全社的リスク管理（ERM）の動向

PwCあらた有限責任監査法人
ガバナンス・リスク・コンプライアンス・アドバイザリー部
パートナー　**辻田 弘志**

PwCあらた有限責任監査法人
ガバナンス・リスク・コンプライアンス・アドバイザリー部
マネージャー　**西村 裕子**

はじめに

2017年にCOSO ERMが改訂[※1]されてから約5年経ちました。その間、コーポレートガバナンスコードの補充原則は拡充され、取締役会によるグループリスク管理体制の構築および運用状況の監督責任の明示、有価証券報告書の事業等リスクの記載の充実化が図られました。また、日本企業のグローバル化、グループ管理の必要性の高まりもあり、全社的リスク管理体制（以降、ERM）の強化に取り組む企業も増えています。

最近のERMの特徴は、各事業部門・事業部署によるリスクの洗い出し、評価とリスク対応を主とするボトムアップによるリスク管理体制の構築から、グループ全体への影響を俯瞰するトップダウンアプローチに移行しつつあることです。これまでトップダウンアプローチが過去に皆無だったわけではなく、ボトムアップアプローチが無効になったわけでもありませんが、近年あらためてERMが焦点を当てているリスクと提供する価値が変化してきていると考えられます。

※1　COSO（The Committee of Sponsoring Organization of the Treadway Commission：米国トレッドウェイ委員会支援組織委員会）によるERM（Enterprise Risk Management：全社的リスクマネジメント）フレームワークの改訂版（2017年）

1 トップダウンアプローチとは何か

本稿で言うトップダウンアプローチとは、組織目標や事業戦略・事業計画の達成に影響を与えるリスクを機動的に捉えるアプローチのことです。このアプローチでは、事業戦略・事業計画、ビジネスモデル・オペレーティングモデルの前提に関わる不確実性を事前に把握するような施策をとります。

環境が大きく変わらない状況では、すでに実行しているオペレーションを着実に遂行することが事業戦略・事業計画を確実に達成するために重要な要素となります。このような状況下では、各事業部門・事業部署の業務に係るリスクを分析することでリスク対応が可能となり、結果として会社全体のリスクの総和を測ることが可能となります。これがボトムアップアプローチです。

一方で、現在のように環境が大きく変わる状況においては、そもそもの事業戦略や経営資源配分が適時に調整されないと、事業遂行の着実性にかかわらずリスクが顕在することになります。そのため、環境変化に伴うリスク要因を特定し、そのリスクに対応するトップダウンのアプローチが必要になってきているのです。

トップダウンアプローチの価値は、環境変化への適時の対応をより着実なものとすることと読み替えることもできます。この手法は、金融機関や一部のエネルギー企業ではシナリオ分析として以前より用いられている手法ですが、他の業態においてもその活用が広がってきていると思われます。

本来はどちらのアプローチでもリスクの総和は同じになるはずですが、ボトムアップアプローチのほうが既存事業のオペレーションやコンプライアンスに関わるリスクがより多く特定される傾向が見られます。また、事業部門内に閉じたリスクが複数事業部門から挙げられ、全社への影響が統合的に把握されるケースもよく見られます。

一方で、トップダウンアプローチは、事業目標達成の前提

に関わる不確実性を機動的に捕捉するアプローチであり、経営者（取締役会、CEOなど）が自ら管理監督すべきリスクに焦点を当てたものと言えます。**図表1**は、経営者の目線で見た一般的なERM実務の改善、さらなる活用余地をまとめたものでトップダウンアプローチの必要性に関連するものとなっています。

以降、トップダウンアプローチによるリスク管理の具体的な特徴を3つの視点で概説します。

2 環境変化を捉えるリスク管理

トップダウンアプローチによるリスク管理の特徴の1つ目は、外部環境変化を捉えるリスク管理です。先述のように、トップダウンアプローチによるリスク管理においては外部環境変化による影響を捕捉することが重要となります。外部環境変化による事業運営への影響は近年特に大きくなっており、世界の経営者を対象に実施したPwCの「2022 Global Risk Survey」[※3]においても、重要なリスクとして挙げられている上位5つのリスクは、「市場環境」「ビジネス・オペレーティングモデル」「サイバーセキュリティ」「外部環境変化」「地政学リスク」であり、多くは外部環境変化に関連しています（**図表2**）。またPwCが2022年8月に国内企業に対して実施したサーベイでも、約8割の企業が過去3年間で地政学リスクが上昇したと回答しています。

外部環境変化によるリスクの捕捉は、世の中のあらゆる環境変化を捉えるのではなく、あくまで事業戦略・事業計画、ビジネスモデル・オペレーティングモデルに影響を与える要因を捉えることとなります。

一般的な手法としては、シナリオ分析がよく使われます。シナリオ分析には外部環境要因を経済・金融市場環境に限定せず、PEST（Politics〔政治〕、Economy〔経済〕、Society〔社会〕、Technology〔技術〕）などのいくつかの要素に整理して、それらの動向について複数の軸で想定される世界を描くことになります。これは特定の将来を予測するものではなく、複数のシナリオにおいて、いずれが実現した場合でも必要な対応が取れるよう、影響評価と対応の十分性の検証をするためのものです。また、オプションを保持しておけば、そのようなシナリオがモニタリング時に実現した場合、早期に対応することが可能になります。これらの影響を

図表1：経営者（取締役会、CEO等）の目線で見た既存のERMの改善ポイント

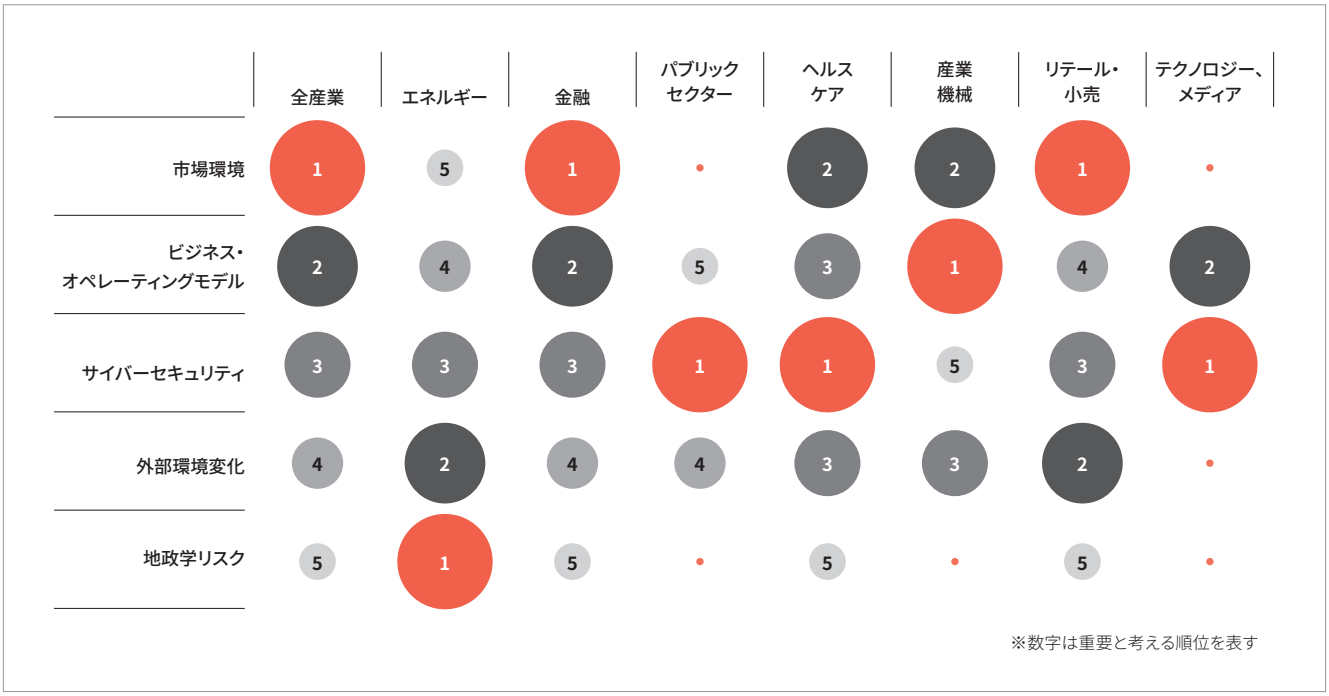
改善を要する兆候	考えられる原因	検討事項
戦略の議論上、主に機会を重視しており、リスクへの言及がない	●戦略の策定にあたり、リスクが十分に考慮されていない可能性がある ●経営層が全体像を把握せず、ポジティブな側面のみに着目している可能性がある	●特定されたERMリスクは、取締役会が事業固有の戦略リスクと位置付けたものと一致しているか？ ●取締役会は、戦略にかかる議論上、機会を特定するためのツールとしてリスクやERMの結果を使用することを検討しているか？
リスクリストに会社の戦略目標との関連性がない	●ERMが最大限に活用されず、コンプライアンスの実践と見なされている可能性がある ●ERMが継続的なプロセスではなく、年次のリスク自己評価の調査手段として利用されている可能性がある	●取締役会はERMに関する最新情報をどれほどの頻度で受け取っているか（年次、またはより頻繁か）？ ●ERMの結果（アウトプット）は、取締役会の戦略的意思決定にどのように活用されているか？
財務報告上のリスク、コンプライアンスリスク、オペレーショナルリスクなどの、理解しやすい個別のリスクを特に重視している	●ERMの手法として、リスクは戦略と関連付けられず、ボトムアップのみに基づき特定されている可能性がある ●リスク管理の重点領域が適切でない可能性がある	●リスクをいかなるプロセスで特定しているか？ トップダウンとボトムアップのバランスは適切か？ ●経営層や取締役会はERMの結果（アウトプット）をどのように審議しているか？
ERMが取締役会や上級管理職のレベルで認識、可視化されていない	●ERMリーダーが社内で十分な支援を受けていない可能性がある	●ERMリーダー（多くの場合、最高リスク責任者またはCFO）は、会社を深く理解し、リスク管理の取り組みを適切に主導できているか？
ERMの議論が陳腐化しており、管理対象のリスクが毎年同じである	●ERMが環境変化や将来の可能性を捕捉するために経営陣に問いを投げかける機能を果たしていない	●ERMのプロセスで、エマージングリスクが検討されていたか？ ●経営陣は、リスクがどのように拡大または発現し、それが事業にどのような影響（ポジティブまたはネガティブ）を及ぼし得るかを検討しているか？

出所：PwC「Risk oversight and the board: navigating the evolving terrain」をもとに作成[※2]

※2 PwC「Risk oversight and the board: navigating the evolving terrain」2022年
https://www.pwc.com/us/en/governance-insights-center/publications/assets/pwc-risk-oversight-and-the-board-navigating-the-evolving-terrain.pdf

※3 PwC「2022 Global Risk Survey」
https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-risk-survey.html

図表2：経営者が重要と考えるリスク



出所：PwC「2022 Global Risk Survey」をもとに作成

評価する際には、自社にとってプラスの側面も存在する点に留意が必要です。

一部の業界では、シナリオから影響を評価する手法に加え、致命的な影響を与えるシナリオ（水準）を逆に導出するリバーススストレスシナリオも活用されています。昨今の想定外の事象が生じる状況においては、事業戦略やビジネスモデルの弱点を特定するのに有用なアプローチと考えられます。

3 バリューチェーン、サプライチェーンでのリスク管理

トップダウンアプローチによるリスク管理の2つ目の特徴は、外部環境、内部環境要因にかかわらず、最終的なサービスの提供（価値提供）を確実に行うために、原材料の調達から販売までの一連の流れでリスクとその影響を捉える、というものがあります。End to Endという言い方をすることもありますが、端から端まで全体を流れで捉えるというものです。

End to Endでのリスク管理は、自社に限らず調達先を含むサードパーティ全体を含むものになります。近年は、外部機関との協働や依存の高まりを受け、サードパーティリスク管理（TPRM）として別途管理を強化する取り組みも多く見られます。サードパーティは直接の委託先や調達先に限らず、利用している外部サービス（クラウドサービス）や再委託先など、幅広く捉える必要があります。そういった先は必ずしも調達部門で一元的に管理されていないこともあるため、ボトルネックにならないように留意したほうがよいでしょう。

機能復旧に限定せず、重要な機能の冗長化など、ビジネスやサービスの提供を維持したり、提供方法を変革したりするためにレジリエンスの考え方が適用されることもよくあります。さらに、後述のように、最近は調達先を含めた人権対応や環境対応など、提供する機能に直接影響しない領域の非財務リスクも管理の範囲となってきています。

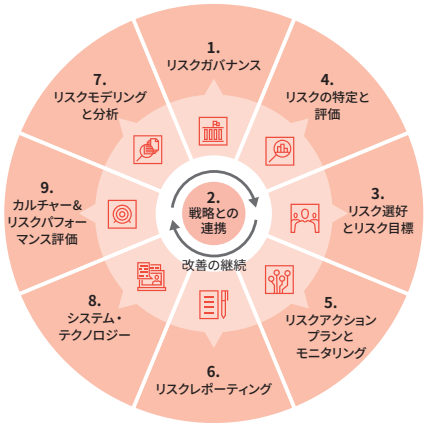
4 ステークホルダー視点でのリスク管理

3つ目は、ステークホルダー視点の拡張です。これはステークホルダー資本主義やESG推進の流れと同様のものであり、自社のリスクに限定するのではなく、広くステークホルダーに与える影響をリスク管理でも捉えるという取り組みです。なお、ステークホルダーには、顧客、株主・債権者、従業員、ビジネスパートナー（調達先、委託先等）、社会などが挙げられます。

現在は過渡期にあると言えますが、すでに一部の企業では、マテリアリティとの関連の整理、ステークホルダー視点でのリスクタクソノミーの再整理などの取り組みが始まって

図表3：PwCのERM成熟度モデル

PwCのERMフレームワーク



PwCのERM成熟度モデル（5段階）

	❶ 初期	❷ 発展中	❸ 発展	❹ 統合	❺ 最適化
1. リスクガバナンス	Limited definition and articulation of risk governance structures, risk roles and responsibilities, and risk policies.	Some definition and articulation of risk governance structures, risk roles and responsibilities, and risk policies. Limited informal interaction between three lines of defence.	Increasing definition and articulation of risk governance structures and risk roles at group level and responsibilities and some coordination between three lines of defence, supported by group wide risk policies that are aligned with risk types.	Risk governance and organisational structures provide clear role and responsibility allocation between group and business unit/functional levels, supported by risk policies that are aligned with the business strategy.	Risk governance and organisational structures are aligned with the business strategy and promote a partnering relationship between 3 lines of defence. risk policies that provide a statement of commitment and define risk management improvement objectives. Effective risk governance, challenge and oversight exists within all key business decisions.
2. 戦略との連携	Risk strategy not defined and does not form part of the business-planning process.	Risk strategy is business unit focused and does not define the link between risk strategy and business strategy.	Business strategy and risk strategy co-exist with specific, defined metrics used to manage and monitor the risk profile of the business.	Risk and business strategy are aligned and jointly form part of the business-planning process.	Consistent and enterprise-wide methodology to assess strategic risks such that risk strategy is embedded and monitored across all core business processes, products, and services.
3. リスク選好とリスク目標	No documented risk appetite statement exists (either qualitative or quantitative) and organisational strategy is established without considering risk appetite.	Basic risk appetite criteria is set, however, risk appetite linkage to risk strategy and business strategy is not clear or consistent.	Risk appetite criteria is set with quantitative and qualitative elements which are applied to business decisions, although business decisions are made without an aggregate view of risk appetite across the organisation.	Risk appetite criteria is set and cascaded for all risk classes, is aligned with the organisational strategy and criteria and parameters are defined and consistently applied, including tolerance and capacity for risks.	Organisational risk appetite informs strategy and business decisions with risk appetite criteria set and dynamically reviewed as the external environment changes. Risk appetite is embedded in strategic objectives and Corporate KPI's.
4. リスクの特定と評価	No formal approach for risk identification and assessment. No risk profiling performed, risks are only managed when they occur.	Limited risk profiling is being performed. Formal risk assessment approach has been developed, but is not applied consistently across the business.	Risk-profiling is consistently performed, covering all organisational units, operations, and risk types. Periodic risk assessment applied consistently across the business, supported by standardised risk universe and evaluation criteria.	Comprehensive and consolidated forward-looking risk profile across the organisation used as an input to strategy and business planning. Dynamic risk assessment approach applied consistently across the business, supported by standardised risk universe and evaluation criteria including qualitative and quantitative measures. Risk assessment results are an input for key business decisions.	Dynamic risk identification and assessment approach which leverages internal and external data points. Enterprise-wide, strategic and emerging risks are linked to a dynamic risk profile. Risks are reviewed collectively, considering trade-offs and correlations, and an indication of the effectiveness of mitigating actions. Risk and opportunity are considered as part of key business decisions.
5. リスクアクションプランとモニタリング	Limited formal capture and monitoring of risk responses.	Basic risk action development and monitoring approach applied to some risks.	Consistent and repeatable risk action planning process for risks outside of tolerance. Some monitoring of risk action status performed by internal audit.	Risk action plans developed for material risks outside of appetite. Integrated assurance (leveraging the 3LOD) performed against risk actions. Risk action status measured and reported to governance stakeholders.	Risk action plans are developed for material risks outside of appetite and are supported by a business case analysis of opportunities for investment decisions. Risk action status is tracked dynamically and linked to risk profile, supported by an integrated GRC platform. Integrated assurance over risk actions (across 3LOD) is supported by continuous monitoring.
6. リスクレポーティング	Nonstandard and/or manual reporting of risk management activities and risk information including risks, controls, and processes is performed. Ad hoc use of KRIs.	Basic standardised monitoring of risk management activities and risk information is in place for some business units, supported by KRIs for some core business processes.	Monitoring results and in-depth analysis is reported to senior management and used to assess significant risks and the risk profile for each business unit supported by defined KRIs.	Monitoring results and analysis reported to senior management and used to assess significant risks and alignment of the risk profile with the business strategy and risk appetite.	Dynamic, automated ERM reporting that facilitates real-time changes to KRIs, risk profiles, and capital allocations. Risk reporting provides valuable insights to support strategic initiatives at the Board, ELT and Management levels.
7. リスクモデリングと分析	No value added from risk modeling or analysis. Risk correlation or interdependencies are not considered.	Risk interdependencies and scenarios are considered for some categories, but not consistently.	A consistent approach to scenario analysis and risk modelling has been applied, aligned with the business complexity and model.	Scenario analysis and stress testing are applied consistently to strategic and emerging risks, and are used as a key input to key decisions and business planning.	Predictive data analytics and stress testing are applied for all material risk types to provide a data-driven basis for driving strategic risk decisions.
8. システム・テクノロジー	Heavy reliance on spreadsheets with limited to no consistency over data across business lines	Single source of truth for risk profile information, including risk owners, controls and mitigating actions	Single Data Repository and Common Risk Taxonomy. Consistent data model driving common understanding across business lines.	Broader GRC capabilities integrated in the platform. Systems facilitate process integration and controls automation, supported by standardised risk and control libraries.	Fully-integrated enterprise GRC platform. Systems are capable of delivering predictive data analytics for material risks and near real-time risk information.
9. カルチャー&リスクパフォーマンス評価	Limited risk awareness with no link between business incentives and the defined risk strategy and appetite and no measurement of risk culture.	Growing risk awareness with performance incentives partially defined at business unit level and some analysis of risk culture performed through broad based people surveys and an attempt to utilise tasks, activities, and initiatives to effect culture change.	Strong tone from the top. All staff are aware of the risk management objectives supported by some risk management training, defined performance objectives, partially defined link between incentives and risk strategy and enterprise-wide analysis of risk culture.	Consistent message from the the executive and management to re-enforce that risk management is part of ongoing business supported by embedded measurement and monitoring to enterprise-wide performance incentives aligned with risk strategy and appetite.	Deep risk awareness is present across the organisation at all levels of seniority. All employees have KPIs for achieving risk management objectives, supported by performance incentives that are integrated and aligned with relevant strategic and tactical business plans in the organisation.

ERM成熟度モデル評価基準例

	❺ 最適化
1. リスクガバナンス	事業戦略と整合したリスクガバナンス、組織構造が構築されている。グループ・グローバルで3つのディフェンスラインの役割責任が明確化され、それぞれが公式／非公式に連携し合い、リスク方針（リスク管理のアプローチや改善目標、そのための対応事項を規定したもの）に基づいてリスクマネジメントを遂行している。効果的なリスクガバナンス、チャレンジ（異議申し立て）とオーバーサイト（監視）が、ビジネス上の重要な意思決定に対して行われている。
2. 戦略との連携	事業環境の変化による戦略（市場優位性を高めるための製品・サービスの変革・差別化等）への影響やリスクを、上級管理職層を交えて定期的に議論、評価し戦略を見直すための公式な枠組みが存在する。戦略リスクを評価するための全社的かつ一貫性ある手法（環境分析、シナリオ分析、戦略リスク評価、またはリスク選好度の設定等）が確立されている。計画の進捗や結果は定期的にモニタリングされ見直しを行う。
3. リスク選好とリスク目標	組織のリスク選好は、定性、定量的な基準を用いて、外部環境の変化に応じて定められ、動的に見直される。リスク選好は、戦略およびビジネス上の意思決定に反映されて、戦略目標および組織のKPIに組み込まれている。KPIやKRI等の評価指標が閾値や警戒値に達した場合、リスク対応策が策定される。
4. リスクの特定と評価	社内外の事象（データポイント）を活用した、動的なリスク特定・評価アプローチが採用されている。全社的リスク、戦略リスク、新興リスクは、動的なリスクプロファイルに関連付けられている。リスクは、トレードオフと相関、および低減策の有効性の程度を考慮し見直されている。リスクと機会が、ビジネス上の重要な意思決定の一部として考慮されている。
5. リスクアクションプランとモニタリング	リスクへの対応策（アクションプラン）が、投資判断時の投資対効果（ビジネスケース）分析を裏付けとして、リスク選好外の重要なリスクに対しても策定されている。リスク対応策の進捗状況は、統合されたGRCプラットフォーム上で動的に追跡されるとともに、リスクプロファイルと連携している。継続的なモニタリングにより、（3ディフェンスライン全体に及ぶ）リスク対応策に対する統合的な監査（保証）が実施されている。
6. リスクレポーティング	動的で自動化されたERMレポーティングの手段として、経営情報システム（MIS）等のテクノロジーが導入され、KRI・リスクプロファイル・資源および資本配分等に対する更新が、社内データを基に体系的かつリアルタイムで反映されている。リスクレポーティングは、取締役会（リスク委員会、監査委員会）、エグゼクティブリーダーシップチーム、上級管理職層での戦略的構想の裏づけとなる、有益な情報、示唆を提供している。
7. リスクモデリングと分析	予測データ分析とストレステストを、あらゆる種類の重要リスクに適用することで、データに基づく根拠を提供し、戦略的なリスク判断を促している。分析には、統計モデリング、リスク調整後パフォーマンス、キャッシュフロー、収益、バリュー・アット・リスク等が含まれる。リスク管理部門はビジネス分析やモデリングの主管部門と連携し、データサイエンスやモデリングに反映するための全社的リスクにかかる見識を提供している。
8. システム・テクノロジー	全社的GRCプラットフォームが他のリスク管理用システム（法令管理用・インシデント管理用・内部監査用データベース、MIS等）と社内で完全に統合されている。GRCシステムはGRC関連業務内での統合にとどまらず、その他の関連業務システム、データとの連携も考慮されている。GRCシステムは重要リスクに関する予測データ分析とともに、リアルタイムのリスク情報を提供することができる。リスク情報の分析は社外の情報（Web、SNS等）を含む幅広い情報が分析されている。当該プラットフォームや保有情報がリスクオーナー、監査、コンプライアンス、コーポレートガバナンス等の業務に活用されている。GRC関連業務の効率化を促進するためにAIやRPAなどのテクノロジーが活用されている。
9. カルチャー&リスクパフォーマンス評価	組織全体にわたり、全ての上級管理職層が深いリスク認識を持っている。全従業員がリスク管理上の目標達成のためのKPIを持ち、その達成を促す統合的なパフォーマンスインセンティブが、関連する組織内の戦略的・合理的な事業計画と整合している。

出所：PwC作成

います。今後は、こうした取り組みがより意識されたものへと発展していくことが期待されます。

取り組みにあたっては、国・地域で進度や捉え方に大きな差があるもの、現時点で必ずしも法制度化されていないテーマ（典型的には人権や環境）についてのリスク対応に注意を払う必要があります。リスクの負担、リターンの配分の公正性や透明性にも留意する必要があります。こうしたリスクに求められる基準や価値観は、社会環境の変化に応じて変わってくるため、自社の方針をグループレベルで定め、定期的に見直しを行うとともに、必要に応じて開示（対話）することで、能動的なリスクマネジメントにつなげることができます。

5 PwCのERMフレームワーク

PwCはこれまでもCOSO ERMなど、ERMのフレームワークについて外部機関からの委託や協働で策定を行ってきました。さらに、それらのフレームワークとも整合したERMフレームワークについての成熟度モデルも策定しています。

図表3は9つの視点でERMを整理したものです。成熟度を5つの段階で表しており、ベストプラクティスとして定義しています。前述の3つの視点に加え、リスク管理の戦略との連携、リスク評価・モニタリング手法、リスクデータを含むインフラ整備など、ERMの重要となる要素について取りまとめています。

本稿で解説してきたものは、PwC Japanグループおよび PwCグローバルネットワークでの整合の状況や、短期・中長期でどの水準を目指すのかといった活用を企図したものであり、今後読者の皆様の組織においてERMの見直しをする際の参考としていただければ幸いです。

辻田 弘志（つじた ひろし）
PwCあらた有限責任監査法人
ガバナンス・リスク・コンプライアンス・アドバイザリー部　パートナー
大手金融機関を経て、現職。ガバナンス・リスク・コンプライアンス・アドバイザリー部においてグループ・グローバルの視点でのガバナンス、リスク管理、コンプライアンス、内部監査についてインダストリーワイドに高度化支援サービスを提供。最近の注力領域としては、テクノロジーやデータ分析によるガバナンスやコンプライアンスの効率化や見える化の促進、法令に留まらないコンダクトリスク管理の高度化、リスクやコンプライアンスの組織内浸透に重要な要素となるカルチャーの醸成がある。
メールアドレス：hiroshi.tsujita@pwc.com

西村 裕子（にしむら ゆうこ）
PwCあらた有限責任監査法人
ガバナンス・リスク・コンプライアンス・アドバイザリー部　マネージャー
金融機関のコーポレートコンプライアンス部門等を経て現職。国内外規制対応、コンプライアンスリスク管理、不正調査等の実務経験を活かし、業界を問わず、全社的リスクおよびコンプライアンスリスク管理態勢・危機管理態勢・ポリシー（規程類）ガバナンス態勢等の高度化およびグローバル展開、コソース内部監査等のプロジェクトに従事。
メールアドレス：yuuko.nishimura@pwc.com