protiviti®
Global Business Consulting

2022年2月2日 Web塾「経営に活かす新COSOERM」第1回「経営に活かす新COSOERM」ご質問とプロティビティの回答

No.	頂いたご質問	Protiviti回答
1	コーポレートガバナンス・コードが言及する全社的リスク管理については、 必ず、COSOのフレームワークに準拠しなければならないのでしょうか。	必ずしもそうではありません。企業によっては複数のフレームワークを参照しながら、独自の全社的リスク管理のフレームワークを構築しているところもあります。 ただし、これから本腰を入れて全社的リスク管理体制を整備する、あるいは、既存の全社的リスク管理をこれから見直す会社におかれましては、COSOのフレームワークを少なくとも参照されることをお勧めします。COSOのフレームワークはグローバルに浸透しており、海外投資家との対話でも、COSOのフレームワークを活用されることが一案です。
2	新COSOERMの構成要素の最初に「ガバナンスとカルチャー」を掲げていますが、やはり、最も重要ということでしょうか。	はい、そのとおりです。「ガバナンスとカルチャー」は全社的リスク管理の他のすべての構成要素の基礎になります。ガバナンスは、全社的リスク管理の重要性を強調し、それに対する監督責任をしっかり確立する組織の気風を醸成します。カルチャーは、組織内の意思決定に反映されます。 例えば、金融庁の金融機関に対する監督や検査も最近はガバナンスとカルチャーを重視しています。また、業種を問わず、インシデントが発生すると、「取締役会は機能していたのか」、「企業風土はどうだったか」が問われる時代となりました。 「ガバナンスとカルチャー」はWeb塾第2回で、「取締役会のリスク監視」等関連の話や実務例を交えて解説します。
3	金融庁の方が今後のリスク管理状況を見ながらというときには何を参照・注視されるのでしょうか。	資料の18ページ「コーポレートガバナンス・コード再改訂の要点全社的リスク管理」でご紹介した、コーポレートガバナンス・コード再改訂版原則 4 － 3. 取締役会の役割・責務 （3）補充原則 4 － 3④「内部統制や先を見越した全社的リスク管理体制の整備は、適切なコンプライアンスの確保とリスクテイクの裏付けとなり得るものであり、取締役会はグループ全体を含めたこれらの体制を適切に構築し、内部監査部門を活用しつつ、その運用状況を監督すべきである。」に関連して、金融庁の幹部の方は、上場企業が今後、全社的リスク管理を整備運用する進展をふまえつつ、我が国の内部統制報告制度の見直しの機を検討していくとコメントされました。内部統制を包含する、上場企業全体のコーポレートガバナンスや全社的リスク管理の進展を参照・注視されていくと察します。

No.	頂いたご質問	Protiviti回答
4	DNAの図がわかりにくいです。統合させるとはどういうことですか。	資料の31ページ目でご紹介したDNAの図においては、5つの構成要素のうち、「戦略と目標設定」「パフォーマンス 」「レビューと修正」の3つの色のリボンが、全社的リスクマネジメントの共通のコアプロセスを表し、「ガバナンスとカルチャー」「情報・伝達・報告」の２つの色のリボンが全社的リスクマネジメントの支援的プロセスを表しています。これらの構成要素からなる全社的リスクマネジメントが、「戦略の策定、事業目標の体系化、その実践とパフォーマンス」からなるビジネスプロセスを貫いてDNAのように組み込まれ統合されることにより、価値の向上が実現できるというコンセプトを表しています。すなわち、戦略を含めたビジネスプロセスと、リスクマネジメントプロセスの統合を意味しています。DNAのようなラセン状としたのは、構成要素がお互い連携し合って、一体となって機能すべきであるとのメッセージを込めたと言われています。
5	リスクマネジメントは大切なことですが、一番の理想はリスクマネジメントしなくても良いことだと思います。リスクリスクと騒ぐばかりでなく、リスクマネジメントしなくても良い時代に向かわせるにはどういったことが必要でしょうか。	COSOERMのリスクの定義は「戦略と事業目標の達成に影響を及ぼす可能性」です。戦略や事業目標は不要、または、事業を取り巻く環境がほとんど変わらない、などの状況であれば、リスクマネジメントも不要かもしれません。しかしながら、我々が活動する事業環境では、目標が必要であり、またその目標に向かうのに多くの変化・不確実性があるのが現実です。不確実性が多いのは必ずしも、悪い意味だけではありません。機会も脅威も多いので、より不確実性に対応する能力の高い企業・組織はチャンスに変えていくでしょう。ダーウィンの言葉が有名です。『最も強い者が生き残るのではなく、最も賢い者が生き延びるのでもない。唯一生き残ることが出来るのは、変化できる者である。』リスクマネジメントをリスクを避ける取り組みと捉えるのではなく、変化に対応する取り組みと捉えれば、リスクマネジメントが事業運営に組み込まれ「リスクリスクと騒ぐ」必要はなくなるのかもしれません。
6	日本でERM活動が優秀、優れている業界や企業はどこでしょうか。やはり金融業界でしょうか。	「内部統制や全社的リスク管理をめぐる歴史」でご覧いただいたとおり、金融危機や個別のインシデントを受けて、金融業界はERM活動を強化してきたことは事実です。また、グローバルな企業と連携してきた商社やエネルギー業界、化学業界も早めに全社的リスク管理を取り入れた業界といえます。ただし、「新COSO内部統制の特徴」で言及したとおり、ERMは経営活動そのものと解していますので、業界で優劣はつきません。

No.	頂いたご質問	Protiviti回答
7	アート＆サイエンスとは、ERMのためには定量と定性双方からのアプローチが必要になるという意味でしょうか。	2017年に公表された新COSOERMのエグゼクティブサマリーは、「変化するリスク情勢」のタイトルのもと、「リスクとは選択の芸術（アート）と科学（サイエンス）である、という理解が現代経済の中核にある。」との一文で始まります。そして、その後に、「起こり得る成果の範囲を最適化しようとするため、意思決定は、正しいか、間違っているかというような二者択一にはめったにならない。これが、全社的リスクマネジメントが芸術でもあり科学でもあるといわれる所以である。」と記述しています。 全社的リスク管理は確かに、ガバナンスやカルチャー、事業の中で経営者や管理者の経験と判断に基づく意思決定など、芸術（アート）的な要素が含まれています。同時に、リスク管理プロセスの体系化や、リスクスコアリング・レーティングなどのリスク評価手法、リスク指標、モニタリング手法の進化に見られるとおり、科学（サイエンス）的な要素も含まれています。これらを「定量と定性双方からのアプローチ」と呼ぶかは、受け取り方によるかと思います。
8	COSOでは、定期的にフレームワークを改定する計画でいるのでしょうか。5年単位等。	COSOはこれまで定期的にフレームワークを改訂することはしていません。改訂には、かなりの労力と時間がかかることも背景にあると思います。内部統制のフレームワークは21年ぶりに2013年に、ERMのフレームワークは13年ぶりに2017年に改訂されました。他方、資料の9ページでご紹介した2018年公表の「ERMのESG関連リスクへの適用」のほか、COSOはこれまでにいくつものガイダンスを公表しています。 https://www.coso.org のGuidanceのサイトをご参照ください。
9	自社ERM活動を評価したいが、ISO14001や45001は認証制度があるので、自社活動の評価につながるのかなと思っています。どういった手法を取るとよいでしょうか。	ERM活動を評価する手法としては、ERM推進部門が独自の評価項目を設定し検証する自己評価や、内部監査部門が評価項目を設定し評価する独立的評価が考えられます。それぞれの評価項目を設定する際には、COSO ERMフレームワークのコンセプトや原則、さらにリスクマネジメントに関するフレームワークISO31000を活用することができます。 外部の専門家を起用することも一案です。弊社も、ERMの有効性評価や内部監査、改善プランの策定等の支援業務を提供しています。

No.	頂いたご質問	Protiviti回答
10	内部統制に関わる者として、経営層がERMのベネフィットに関心を示し難く、すなわちリスク管理は法務や経理や内部監査のレベルでの「担当業務」とされています。他社におかれましても直面されている課題かもしれません。どのようにブレイクスルーできますか。特効薬はないまもしれませんが、幾つかの方法をご教示いただけますか。	講義でも解説したとおり、ERMは経営そのもの、と私どもでは捉えています。海外でも浸透しているCOSOの枠組みを用いて貴社の経営活動を整理して説明することは、海外投資家ほかのステークホルダーとの対話に役立つことにはならないでしょうか。　金融庁の「スチュワードシップ・コード及びコーポレートガバナンス・コードのフォローアップ会議」第25回において、ICGNのケリー・ワリング氏が、海外投資家の立場を代表して、リスク管理ほかに対する期待を表明した書簡が公表されていますので、その内容を経営層にご覧いただくのも一案かと思います。 海外企業では、全社的リスク管理のベスト・プラクティスを、社外取締役が他に関与する会社に紹介することも珍しくありません。社外役員の方と連携することも一案かと思います。 もし貴社が全社的リスク管理を導入されているのであれば、毎年同じようなリスクが列挙されることにより、経営層の関心が薄れている可能性はありますか。かかる場合には、経営戦略の展開に合わせてリスクを列挙出来ているかを点検されることも一案かと思います。
11	講義中のアンケートにあったとおり、COSOERMは概念論であるため、その概念を用いて経営のどういう課題を解決したいかの具体化が必要になるが、この概念を具体化していくプロセスが難しく感じています。何のためにERMを導入するのか、この問いに答えていくためのステップやガイドラインがあれば、教えてください。	何のためのERMかというメッセージについては、プロティビティの発行している下記の「取締役会のリスク監視」シリーズが参考になると思います。 Risk Oversight vol.95：今こそERMを見直す時 （https://www.protiviti.com/sites/default/files/japan/insights/riskoversight_vol95_j.pdf） Risk Oversight vol.117 ：取締役会は、適切なリスクに焦点を当てていますか （https://www.protiviti.com/sites/default/files/japan/insights/riskoversight_vol117_j.pdf） 日本内部監査協会のERM資料集も参考になると思います。 https://www.iiajapan.com/leg/data/ERM_TOP.html なお、第2回では「ERMを効果的に推進するための業務構造」について解説するほか、次回以降に概念を具体化するためのヒントをお伝えする予定です。
12	リスクマネジメント人材は、どのように育成すれば良いでしょうか。	第2回でご紹介する予定ですが、2017年COSOERMは、構成要素「ガバナンスとカルチャー」の原則５「有能な人材を惹きつけ、育成し、保持する」にて、育成の要点を解説しています。同時に、エグゼクティブ・サマリーで、「いくつかの疑問を解く」として、「全社的リスクマネジメントは機能や部門ではない。」と述べています。 ご質問の「リスクマネジメント人材」の育成には、研修を重ねることも必要ですが、オンザジョブトレーニングが極めて重要です。経営陣以下、リスクマネジメントを理解する人材が、各部門におけるリスクマネジメントを指導していくことが重要です。

No.	頂いたご質問	Protiviti回答
13	お話いただいた内容を全社的に共有していくためには、どのような方法があるでしょうか。内部監査担当者は理解してもそれを共有する方法がなかなか難しいと感じています。	資料の16ページ「コーポレートガバナンス・コード再改訂の要点 全社的リスク管理」で解説したとおり、上場企業においては、全社的リスク管理の体制整備と運用状況の監督を取締役の役割・責務として対応する必要があります。まずは、取締役会事務局や経営企画部門と講義内容を共有して、取締役会や経営陣の皆様向けの説明の場を企画したり、本講義のオンデマンドのビデオを観ていただくのは、いかがでしょう。