KPMG あずさ監査法人

銀行業界を取り巻く金融犯罪について

変化への対応にあたっては、迅速な対応、リスク、文化の3つが重要

September 2018

絶えず変化する課題：主要な調査結果

金融犯罪の防止・探知にあたり効果的なリスク管理を行うには、プロフェッショナルな個別金融機関ごとのアプローチが必要となります。

スイスの銀行が金融犯罪のリスクを判断するために採用した一部のアプローチは不十分なものです。高リスクの国、セクター、顧客を特定する際に、標準化された公表リストや購入リストに依拠しすぎており、銀行特有の市場、商品、サービス特性といった個別金融機関ごとのリスクへの配慮が全般的に欠けています。

しかし、個別金融機関ごとのリスクに配慮した対応を行うには、個別金融機関ごとにリスクアペタイトを明確かつ包括的に定義し、適用することが不可欠であり、これはすべての銀行にとっての課題であり、取締役会の関与が必須です。

銀行による審査ロジックおよびシステムのレビューが十分でない。

スイスの銀行は審査の在り方に対する監視が非常に緩く、最新の経済制裁措置にシームレスに対応するためのシステムおよびプロセスが欠如しています。経済制裁スクリーニングのロジックの定期的かつ体系的な見直し、制裁対象者リストの更新、トランザクションモニタリングシナリオおよび閾値に関し、行動を起こす必要があります。

- 29%の銀行は「必要に応じて」アプローチの見直しを行っていますが、定期的に実施しているわけではありません。
- 年1回またはそれ以上の頻度で見直しを実施している銀行は半数未満です。

突然改正された制裁対象者リストが常に考慮されているとは限らない。

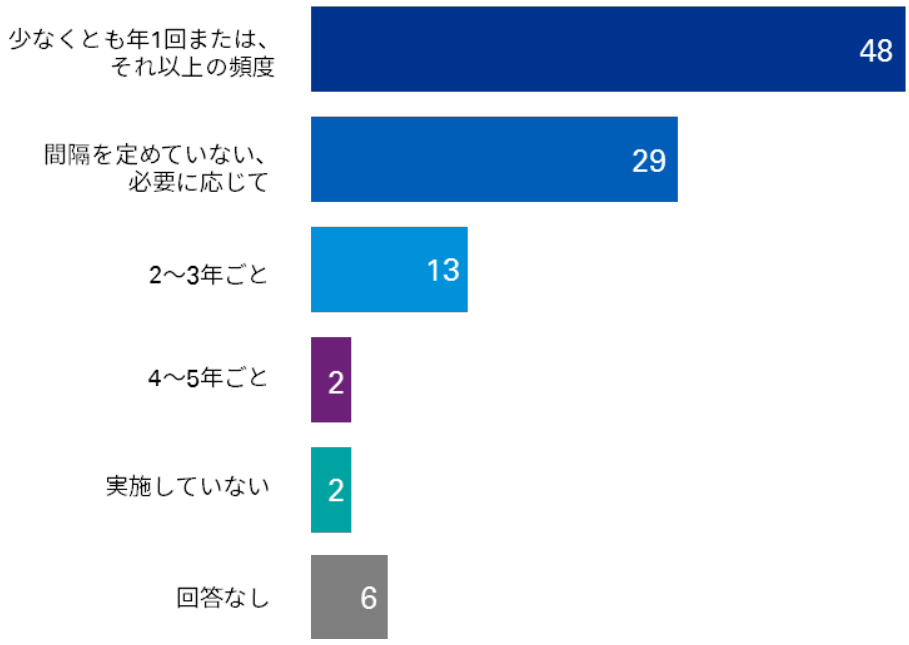
- 制裁対象者リストが急遽改正され、十分な警告もなかった場合には、ある顧客が突然、銀行にとって高リスク顧客になることにもなりかねません。銀行が制裁対象者リストの変更を予期していない場合、または変更に対して速やかに行動しない場合、改正と銀行が行動（顧客関係の遮断または解除）を起こすまでのタイムラグによって、銀行がリスクにさらされる可能性があります。
- 銀行は制裁対象者リストの改正を継続的に監視して、状況に応じて内部データの更新や見直しの実施を確実に行う必要があります。

高リスク対象を定義する際に、個別金融機関ごとのリスクがほとんど考慮されていない。

金融犯罪のリスクエクスポージャーを評価する場合、銀行はしばしば、個別金融機関ごとの市場、サービス提供、商品戦略を考慮しません。そのため、顧客情報および関連するプロセスを銀行の現行のリスクアペタイトに反映する態勢が整っていません。

- 69%の銀行は、陳腐化した主要なリスクファクターと個人の専門知識に基づく判断を組み合わせて商品やサービスのリスクを評価しています。
- 高リスク国を定めた公表リストまたは購入リストを事業やリスク特性に合わせて調整している銀行は10%しかなく、高リスクセクターを定めたリストを同様に調整している銀行はわずか20%にとどまります。

経済制裁スクリーニングのロジック、制裁対象者リストの更新、トランザクションモニタリングのシナリオおよび閾値のテスト、レビュー、監査をどの程度の頻度で実施していますか。（単位：%）

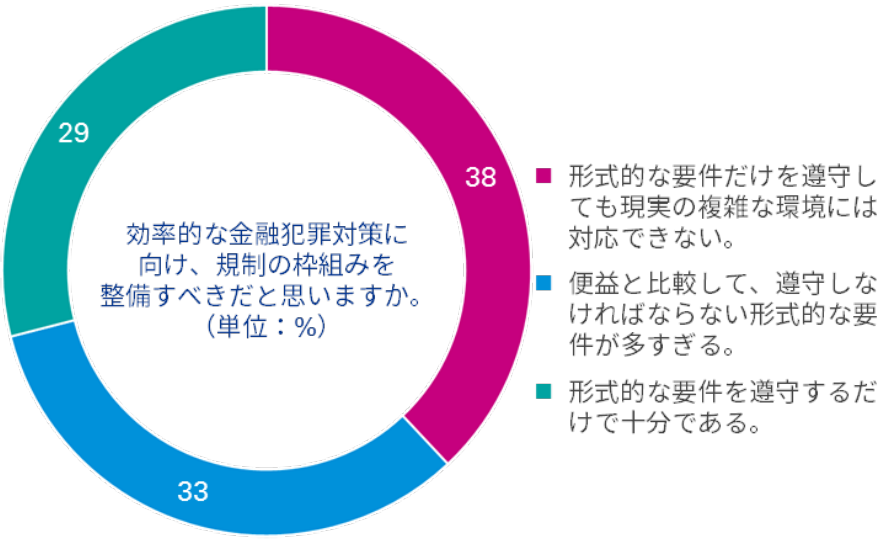


基本的な規制要件を遵守していれば十分と考えている銀行が多すぎる。

- 規制が文書で要求する最小限のものを遵守していれば十分というわけでありません。金融犯罪対策で効果を挙げるには、現実の複雑な環境では、より多くの要素を考慮することが求められます。
- 顧客の取引を深く理解することが鍵となります。

✓ 回答者の29%は基本的な規制要件を遵守していれば十分であると考えています。

✓ 回答者の3分の1は、潜在的利益に関連して遵守を余儀なくされている形式的な要件が多すぎると感じています。



行動に向けての課題

- 個別金融機関ごとのリスクアペタイトの包括的枠組みを定義・設定する際には、取締役会を関与させること。銀行の金融犯罪リスクへの対応の一環として、これには個別金融機関ごとの市場、商品、サービス戦略に内在するマネーロンダリング対策（AML）および経済制裁のリスクが含まれます。
- 取締役会はリスクアペタイトに合致する適切なリスク対策をとれるよう、十分な予算を割り当てること。
- 効果的にリスクを軽減するため、フロントオフィスの権限を拡大するなど、定義されたリスクアペタイトを日々主導する経営トップの基本姿勢を徹底すること。
- マネーロンダリング対策のため、トランザクションモニタリングのシナリオおよび閾値の更新を確実に実施すること。
- 制裁対象者リストを少なくとも週に1度更新すること。
- 新たに策定・更新された経済制裁の、銀行の事業および顧客に対する影響を考慮すること。
- 顧客、顧客と銀行との関係、顧客の事業および取引を理解すること。
- 背景にある事業上の根拠などの、顧客の取引の妥当性を確認すること。

絶えず変化する課題：論説

金融機関とマネーロンダリング対策

組織的犯罪が増加しています[1]。また、その手段としてマネーロンダリングなどが利用されています。一段と厳しい規制が施行され、注目度の高い汚職事件に大手金融機関が巻き込まれているにもかかわらず、なぜ銀行や金融仲介機関は依然として不正に対して脆弱なのでしょうか。

違法な出所を隠蔽するマネーロンダリングのプロセスには、通貨の密輸（物理的に国境を越えて通貨を移動させる）、スマーフィング、ストラクチャリング（取引報告要件に抵触しない程度の少額の資金を預金する）から、いわゆる地下銀行や「ハワラ」（仲介業者のシステムを経由して匿名での支払いを可能にする）まで、いくつもの形態があります。利用される手口はどれも、金融システムの悪用または不正操作に関連しています。スイスでは近年こうした問題が数多く発生しており、注目を集めたものとしては、ワン・マレーシア・デベロップメント（1MDB）やペトロブラスなどの汚職事件に関連した事件があります。違法な資金を保有する銀行は甚大な影響を被ることになり得ます。

規制は常に後手に回る

銀行がマネーロンダリングに利用されることを防ぐために、さまざまな規制上の義務がすでに導入されています。資金洗浄防止法（AMLA）、スイス連邦金融市場監督機構（FINMA）の資金洗浄対策令（AMLO）、およびスイス銀行協会のCDB（デューデリジェンスに関する行動規範）16は、金融仲介業者に一定の注意義務を課しています。代表的なものを挙げると、金融仲介業者は顧客の身元確認、資産や資金の出所を含む受益所有者の身元確認、取引の経済的背景や目的の明確化、リスクが高い場合のより詳細な明確化を実施しなければなりません。

しかしながら、規制に伴う課題の1つとして、規制が施行される頃には内容が陳腐化し、実際に適用する際の問題となる場合があることが挙げられます。その理由は、第1に、規制はすでに悪影響を及ぼしている問題に対応する形で策定される場合が非常に多く、第2に、その一方で犯罪者は目的を達成するための新しい、より独創的な手法を開発しているためです。例えば、サイバー犯罪や仮想通貨は、マネーロンダリング対策を実施する者が直面している新たな課題です。当局は関連規制を今後の動向に対応できるよう（例えば、AMLA第8条に記載されているマネーロンダリング対策を、マネーロンダリングの手口の実態に合わせて自動的に変更するなど）にするために最善を尽くすはずですが、十分に具体的なガイダンスを仲介業者に提供できない可能性もあります。

1 複数の犯罪に関与する組織的犯罪グループの割合は45%上昇しており、2013年の33%の上昇を大幅に上回りました。2017年3月9日付の欧州刑事警察機構のプレスリリース

金融機関はさらなる取組みが必要

2つ目の要素は仲介業者における効果的な管理メカニズムの必要性です。言い換えると、金融機関は規制の効果的な実施を徹底するため、さらなる取組みを進める必要があるということです。スイス連邦金融市場監督機構（FINMA）は、1MDBの事件に巻き込まれた銀行の過ちについて調査した際、この問題を強調しました。それによると、高まったリスクが十分に考慮されず、不完全で矛盾する顧客情報も問題視されることがなく、妥当性評価も入念に実施されていませんでした[2]。

金融仲介業者は内部プロセスの有効性を向上させることに投資することによって、こうした問題に対処することが可能です。第1の防衛ラインは予防措置にあります。新たなリスクやエクスポージャーに対応できるよう、リスクや妥当性の分析を継続的に適合させる一方、ITシステム、内部ガイドライン、従業員教育を定期的に評価・更新する必要があります。また、第1および第2の防衛ラインにおける内部統制の有効性を継続的に精査すべきです。

両防衛ラインにおける防備手段への投資は、金融仲介業者がマネーロンダリングのリスク低減のために必要な枠組みや環境を確実に推進することに役立つはずです。スイスの金融機関の脆弱性を是正するには、規制や政策文書では不十分なのです。金融機関自体が、より適切に課題克服に向けて取り組む必要があります。

仮想通貨時代のマネーロンダリングと金融犯罪

ピア・ツー・ピアで取引について、銀行システムを回避する目的で設計された仮想通貨の動きは、ある意味で透明性とトレーサビリティが確保されていると言えるかもしれません。しかし、受益者の身元は匿名の暗号によってしか特定できません。犯罪者がこの弱点を悪用しようとしている状況において、こうしたマネーロンダリングや金融テロの新たな手口に金融機関はどのように対処すればよいのでしょうか。

仮想通貨の成長はこの10年間勢いを増していますが、多くの金融機関はこの非常に複雑なテーマを理解し始めたばかりです。仮想通貨を支えるブロックチェーンは一般的に、IPアドレスや個人データなどの情報を蓄積しないとされており、金融機関が匿名の番号口座の受益者の身元を突きとめることはほぼ不可能です。銀行はもはや、法定通貨（従来の法貨）に関して機能していたマネーロンダリング対策の概念に頼ることはできません。より多くの高度な経済制裁が課される時代には、これは実に危険なことと言えるでしょう。

犯罪の選択肢：仮想通貨によるマネーロンダリング

仮想通貨によるマネーロンダリングは国際的な経済制裁を回避するために利用されるおそれがあります。一般的なマネーロンダリングのプロセスは次のとおりです。

2 2017年12月21日付のFINMAのメディアリリース、『FINMA informiert über 1MDB-Verfahren gegen J.P. Morgan』

1. デジタル取引所で仮想通貨を購入するか、デジタル通貨ATMで現金またはデビットカードで仮想通貨を引き出します。大半の仮想通貨ATM業者は規制の対象になっているため、デジタル取引所が選択される傾向にあります。デジタル取引所では、前科のない、信頼性のある職に就いている人の名義を借ります。仮名、匿名の電子ウォレット、ログの残らない仮想私設ネットワーク（VPN）、ブロックチェーン用に最適化されたスマートフォンを使用して匿名性を高めます。
2. 借りた名義がデジタル取引所で認証されたら、法定通貨または銀行口座振替を利用してプライマリー通貨を購入するための資金を預け入れます。すると、最先端のデジタル取引所でいわゆるアルトコインを購入することができます。アルトコインには匿名性の高い匿名通貨も含まれます。
3. マネーロンダリングを行う者はミキシング（またはタンブリング）サービスを利用して、プライマリー通貨のアドレスをデジタルウォレットの一時的なアドレスと交換してブロックチェーンを欺き、監査証跡を確認できないようにします。その他、不正な受信アドレスを使用して取引をバックアップアドレスへ迂回させ、監査証跡を確認できないようにするものもあります。ミキシングされたプライマリー通貨はその後、最先端のデジタル取引所に送金され、匿名通貨の購入に用いられます。
4. 次のステップは、複数の匿名通貨、取引所、デジタルアドレスを経由させることです。幾度か経由させるうちに監査証跡が途絶え、マネーロンダリングされた違法資金が伝統的な金融システムに還流されます。
5. マネーロンダリングを行う者は以下に挙げる方法により、デジタル通貨から法定通貨まで、マネーロンダリングされた資金を引き出すことが可能になります。
    a. 増大する複合化：匿名通貨をプライマリー通貨に交換後、これを基本通貨にし、取引のある銀行口座から引き出すか、キャピタルゲイン税を逃れるために不動産の購入に充てます。
    b. デジタル通貨を仮想通貨ハードウェアウォレットに保管するか、QRコードに印刷し、世界中の任意の受取人に送付します。

金融機関と規制当局はさまざまなソリューションを駆使している。

AMLの手順

金融機関は再評価システムおよび再評価プロセスによって、より高いリスクに対応できるようにし、以下の事項を確実に阻止する必要があります。

- 身元確認情報や本人確認（KYC）情報を必要としない取引フロー
- 匿名通貨による収益（探知可能な範囲で）

取引の監視

仮想通貨の匿名性は、金融機関が取引の受益者を特定することを困難にするかもしれませんが、ITシステムでアルゴリズムを活用すれば、法定通貨のパターンや動き

を特定することで、行われているマネーロンダリングの手口を示すことができます。これにより、犯罪とつながっている可能性のある口座の特定につながります。

より的を絞った規制

仮想通貨を批判する人々は、デジタル取引には身元確認情報が不足しており、これが既存のAMLにおける監視や執行能力に対する大きな障害となっているとしばしば言及します。しかし、これに関しては、関係者および情報の確認、取引の履歴といった規制や執行の要素となるものが、仮想通貨の世界に存在することを認識することこそ重要であると言えます。少なくとも理論的にはそうなります。仮想通貨のリスクを効果的に抑制するには、KYCの国際基準を拡充したうえで電子ウォレットを提供することが必要です。

マネーロンダリング対策分野における国際基準の設定者として、金融活動作業部会（FATF）は2018年2月、韓国金融委員会による同国の仮想通貨取引所のマネーロンダリング対策に関するコンプライアンスルールへの取り組みを推進しました。これは、韓国の匿名取引口座の禁止措置と、取引プラットフォームへの新たな要件として実施された本名確認について取りあげたものです。韓国では匿名や偽名のウォレットはもはや認められていません。

サードパーティーのIDプロバイダー

当局に犯罪要素の追跡を可能にする一方、法律を遵守している人に対しある程度の匿名性を確保するために、サードパーティーのIDプロバイダーは煩雑な身元確認やKYC情報の照合を回避する鍵となるかもしれません。

最先端のデジタル取引所に対する規制

プライマリー通貨を提供する取引所は、ビットコインなどのプライマリー仮想通貨を法定通貨と交換してきた経緯があるため、規制するのはより容易です。しかし、プライマリー通貨をアルトコインに交換するだけの、いわゆる最先端のデジタル取引所に対する規制も重視する必要があります。こうした取引所に対する規制は有効かもしれません。匿名通貨の監査証跡を追跡しても特定することはできないかもしれませんが、デジタル取引所ではその取引所の取引やデジタルウォレットの残高を確認することができるためです。

ブロックチェーンをより効果的に活用する

ブロックチェーン技術は本質的に、法定通貨に比べてAMLのリスクを低減する可能性を秘めています。ブロックチェーンはオンラインの公開元帳を通じて管理されており、これは、各取引の完全な履歴が監視、認証、記録されることを意味します。また、各仮想通貨はエンドツーエンドのマイナーによって確認されている固有の特徴を有しているため、偽造するのはほぼ不可能です。送金元のウォレット、送金先のウォレット、通貨種類、金額を含むすべての取引フェーズが確認されない限り、取引はただちに遮断され、人が関与する余地はありません。こうした意味において、デジタル通貨の証跡は既存の法定紙幣の証跡に比べ、AMLで優れた効果を発揮すると考えられます。さらに、ブロックチェーンのプロトコルを書き換えることで、KYC認証済みのウォレットを利用した取引に限定することも技術的に可能ですし、AMLにおけるリスク分析、警告メカニズム、報告メカニズムを暗号システムに統合できる可能性もあります。

結局のところ、最も効果的なアプローチは、これらの考慮すべき要素を組み合わせたものになると思われます。規制当局は、この急速に進化し続ける分野の課題に対応できる、より新しくかつ的を絞った基準を開発する必要があります。そして、金融機関もシステムやプロセスによって、可能な限りのリスク軽減を徹底する責任があります。そうすることによって、すべての関係者がブロックチェーンを始めとする最新のテクノロジーを利用して、金融犯罪に自発的に立ち向かうことが可能になるでしょう。

絶えず変化する課題：インタビュー

大規模な課題：多国籍銀行と金融犯罪の防止

金融犯罪に取り組むうえでの解決策は、コンプライアンス機能を拡大させることではありません。予算や人員の追加によってできることには限りがあります。解決策となるのは、従業員を教育するとともに、ITセキュリティからサイバー犯罪まで、より幅広い課題においてリスクを特定できるようにするよう権限を付与することです。UBS スイス AGの取締役会メンバーで、コンプライアンスおよびオペレーショナルリスク管理の責任者であるMartin Peter氏に、犯罪に対処するうえで大手銀行が直面している特有の課題について意見をうかがいました。

KPMG：UBSで20年以上にわたり、法務やコンプライアンスの職務を歴任されていますが、この間にこれらの機能が果たす責任はどのように進化してきたのでしょうか。

Peter氏：当初、コンプライアンスは法務の一部でした。時の経過とともに、法や規制の期待や変化が増えるにつれて、コンプライアンス機能は進化し、規模や重要性を増しています。コンプライアンスは本来、本人確認とマネーロンダリング対策の課題に主眼を置くもので、顧客アドバイザーに対する教育やアドバイスが重視されていました。プライベートバンキングではよりきめ細かいアドバイスが必要とされており、コーポレートバンキングでもある程度そうでした。現在では、規制要件を確認し、コンプライアンスリスクの適切な把握・責任者の指定・管理を徹底する、独立した管理機能へと進化を遂げています。私たちは第2の防衛ライン機能として、事業を管理し、事業の指針を提示し、意思決定に関して鋭い質問を投げかけています。かつては主に金融犯罪対策に従事していましたが、現在ははるかに広範囲にわたる重要テーマや、幅広い活動に取り組んでいます。マネーロンダリング対策から、適格性審査、クロスボーダー業務、利益相反、サイバー犯罪に対抗するITセキュリティおよび予防策、規制上の報告まで、テーマは多岐にわたります。このことが従業員に求められる一連のスキルに影響を与えています。そのため、従業員のプロフィールは法律のバックグラウンドを持つ人、銀行業務のスペシャリスト、ITやデータマイニングの専門家などさまざまです。コンプライアンス部門では、非常に専門性の高い従業員がますます増えています。大手銀行では、ゼネラリストのコンプライアンスオフィサーは減る一方です。

私たちは第2の防衛ライン機能として、事業を管理し、事業の指針を提示し、意思決定に関して鋭い質問を投げかけています

（UBS スイス AGの取締役会のメンバーで、コンプライアンスおよびオペレーショナルリスク管理部門の責任者であるMartin Peter氏）

KPMG：私たちは銀行の金融犯罪対策の有効性に直接影響を与えるのは、経営幹部、従業員の態度、企業文化だと考えています。この考えはあなたの意見と一致するものでしょうか。

Peter氏：最も重要なのは経営トップの基本姿勢です。経営トップは業務遂行のための原則や実践方法を設定し、銀行のリスク許容度、コンプライアンスおよびマネーロンダリング対策、経済制裁などのプログラムを定義します。また、適切なリソースおよび支援を提供することによって、基準や規則を確実に実践できるようにします。これにはコンプライアンス上の過失への適切な対応も含まれます。受け入れ可能な過失許容性、一貫性のある介入、失敗を恐れる文化の回避の間で、慎重にバランスを取ることが求められます。私はコンプライアンス要件を遵守する行動は報われるべきだと考えています。例えば、顧客アドバイザーがインシデントを報告するというコンプライアンス要件に従った結果、顧客を失うことになったとしてもです。

KPMG：ITツールへの投資は効率化推進の鍵なのでしょうか。それとも、さらに重要な要素が他にあるのでしょうか。

Peter氏：質問の意図は、より自動化された効率的なツールを活用してマネーロンダリングに関連する状況をより多く検出しているか、ということでしょうか。これを実現するには、明示的にプログラムしなくても学習する能力を備えたツールを使う以外にないと思います。近年、継続的なリアルタイムの監視に向け大きく前進しています。しかし、こうした監視手法によって、資金洗浄防止法への抵触が検出されたケースはほとんどありません。規制当局や銀行業界は当然のことながら、現状以上の成果を見込んでいたはずです。この結果はパラメータが不適切に設定されているか、送られてきた資金が実際にクリーンで、厳格な前提条件を満たしているかのどちらかということになります。

KPMG：従業員の意識を高めて、新たな犯罪シナリオについて警戒・認識できるようにするために、どのようなことを行っているのでしょうか。

Peter氏：コンプライアンス部門の従業員は非常に専門性が高く、さまざまな作業部会に参加していることを考慮し、こうした知識をコンプライアンス部門内や事業全体で共有するために、継続的な集合研修やウェブベースの研修を提供しています。顧客アドバイザーへの継続的な訓練や教育も実施しています。さらに、仮想通貨を始めとする新たなテーマに関するファクトシートと質疑応答を継続的にアップデートして利用できるようにしたり、経営幹部や他のリスク機能と定期的なミーティングを実施して新たな動向や課題について議論したりしています。その一方で、交流の場で特定の対象グループに対し、具体的な警告やブリーフィングも実施しています。

KPMG：銀行の商品およびサービスの中で、最大のリスクをもたらしていると考えているものはどれでしょうか。

Peter氏：AMLの観点から言えば、取引レベルか、商品レベルか、透明性が低い可能性のあるカウンターパーティーレベルかを問わず、顧客にかかわる活動ということになります。例えば、物理的な現金取引、貴金属取引、仮想通貨はより高いリスクをもたらします。そしてもちろん、特定の地域や国、または注意を要する産業に属する顧客は、スイス人の給与振込口座所有者とは大きく異なるリスク特性を持っています。

KPMG：スイスの銀行がマネーロンダリングやテロ資金供与への対策で直面している課題とは何でしょうか。

Peter氏：スイスでは外国人顧客の多額の資産を管理しているため、こうした顧客との関係を継続的に監視するための取組みを強化しています。スイスはブラックマネーの温床という悪いイメージに依然として悩まされており、海外の規制当局はスイスの銀行に引き続き目を光らせています。最終的に銀行は、特定の国または産業に属する顧客を監視するための追加費用を明確にせざるを得ないでしょう。

KPMG：マネーロンダリングの可能性がある取引を突きとめる場合、顧客書類またはKYC書類を把握することや、支払いフローを分析することは難しいことでしょうか。

Peter氏：顧客アドバイザーが適用するデューデリジェンスの手法は、KYC書類の基盤となるもので、特定の顧客関係の潜在的リスクに関連しています。さまざまなデューデリジェンスのレベルには顧客窓口のほか、公的に利用可能なソース、ならびに必要に応じて信頼性のあるサードパーティーのソースの追加的なスクリーニングも含まれることがあります。これらは取引レベルでのさらなる監視措置によって補完されますが、顧客行動、金額、取引パターンに依拠するため、困難を極める場合があります。あらゆる手法を組み合わせて、贈収賄やテロを含む、マネーロンダリングが疑われる事例を防止・探知することを目指しています。

KPMG：当社が実施した調査で、組織内の金融犯罪対策で改善したい点を尋ねたところ、回答者の大半が人材または予算の増加を希望していました。UBSであなたが希望することはどのようなことでしょうか。

Peter氏：人材や予算の増加は魅力的に思えるかもしれませんが、私たちの主要な目標はやはり、あらゆるレベルの事業との相互作用やプログラムの設定を通じ、状況に応じて潜在的なコンプライアンスリスクの正確な把握・管理・責任者の指定ができるよう万全を期すことにあります。この目標に向かい、そしてこれを支えるために、より多くのリソースまたは予算を適切な部門に配分することは目標達成の1つの手段であることは間違いありません。銀行業界はリソース（プログラムの適切な機能を支える人材または高度なツール）を手にしているにもかかわらず、スイスのさまざまな監督機関からの時として異なる期待、マネーロンダリングの報告制度における環境の変化、解釈の余地を残した適用法令といった課題に直面しています。

なお、当局と民間セクターとの情報交換の改善も望まれます。一部の政府機関は、私たちよりも詳細な顧客情報を保有しているとみられています。しかし、厳格化を増す情報保護規定が立ちはだかっているため、この希望がかなうことはまずないでしょう。

編集・発行

KPMGファイナンシャルサービス・ジャパン

フィンテック推進支援室

fintech@jp.kpmg.com

この文書はKPMGドイツが2018年6月に発行した「Clarity on Financial Crime in Banking」の「EVER-CHANGING CHALLENGES: KEY FINDING 2」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。