

The Bulletin

Volume 6, Issue 2

改訂版COSO ERMのフレームワーク：何が新しいのか？

2016年6月14日、米国トレッドウェイ委員会支援組織委員会 (The Committee of Sponsoring Organizations of the Treadway Commission: "COSO") は、「Enterprise Risk Management – Aligning Risk with Strategy and Performance」¹の公開草案をリリースし、2016年9月30日までコメントを募集しています。2004年に発表された「ERM統合フレームワーク (ERM – Integrated Framework)」になじみのある方にとっては、改訂されたフレームワークのコンセプトは全く「新しい」とは思われなくてもいいかもしれません。しかし、強調されている点は明らかに異なるとお気づきになるでしょう。それは、Enterprise Risk Management (ERM) が組織において機能する上で、何が本当に重要なことなのかという点に注目しているからです。

なぜ改訂されるのか？ 過去10年間を振り返る

ERM統合フレームワークが公開された2004年においては、企業はいくつかの重大な課題に直面していました。最も大変だったのは、米国の証券取引所に上場している企業は、Sarbanes-Oxley Act (SOX法) に対応すべく、総力を挙げて取り組まなければならなかったという点でしょう。

またSOX法対応以外にも、ERM導入に際しては以下の課題がありました。

- ERMを導入する際、企業全体が対象とされていないことが往々にしてあり、さらに戦略策定と併せて検討されることは稀であったということです。その結果、COSOフレームワークにおけるERMの定義として最も重要かつその特徴である、「戦略策定の段階で、企業横断的に適用する」、という点が、実質的に誤解もしくは無視されていたことです。
- COSOは、ERMフレームワークを考案する段階で、内部統制の基盤であるおなじみのCOSOキューブからは切り離して検討を行いました。COSOは、活動とプロセスへの参照を削除してキューブの右側面を修正し、より広く、企業や機能、部署にフォーカスを当てたにも関わらず、多くの企業は戦略策定で

はなくプロセスレベルで適用するかのようになり、フレームワークをより細かいレベルで導入しようとしていました。その結果、ERMの導入を担当する人が些末な点にとらわれて窮地に陥り、多くのCレベルのエグゼクティブ (注:CEO・COO等、「CxO」と呼ばれる経営幹部) が早々に興味を失ってしまいました。

- また、いくつかの組織では、ERMをビジネスの推進・管理の改善のためではなく、保証活動の一環として導入しようとしていました。このようなアプローチを取ったことにより、事業部門のリーダーとのやり取りの過程で、ERMは役に立たないものとの認識が多くの企業で広まった。特に、この傾向は内部監査主導でERMを導入しようとした場合において顕著でした。
- 2008年の金融危機を発端とする大不況により、多くの企業がクライシスマードに突入せざるを得ず、ERM導入の障壁の一つとなりました。
- 最終的には、2008年の大不況、さらに多少は影響は低いものの、2011年の日本の津波といった劇的なイベントが、真の意味でERMへの関心が高まる契機となりました。

要約すると、COSOがフレームワークを公表した以降、経営幹部からの注目は限定的であり、実践のレベルは企業によってばらつきがあったということです。

これら全ての理由により、公開してしばらくの間、ERMのフレームワークは適切な評価を受けていませんでした。また、大不況が起こるまでの間、多くのシニアエグゼクティブはフレームワークに対し何をすれば良いのか、認識すらしていない、もしくは分からないという状態が続いていました。しかし、大不況が起こると、課題と提示された価値が明らかになったのです。

世界的な景気後退を引き金に、産業界は「バスが崖から落ちる」がごとく、崖から転落していきました。この大不況は、想定外の潜在的な危機に対する貴重な教訓となり、「ブラック・スワン (Black Swan) 現象 (注:滅多に起こらないものの、壊滅的な被害を及ぼすこと)」と呼ばれ、ビジネス用語入りを果たしたほどです。この教訓は、実効性のあるリスク管理のための重要な要素 – 取締役会や最高経営責任者 (Chief-Executive Officer (CEO)) の

1. 「Enterprise Risk Management – Aligning Risk with Strategy and Performance, COSO, June 2016 Exposure Draft」をご参照ください。(www.coso.org)

十分な関与、オープンかつ透明性のある企業カルチャー、長期・短期のバランスを取るための補完構造、そして最も重要なものとして、危機が迫っていることを知らせる警報が発動した際に適切な行動を取るための経営陣の意思と規律—について、その重要性を実証したのです。これらの要素については、ERMを維持・存続するために、常に警戒しなければならないことです。

このように、Early Moverとして群れの中から一歩先んじることが、いかに重要かが評価されるようになりました。取締役会は、多様で難しい疑問を投げかけ始め、CEOは取締役会との対話に専念するための方法を探り、組織内の人々にリスク関連事項に目を向けさせる方法を模索し始めています。

注目すべきもう一つの変化は、ビジネスモデルの盛衰期間が短縮し、ビジネス環境が絶え間なく変化していることです。かつてない速度で、確立されたビジネスモデルを破壊するポテンシャルをもったメガトレンドが姿を現しています。それは、着実に進化するデジタルテクノロジーの分野に限りません。その結果、消費者やビジネスの現場は、過去に類を見ない情報量を消費・吸収するようになりました。また、我々が目撃した少なからずの事象を述べると、「アラブの春」、国民心理や地政学的な緊張、高齢化社会、サイバースペースへのますますの依存、所得格差の増加、テロカリフの出現、大規模な移民の移動、そして最近の原油価格の崩壊等—ここに挙げたものは、ごく一部の変化に過ぎません。

適用レベルにばらつきのある2004年のERMフレームワーク、2004年以降に発生したリスク管理の大規模な崩壊、そして、ビジネス環境の複雑化に伴い、透明性の向上が叫ばれています。

この変化は、現実には起こっていることなのです。混乱局面においても先頭に立ち続けるため、ビジネスリーダーは極めて重要な変化の兆候と、自社に関連する市場やビジネスモデルの関連性をスピーディに識別しなければならないのです。

総括すると、適用レベルにばらつきのある2004年ERMフレームワーク、2004年以降に発生したリスク管理の大規模な崩壊、そして、ビジネス環境の複雑化に伴い、透明性の向上が叫ばれています。COSOはこのような声を受け、ERMとさまざまなステークホルダーの期待とをより明確に結びつける機会が到来したと考えました。具体的には、リスクの識別は、独立的に実施するよりも企業のパフォーマンスのコンテキストの中で実施すること、そして組織がさらなる先見性をもって行動できるようにすることです。確かに、先頭に立って行動している組織は、変化の兆候を潜在的な危機と捉えるだけでなく、潜在的なマーケット獲得機会と捉えています。

何が新しいのか？ 原則主義のアプローチ

改訂されたCOSOのフレームワークは、全ての企業はステークホルダーに価値を提供し、その過程で不確実性に直面するというこ

とを前提としています。ここで言う「不確実性」とは、まだ知られていないことと定義されています。そして「リスク」は、事業戦略の策定や遂行、ビジネスの目的の達成に影響を与えるような不確実性と考えられています。そのため、改訂後のフレームワークによると：

経営陣の課題の一つは、どの程度の不確実性 — つまりどの程度のリスク — に対し、組織が準備しているのか、そして受け入れることができるのかということです。実効性のあるERMは、機会や拡大が見込まれる能力、価値の維持、そして究極的には実現見込みの価値と、リスクに晒される度合いのバランスを考慮しています。

このようにリスクと価値の関係を明確にすることは、COSOがERMの定義を簡素化し、焦点を当てようとしていることにつながります。

組織が価値を創造、維持し、実現する過程でリスクを管理できるか否かは、戦略策定や実行段階に統合された組織のカルチャーや能力にかかっています。

改訂されたフレームワークのタイトルからは、リスク・戦略・業績間の関係が重要であると認識されていることが窺えます。COSOによると、改訂後のフレームワークは、

- 戦略を策定・実行する上での、ERMの役割について、より深い洞察を提供する
- 企業のパフォーマンスとERMとの整合性を拡充する
- ガバナンスや監視に対する期待を反映する
- 市場やオペレーションの絶え間ないグローバル化を認識し、テイラーメイドでありながらも、地域を問わず共通のアプローチを適用する
- 一層複雑化するビジネスコンテキストを捉え、斬新な方法でリスクを認識する
- ステークホルダーへの透明性向上の期待に応えるべく、リスク報告を拡充する、そして、
- 意思決定に資するよう、先端テクノロジーや高度なデータ・アナリティックスを導入する

COSOが2013年に改訂した内部統制のフレームワークと同様、改訂フレームワークでは、相互に関連する5つの構成要素と、各構成要素に紐づく原則が取り入れられています。各構成要素と原則は以下のとおりです。

リスクガバナンスとリスクカルチャーのいずれも、実効性のあるERMの強固な基盤を築くにあたって必要である。

リスクガバナンスおよびカルチャーの重要性

改訂フレームワークの1つ目の構成要素は、他の4つの構成要素の基礎となります。リスクガバナンスは、企業の風土を決め、ERMの重要性を強め、監視責任を確立します。企業カルチャーは、倫理的な価値観、責任ある企業行動、およびビジネスコン

テキストの理解と結びつき、意思決定に影響を及ぼすものです。リスクガバナンスとリスクカルチャーのいずれも、実効性のあるERMの強固な基盤を築くにあたって必要です。この構成要素の基礎となる原則は、6つあります。

リスクガバナンスとカルチャー

1. 取締役会によるリスクの監視がなされている
2. ガバナンスおよびオペレーティングモデルが確立されている
3. 望ましい組織行動が定義されている
4. 誠実さと倫理観に対するコミットメントを実践する
5. 説明責任を果たしている
6. 有能な人材を惹きつけ、育成し、保持する

取締役会によるリスクの監視がなされている — リスクガバナンスや企業カルチャーは、取締役会の影響力や監視と共に、組織の上位者によって大きく左右されます。監視にあたって、取締役会は説明責任とリスクを監視する責務を負っており、それに見合うだけのスキルや経験、ビジネスに関する知見を有していなければなりません。取締役会が、独立した立場の人が多数を占める場合、エグゼクティブマネジメントや組織的な偏った見方を監視するにあたって、有効なチェック機能が働きます。

COSOは、「戦略におけるリスク」が戦略的に検討する唯一のリスク特性ではないと述べています。戦略を策定する際に、企業のリスクプロファイルに著しい影響を与え得る2つの追加的特性があります。

ガバナンスおよびオペレーティングモデルが確立されている — 経営目的を達成するため、企業戦略は経営管理部門によって策定され、日々の業務を通じて実行されています。一般的にオペレーティングモデルは、レポートラインを含む法律上・経営上の体制を反映しています。これらをいかに運営・統治するかが、組織の戦略遂行やリスク管理、目的の達成を左右する新しく多様なリスクや複雑性をもたらします。従って、ERMのプロセスでは、企業のオペレーティングモデルに関連するリスクプロファイルを考慮する必要があります。

望ましい組織行動が定義されている — COSOは、各組織のコアバリューやリスクに対する姿勢というコンテキストを踏まえた、望ましい行動の枠組みを提示しています。組織が自らをリスク回避型、リスク中立型、リスク積極型のいずれかであると判断としても、COSOはリスクに注意を払うカルチャーを推奨すると述べています。このような企業カルチャーは、強力なリーダーシップ、参加型のマネジメントスタイル、結果と行動への説明責任、リスクを考慮した意思決定プロセス、そしてリスクに対するオープンかつポジティブな対話が存在することが特徴です。これらの特徴は、リスクに対する意識を日常業務に組み込むという点にあると言えます。

誠実さと倫理観に対するコミットメントを実践する — 注目すべきは、COSOが組織全体の風土に着目しているという点です。上層部の風土は、オペレーティングスタイルや経営者個人の判断、取締役会によって決定されるものの、これを組織全体に深く浸透させなければなりません。従って、組織にとって望ましいコアバリューやリスクに対する姿勢について、上層部の意向を下層部に反映させるには、中間層と上層部との間でトーンを合わせなければなりません。

組織横断的な風土には境界線はありません。これは、組織の従業員であれ、協力会社であれ、経営者や取締役会からの期待に応えなければならないことを意味します。従って、行動規範の策定や評価を実施し、規範を逸脱する行為があれば、タイムリーに議論しなければなりません。適切な風土を醸成するにあたっては、リスクとリスクテイキングが期待される行動について、オープンな対話と透明性を確立することが肝要です。

説明責任を果たしている — 企業内の全ての人は、階層に関わらず、ERMに対する説明責任を負わなければなりません。同様に、企業はERMに関する適切な基準やガイダンスを彼らに提供し、自らの説明責任を果たし続ける必要があります。これらの説明責任は、取締役会やCEOといった上層部から始まり、業績に対する適切な期待、インセンティブや報酬制度を通じて、組織全体に浸透していきます。取締役会やCEOは、プレッシャーによって無責任かつ／あるいは違法な行為を招かないよう、留意しなければなりません。

COSOは、非現実的な業績目標、ステークホルダーによって異なる経営目標、そして、短期的な財務上の目標と長期的なステークホルダーの期待（企業の持続可能性に関する目標）とのアンバランスが、過剰なプレッシャーを引き起こすと述べています。また、プレッシャーは内部（成績に対して不適切なインセンティブや戦略の変更）および外部（販売実績に影響を与える顧客ニーズの変更、またはオペレーティングモデルの混乱）の双方によって生じ得るとも述べています。

有能な人材を惹きつけ、育成し、保持する — 最後に、リスクガバナンスおよび企業カルチャーの醸成には言うまでもなく、人的資源が重要であり、経営目的に沿った個々人の能力開発が求められています。経営者は、戦略を実行するために必要な知識・スキル・経験を定義し、適切な業績期待を定めると共に、有能な人材や戦略的なパートナーを惹きつけ、育成・保持し、後継者を育てる必要があります。

戦略策定に対する、さまざまな観点からの注目

多くの組織は、戦略実行時に起こりうるリスクの特定に注力しています。しかし、この2つ目のERMの構成要素では、この「戦略に対するリスク」だけが、戦略的に考慮すべき唯一のリスクの特性ではないとCOSOは述べています。戦略を策定する際に考慮すべき点として、企業のリスクプロファイルに著しい影響を与える2つの特性がさらに存在します。2つ目の特性は、企業が何を成し遂げ、

どのようにしてビジネスを遂行するかということを決する、企業のミッション・ビジョン・コアバリューと、「戦略が合致しない可能性」です。例えば、戦略が成功したとしても、ここが不整合なままでは、企業のミッションやビジョンの実現に結びつかない可能性があります。

考慮すべき3つ目の特性は、「選択された戦略が示唆するもの」です。COSOは以下のように述べています。

経営者が戦略を打ち立て、取締役会と共に代替案に向き合った場合、戦略固有のトレードオフとなるものを考慮して、彼らは最終的な意思決定を行います。各代替案には、それぞれリスクプロファイルが存在するわけですが、これこそが戦略が示唆するものなのです。取締役会と経営陣は、戦略が組織のリスクアペタイトの中でどのように機能し、どのように組織の目標設定を促し、そして究極的に如何に効率的な資源配分を行うかについて考慮する必要があります。

要約すると、COSO改訂フレームワークでは、戦略策定プロセスで3つの特性全てを検討する必要があると強調しています。これにより、戦略の議論が昇華し、戦略とERMとが結びつくことになるのです。ERMのリスク戦略および目標設定に関する構成要素には基礎となる5つの原則があります。

リスク戦略と目的の設定

7. リスクおよびビジネスコンテキストを検討する
8. リスクアペタイトを定義する
9. 代替戦略を評価する
10. 事業目的策定時にリスクを検討する
11. 受容できる業績の変動幅を定義する

リスクおよびビジネスコンテキストを検討する — 改訂フレームワークでは、ビジネスコンテキストを内外環境双方のレンズを通して見えています。加えて、内外環境に多大な影響を与え得る内外のステークホルダーの役割も考慮します。要するに経営者には、ビジネスコンテキストにおける変化から起こり得るリスクを検討し、それに応じて戦略の遂行や事業目的の達成に向けて対応していくことが求められているのです。

リスクアペタイトを定義する — 組織は価値を創造・維持・実現するコンテキストにおいて、リスクアペタイトを定義します。リスクアペタイト・ステートメントは、戦略策定プロセスにおいて検討され、経営陣と議論され、取締役会によって承認された後、組織全体に展開されます。リスクアペタイトは、企業のミッション・ビジョン・コアバリューによって形成され、企業のリスクプロファイル、リスクキャパシティ、リスク対応能力および成熟度、カルチャー、ビジネスコンテキストによって精緻化されます。

代替戦略を評価する — 代替戦略は異なる前提に基づいて策定されていますが、これらの前提はさまざまな形で極めて変化しやすいという特徴を持っています。組織は戦略の選択肢を評価し、

組織の価値を高める戦略を選択するわけですが、それを選んだことによって生じるリスクを考慮します。なぜならば、重要な要素が変更されることにより、戦略の基礎とした前提が無効となることもあるためです。取締役会や経営陣は、戦略を承認する前に、変化に対する感受性—戦略が示唆すること—を十分に理解しておく必要があります。戦略が承認された際には、前提を無効とし得る重大な環境要因を特定し、長期に亘って監視する必要があります。

事業目的策定時にリスクを検討する — 経営者は、ビジネスのさまざまなレベルにおいて、戦略をサポートし、戦略に沿った事業目的を策定します。この目的は、企業のリスクアペタイトを考慮し、それに沿ったものでなくてはなりません。実際、組織の事業目的はさまざまな部署、オペレーティング部隊および機能に展開されていなければなりません。

受容できる業績の変動幅を定義する — COSOは「許容可能な業績の変動幅」(「リスク許容度」と呼ばれることもある)について、「特定の事業目的を達成する際に許容される結果の幅」と定義しています。リスクアペタイトは広範囲におよびますが、許容可能な業績の変動幅とは、戦術的かつ実務的なものです。「許容可能な業績の変動幅」は、リスクアペタイトと特定の事業目的とを紐づけ、目的を達成する上で、出現するリスクに対して測定基準を提供します。一般的に、目的が顧客満足、コストパフォーマンス向上、経過時間、プロセスおよび製品の革新、あるいは従業員のエンゲージメントのいずれに属するものであっても、事業目的の達成度合いを測るために使用されている方法と同じ方法を用いて測定されることが往々にしてあります。「許容可能な業績の変動幅」の範囲内で業務を遂行することは、企業がリスクアペタイトの範囲内であるという、経営者にとっては大いなる自信につながるようになります。また同時に、ミッション・ビジョン・コアバリューと一貫性を保ちつつ、事業目的を達成できるという大いなる安心感にもつながります。

リスクをしっかりと把握する

戦略および事業目的の達成を妨げるリスクは特定され、評価されなければなりません。このような「実行段階のリスク」については、重要度やリスクアペタイトのコンテキストを踏まえ、優先順位をつけなければなりません。そこから組織はリスクへの対応について、許容できるリスク量を明示するポートフォリオを踏まえて判断します。このERMの3つ目の構成要素は、6つの原則によって支えられています。

実行段階のリスク

12. 実行段階のリスクを特定する
13. リスクの重要性を評価する
14. リスクの優先順位づけを行う
15. リスク対応策を特定し、選定する
16. 実行段階のリスクを評価する
17. ポートフォリオ視点を策定する

実行段階のリスクを特定する — 事業目標達成のために戦略を実行する際、組織は新たに顕在化したリスクのみならず、既知のリスクに起きた変化についても特定しなければなりません。その際、ビジネスコンテキストの変化に伴って出現するリスクの他、存在するが未発見のリスクについても考慮すべきです。

リスクの重要性を評価する — 予想されるリスクの重要性によっては、リスク評価の段階で定性的・定量的アプローチを用いることを、COSO は提唱しています。

定性的な評価アプローチは、リスクの定量化が出来ない、あるいはそのためのデータ収集が現実的ではない、費用対効果に見合わない時に用いられます。COSO が示すとおり、経営陣は、極端なインパクトが生じた場合を想定する時に、シナリオ分析を用いることがあります。また、複合的な要因によって生じる事象の影響を分析する場合は、シミュレーション分析を用いることもあるでしょう。反対に、多頻度かつ影響が小さいリスクについては、リスクの重大性を決定する方法として、データ分析、またはワークショップやインタビューといった、他の内部情報を用いることがより適しているときもあります。より定量化が容易なリスク、あるいは、より細かな粒度・精度が必要な場合においては、確率モデルによるアプローチが適しているかもしれません。

リスクの優先順位づけを行う — 組織は、しかるべき基準を用いてリスクへの対応を検討するために、リスクの優先度を決定します。リスクの優先度を測る基準としては、適応可能性、複雑性、速度、持続性、回復可能性を検討することが考えられます。さらに、リスクが、企業が設定した事業目的を達成するにあたり、リスクの許容限度、もしくはリスクアペタイトに近づいた場合、一般的に高い優先度が与えられます

リスク対応策を特定し、選定する — 特定されたリスクに対しては、経営陣は適切なリスク対応を選定し、実行することになります。その際、リスク対応策としては、受容・回避・活用・軽減・共有といった選択肢が選ばれることでしょう。リスク対応策を検討するにあたっては、経営者は、ビジネスコンテキスト、費用対効果、責務と期待、優先度、リスクの重要性と企業のリスクアペタイトといった要素を考慮する必要があります。

実行段階のリスクを評価する — リスクへの対応策が選択され、実行される際、それが意図されたとおりに実行されているかどうか、評価しなければなりません。リスク対応策の評価は、一般的に、特定されたリスクの効果的な管理に責任を負う立場の人や、企業の業績とリスク対応の有効性について保証を提供する立場の人によってなされます。彼らのガバナンスと監視責任の履行の一環として、企業の重大なリスク対応関わる評価を通して得られた透明性をもって、経営者と取締役会に対して報告がなされます。

ポートフォリオ視点を策定する — ERM は、リスクを全社レベルで、もしくはポートフォリオ視点で考えることを推奨しています。

COSO によると、「ポートフォリオ視点」とは、ビジネス上の目標達

成に伴って企業が直面するリスクに関して、複合的な視点で、経営者や取締役会がリスクの特徴や発生可能性、リスクの大きさや相互依存性、そしてパフォーマンスへの影響を検討すべきであるとしています。ポートフォリオ視点を通して、組織は全社レベルで重要リスクを特定し、残存リスクのリスクプロファイルが、全体のリスクアペタイトと整合しているかどうかを判断することになります。

リスク情報とレポートの価値を最大化する

4つ目の ERM の構成要素は、内外の情報ソースから、必要な情報を確保し、共有するためには継続的なプロセスが必要であるということです。決断に際して必要な情報は、組織の中で垂直的、水平的に広範囲に亘って流れる必要があります。このプロセスは、重要なリスクのステークホルダーに必要な洞察を提供します。4つの原則がこの構成要素を支えています。

リスク情報、コミュニケーションと報告

18. 関連情報を利用する
19. 情報システムを活用する
20. リスク情報に関するコミュニケーションを行う
21. リスク、カルチャーそしてパフォーマンスを報告する

関連情報を利用する — COSO は、「関連する情報」をビジネス上の意思決定を促進する情報と定義しています。情報が敏捷性の向上、先見性の向上、および予測の向上に貢献するほど、それはより「関連する情報」であるということになり、そして経営戦略を首尾よく遂行し、事業目的の達成へと導き、持続的な競争優位の確立に寄与することになります。

情報システムを活用する — 情報システムは、人やデータ、テクノロジーから成り立っており、ERM をサポートする上で必要なデータ・情報を組織に提供しています。COSO は、どの組織にも適用可能な特定のシステムはないと主張しています。しかし、経営をサポートするテクノロジーやシステムの選択・設計は、経営目的の達成や経営戦略遂行において重要なカギとなります。システムの選択と導入に影響する要因は、企業の目標、市場ニーズ、競合に勝ち抜く要件、コスト・ベネフィットです。

リスク情報に関するコミュニケーションを行う — 組織はいくつもの階層で、組織横断的にリスクに関する報告を行います。組織は、リスクのデータと情報を社内外のステークホルダーと共有するために、さまざまなチャネルを用います。これらのチャネルは、経営者が取締役会の監視の下、戦略を推し進め、事業目的を達成する意思決定をする際に役に立ちます。

リスク、カルチャー、パフォーマンスを報告する — リスク報告は、意思決定の支援・促進に貢献するもので、取締役会等がリスク監視責任を果たすために必要な情報を含んでいます。これには、リスク・カルチャー・パフォーマンスに関する数多くの報告があり、組織のサイズ・スコープ・規模や複雑性によって、単純なものから複

雑なものまで定量的・定性的なリスク情報が存在するのです。

リスク情報は、特定のビジネスエリアあるいはビジネスセグメントに関連するものであったり、さらには特定のリスクあるいは関連するリスクグループに的を絞ったものだったりするかもしれません。リスク報告は、組織内の異なる階層にごとに内容が調整され、企業の意思決定プロセスで役立ちます。しかし、経営者は報告されたデータや情報を使用し、重要な決定を行う際に、判断は経営者が下さなければなりません。

重要事項をモニタリングする

5つ目となる最後の構成要素は、組織がリスクマネジメントのパフォーマンス如何にモニターするか、さらにERMの構成要素が時の経過する中で、この変革期において如何に機能しているかという点に注目しています。効果的なモニタリングプロセスは、組織のリーダーがリスクとパフォーマンスの関係に対する洞察を得られること、戦略から生じるリスクがいかにパフォーマンスに影響を与えているか理解できることと、戦略を達成する際に生じるリスクを特定することを可能にします。この構成要素は、2つの原則によって支えられています。

リスクマネジメントの実効性のモニタリング

- 22. 大きな変化をモニタリングする
- 23. ERMをモニタリングする

大きな変化をモニタリングする — タイムリーに検討がなされない場合、変化が競合他社との大きなパフォーマンスギャップが生じたり、あるいは、戦略上の重要な前提が無意味なものとなる可能性があります。大きな変化についてのモニタリングは、平時のビジネスプロセス上に構築され、リアルタイムに行われるべきものです。

ERMをモニタリングする — ERMは、他のあらゆる業務と同様、継続的に改善されなければなりません。たとえ成熟したERMプロセスを有する組織であっても、さらなる価値向上を目指し、効率性・実効性の向上を図ることはできるのです。ERMが組織に浸

透するにつれ、絶え間なく行われる評価によって、改善すべき点が自然と明らかになります。独立的な評価（例えば、内部監査）もまたERMにおける改善の余地を発見する機会を提供します。

取締役会と経営陣への示唆

COSOの改訂ERMフレームワークは、組織のリーダーが検討すべき事項を提供する恰好の材料です。フレームワークに組み込まれた原則主義のアプローチは、あらゆるものに当てはめることができる、汎用性のあるソリューションがないことを示しています。なぜなら、どの組織も業界・戦略・構成・企業カルチャー・ビジネスモデル・財務状況は他の企業と異なる固有のものを持っているからです。

実務上、企業は取り巻く現実と環境に照らし合わせて、最も意味のある方法でフレームワークを導入することが可能です。私共は、企業リーダーが改訂フレームワークを用いて自社のリスクアプローチの評価を実施することは、自信をもって未来に臨む上で有益だと考えます。いくつかの課題には議論の余地があり、例えば、戦略の策定と完全に統合されたリスクといったものがあります。しかし、それらの課題を無視しておくことは、今日の予測不可能な世界でビジネスを行う際、コストがかさむ要因になるかもしれません。あるいは、致命的な結果を招くかもしれません。

結論

ERMフレームワークを更新する際、COSOは組織がより円滑に変化に対応できるようになる必要があると述べています。経営者は、大きな変動や複雑性、不確実性といった市場の動きに対し、いかに対処すべきか、考えなければなりません。

COSOは、本フレームワークを取締役会および経営者のニーズに合うよう、リスクを戦略およびパフォーマンスに組み入れるという、原則主義を用いて策定しました。コメントレーターやオンラインサーベイ (erm.coso.org) により、COSOに対して意見やフィードバックを提供する機会も与えられています。なお、最終的なフレームワークについては、2016年末となる見込みです。

Let's talk

企業のリーダーが本フレームワークを用いて自社のリスクアプローチの評価を実施することは、自信をもって未来に臨む上で有益だと考えます。COSO ERMについて、議論をしませんか。

www.protiviti.com/cosoerm

プロティビティについて

プロティビティ(Protiviti)は、リスクコンサルティングサービスと内部監査サービスを提供するグローバルコンサルティングファームです。北米、日本を含むアジア太平洋、ヨーロッパ、中南米、中近東、アフリカにおいて、ガバナンス・リスク・コントロール・モニタリング、オペレーション、テクノロジー、経理・財務におけるクライアントの皆様の課題解決を支援します。プロティビティのプロフェッショナルは、経験に裏付けられた高いコンピテンシーを有し、企業が抱えるさまざまな経営課題に対して、独自のアプローチとソリューションを提供します。

© 2016 Protiviti Inc. All rights reserved. 複写禁、転載禁