DORA 対応に向けた 10の重点課題

デジタル・オペレーショナル・
レジリエンスの要素統合

pwc

リスクの捉え方を変革する

はじめに

本レポートは、PwCフランスが2022年11月24日に開催した会合「DORA規制：概要、主な課題、実績からのフィードバック（DORA Regulation: overview, main challenges and experience feedback）」の内容を取りまとめたものである。

特に、本会合における以下の講演者に謝意を表したい。

Céline Samain（AXAのHead of Operational & Information Risk, Internal Control and Standards Management）
Caroline Cerval（LCH SAのChief Operating Officer, Head of Operations and Technology）

また本レポートは、DORAに関する以下の専門家各位の協力を得て作成された。

Romain Camus（PwCフランス、銀行セクターのテクノロジーリスクパートナー）
Karine Pariente（PwCフランス、保険セクターのテクノロジーリスクパートナー）
Jamal Basrire（PwCフランス、サイバーインテリジェンス担当パートナー）

PwCフランスの、以下の規制専門家にも謝意を表したい。

Monique Tavares（銀行セクターのディレクター）
Olfa Ehrhard（保険セクターのシニアマネージャー）

目次

DORAの全体像

「DORA」として一般的に知られているデジタル・オペレーショナル・レジリエンス法（Digital Operational Resilience Act）は、デジタル・ビジネス・トランスフォーメーションの進展や、サイバーリスクやITリスクへのエクスポージャーの拡大を受け、金融セクターのデジタル・オペレーショナル・レジリエンスを強化することを目的に策定された欧州の規制[1]である。2023年1月16日に発効され、2025年1月17日からEU加盟国に適用される予定である。

レジリエンスは、金融機関と金融セクター全体の課題である。サイバー攻撃の増加や金融システムがの相互関連性を踏まえると、レジリエンスの重要性は著しく増している。PwCフランスのパートナーであるKarine Parienteは、次のように説明している。「銀行や保険会社は、増加し続ける社内外のデータにアクセスする必要がある。また、情報通信技術（ICT：information and communications technology）のサードパーティへの依存度が高まっている。欧州の規制当局は、このような発展に伴い生じるリスクが効果的に管理されるよう、対策を講じることを考えている」

また、PwCフランスのパートナーであるJamal Basrireは「デジタルテクノロジー活用の進展に伴い、サイバーリスクのエクスポージャーが拡大し、金融セクターが不安定化する要因となり得る」とコメントしている。

これまで、規制当局や監督当局は、金融のレジリエンスの強化に重点を置いてきた。一方、DORAの規制は、デジタル・オペレーショナル・レジリエンスの枠組みを確立するものである。この枠組みにおいて、全ての金融機関は、ICTに関連するあらゆる種類の混乱や脅威に耐え、対応し、回復できるようにすることが求められる。

オペレーショナル・レジリエンスの考え方は、オペレーショナルリスク管理に対するアプローチを、リスクの予防と損失の軽減に焦点を当てたものから、より広範で、主体的なアプローチに移行する必要性を強調している。この考え方は、インシデントは必ず発生することを前提としており、インシデントへの対応を事前に整備して、重要な中核事業活動やサービスの継続性を確保するというものである。

これを踏まえ、DORA規制においては、金融機関が遵守を求められる5つの主要な柱を特定し、その要件を提案している。具体的には、以下のとおりである。

- ICTリスク管理態勢
- ICTインシデント管理（関係当局へのより効率化された報告を含む）
- デジタル・オペレーショナル・レジリエンスの検証
- ICTサードパーティリスク管理（EU域内で活動しているクリティカルなICTサードパーティ・サービスプロバイダーの監視体制を含む）
- サイバー脅威に関する情報共有

1 Regulation（EU）2022/2554 of the European Parliament and of the Council of December 14, 2022 on the digital operational resilience of the financial sector

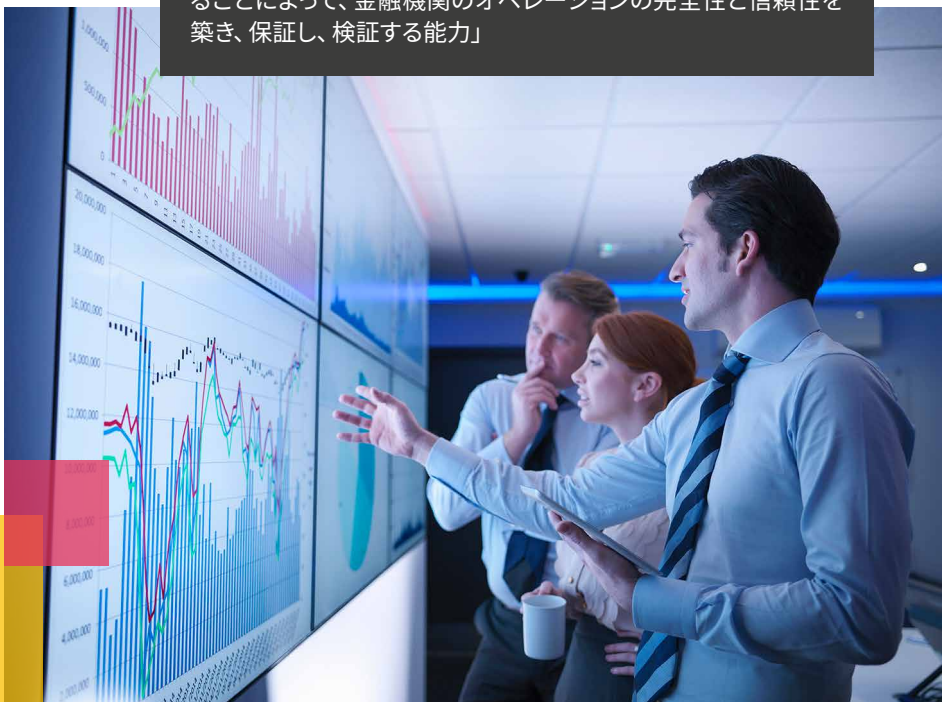
DORA規制は、EUで初めて、金融機関のデジタル・オペレーショナル・レジリエンスに係る具体的かつ包括的な枠組みを1つに法制化したものである。

デジタル・オペレーショナル・レジリエンスの5つの柱

1. ICTリスク管理態勢
2. ICT関連インシデントの管理・分類・報告
3. デジタル・オペレーショナル・レジリエンス検証
4. ICTサードパーティリスク管理・監視体制
5. サイバー脅威に関する情報共有

DORAでは、デジタル・オペレーショナル・レジリエンスを以下のとおり定義している。

「中断時も含め、金融機関が利用し、また金融サービスとその品質の継続的な提供をサポートするネットワークや情報システムのセキュリティに対応するために必要なあらゆる種類のICT関連のケイパビリティを、直接的またはICTサードパーティ・サービスプロバイダーが提供するサービスの利用を通じて間接的に確保することによって、金融機関のオペレーションの完全性と信頼性を築き、保証し、検証する能力」



DORAの適用対象

DORAは、EUに拠点を置くさまざまな金融機関の他、金融機関に対しICTサービスを提供するサービスプロバイダーにも適用される。

金融機関

- 信用機関
- 決済機関
- 電子マネー機関
- 投資会社
- 運用会社・オルタナティブ投資ファンドマネージャー
- 口座情報サービスプロバイダーまたは銀行口座アグリゲーター
- 暗号資産市場規制（Markets in Crypto-Assets Regulation）に基づいて承認された暗号資産サービスプロバイダー

- 保険・再保険会社
- 保険仲立人、再保険仲立人、付帯保険仲立人
- 職域年金基金

（注）適用される規制要件は、規模に基づき決定される。

- 清算機関
- 証券集中保管機関
- 取引所とレポジトリ
- データ報告サービスプロバイダー
- 信用格付機関、重要な金融指標の運営機関
- クラウドファンディング・サービスプロバイダー

ICTサードパーティ・サービスプロバイダー

1人以上の内外のユーザーに対し、ICTシステムを通じて継続的にデジタル・データサービスを提供している企業。サービスとしてのハードウェアの他、ハードウェアサービス（ハードウェアプロバイダーによるソフトウェアまたはファームウェアの更新のためのテクニカルサポートの提供を含む）を含み、従来のアナログ電話サービスを除く。

ICTサードパーティリスク管理態勢

ICTサービスプロバイダーとは、以下に該当するものをいう。

- 親会社、または親会社の子会社もしくは支店に対し、主にICTサービスを提供するグループ内のICTサービスプロバイダー
- ICTサービスを他の金融機関に提供する金融機関
- 決済サービス・エコシステムの参加者

監視体制

「重要（critical）」として指定されたICTサービスプロバイダー、ただし以下を除く。

- ICTサービスを他の金融機関に提供する金融機関
- ICTグループ内のサービスプロバイダー
- EUのバンキングシステムの業務を支援するために構築された監視体制の対象となるICTサードパーティ・サービスプロバイダー

課題1 DORAのアプローチの理解

DORAは、監督当局がこれまで公表した従来のガイドラインで定める原則と整合する内容になっているが、金融機関に対し大きな影響を与えるものである。DORAの具体的な要件を理解する前に、まず、監督当局の期待が高い点を認識する必要がある。

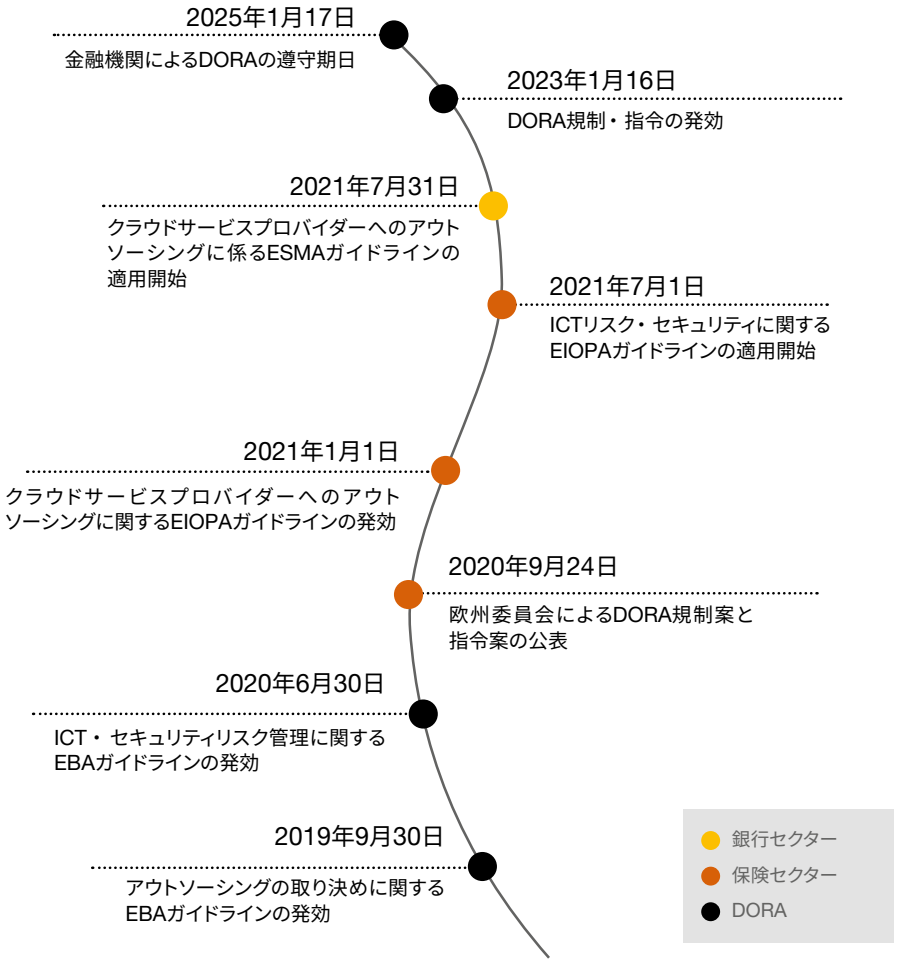
銀行に対する現行の規制には、アウトソーシング、ICT・セキュリティリスク管理に係る欧州銀行監督局のガイドラインの要件の他、クラウドサービスプロバイダーへのアウトソーシングに係る欧州証券市場監督局のガイドラインが含まれる。また、保険会社に固有のガイドラインとしては、例えば、クラウドサービスプロバイダーへのアウトソーシングに係る欧州保険職域ガイドラインなど、銀行に適用される要件と類似する要件が定められている。

しかし、DORAにより、リスク管理やデジタル・オペレーショナル・レジリエンスに関連する要件が1つの規制に集約されることになる。

「現行の規制の枠組みは分断化され、均質ではなかった。さまざまなセクター別の規制が存在しているが、規制の水準が異なり、また程度の差はあれ、限定的であった。このため、欧州の各国間で規制が重複し、解釈が異なる状況にあり、その結果、コンプライアンスコストが非常に高かかった。

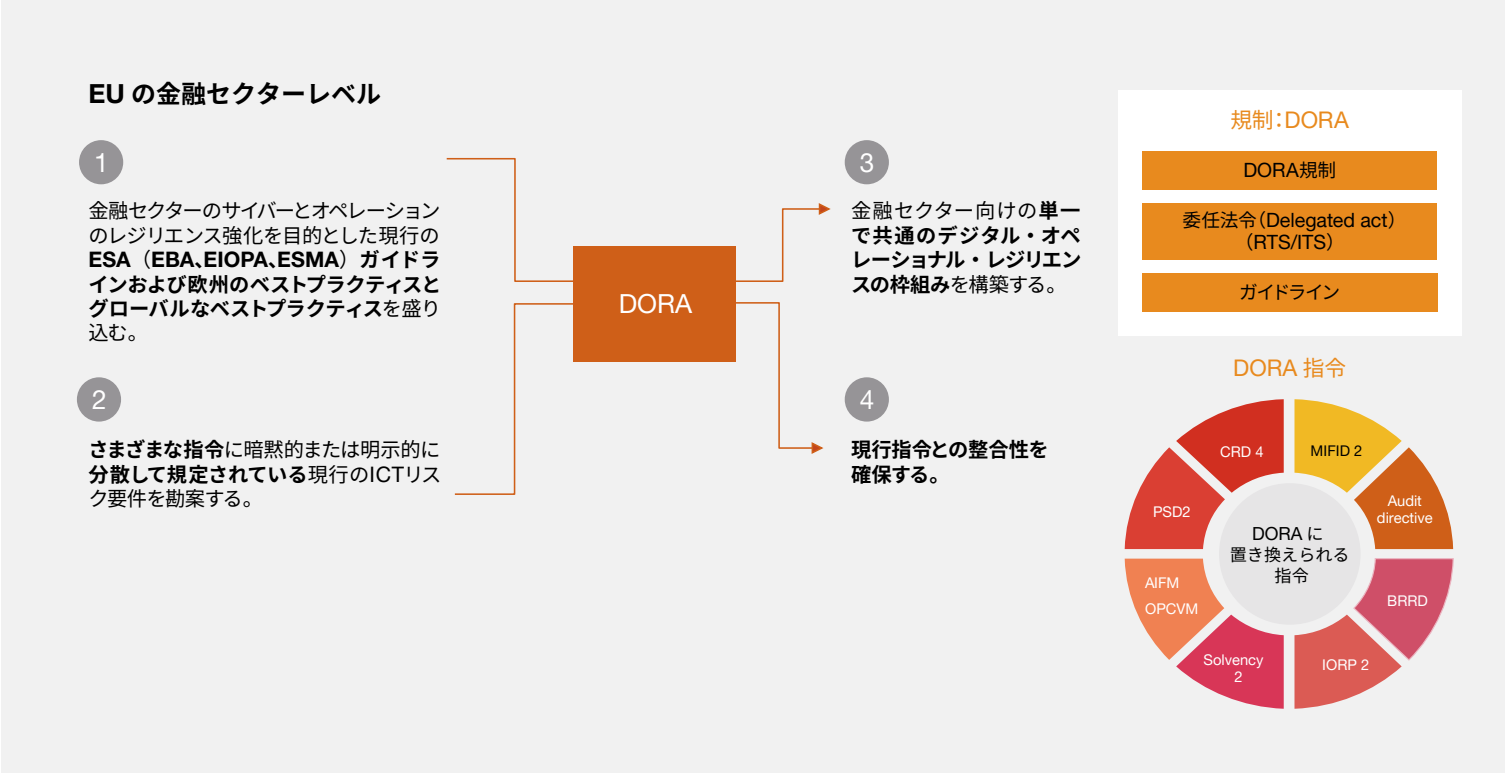
DORAは、単一の規制の枠組みを構築し、欧州の監督当局が公表したこれまでの全てのガイドラインに加え、サイバーレジリエンスやICTリスク管理における欧州のベストプラクティスとグローバルなベストプラクティスが盛り込まれている。この新たな規制により、ITリスク、サイバーセキュリティ、サードパーティ管理、事業継続に関して、既存の全ての要件の整合性がある程度確保される」とPwCフランスのパートナーのKarine Parienteは説明している。

ICTリスク管理に関するセクター別要件の段階的な強化と調和



DORA規制に加えて、当規制の要件に従ったものにするために、関連指令[2]も改訂される。例えば、信用機関は、これまで決済サービス指令2（Payment Service Directive2）に基づき報告することが要求されていたオペレーション上または決済上のセキュリティインシデントを、DORAに基づき報告することになる。DORAは2023年1月16日に施行され、2025年1月17日までに加盟国の導入が求められる。

調和のとれた一貫性のある規制枠組みの構築



2 Directive（EU）2022/2556 of the European Parliament and of the Council of December 14, 2022

一般的に、DORAの規制アプローチは、以下の3つの主要な原則に基づいている。

1. コンバージェンス（差異の解消）

欧州で初めて、監督当局が連携して、ICTに関連するリスクに対応し、オペレーション上およびIT上の課題を解決するための基本原則と主要な要素を定めている。

「DORAが共通の要件と調整されたスケジュールを提供することによって、当社が事業を展開している各国の異なる要件に準拠する必要がなくなることを期待している」とAXAのOperational & Information Risk, Internal Control and Standards ManagementのCéline Samainはコメントしている。

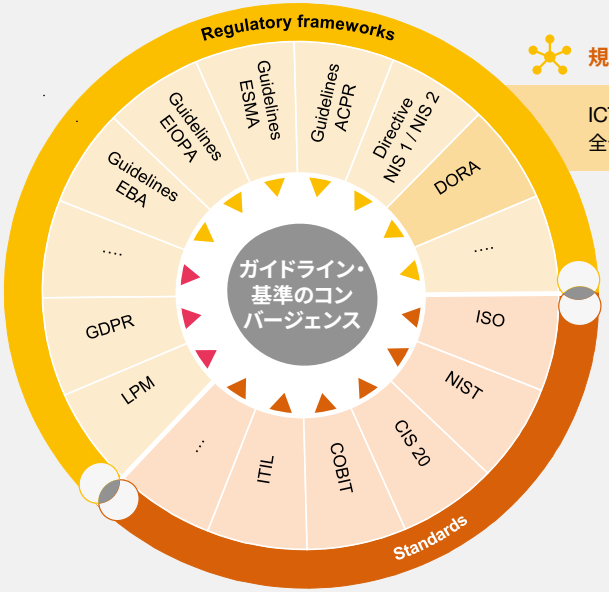
ただし、一から体制を整備するのではなく、サードパーティリスク管理、事業継続性、サイバーセキュリティの分野を問わず、さまざまな規制枠組みの中で既に実施してきた取り組みを活用する必要がある。

同氏は次のようにも述べている。

「例えば、ここ数年、当社では、サイバーセキュリティ戦略を積極的に推進しており、大規模な数々の投資を行い、業務のセキュリティ強化のため内部統制を運用してきた。また、直近では、戦略を変更し、アタックサーフェスの対象範囲の拡大を図った」

これを実現するためには、組織とリスク管理アプローチの統一が必要となる。この点について、PwCフランスのパートナーのJamal Basrireは**「コンバージェンスの原則を満たすために、企業は、リスク管理手法を統一し、組織でよく見られる、IT、サイバー、事業継続、サードパーティリスク管理間のサイロ化の問題に対処していかなければならない」**と指摘している。

規制要件のコンバージェンスと既に実施された取り組みの活用



規制動向：ICTとセキュリティリスク管理に係る規制枠組みのコンバージェンス・調和

ICTおよびセキュリティリスク管理に関するEBA、EIOPA、ESMAガイダンスをカバーし金融セクター全体のICT・セキュリティリスク管理を強化、調和させるための要件による規制フレームワーク

コンバージェンスの主な目的

- 適用される規制要件を単一の枠組みに集約することにより、**コンプライアンスを簡素化する**。
- コンプライアンス態勢の取り組みを最適化するため、**強固で包括的かつコンプライアンスが確保された変革体制を構築する**。
- 規制当局や経営主体への**報告を容易にする**。
- 新たな規制枠組みとの相乗効果を特定し、追加的な新しい要件への**遵守を期待する**。

組織を複雑化することなく、レジリエンスを強化するためには、金融機関は、これまでの取り組みを活用できることが前提となる。PwCフランスのパートナーのRomain Camusは**「この原則を適用した結果、最終的には、金融機関にとって、コンプライアンスが簡素化されることを期待している」**とコメントしている。

2. 比例性

比例性の原則の下で、金融機関は、その規模や全体的なリスクプロファイルの他、サービス、活動・業務の内容、範囲・複雑性を考慮して、要求事項を実施しなければならない。

PwCフランスのパートナーのJamal Basrireは**「DORAが広範囲に及ぶことを踏まえると、取り組みと対応の深度を、金融機関の事業と金融機関が晒されているリスクに合わせて調整することが重要である」**と述べている。

3.「セキュリティ・バイ・デザイン」の推進

最後に、このアプローチは「セキュリティ・バイ・デザイン」という一般的な原則（製品やサービスの設計から顧客への販売、またライフサイクル全体を通じて、セキュリティを設計し、かつ、この問題を金融機関のガバナンスの中心に据えることを求める考え）を組み込んでいる。当原則を充足するために、ICTサプライチェーンの全体的なビジョンを策定し、レジリエンスを評価することが必要となる。

課題2 一刻も早い着手

このEUの新規制の遵守に向け、金融機関に2年間の準備期間が与えられている。これは一見十分と思われる期間であるが、すでに取り組みに着手している金融機関は、対応すべき作業は膨大であることを実感している。

LCH SAのChief Operating Officerであり、Head of Operations and TechnologyのCaroline Cervalは次のようにコメントしている。

「2022年初頭からDORAへの対応を開始した。まず、サービスの提供を受けているサードパーティのリスクプロファイルを把握・分類しなければならなかった。次に、情報システム、プロセス、データ間の相互依存関係を整理した。リスク管理は私たちの業務の中核であるが、サイバーのエリアについては、ビジネスラインと全てのマネジメント層による変更管理とサイバーリスクの割り当てが必要となる」

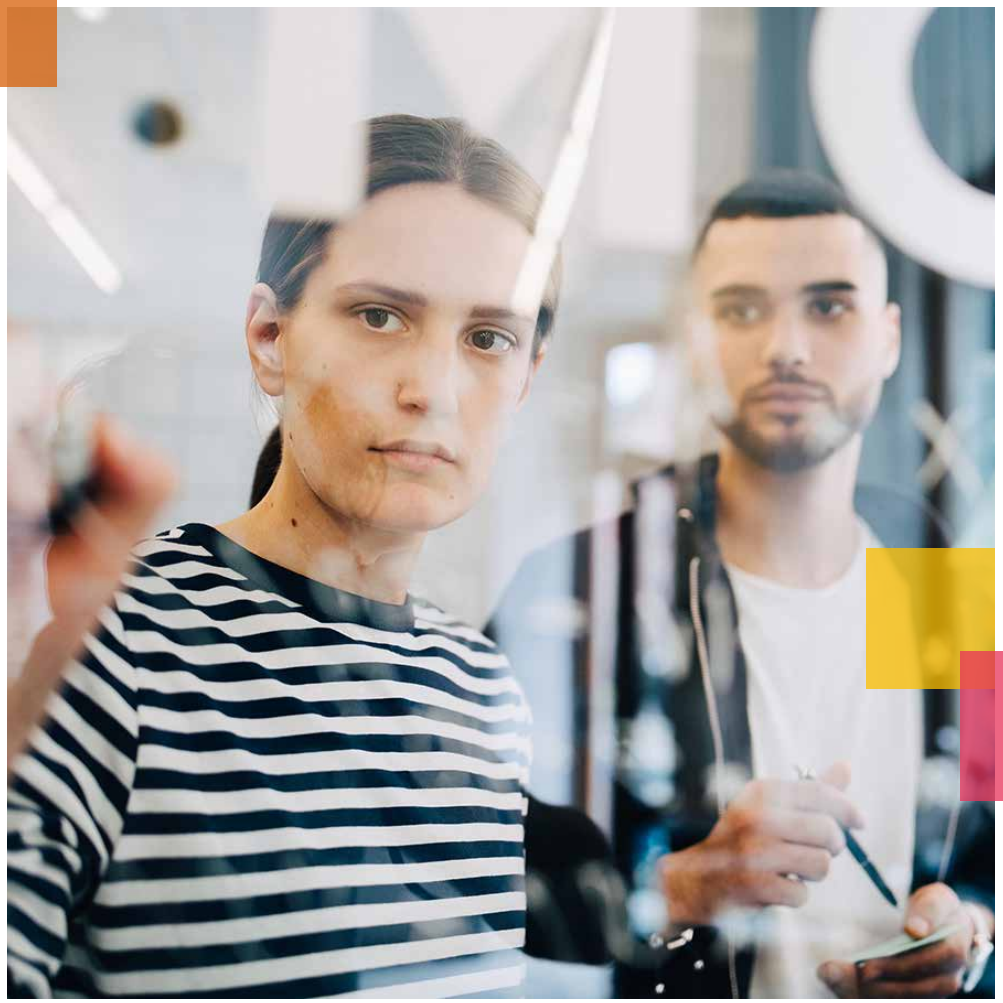
2025年1月17日までにDORAに準拠するための計画策定には、規制技術基準（RTS：regulatory technical standards）を考慮しなければならない。当基準は、DORAの要件をさらに具体的に定め、追加の規定を導入している。RTSは2つのバッチで策定され、それぞれ遅くとも2024年1月17日と2024年7月17日までに欧州委員会による採択のために提出されなければならない。本レポートの作成時点で、RTSの最初のバッチの草案が市中協議のために公表された。次のバッチは、2023年11月か12月となる見込みである。AXAのOperational & Information Risk, Internal Control and Standards ManagementのCéline Samainは**「詳細な規制（RTS/ITS）の公表後、導入までには1年もない。これは技術的リスク対応の観点からは非常に短い時間である」**と指摘している。

2025年1月17日から適用開始

マイルストーン

ESAは、以下に記載の内容について、それぞれに掲げる期限までに、RTS/ITSを欧州委員会に提出しなければならない。

- **2024年1月17日まで**：① ICTリスク管理ツール、手法、プロセス、方針、② 簡素化された枠組み、③ インシデントおよびサイバー脅威の分類、④ ICTサービスプロバイダーの情報レジストリの標準的テンプレート（ICTサービスの利用に係る全ての契約上の取り決めに共通する情報を含む）
- **2024年7月17日まで**：① 通知レポートの内容とテンプレート、②高度なテスト、③ICTサービスのアウトソーシング、④ 重要なICTサービスプロバイダーの監視



レベル2の規制の最終版の公表前に、遵守に向けた取り組みを推進しなければならない。PwCフランスのパートナーのKarine Parienteは**「これには不確実性が伴うが、最終版の規制の多くの要素は既に分かっており、現行の規制における取り組みを参考にすることができる」**と述べている。

ロードマップの主要なステップは既に判明している。PwCフランスのパートナーのJamal Basrireは次のように説明している。

「金融機関が実施している体制とDORA規制において定められている期待とのギャップ分析を実施することはできる。企業の状況分析（特にデジタル化、事業展開先、外部のパートナー、サプライヤー、顧客との間の相互関連性を踏まえたビジネスモデルの進展）とそのリスクに基づき対応策を策定する必要がある。

また、比例性の原則に従って、企業の状況に合わせて、体制を適応させることになる」

また、このような取り組みを実施することで、強力なガバナンスが整備されていることの確認もできる。

課題3 ガバナンスの適応と経営陣の意識向上

ガバナンスは、新たな規制における中心的な課題である。その目的は、DORAが構築した新たな枠組みであるデジタル・オペレーショナル・レジリエンスを確保するための包括的なリスクガバナンスを整備することである。PwCフランスのパートナーであるJamal Basrireは次のとおり説明している。

「IT、サイバー、サードパーティ、事業継承のリスク管理間に存在するであろうサイロ化を解消する必要がある。これは多くの金融機関にとって、変革である。最近まで、リスクを管理する唯一の方法は事業継続計画であった。しかし、2022年からは、ランサムウェアの攻撃が、情報システムに多大な混乱を招く恐れのある主要な脅威の1つとして捉えられるようになった。それにもかかわらず、多くの金融機関の事業継続計画では、サイバーリスクは考慮されていない」

実務の観点からは、金融機関は、ICT関連リスクが実効的かつ慎重に管理されていることを評価し「高い水準の」デジタル・オペレーショナル・レジリエンスを実現できるようなガバナンスルールを整備するか、引き続き整備を進めていく必要がある。

規制当局は、ICTリスク管理・モニタリング態勢の実施責任を経営陣が担うこととしている。特に、以下の責任を担う。

- デジタル・ビジネス・レジリエンスの定義（ICTのリスク許容度の設定）
- ICT事業継続方針、ICT対応・復旧計画の承認、監視、定期的見直し
- ICT監査計画とICT監査の承認・検証
- （少なくとも）重大なICTインシデント、それらの影響、実施された是正措置の確認
- サードパーティが提供するICTサービスの利用に関する方針の承認と見直し、新規契約書または既存契約書の変更の確認
- 必要なリソースの配分

したがって、リスク管理・ガバナンス体制を見直し、3つのディフェンスライン・モデルを維持しつつ、デジタル・オペレーショナル・レジリエンスの枠組みを組み込み、特に既に整備されている体制を再検討する必要がある。また、金融機関は、IT管理機能、統制機能、内部監査機能が適切に分離されていることを確保しなければならない。

また、ICTリスク管理態勢を文書化し、少なくとも年1回検証しなければならない。

経営陣は必要なスキルを備えていなければならない。

これを実現するためには、意識向上の取り組みと研修も実施する必要がある。AXAのOperational & Information Risk, Internal Control and Standards ManagementのCéline Samainは**「ITリスクガバナンスは、CIOの責任の一部であり、IT資産に関する知識や陳腐化管理といった幅広いテーマが、リスク委員会または経営委員会の間で議論されている」**としている。しかし、脅威が急速に進化しているため、その責任を果たすためには、経営陣のスキルを強化する必要があり、特にサイバーリスクとITリスクに関する最新の知識を維持することが期待されている。

課題4 ステークホルダーの関与

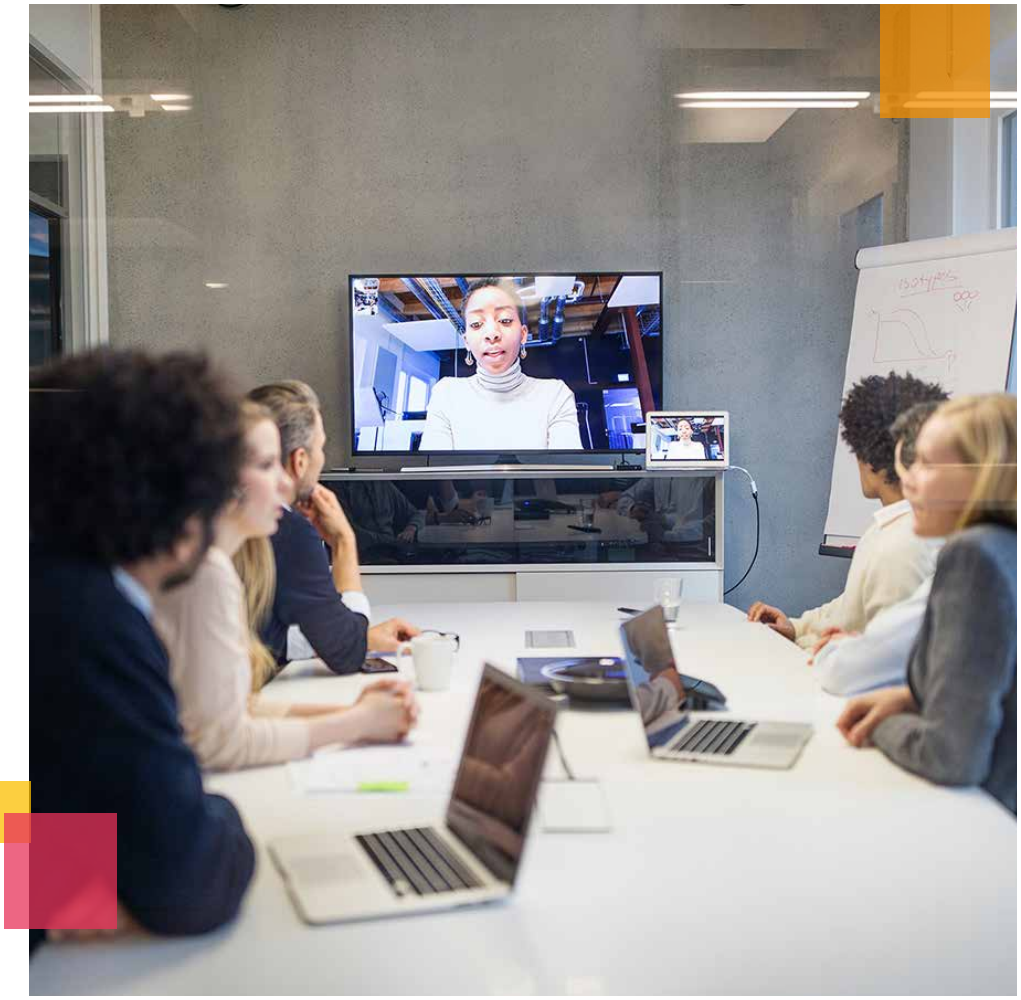
まず、留意すべき点は、DORAはサイバーセキュリティのみに関連するものではないという点である。確かに、DORAの要件は、サイバーリスクやネットワーク・情報システムのセキュリティを取り扱っているが、それ以外のサードパーティリスク、事業継続性、ITリスクなどの分野にも関連する。PwCフランスのパートナーのJamal Basrireは**「オペレーショナルレジリエンスは、ITセキュリティにとどまらず、より広範な問題を包含するものである。DORAへの遵守の責任主体は、IT部門であると考えるべきではない。これは、より幅広いリスク関連の問題でもある」**と述べている。

実際、これは戦略的なテーマでもあり、戦略面での課題として、会社の上層部の支援の下、役員が主体となって対応すべきものである。ITやサイバー担当の管理職に加えて、他の多くの部門に対してDORAに対する意識を高め、プロジェクトに関与させなければならない。何よりも重要なのは、経営陣の関与である。

「主要なステークホルダー間の意見・対応を調整することが重要な課題である。これには、ガバナンスの強化が求められ、上層部の関与がなくては実現できない」と、PwCフランスのパートナーのKarine Parienteは指摘する。

オペレーショナルリスクの課題であるため、多くの金融機関は、通常、リスク管理部門またはコンプライアンス部門を所管部門とし、IT部門、セキュリティマネージャー、事業継続担当チームの他、外部との業務契約書については購買部門と法務部門からの強力な支援を受けるという体制を整備している。

DORAの遵守には、事業部門、リスク管理部門、IT部門、オペレーション部門、サイバーセキュリティといったあらゆるステークホルダーの関与が必須である。



課題5 現行の規制と今後の規制との関連性の整理

前述したとおり、遵守までの期間が短いため、規制遵守対応や、今後公表予定の規制技術基準・実施技術基準の草案の動向の把握に直ちに着手しなければならない。

PwCフランスのパートナーのJamal Basrireは**「DORAは、全体的な規制動向、特に新たなNIS 2指令[3]との関連性において、検討することが重要である」**と述べている。

実際、DORAの規制は、新たなNIS 2指令（2022年11月28日にEUにおいて採択されたNIS指令の改正版）と関連する。同指令は、2023年1月16日に発効され、最低限の措置を組み込んだ水平的枠組みを構築することによって、EU全体で高度かつ共通の水準のサイバーセキュリティを確保することを目的とする。DORA規制は、サイバーセキュリティリスク管理措置やインシデント報告要件に関する金融セクター向けの「lex専門」の規制である。

NIS 2指令の適用範囲が、指令の対象となる活動のセクターに属する全ての中規模・大規模企業（「不可欠な事業体（essential entities）および重要な事業体（significant entities）」）に拡大され、基幹セクターの事業者（OES：operators of essential services）として指定された事業体のみが適用対象ではないため、両規制を読む必要がある。NIS 2指令は2024年10月17日までに各加盟国において法制化されなければならない。

この取り組みに加えて、サイバーセキュリティに関するその他の現行の規制または進行中の法制化とどのように関連するかも検討する必要がある。まず初めに、2019年以降に施行されたサイバーセキュリティ規制について検討する。NIS 2指令に基づき、要求される重要な（critical and important）事業体の特定の区分について、事業体が開発した、または外部から購入した特定のICTプロダクト、サービスまたはプロセスを認証することが求められる。

次に重要なのは、2022年9月15日に公表されたサイバーレジリエンス法案である。同法案は、デジタル関連のプロダクトやサービスの開発または販売に適用されるサイバーセキュリティ要件について定めている。

これらの取り組みの全ては、ICT資産のセキュリティ強化だけではなく、ICTサプライチェーン全体のセキュリティを強化することを目的としている。

3 Directive（EU）2022/2555 of the European Parliament and of the Council of December 14, 2022

課題6 レジリエンスの視点を取り入れた、現在の取り組みの活用

ITリスク管理、サイバーセキュリティやサードパーティ管理に関する現行の規制に既に懸命に取り組んできた、成熟度の高い金融機関の場合、取り組むべきことはより少ない。

そのような金融機関にとっての重点課題は、デジタル・オペレーショナル・レジリエンス戦略に基づき、DORAに関する包括的なビジョンを設定し、要件の影響度を検討することである。取り組みの難易度は、リスク管理をレジリエンスという観点からどの程度検討してきたか、またガバナンス機関においてレジリエンスがどの程度考慮されているかに拠る。PwCフランスのパートナーのJamal Basirieは**「従来のリスク管理に対する分断化・サイロ化されたアプローチによって、各エリアの成熟度を高めることはできた。しかし、DORAが構築した新たな枠組みに対しては、このアプローチは有効ではない」**と指摘している。

したがって、規制のコンバージェンスによって、既に実現した取り組みを活用することができるのであれば**「DORAの遵守対応にあたっては、合理化・共通化を図り、横断的アプローチを適用する必要がある」**と同氏は述べている。

一方、より成熟度の低い金融機関にとって、新たな規制は真の課題となり得る。LCH SAのChief Operating Officer, Head of Operations and TechnologyであるCaroline Cervalは次のように述べた。

「ITリスク管理の強化には、当社のガバナンスの変革とディフェンスラインの強化が求められる。また、戦略と経営管理の視点から、リスクを俯瞰的に捉え、モニタリングし、報告体制を整備しなければならない」

組織全体でDORAを実施する際には、横断的アプローチを適用する必要がある。

課題7 サイバー脅威に関する情報共有の推進

「インシデント報告の申請件数が増えている」と、AXAのHead of Operational & Information Risk, Internal Control and Standards ManagementのCéline Samainは述べている。また、同氏は**「システム面で問題が発生した際に即座に対応し、脅威の再発防止のためにその内容を十分に理解するというインシデント報告の目的を達成するには、報告に一貫性を持たせなければならない」**ともコメントしている。

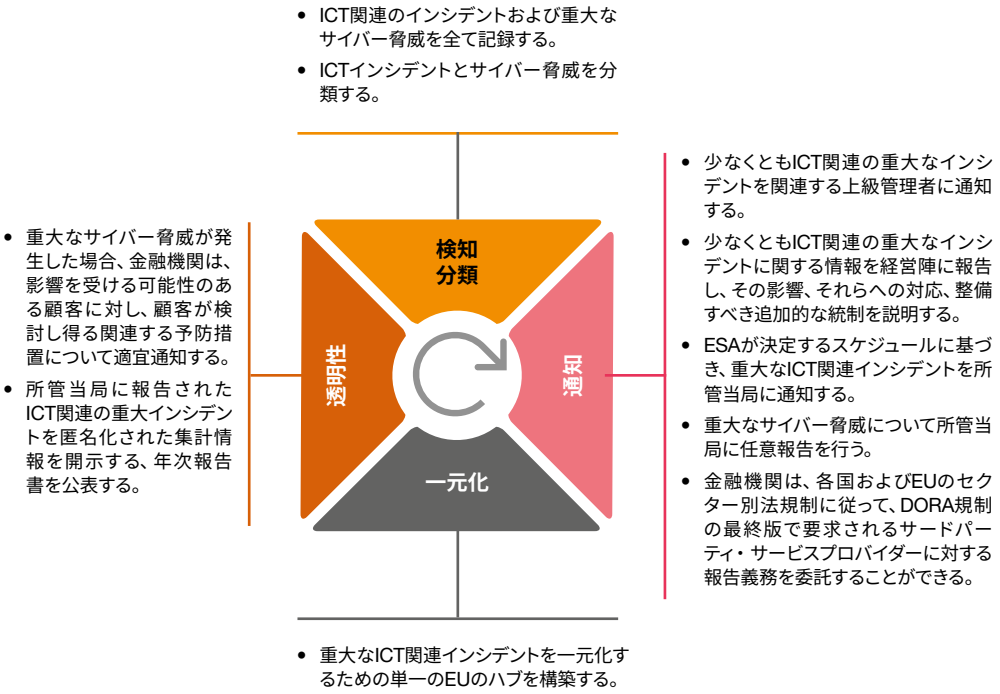
これは、DORA規制の目的の1つである。具体的には、DORAは、重大なICTインシデントの必須報告のプロセスを共通化・簡素化するとともに、重大なサイバー脅威に関する任意報告を導入することを目指している。DORAのレベル2の要件として、インシデントの重大性を判定するにあたっての閾値や、所管当局へのインシデントの報告期限が定められている。

また、DORA規制は、金融機関間の情報共有を推進するための規定をいくつか定めている。

Romain Camusは次のように指摘している。**「全てのステークホルダーの利益のために、そして、全ての者のレジリエンスを向上させるために、重大な脅威を共有する必要がある。ただし、これは機密データであり、このような情報共有のためには、安全で信頼性のある仕組みを構築し、金融機関、サードパーティ、当局などの間で締結された情報共有の取り決めを当局に通知しなければならない」**

DORAは、金融機関間の情報共有を可能にするため、一定の基準の下で運営することを要求している。これに加えて、このような報告を一元的に推進するために、各金融機関を規制するそれぞれの監督当局が連携することが求められる。このような一元化された仕組みの構築によって、ICT関連の重大なインシデントに対応するEUのハブを1つにすることができる。

ICT関連のインシデントの管理・分類・報告



課題8 ICTサービスプロバイダーとの関係を見直す機会の捕捉

最近、金融機関がIT業務を委託しているケースが増大している。しかし、契約関係に不均衡が生じることがある。例えば、小規模銀行や小規模金融機関が、大手のサービスプロバイダーと取引する場合、交渉の余地がほとんどない場合がある。DORAのおかげで、このような状況は改善し得る。PwCフランスのパートナーのRomain Camusは**「本規制は、重要なICTサービスプロバイダーの監督のための、金融機関にとって非常に明確で、安心できる法的枠組みを確立するものである」**と述べている。

終了条項や出口戦略を含む標準的な契約条項の導入が、ICTサービスプロバイダーとの契約の標準化につながるはずである。LCH SAのChief Operating Officer, Head of Operations and TechnologyであるCaroline Cervalは**「DORAは、当社が大きく依存しているサードパーティの管理について、共通の枠組みを整備するのに役立つだろう」**とコメントしている。また、AXA のHead of Operational & Information Risk, Internal Control and Standards ManagementのCéline Samainは**「DORAによって、サービスプロバイダーにする当社の要請の正当性が高まる」**と述べている。

同氏はまた**「レジリエンスが効果的であるためには、業務関係の両当事者がこれを実現しなければならず、バリューチェーン全体を強化しなければならない」**とコメントしている。

これにより、バリューチェーン全体が強化され、金融セクターの全体的なレジリエンスの向上につながる。**「サードパーティリスクに係る新しい要件により、プロバイダーは顧客に対して情報を提供することが求められるようになる。また、監督当局にもフォローアップの権限が与えられる。サービスプロバイダーが期待に応えなければ、顧客はプロバイダーを変えなければならない。そのため、コンプライアンスは競争上の優位性をもたらすものとなり、市場のあらゆるプロバイダーとの関係の全体的な改善につながる」**とRomain Camusは指摘する。

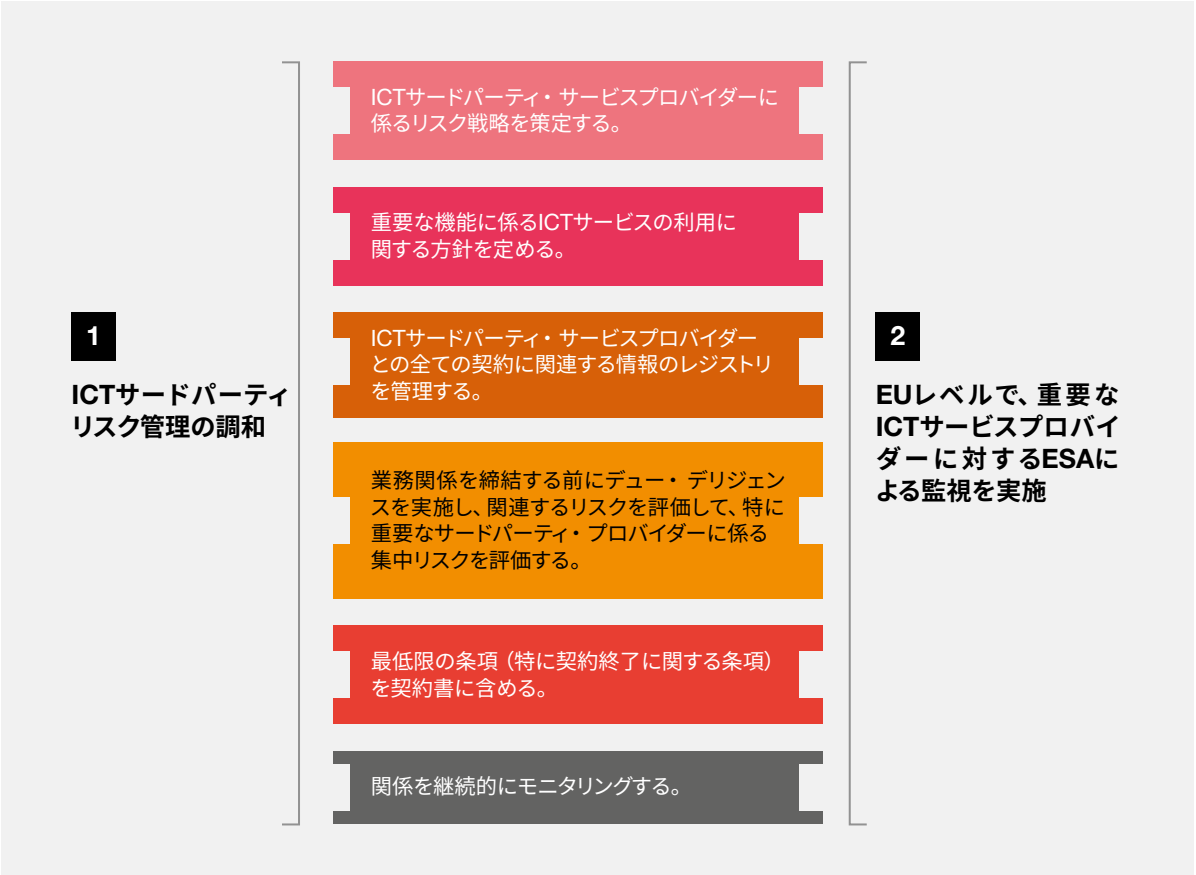
最後に、ICTサービスプロバイダーが金融セクターの特殊性を検討したうえで、より適応したサービスを提供し、さらにはより変化に対応することが期待される。

サードパーティの管理にあたっては、比例性の原則も重要である。Céline Samainは次のように説明している。

「当社は、さまざまな基準に基づき、それぞれのサービスプロバイダーに対する取り組みを決定しなければならない。例えば、当社には、ディシジョンツリーに基づき設計されたプロバイダー向けの統制の枠組みが整備されている。当枠組みは、データ、コネクション、関係の深度等を踏まえて、今後変更し、強化され、更には簡素化される可能性もある」

金融機関により適応した重要なICTプロバイダーの監視体制を整備する。

ICTサードパーティ・サービスプロバイダーに関連するリスク管理

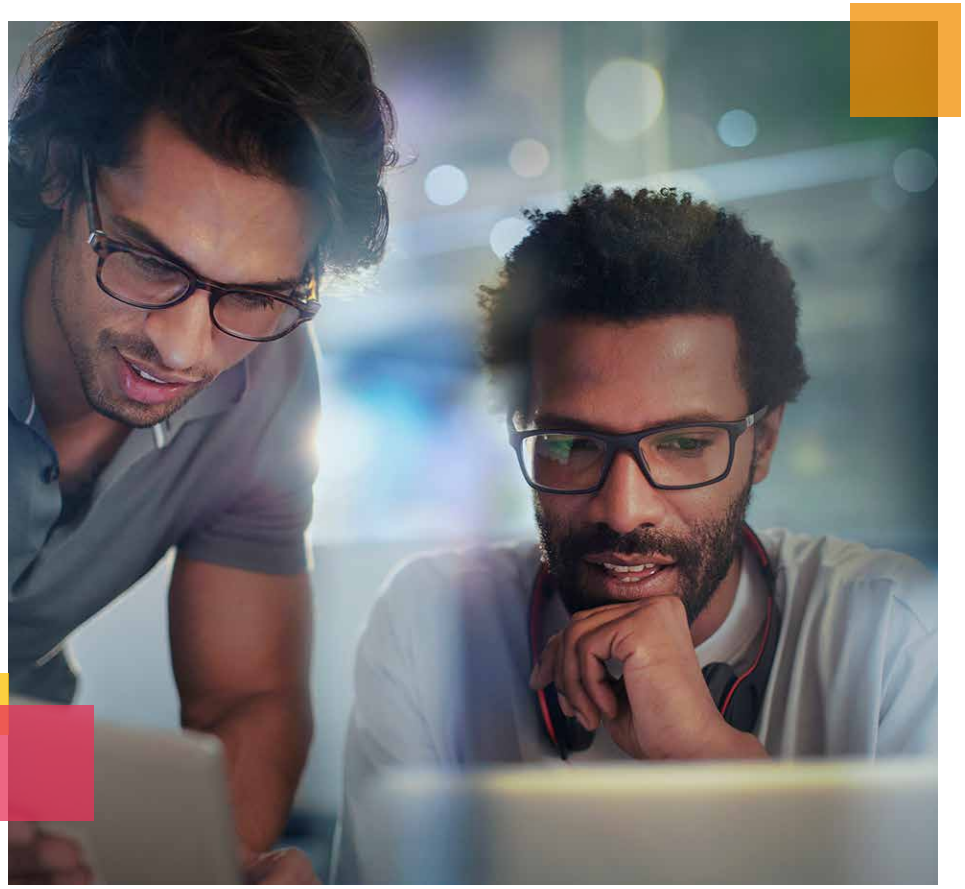


課題9 レジリエンスケイパビリティの定期的なテスト

ギャップや不具合の可能性を把握するために、デジタル・オペレーショナル・レジリエンスのケイパビリティを、実際の状況でテストしなければならない。**「DORAは、テストプログラムの整備と、現在既に実施している水準を上回るような、運用面での対策を講じる必要があることを強調している。そのため、危機シミュレーション下の確固たるテストを確立しなければならない」**とPwCフランスのパートナーのKarine Parienteは説明する。

実際、零細企業を除き、金融機関は、堅牢で包括的なデジタル・オペレーショナル・レジリエンスのテストプログラムを策定、維持、検証しなければならない。総合的なデジタル・オペレーショナル・レジリエンス戦略の不可欠な構成要素として、また、ICTリスク管理態勢の一部として、インシデントまたはサイバー攻撃が発生した場合、ICT機能とセキュリティを定期的に評価すべきである。

DORA規制では、金融機関の規模、活動、リスクプロファイルに応じて、レジリエンステストを実施するための要件を比例的に適用することが求められている。したがって、小規模企業を含む全ての金融機関が自社のICTツールやシステムをテストしなければならない場合であっても、重要かつサイバー成熟度が高くあるべきものとして監督当局に指定されたもののみが、高度なテスト（脅威ベースのペネトレーションテスト、Threat-Led Penetration Testing：TLPT）を実施することが要求される。「重要かつサイバー成熟度が高い」の指定は、規制で定められ、今後のレベル2規制で明確化される基準に基づく。**「これは、EUレベルまたは各国でシステミックリスクをもたらし得る金融機関に影響を与える。これらの金融機関は、3年ごとに、独立した立場にある内部または外部の者に依頼して、重要な機能をテストしなければならない」**と、PwCフランスのパートナーのJamal Basrireは説明する。また、テストプログラムは、リスクアプローチに基づき策定すべきである。



高度なテストを実施するための新たな枠組みには、重要なメリットがある。また、EUレベルで相互認識があれば、テストに有用である。一方で、テストを実施するためには、準備と調整の面でより大きな労力が求められる。

金融機関は、重要な機能に関与するICTサービスプロバイダーの対象を拡大し、強化されたテストに関して契約に盛り込む必要があることに留意しなければならない。

最後に、動的なプログラムの一環として実施する定期的なテストは、オペレーショナルレジリエンスに焦点を当てた強固なカルチャーを醸成することをお伝えする。

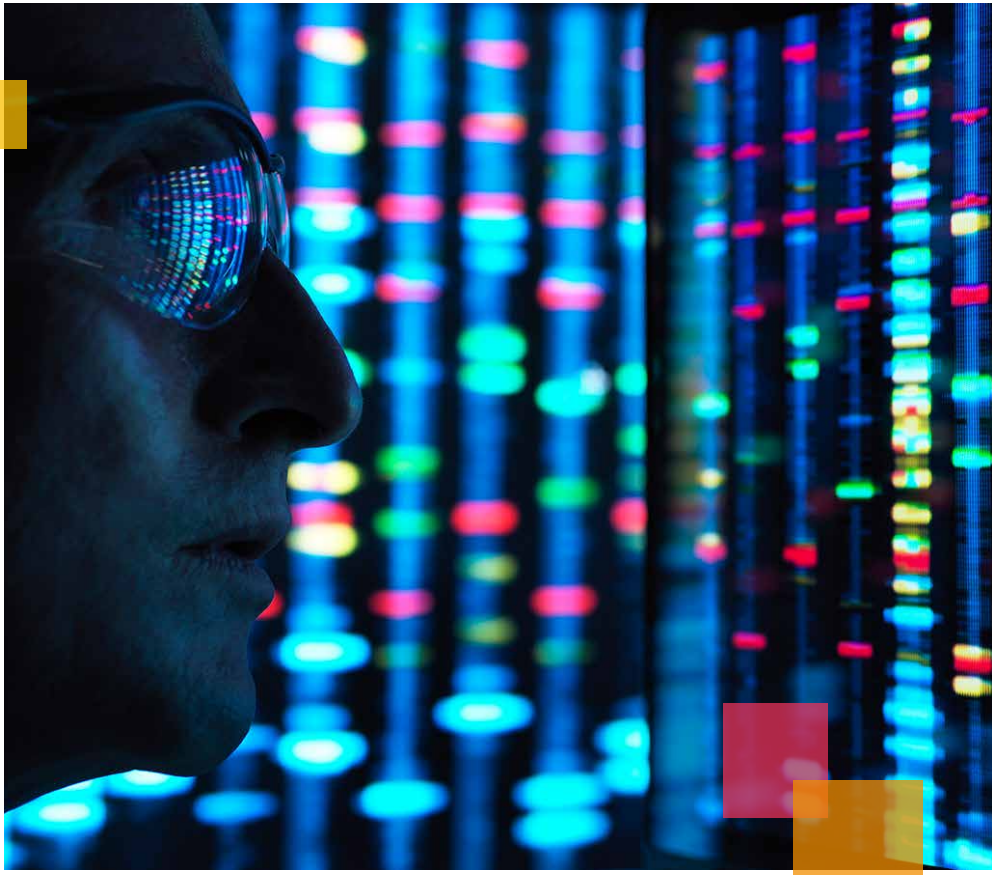
デジタル・オペレーショナル・レジリエンスのテスト

（零細企業以外の金融機関の場合）ICTリスク管理態勢の不可欠な要素として、デジタル・オペレーショナル・レジリエンス・テストプログラムを策定、維持、検証することが求められる。

デジタル・オペレーショナル・レジリエンス・テストプログラム

- 比例性の原則を考慮して、リスクアプローチに基づき設定される。
- 全ての重要なICTシステムおよびアプリケーションについて、少なくとも年1回、独立した内部または外部の者によるテストを実施する。
- さまざまな評価、テスト、手法、実務、ツールを統合する。
- 所管当局が指定した特定の金融機関について、脅威ベースのペネトレーションテストを少なくとも3年ごとに実施する。

課題10 真のデジタル・オペレーショナル・レジリエンスのカルチャーの醸成



デジタル・オペレーショナル・レジリエンスの原則は、まさにDORAの指針といえる。金融システムの頑健性を確保するためには、金融機関はあらゆる類型のICT関連インシデントに対応できることが求められる。

「多くの企業がサイバーリスク管理を改善している。これは、出発点としては非常にポジティブな傾向であるが、DORAの新しい枠組みであるデジタル・オペレーショナル・レジリエンスに対応するためには十分ではない。今後は、DORAの全体像を把握し、オペレーショナルレジリエンスのカルチャーを醸成するために機能を共通化し、機能横断的に取り組まなければならない」とPwCフランスのパートナーであるJamal Basrieは指摘している。

DORAを導入するあたっては、新たなレジリエンスカルチャーへの移行が課題となる。最近経験したCOVID-19やサイバーインシデントからの教訓を活かし、一部の金融機関は顧客の期待に合わせて自社のカルチャーを発展させてきている。

AXAのOperational & Information Risk, Internal Control and Standards ManagementのCéline Samainは、次のように説明している。

「オペレーショナルレジリエンスのカルチャーは、顧客にとって非常に重要である。当社は、それを強化するための組織を設置し、重要なリソース、クライシスガバナンス、事業継続計画の分析を実施している。これらを対象に定期的にテストを実施しているが、社会不安やパンデミック、戦争といった最近の数多くの事象によっても、それらの有効性が証明されている」

一方で、他の金融機関にとっては依然として重大な課題である。

デジタル・オペレーショナル・レジリエンスのカルチャーを醸成しなければならない。

略語

EBA（European Banking Authority）：欧州銀行監督機構

EIOPA（European Insurance and Occupational Pensions Authority）：欧州保険・企業年金監督機構

ESA（European Supervisory Authorities）：欧州監督機構

ESMA（European Securities and Markets Authority）：欧州証券市場監督機構

AIF（Alternative Investment Fund）：オルタナティブ投資ファンド

MiCA（Markets in Crypto-Assets）：「MiCA」として知られる暗号資産に関する欧州の規制案

NIS（Network and Information Security）：ネットワークおよび情報システムのセキュリティに関連する、ネットワークおよび情報セキュリティ指令

BCP（Business Continuity Plan）：事業継続計画

OES（Operators of essential services）：基幹セクターの事業者

ICT（Information and Communication Technologies）：情報通信技術

TLPT（Threat-Led Penetration Testing）：脅威ベースのペネトレーションテスト

おわりに

地政学的な不確実性が増し、サイバー攻撃が増加している中、金融セクターではデジタル化が推進されている。DORA規制は、EUで、金融機関および金融機関にICTサービスを提供しているサービスプロバイダーに対し、デジタル・オペレーショナル・レジリエンスに関する単一かつ共通の枠組みを構築するものである。

提起された戦略上・業務上の課題は複雑であり、リスク管理部門、コンプライアンス部門、IT部門、セキュリティ部門、購買部門といった複数の内部機能の関与が求められ、特に適切なガバナンスの構築には、経営陣の強力なサポートが必須である。

本レポートにおいて特定した「重点課題」は、早期にコンプライアンス対応するための指針となる。これらはDORA導入のベンチマークとなるものであるが、DORAが金融機関にとって追加の規制上の制約となることは避ける必要がある。むしろ、IT、サイバーセキュリティ、事業の継続性、サードパーティ関連のリスクに対するオペレーショナルレジリエンスを強化することによって、DORAが市場における他社との差別化機会となるために、各金融機関の状況に応じて、これらの重点課題を適合させていく必要がある。

日本のお問い合わせ先

PwC Japanグループ

www.pwc.com/jp/ja/contact.html

辻田 弘志（Hiroshi Tsujita）
PwC Japan有限責任監査法人
パートナー
ガバナンス・リスク・コンプライアンス・アドバイザリー部

山本 直樹（Naoki Yamamoto）
PwCコンサルティング合同会社
パートナー
リスクコンサルティング

www.pwc.com/jp

本報告書は、PwCメンバーファームが2023年12月に発行した『DORA The 10 key challenges of a successful compliance journey』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
オリジナル（英語版）はこちらからダウンロードできます。 https: //www.pwc.com/gx/en/issues/risk-regulation/DORA-10-key-challenges-of-a-successful-compliance-journey.html

日本語版発刊年月：2024年4月　　管理番号：I202403-09