KPMG

金融機関における テクノロジーと サイバーリスク管理

ビジネスを守るリスク・ガバナンス フレームワークとは?

著者紹介

Charlie Jacco
Principal, KPMG LLP
Cyber Security Services

セキュリティ戦略、トランスフォーメーション、デジタルアイデンティティ、エンタープライズアイデンティティとアクセス管理、サイバー制御、サイバーリスク管理等の情報セキュリティを専門とする。セキュリティソリューションの設計・導入をはじめとする多くの経験を持ち、テクノロジーとリスク管理のバックグラウンドを有す。また、FS-ISACのアフィリエイト会員として、金融サービス業界の経営者とともにサイバーセキュリティやサイバーリスクの様々なテーマに取り組む。

Vivek Mehta
Partner, KPMG LLP
Emerging Technology Risk

グローバルに多角化した金融機関、ブローカーディーラー、プライムブローカー、リテールバンキング、プライベートエクイティ、資産運用会社等、フォーチュントップ100の金融機関を15年以上支援。専門分野はITリスク管理であり、特にIT規制管理、ITガバナンス・戦略、ITコントロール施策の導入を得意とする。

Steve Barlock
Principal, KPMG LLP
Cyber Security Services

ビジネスとテクノロジー分野のシニアリーダーであり、25年以上にわたるIT戦略・導入の経験を有す。テクノロジー関連の幅広いバックグラウンドを持ち、直近15年間で情報セキュリティ、およびビジネス現場への施策導入に深く携わり、専門性を高めた。

KPMG

サイバーセキュリティリスクは、単にIT部門にまかせるのではなく、ビジネスの観点から取り組むべきである

進化し続けるデジタル時代において、技術は日々変化し、金融機関が曝されるリスクはさらに大きく、規制当局の監視はさらに厳しくなっているように感じられます。しかし、これは戦略的投資によって価値を創出する新しい機会でもあります。金融機関は、サイバーセキュリティを基本要素とする、全体的なオペレーショナルリスクのフレームワークによって、その最も重要な資産をサイバー脅威から守りながら競争上の優位性を築くことができます。

金融機関は、規制・基準を順守しながら、新しい収益源を追求し、経済混乱期にはビジネスを支える役割も担っており、その中にどの程度のリスクエクスポージャーを受け入れられるかを決めなければなりません。包括的なコーポレートガバナンスモデルを構築するにあたり、これを最初に評価し文書化する必要があります。

この新しいモデルにより、各企業はリスクエクスポージャーを最小限に抑えつつ機会を最大化する上で必要な、知見・展望・見通しを得ることができます。

ビジネスに立ちはだかるサイバーリスクの増大に対し、どのように取り組んでいますか？　KPMGは、相互に関連する3つのことから始めるべきであると考えます。

1. 第1と第2のディフェンスラインを分離する。

サイバーリスクの特定・軽減・管理には、第1のディフェンスラインとして最高情報セキュリティ責任者（CISO）の目線、第2のディフェンスラインとしてサイバーリスク管理責任者の目線が必要です。これによりサイバーリスク管理責任者の地位は上がり、企業の意思決定プロセスの中心に加わることになります。このアプローチによって、サイバーリスク関連のすべての役割と責任をオペレーショナルリスクの大きなフレームワークの一部として明確に定義するガバナンスモデルが確立されます（5ページ 組織構造図参照）。これはまた、責任の所在を明確に定義したリスクポリシーによってビジネスを成功に導くべく、第1と第2のディフェンスラインに権限を与えるものです。

この方式は、チェックとバランスから成るシステムを確立し、ここ数年に登場した従来型のITリスク管理機能とは一線を画すものです。

「サイバーセキュリティは、企業が適時に戦略的なリスクベースの意思決定を下せるように、基本的なオペレーショナルリスク管理のフレームワークに組み込まれるべきものです。そうすることで、CISOは過度にリスク回避的でビジネスを阻害する存在であると見られることなく、企業を守ることに専念できます」

— Charlie Jacco, Principal, KPMG LLP

2. 企業全体のサイバーリスクアペタイトとリスクの閾値を定義する。

これは、新しい包括的なオペレーショナルリスクのフレームワークの土台となり、第2のディフェンスラインのサイバーリスク管理責任者がこのプロセスで責任を負います。全体的なサイバーセキュリティポリシーや、アジャイル的な「レビューアンドチャレンジ」手続に役立つ重要リスク指標はこのプロセスで示されます。これは、規制要件を満たすためだけではなく、金融機関が積極的にリスクエクスポージャーに対応・管理するための指標に基づくビジネス主導の手法です。

3. データ分析などの自動ツールを利用して、関連のリスクトリガーを特定・対応することによってビジネスをサポートする。

様々なリスク要因が最終利益、業績、ブランドに影響を与える前に、それらを特定することが目的です。これは、全体的なオペレーショナルリスクと密接に連動し、特にサイバーセキュリティに関連する重要リスク指標を導入することにより達成されます。このような自動ツールの導入により、組織のリスクアペタイトに照らして、潜在的リスクエクスポージャーを測定・監視し、管理することができます。

KPMG

第1と第2のディフェンスライン：CISOとサイバーリスク管理

多くの金融機関はこれまでサイバーセキュリティの課題をIT部門に任せきり、組織を潜在的な脅威や攻撃から守るニッチな業務と見なしてきました。このような体制においては、CISOは新しいビジネス機会の妨害者として位置づけられることも少なからずありました。

サイバーセキュリティリスクとオペレーショナルリスク管理全体を分離することにより、金融機関はビジネス目標を達成する上で不可欠な洞察力を失います。

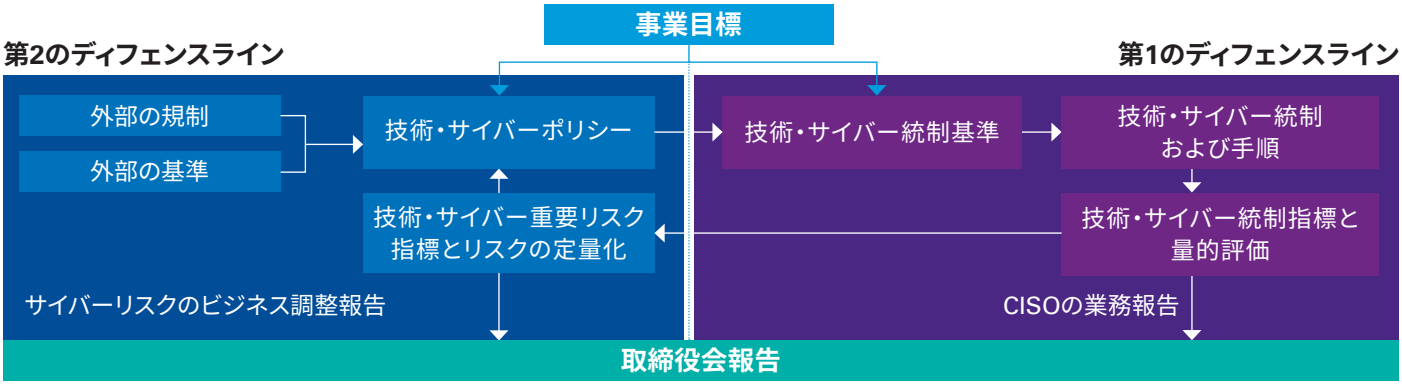
KPMGは、企業全体でリスクを管理するための徹底したフレームワークを構想しています。このフレームワークでは、サイバーセキュリティリスクはオペレーショナルリスクのフレームワークの重要な要素の1つと考えられます。担当責任者と監督者の役割を明確に定義し、新しいガバナンスモデルを作り、重要な指標を確立することから始まります。

サイバーリスクの監督者と担当責任者の役割に関して、金融機関には2つのディフェンスラインが必要です。それは、CISOとサイバーリスク管理責任者です。CISOは、これまでは組織がリスクアペタイトの境界を押し広げることに対する阻害勢力と見られることもありましたが、最高情報責任者（CIO）直属の第1のディフェンスラインとなるべきです。

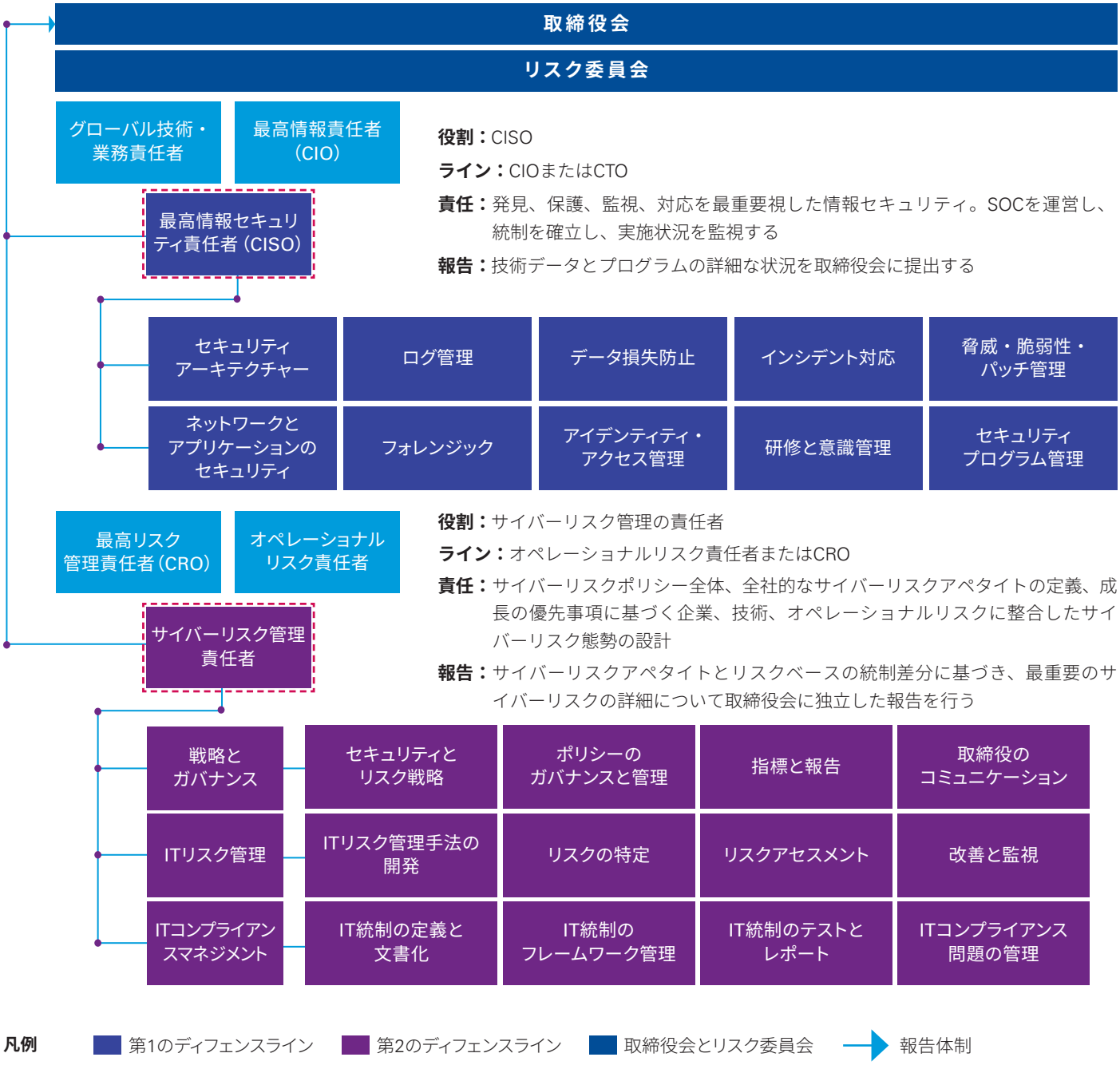
CISOが第1と第2どちらのディフェンスラインになるべきかについては、各業界で曖昧な点がありましたが、KPMGとしては、この任務は第1のディフェンスラインに属すると見ています。CISOは、技術・コントロール施策の導入のみならず、企業の安全を確保する上で必要な最前線の技術リスクフレームワークに特有のオペレーショナル指標にも重点を置くべきです。**しかし、CISOは全体的なサイバーリスク管理とサイバーセキュリティポリシーの責任者になるべきではありません。それらに対するオーナーシップを持たないことで、CISOはイノベーションの妨げとはならずに、企業を保護することに集中できます。**また、CISOは取締役会へ継続的に報告をしますが、（脅威と脆弱性の管理等の）重要な機能の短・長期動向、（アイデンティティ・アクセス管理等の）現行の重要な取り組み状況、サイバー研修・啓発の進捗状況等、情報セキュリティ全体にかかわるオペレーショナル指標に的を絞るべきです。

サイバーリスク管理責任者は、オペレーショナルリスク管理責任者直属の第2のディフェンスラインとなります。この職務は、企業全体のオペレーショナルリスクとサイバーリスクの管理に責任を負うのが理想です。この新しい第2のディフェンスラインは、リスク執行委員会とともに、サイバーリスクの全体的なガバナンスに重点を置き、その考え方を組織トップレベルのオペレーショナルリスク管理機能に組み込む必要があります。これに伴い、サイバーセキュリティポリシーと重要リスク指標の元となるリスクアペタイト宣言が確立されます。そして、企業は自身のリスクアペタイトとリスクエクスポージャーに基づき、賢明な意思決定が下せるようになります。**これにより、サイバーセキュリティリスクが、技術主導ではなくビジネス主導の検討事項になり、企業ははるかに速いペースで、新しい収益源の追求に取り組めるようになります。**

効果的にビジネスを成功に導くには、第1と第2のディフェンスライン全体でリスクと統制のタクソノミを定義し、それに準拠する必要があります。サイバーリスク管理組織は、事業目標と外部の規制・基準に合致したポリシー等に対して責任を持つべきです。そしてCISOの組織は、それらのポリシー等の土台である統制目標に責任を持ちます。



未来の理想的なディフェンスラインモデル



金融機関にとって、サイバーセキュリティリスク管理フレームワークを効果的に機能させるには、サイバーリスクを巡るCISOおよびサイバーリスク管理責任者またはオペレーショナルリスク責任者の具体的な役割を明確に示すガバナンスモデルが有益です。規制当局が金融機関内の「レビューアンドチャレンジ」プロセスに対して基準を定めている場合もありますが、このモデルでは義務づけられた独立したリスク監視機能も提供されます。

明確に定義されたこれら2つのディフェンスラインにより、金融機関は、技術とビジネスが急速に変化する中で効果的にサイバーリスクを管理し軽減することができます。CISOはビジネス上の意思決定に基づいて企業を保護するために必要な重大セキュリティ課題に専念することができ、サイバーリスク管理責任者は金融機関全体のオペレーショナルリスクを360度見渡すことができます。

サイバーリスクアペタイトとエクスポージャー：独立した監視機能と規制コンプライアンス

現在の規制環境（特に金融サービス業界のサイバーリスク管理の規制環境）では、規制順守とコンプライアンスの強化が求められます。米国では、NISTサイバーセキュリティフレームワーク（CSF）等、サイバー攻撃を検知・防御・対応する測定可能な方法といった業界基準を規制当局が推進しています。

二重の規制

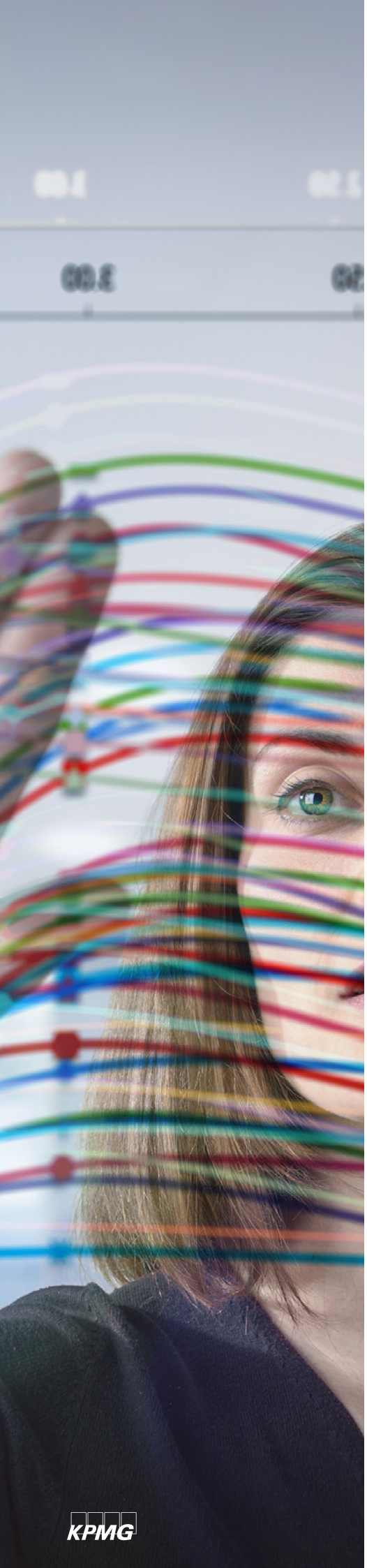
しかし、特に金融業界では、複数の規制機関がそれぞれの要件を押し進め、NIST CSFに緩やかに沿った規制もあれば、異なる優先順位で基本方針を推進する規制もあります。通貨監督庁とFRBのサイバーセキュリティ関連の方針と報告要件は、一見同じようで異なります。一方、証券取引委員会も最近この分野に踏み込み、さらに州政府までもが参入し、ニューヨーク州金融サービス局が独自のサイバーセキュリティ規制を打ち出しました。企業は、規制要件を満たすための証拠収集に時間と労力を費やす中で、どのように悪意のある攻撃者から自らを守ることに集中していけばよいのでしょうか。

現実的な方策

企業のオペレーショナルリスクとサイバーリスク管理フレームワークは、コンプライアンスを重視すると同時に、企業のサイバーリスクアペタイトを基準とした全体的なポリシーを作成することが重要です。それは規制当局の「最低限」の要件以上にリスク回避的であるべきです。

「ポリシーを策定したら、第1と第2のディフェンスラインにわたる適切なガバナンスと指標を作成し、有効性を測定してフレームワークを規制要件と対応付ける必要があります。それにより、要件が満たされていることを証明しやすくなります」

— Steve Barlock, Principal, KPMG LLP



第1、第2のディフェンスラインの行動計画

この全体的なフレームワークを実際に適用するには、第1と第2のディフェンスラインが適切なデータを積み重ね、取締役会と規制機関に向けて適切な指標を作成する必要があります。第1のディフェンスラインでは次のことを行うべきです。

- 業務プロセスを情報資産とデータ分類に関連付けるとともに、資産とデータの責任所在を定義するプロセス、および資産のインベントリをメンテナンスする。
- 第2のディフェンスラインが管理するポリシーと基準を、第1のディフェンスラインが管理する統制活動とコントロール施策導入に結び付け、企業のリスク統制自己評価を組み込み、CISOと取締役会にオペレーショナル指標を提供する、統制タクソノミを作成する。
- 脆弱性スキャン、侵入テスト、レッドチーム演習、回復性テスト等のシナリオテストを定期的に実施し、委託先のリスク管理アセスメントの結果を反映する。

最も重要なことは、規制コンプライアンス上の理由からであれ、(望ましくは) 全社的なサイバーリスク態勢を向上させるためであれ、**第2のディフェンスラインのリスク委員会と最高リスク管理責任者 (CRO) のもと、オペレーショナルリスク管理機能の一部として、独立したリスク管理監視機能を設け、**以下を行うことです。

- NIST CSFなどの業界標準のサイバーセキュリティフレームワークに基づいて、企業のサイバーリスクアペタイト、そして独立したリスク管理フレームワークを定義し、独立した評価を実行する。
- 第1のディフェンスラインから蓄積してきたデータに基づきつつ、新しいサイバーリスクアペタイト宣言にも合わせた限度、閾値、重要リスク指標を定義する。
- リスク委員会と取締役会に報告するための、リスクの定量化、シナリオライブラリー、サイバーバリューアットリスク (CVaR) を含む新しい指標と測定モデルを作成する。
- 第1ライン向けに、ビジネス、技術リスク、情報セキュリティを含むアドバイザリーサービスを提供する。
- サイバーセキュリティ対策を組み込んだ標準的な業務オペレーショナルリスク全般にわたり、ストレステストを実施する。

このようなガバナンスフレームワークは、サイバーリスク管理と技術リスクを全体的なリスクフレームワークに統合しています。これにより、事業部門や経営層が企業全体のリスクアペタイトを根本的に理解した上で革新と投資を行うことが可能になります。

KPMG

サイバーリスク管理のための インテリジェントオートメーション

予測データ、ビジネスインテリジェンス、人工知能によってリアルタイムでの意思決定が可能になることで、これらのインテリジェントオートメーション技術は、オペレーショナルリスク（サイバーリスクを含む）の測定にも重要な役割を果たすと考えられます。データ分析によって実現するオペレーショナルリスクとサイバーリスクの管理は、リスクに関する組織戦略の枠組み作りにつながります。第2のラインは、第1のラインからの業務データと指標データを使ってその知識を活用、強化するモデルを開発し、それをリスクアペタイト宣言の明確な要素にすることができます。この方法によって測定可能な重要リスク指標を開発し、リスク管理部内でリスクを定量化して、取締役会が慣れ親しんだビジネス用語で表現することが容易になります。

適用可能な知見を引き出す

CISOが取締役会に報告する場合、その議論は通常は技術的なものであり、前月、前四半期あるいは前年に解決した脆弱性件数などの要素に注目しがちです。これは第1のディフェンスラインがいかに効率的に業務を遂行しているかを示す重要業績評価指標ではありますが、それだけでは以下のような実際的な疑問に答えることにはなりません。

その結果、サイバーリスクは軽減できたのか。
脆弱性のうち重大なものは何件か。
それらの重大な脆弱性のうち、重要な事業資産に影響するものは何件か。

サイバーリスク管理において、これらの認知技術を採用することによる最も重要な効果は、ビジネスのコア資産、すなわち「クラウンジュエル」全体のリスクを定量化・明確化することです。これらのツールは、特定の重要資産にあるリスク水準も明らかにすることができるため、取締役会は、リスク軽減のためにどこへ予算を振り向けるべきかを判断できます。

企業の最高リスク管理責任者であるCROは、必要なリスクツールを活用することでリスクを可視化でき、サイバーリスクエクスポージャーを増大させる潜在的リスクも発見・特定できます。モニタリングツール、経営モデル、自動プロセス、サイバーセキュリティリスク評価を通じて、潜在的な収益創出活動や効率化活動をいかに現在のリスクアペタイトに整合させることができるか、あるいは許容しうるリスクエクスポージャーの水準を引き上げてもよいかを示す、リスクエクスポージャーのロードマップを定義できます。

さらに、データを収集・保存・分析し、そのデータを複数のリスク診断のレンズを通してふるいにかけることで、金融機関は第三者である規制団体や規制機関からのコンプライアンス要求に迅速かつ効果的に対応できます。

「先見の明のある技術リスクの管理組織は、リスク管理以上のことを行っています。そうした組織は、リスクを予測し、十分な情報に基づいて迅速に意思決定を行うことが可能です」

— Vivek Mehta, Partner, KPMG LLP

適切にリスクに取り組む姿勢はビジネスを成功に導く

現在の変化し続ける環境の中で計算に基づいてリスクを取るには、新しい考え方が必要です。そのためには、サイバーリスク管理を十分に取り込みモデル化したオペレーショナルリスクフレームワークを定義し、それに基づいて行動することも必要です。金融機関は、CISOとサイバーリスク管理責任者の役割を明確に定めることによって、規制順守とともに、組織のリスクアペタイト宣言に示された基本方針の中で革新と投資を行う最善の方法を判断することができます。

サイバーセキュリティの明確なディフェンスライン、ダイナミックなリスクガバナンス、独立したリスク管理監視機能、重視されたサイバー重要リスク指標、インテリジェントな自動リスク管理等、これらの要件を満たすことで、金融機関は組織の安全性を確保し、成長機会を追求できるリスクフレームワークを設計・構築することができます。

KPMGが推奨する3つの取り組み

組織モデルをアップデートする。つまり、CISOをCIO直下の第1ラインとし、サイバーリスク管理責任者をオペレーショナルリスク責任者直下の第2ラインとして新たに設置し、リスク管理を独立して監視する、明確なディフェンスラインを作る。

オペレーショナルリスク管理フレームワークに整合するサイバーリスクアペタイト宣言、閾値、重要リスク指標を設定して、リスクに基づいたビジネス上の意思決定を可能にする、第2ラインで管理するサイバーセキュリティポリシーを確立する。

適切なインテリジェントオートメーションツールと報告手段を取り入れ、重要な事業資産のサイバーリスクを定量化することで、取締役会や社内のビジネスリーダーが賢明な意思決定を行えるようにする。

KPMG

KPMGでは、第1、第2のディフェンスラインにわたるテクノロジーとサイバーリスクの管理フレームワークを確立しています。サイバーリスクを管理するための全面的な考えへと組織を移行させることで、事業部門はリスクに基づいたより優れた意思決定が可能になると考えます。

KPMGによる支援

サイバーセキュリティリスクは、ITの範疇をはるかに超える戦略的企業リスクです。KPMGは、企業の取締役会、バックオフィス、データセンターのいずれを支援する場合でも、サイバー脅威、重要資産に対する潜在的な影響、推奨対応についてわかりやすく説明することを旨としています。人材、変革、財務、リスク管理を網羅した、部門横断的でビジネスの視点を踏まえたサイバーセキュリティを考えます。

KPMGのインテリジェントオートメーション支援部門は、企業がAIの価値を存分に活用し、自動化とコスト管理、成長と顧客エンゲージメント、リスクと規制ポリシーに関連する戦略をより迅速に策定・実行することを支援します。KPMGは企業とともに、バリューチェーン全般にわたってインテリジェントオートメーションを最大限に活用し、ビジネスモデルと経営モデルに変革をもたらすソリューションを創造します。

Contact us

KPMGコンサルティング株式会社
TEL : 03-3548-5111
kc@jp.kpmg.com

田口　篤　Atsushi Taguchi
Technology Risk Services
パートナー

kpmg.com/jp/kc

kpmg.com/jp/socialmedia

本冊子は、KPMG米国が2018年9月に発行したTechnology and cyber risk managementを翻訳したものです。翻訳と英語原文間に齟齬がある場合には、当該英語原文が優先するものとします。