュリティー・リスク、事業継続リスクなどの高リスク特性を持つ関係においては、サイロ化されたアプローチでは基本的に不十分であると指摘しています。その場合の課題は、金融機関が第1および第2の防衛ラインにいる既存のリスク、およびコンプライアンス分野の専門家を第三者委託先に対する監督・管理プロセスに関与させることです。さらにOCCは、特に「重要活動」に第三者委託先が関与する場合、第三者リスク管理プロセスに対して独立したレビューによる評価を求めており、これに対応するためには内部監査、または他の第三者委託先による第3の防衛ラインからの関与者を増やすことが必要となります。

連邦準備制度理事会のガイダンス（監督および規制に関する公式文書13-21、「外部委託リスクの管理に関するガイダンス」、2013年12月5日付）は、おおむねOCCガイダンスと類似した内容ですが、その焦点は絞られています。対象となるのは、銀行の伝統的中核業務および情報技術サービス以外の分野における、外部委託活動におけるサービスプロバイダー・リスク管理プログラムの特性、ガバナンス、運用の実効性です。これらの分野には、会計、査定管理、内部監査、人事、販売・マーケティング、貸出金のレビュー、アセット・マネジメント、資金調達、債権回収業務などが含まれています[3]。

これら規制当局の各ガイダンスはプリンシプルベースであり、評価・リスク管理プロセスを金融機関のERMおよびコンプライアンスの諸機能とどの程度調整する必要があるかについては、金融機関に一任されています。第1、第2の防衛ライン全体でこうした統合に非常に積極的な金融機関もあれば、細かい指示が載ったガイダンスが公表されるのを待つか、または業界慣行の形成をチェックしつつ「様子見」のアプローチを取る金融機関もあるようです。OCC、連邦準備制度理事会などの銀行監督当局が第三者委託先リスクにターゲットを絞ったレビューを継続的に実施していることを考慮すると、後者の金融機関は監督当局から厳しい非難を受けるリスクがあるとKPMGは考えています。また、消極的アプローチによって優れた実務慣行を形成できる機会を逃してしまう可能性もあるでしょう。

最近の動向を見ても、消費者と接触する第三者委託先に関連するコンプライアンス・リスクの監督と管理を適切に検討しているかどうかを、銀行業界が自己評価する必要があるのは明らかです。コンプライアンス・リスクに対し、業界はより「現場主義的な」全社的評価の方向に向かっている様子ですが、なお一層の前進が必要であるとKPMGは考えています。ガイダンスは、企業リスクおよびコンプライアンス評価の重要な側面について、金融機関を啓蒙するための警鐘なのです。

金融機関がリスクとコントロールに関する自己評価の包括性を強化しようとしている中、系列組織を含む第三者への委託内容に特別の注意を払うとともに、委託先の関連リスクと必要なコントロールの見極めにも注意を払うことが肝要です。これらのリスク評価は、リスクの特定、測定、監督、管理、報告の能力を持つとともに、企業／事業部門（LOB）のリスク・アペタイト・プロセスの実効性と持続性を確保するための基本となるものです。

3 連邦準備制度理事会のガイダンスにおいて、「サービスプロバイダー」は、ビジネス機能または活動の提供を目的として金融機関と契約関係にある（銀行またはノンバンク、関連または非関連、規制対象の、または非規制対象の、国内または国外を問わない）あらゆる組織という広義の定義がなされている。ここでおおむねカバーされるのは、サービスプロバイダーの使用にかかるリスク、取締役会および上級管理者の責任、サービスプロバイダー・リスクの管理プログラムである。

第三者リスク管理は根本的に契約管理機能とは異なっています。金融機関は様々な業務や活動を外部委託できますが、金融機関に代わって遂行されている活動の説明責任は外部委託できないかもしれません。OCCはガイダンスの中で、「銀行による第三者の使用は、安全かつ健全な方法で、そして関連法規に準拠して活動が行われることに対する取締役会および上級管理者の責任を減ずるものではない」と述べています。連邦準備制度理事会のガイダンスにもこうした考え方が反映されています[4]。

新ガイダンスは、国内外いずれでも第三者への委託件数および委託内容の複雑性が増し続けているとしており、「第三者委託関係のリスク管理の質が、こうした関係のリスクの水準と複雑な性質に追いつかない可能性がある」[5]とする規制当局の懸念に対応したものです。第三者への委託件数が拡大しているのみならず、既存のビジネスモデルが第三者により大きく依存したものに明らかに変化している状況が見られます。

OCCは、第三者委託関係のライフサイクルにわたり、端から端まで、そして継続的に各関係をカバーする新たな第三者リスク管理プロセスを特定しています。プロセスは次の8段階に分類されます。

- 計画策定（リスク戦略への反映、固有リスクの特定、第三者委託先の使用）
- デューデリジェンスおよび第三者委託先の選定
- 契約交渉
- 継続的モニタリング
- 解約（緊急時対応策を含む）
- 監督および関係管理における役割と責任
- 文書化と報告
- 独立したレビュー

こうした枠組みに則して[6]、金融機関は様々な問題を考慮した上で、第三者管理に対する適切なリスクベースのアプローチを開発する必要があります。

第三者とは？

OCC（およびその他の銀行監督当局）は、第三者委託関係について非常に広範な見方をしています。一般に顧客はそこから除外され、次の者が含まれます。

- ベンダー、およびその下請けベンダー
- サプライヤー
- 外部委託業者（IT外部委託業者、業務プロセス外部委託業者、コールセンター業者、人事外部委託業者、および不動産・施設管理業者が含まれる）
- 合弁事業パートナー
- 当該金融機関が支配権を持つと見なされる関連会社
- 専門サービス提供企業

防衛のための3ライン

「防衛のための3ライン」モデルでは、組織全体にわたる役割と責任が明確に定義され、ガバナンス・リスクの管理、およびそれを確実なものにするための実効性のある枠組みが提供されます。

- 「第1のライン」はビジネス担当部署です。リスク管理のプロセスおよび手続を遵守し、リスクの管理と対処、そして新たに生まれつつあるリスクを見極める行動を起こす責任を持ちます。
- 「第2のライン」は様々な基準を設定する部署であり、そこには監督の諸機能も含まれます。各部署は、リスク管理用の方針と手続の構築、特定のリスク領域の監督、そして企業全体のトレンド、事業間のシナジー効果、変革の好機の見極めに責任を持ちます。
- 「第3のライン」は管理が確実なものであることへの保証を提供する部署（内部および外部監査）です。リスク管理プロセスの適合性と適切性について、独立した客観的保証を行う役割を担います。

4 「銀行による第三者委託先の使用は、安全かつ健全な方法で、かつ関連法規と規則に準拠した活動を行う上で取締役会および上級管理者が負う責任を減ずるものではない」連邦準備制度理事会の監督および規制に関する公式文書13-19、全12ページの内の2ページ

5 OCC公報 2013-29

6 連邦準備制度理事会の監督および規制に関する公式文書13-19には、リスク評価、デューデリジェンスおよびサービスプロバイダーの選定、契約と条項および検討すべき事項、インセンティブ報酬の審査、サービスプロバイダーの監督モニタリング、事業継続計画および緊急時対応策の検討に関する記述がある。

- 業務提携先
- 緊急時対応策への参加者
- 臨時の雇用者
- 取引カウンターパーティー

また第三者委託関係には、オンサイトあるいはオフサイト、国内あるいは国外、「クラウド」、外部委託されているか社内外協働のもの、統合されたもの、継続的なものなど、金融機関がこれらの第三者と関係を持つ全ての経路が含まれます。

金融機関の関連第三者委託先とその業務

金融機関には自社が関与する、あるいは関与の義務を持つ全第三者委託関係のリストの作成が必要かもしれません。おそらく、金融機関の多くが何千先ものリストを持つことになるでしょう。

各委託関係の分類／優先順位の設定に使えるリスク情報マトリックスの作成を検討しましょう。そうしたマトリックスに含まれる情報は、たとえば、その第三者委託関係の自社顧客への関与の有無、機密データや重要なITシステムの関与の有無、規制対象の商品やサービスの関与の有無、当該第三者委託者の国内拠点の有無、当該第三者委託者が契約義務不履行の場合、その第三者の役割は簡単に代替できるか、当該第三者委託者の「重要活動」への参加如何などです。

金融機関にとっての「重要活動」、および参加する第三者委託先の特定

OCCのガイダンスは「重要活動」について、「重要な銀行機能（支払、精算、決済、保管等）もしくは重要な共有サービス（例：ITなど）、または下記の性格を持つその他の活動」が含まれると定義しています[7]。

- 第三者委託先が期待通りに動かなければ、銀行が深刻なリスクに直面する可能性がある。
- 顧客に深刻な影響を及ぼす可能性がある。
- 第三者委託関係の実施とリスク管理には大規模な投資が必要である。
- 銀行が代わりの第三者委託先を見つけなければならないか、外部委託された活動を社内に移管しなければならない場合、銀行業務に深刻な影響を与える可能性がある。

「重要活動」に関与する第三者委託先の使用においては、「より包括的で厳格な」監視が期待されており、それには次の内容が含まれます。

- 上級管理者によるデューデリジェンスのレビューの概要、および重要活動への第三者委託先の継続関与の推奨に対する取締役会のレビュー
- 重要活動に関与する第三者委託先との関係を始める前の、管理計画に対する取締役会の承認
- 重要活動に関与する、第三者委託先との契約締結に対する取締役会の承認
- 重要活動に関与する、第三者委託先に対する継続的モニタリング結果についての取締役会のレビュー
- 第三者委託先のリスク管理で生じる責務に取締役会はどのように対応できるか、各金融機関は新たな報告ラインや要件の設定、部署の責任範囲の策定などの検討が必要

7 連邦準備制度理事会ガイダンスは、銀行の伝統的中核業務および情報技術サービス以外の外部委託活動を対象としたものであることに留意する。

一般的に、金融機関が第三者委託先を使う理由は、(1)社内業務の外部委託、(2)自らが通常提供しない商品やサービスを顧客に提供するため、そして、(3)他社が提供する活動やサービスに自社の名称や信用を有償で貸与するためです。リソースの制約への対処、追加の商品やサービスの開発、そして社内にはないと考えられる専門知識の提供のために、第三者が利用されることもあります。

第三者委託先は、金融機関の業務、商品／サービスのライフサイクルのうち、各々どこに組み込まれているか？ 第三者委託先はそのプロセスにとってどの程度重要か？

重要プロセスとサービスに関し、第三者委託先への正確な業務委託の範囲はどこまでであるのかを、プロセスマッピングを用いて確定するべきです。

業務または商品の委託に関連するリスクをどのように特定するか？

プライバシー、規制コンプライアンス、事業継続計画の策定、情報セキュリティーといった、第三者委託先がリスクに影響を与える多くの要素に基づいて、第三者委託先との関係のライフサイクル(関係開始時、およびその後定期的に)の様々な地点におけるリスクを特定する必要があります。ただし、これらの定期的な評価以外にも、潜在リスクの拡大を経営陣に警告する早期警告システムが必要であり、こうした分野ではリスク・アペタイト、主要パフォーマンス、およびリスクの諸指標へのリンクが役立つことになります。

リスク管理を行う諸部署は、活動に付随する固有リスクの評価に加えて、活動の第三者委託に関連したリスクの増大、こうしたリスクの制御に向けた当該金融機関や第三者による既存の手法による補完、および金融機関が負い続ける残存リスクの特定に当たって、互いに協働する必要があります。これらの評価は柔軟で、初期リスクについてのデューデリジェンス、継続的なモニタリングと検証の評価、および、オンサイトやオフサイトの審査にも対応できるものである必要があります。残存リスクが金融機関のリスク・アペタイト閾値を上回って増えた場合、更なる評価が必要です。

第三者委託関係の管理責任者は誰か？ 監督に使われるパラメータとは？

日常管理は第2ラインの監督諸機能に権限移譲されているものの、リスクの観点から見ると、その管理に最終責任を有するのは取締役会です。組織が従うべき基準と方針は取締役会が策定します。そして、各事業部門(LOB)にこれらの基準と方針を実行・遵守させることが取締役会の責任となります。

第三者委託先管理に対し日常的な責任を持つLOBは、各第三者委託先をLOBの社内業務の一部であるかのように管理しなければなりません(すなわち、所属するLOBで監督を行う場合、それは第三者委託先も対象とする必要があります)。契約には、リスクが増大した場合にLOBによる監督の拡大が可能となるようトリガーを組み込んでおく必要があります。

どのように問題が特定されるのか？ どのように対処されるのか？

第三者委託先から生じるリスクに関する理解を深めることで、関係開始時、およびその後の継続的な公式のリスク評価活動ではカバーされないリスクの見極めを目的とした、早期警告システムの構築が可能になります。管理・監督機能を支援するために、リスクとコントロールに関する様々なパフォーマンス測定基準および評価基準を第三者から入手できるよう、契約書を設計することが望まれます。ただし場合によっては、信頼できるパフォーマンス測定基準および評価基準を入手するために、第三者委託先の監督強化が必要となるかもしれません。このような追加的な監視コストは、特定の第三者委託関係に関連する利益を減少させてしまいかねず、トータルコスト(モニタリング、コントロール、リスク)が第三者委託先との契約から得られる利益を上回る結果となる場合があります。加えて、コストが利益を上回りかねないというリスクがあることから、徹底したリスク評価、および第三者委託先、その金融機関との関係性について広範に理解することが重要です。

既存の第三者委託先とどう付き合うべきか？

OCCガイダンスに照らし合わせて、既存の第三者委託との関係にどう対処するか金融機関は悩むかもしれません。しかし、他の全ての（将来契約するかもしれない）潜在的第三者委託先同様、既存の委託関係を計画とリスク分析に組み込む必要があります。OCCガイダンスには、第三者委託先と関わった経験や第三者委託先に対する予備知識は、客観的かつ詳細なデューデリジェンス評価の代用とはならないと明確に述べられています。加えて、既存の契約、特に重要活動が含まれる契約は定期的な見直しを実施し、適切なリスクコントロールと法律的な保護に対応していることを確認する必要があります。問題が特定されたときには、金融機関はできる限り早期に契約の再交渉を求めなくてはなりません。

独立したレビューのために第三者委託先の使用を検討する際に考慮すべき要素とは？

特に第三者委託先が重要活動に関与している場合、第三者委託先のリスク管理プロセスに対する独立したレビューを定期的に実施することを、新ガイダンスは金融機関に求めています。金融機関の内部監査人または独立した第三者によるレビューを実施する場合には、上級管理者はその結果が取締役会に必ず報告されるようにしなければなりません。こうした審査の規模、内包するリスク、そしてレビューが必要な時期と頻度により必要な人材の数とタイプが決まります。金融機関の内部監査グループが独立したレビューの要件を満たすことができる場合もありますが、評価の実施に外部の第三者委託先を使う必要がある場合もあります。

一般的に、金融機関が第三者委託先を使う理由は、（1）社内業務の外部委託、（2）自らが通常提供しない商品やサービスを顧客に提供するため、そして、（3）他社が提供する活動やサービスに自社の名称や信用を有償で貸与するためです。リソースの制約への対処、追加の商品やサービスの開発、そして社内にはないと考えられる専門知識の提供のために、第三者が利用されることもあります。

業界で見られる第三者委託先の活用拡大の動きは、金融機関のビジネスモデルの根本的かつリアルな変化であり、それが弱まる気配はありません。この変化をもたらしている主要因はコスト高です。ただしコスト削減によって、それらの第三者委託先から生じるリスクが増大しているという状況が生じているのです。こうしたことに鑑みて、第三者委託先に対する過去の管理手法を新たに進化させ、リスク管理に包括的なアプローチを導入する必要があります。

ますます多くの金融機関が自社業務を外部ベンダー、時にはその下請けベンダーに委託する度合いが増していることをOCCは認識しています。変化の速さに呼応してリスクが増大している状況を踏まえ、OCCの第三者委託先管理の枠組みは、ここでもこうした変化に対応したものとなっており、OCCをはじめとする銀行規制当局は次のような方策を取っています。

- リスク管理に対する注目度を高め、委託関係の継続的ライフサイクルにわたり、端から端までの全関係を評価するプロセスを導入する。
- 金融機関を最大のリスクにさらす第三者委託先に対する、上級管理者および取締役会の役割を強化する。
- 義務を履行しない第三者委託先を変更するか、またはより良いオプションを検討するための緊急時対応策の検討を求めることにより、第三者委託先の義務不履行に伴う事業中断の影響から金融機関を守る。

断片的なまたはサイロ化されたアプローチの中でこれらの要請に対応することは、より優れたリスク管理実施の好機を逃すことになるでしょう。金融機関は企業リスク・プログラムとコンプライアンス・プログラムを構築した自社の経験を活かして、全社的なリスクに対する目と思考を持って、第三者委託先から生じるリスクを包括的に概観する必要があります。

OCCが提供する枠組み、社内の既存のリスクカルチャー、および企業リスク管理の枠組みと整合性を持つ第三者委託関係の管理プログラムを完全に構築するためには、金融機関の集中的な企業努力が必要となるでしょう。デューデリジェンスと同様、知らなかったということは理由になりません。第三者委託先リスク管理の枠組みを進化させていること、実効性と一貫性のあるリスク評価を実施していること、第2ライン、第3ラインによる実効性のある問題指摘の余地を確保していること、そして第三者委託先リスクを取締役会に効果的に報告しているということを、金融機関は規制当局に示せるようになる必要があります。

スターティングポイント：今後のステップ

第三者委託先リスク・エクスポージャーと管理の現状を明確化しなければなりません。たとえば、

- 自社の重要活動を定義する。
- 既存および計画中の第三者委託関係を全て特定し、その契約遵守状況を確認する。
- 第三者委託関係のマトリックスを作成し、明確になった重要活動への関連性に基づいて、それぞれの関係について優先順位を決定する。
- 第三者委託関係に対する既存の管理と監督状況を確認する。
- 第三者委託先に対する委託および／または参加の時点を識別するため、商品・サービスのプロセスのマッピングを始める。
- リスク管理プロセスのベースラインを設定するために、特定の重要活動に対する独立した審査を受けることを検討する。

必要に応じて第三者委託先リスク管理プロセスを変更します。

- 取締役会メンバーおよび上級管理者が負う監督の役割と責任を明確化する。
- 各部門が負う監視の役割と責任を明確化する。
- 契約を査定し、必要かつ可能な場合は再交渉を行う。
- 重要活動に関与する第三者委託先に対するモニタリング、検証、内部管理のプロセスと報告要件の評価と強化を行う。
- 可能な限り第三者委託関係を合理化する。

第三者委託関係へのシフトは継続的に拡大しています。将来の究極的な形態は、一部門の活動をまとめて外部委託することでしょう。おそらくリスク管理プロセスすら外部委託される可能性があります。このような状況に対処するときに、規制当局が期待するのはどのようなことなのでしょうか。監督の厳格化、監督強化でしょうか？また、金融機関はリスク・エクスポージャーをどのように管理すればよいのでしょうか。独立監査でしょうか、部内への監査チーム設置でしょうか？これらについて考慮して、戦略的な分析を行う価値があることは確実です。

編集・発行

有限責任 あずさ監査法人
KPMG ファイナンシャルサービス・ジャパン
e-Mail: financialservices@jp.kpmg.com

この文書は KPMG's Americas' FS Regulatory Center of Excellenceが2014年2月に発行した「The New Third-Party Oversight Framework: Trust but Verify」をベースに作成したものです。

翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。