protiviti®
Face the Future with Confidence

取締役会のリスク監視：Risk Oversight

内部監査の監督における4つのC

プロティビティは常に、取締役会は自社の内部監査の潜在力を最大化すべきであると考えてきました。リスクベースの監査計画の十分性を評価する際に、取締役は4つのCを考慮すべきです：文化（culture）、競争力（competitiveness）、コンプライアンス（compliance）、およびサイバーセキュリティ（cybersecurity）。

ISSUE 88

2016年、内部監査人協会とプロティビティは、取締役を含む重要なステークホルダーが内部監査に期待するパフォーマンスを見定めるべく、内部監査の実務家を対象とした世界最大規模の継続的取組みである「内部監査の国際的共通知識体系（CBOK）」調査を実施しました。調査結果は、取締役は内部監査に以下を含む事項を求めていることを明らかにしています。それは、戦略リスクへの焦点、監査計画の対象範囲を超えた思考、およびコンサルティングを通じた価値の付加です。

主要な考慮事項

CBOKの調査が示す取締役の期待と、プロティビティの取締役会支援における経験から、内部監査にとっての複数の機会があると考えます。

- リスク文化の退廃の兆候に注意する。
- 市場における組織の競争力の土台を理解した上で内部監査に臨む。内部監査担当役員と内部監査スタッフは、監査における複数の気付き事項、とりわけ事業モデルの効率性と実効性の改善機会につながる可能性のある気付き事項を検討する際に、「点と点をつなげる」べきである。
- コンプライアンスに関する重要事項および関連する報告の品質に対して、監査計画の焦点を広げる。
- 重要性の高いリスクに焦点を当てる。現在、サイバーセキュリティが多くの企業にとって重要性の高いリスクとして挙げられる。

これらの4つのC－文化（culture）、競争力（competitiveness）、コンプライアンス（compliance）、およびサイバーセキュリティ（cybersecurity）－は、取締役がリスクベースの監査計画に対して期待すべき事項を示唆しています。以下ではこれらの4つのCについて詳細に考察します。

文化

経営者と取締役は、リスクマネジメント、内部統制、あるいはコンプライアンスの破綻のほとんどが、常に機能不全の文化によるものであることを理解しています。経営者と取締役は、文化的な機能不全は一夜にして生じるものではないことも理解しています。文化的な機能不全が生み出すリスクの兆候が明らかになるには長い期間を要し、レピュテーションを損なう事象を生じさせ得ることは必然の帰結といえます。

機能不全の文化の例としては、以下のようなことが行われてしまう環境が挙げられます：上級リーダーが事業の現実を認識していない、公衆の安全よりもコストと納期が優先されている、排出に関する虚偽報告を可能とする、あるいは不適切なパフォーマンスに関するインセンティブのために受容し得ないリスクテイクが行われている。これらの種類の環境を生み出すような文化が形成されてから、その帰結が明らかになるまでには長い時間がかかります。しかし、機能不全が放置された場合には、その帰結はいずれ明らかとなります。そして、重大な帰結が明らかとなるごとに何が起きるでしょうか。誰もが逃げ場所を求めて走るのです。

組織の文化とは、倫理的で責任ある企業行動へのコミットメントだけではありません。組織の文化は、組織を特徴づける共有される価値、心構え、および行動パターンが混じり合ったものです。バリュー・ステートメント、行動規範、および倫理プログラムに加えて、リスクマネジメントに関連する文化

は、確立した方針と手続き、リスク委員会の監視活動、インセンティブ・プログラム、リスク評価プロセス、重要リスク指標に関する報告とパフォーマンス・レビュー、および改善・強化プロセスなどによっても影響されます。それはまた、経営者チームと取締役会のリスクアペタイトに関する対話、リスクアペタイトのリスク許容度への分解、および企業戦略の日々の実行に用いられるリスクの制限への仕組みも含みます。

取締役会が文化の問題を十分に理解するにはどうすればよいのでしょうか。取締役と経営者は文化的な機能不全の存在をどのように認識するのでしょうか。最も重要なことは、手遅れになる前に取締役会が機能不全の芽を摘むにはどうすればよいのかということなのです。

取締役は、監査担当役員が組織の文化に関する独立的な「目と耳」としての役割を果たすと期待できるでしょう。特に、内部監査には以下の事項が求めることが可能でしょう。それは、全体的な業務環境の理解、従業員の相互コミュニケーションと職場の習慣を規定する不文の規範とルールの特定、有効な内部統制環境とコミュニケーションの流れに対する障害の明確化、リスクテイクとリスクマネジメントに関する受容し得ない行動、決定、心構えについての報告、および特定された問題への対応に関する推奨の作成などです。

内部監査は、一層の調査が必要な事項について警告を発することができます（例としては、短期的な目標を達成するためのリスクテイクを促す非現実的なパフォーマンス指標、複雑かつ不明確な法的な組織構造と報告体系、企業買収がうまく実行されないことにより局所的に蔓延する不適切行動、財務上の規律の欠如、および解雇の恐怖のために常に神経が高ぶっている従業員などが挙げられます）。内部監査は、中間層および下部層の姿勢が、リーダーが認識している上層部の姿勢と合致しているかについての評価を支援することができます。上層部の姿勢と中間層および下部層の姿勢の比較は実に意義深いものであり、本当に耳を傾けたいと考えている経営者が現実を認識する上で特に有用です。

競争力

自社の業務プロセスが、他社あるいは業界で最も優れた企業よりも劣った実務のために、十分な競争力を持つ水準で実施されていない場合、それは内部監査にとって業務の効率性と実効性を改善する機会となります。つまり、取締役会は内部監査に対して、伝統的なコンプライアンスに関する領域や財務報告に留まらず、組織の業務の継続的改善における支援を期待すべきです。

ほとんどの組織は、市場における競争優位を成功裏に確立し維持しているかについてモニタリングを行う際に、何らかの形でバランスト・スコアカードを用いています。重要業績指標（KPI）は、品質、納期、コスト、およびイノベーションにおけるパフォーマンスといった重要な領域に対応します。それらは多くの場合、顧客と従業員の満足度に関する指標を含みます。内部監査は、意思決定に用いるこれらの指標の信頼性についての評価を支援することができるでしょう。加えて、内部監査は、特定の指標について、競合他社および業界で最も優れた企業との比較を行い、適時に是正が必要なパフォーマンス・ギャップを特定することができるでしょう。

コンプライアンス

伝統的に、内部監査計画は、法令と内部方針に関する組織の遵守に関連する重要領域に問題がないことを確保することに対応しています。第3のディフェンスラインとして、内部監査は以下の事項を確認すべきです。

1. コンプライアンスに大きく関係する活動を行っている第一線の業務担当者と職能部門のリーダーは、コンプライアンス・リスクの特定と管理は自己の責任であると認識しており、コンプライアンス違反のリスクを受容可能な水準にまで低減するために有効な統制を整備しているか。
2. 独立したコンプライアンス部門（第2のディフェンスライン）の対応範囲は、企業が抱えるコンプライアンス上の課題の重要性に釣り合っており、経営者と一義的なリスクオーナーに対して信頼性のある洞察を適時に提供できているか。

コンプライアンス部門が存在するか否かに関わらず、内部監査は、最も重要なコンプライアンス・リスクに対応する、費用対効果に優れたモニタリング・プロセスが整備されているかを判断することができます。また、内部監査は、コンプライアンス・プログラムの全体的な実施と、適用される法令と企業の必要に応じたプログラムの定期的な更新について評価を行うことができます。

サイバーセキュリティ

この領域は取締役会にとって引き続き重要な関心事であり、当面は注視すべき分野であると考えられます。最近の調査では、サイバーセキュリティは2017年において3番目に重要な企業が直面する不確実性であることが示されています。[1] 内部監査は、複数の方法により、この領域において取締役を支援することができます。

第一に、内部監査は、企業の業務プロセスが価値の高い情報と情報システムに対して十分な注意を向けているかについて、評価を行うことできます。全てのシステムは等しく重要

1 Executive Perspectives on Top Risks for 2017, Protiviti and North Carolina State University's ERM Initiative (www.protiviti.com/TopRisks)

であるという前提に基づいて保護措置を取り、不必要なコストと特に重要な資産に対する注意の欠如を生じさせるのではなく、内部監査は、企業の最も重要な資産が何であるかについてIT組織と事業部門のリーダーが合意しているかを評価することができます。この評価には、組織の最も重要なデータと情報資産、情報システムの特定、およびなぜそれらが最も高い価値を持つのか、企業にとって喪失を許容できないものが何であるのか、そしてこれらの重要な資産にアクセスする権限を誰が有しているのかについての理解も含まれます。

第二に、内部監査は、脅威の状況を理解する上で取締役会と上級経営者を支援することができます。経営者は、自社の最も重要な資産、自社の業種と業務の特質、および潜在的なターゲットとしての自社の目立ちやすさに基づいて、自社のサイバーセキュリティ・リスクを評価すべきです。例えば、誰が攻撃を仕掛けてくるでしょうか、どのような攻撃が行われるでしょうか、自社の最大の脆弱性はどこにあるでしょうか、現状の内部統制はどの程度効果的でしょうか、侵入テストを行っているでしょうか、行っているとすればどのようなテスト結果でしょうか。これらの問いや他の問いに答えることは、変化し続ける脅威の状況を明確化する助けとなります。

最後に、内部監査は、組織のサイバー事故への対応準備を評価することができます。ここにおける問いは、企業が実効性のある対応計画を整備しているかということです。サイバー攻撃は比較的発生可能性の低い事故であるとの前提は過去のものとなり、そのような攻撃は発生可能性が高いだけではなく、事実として不可避であることが認識されるようになりました。従って、攻撃の影響と拡散を低減する上で、実効性のある事故対応プロセスは企業の対応準備において大きな重要性を有します。

内部監査は、セキュリティ事故のリスクを受容し得る水準に低減するための戦略が適切であり、焦点を定めたものであるか、事故対応の実効性についての定期的なテストを組織が積極的に行っているか、および具体的な事故の種類に応じて取るべき対応についての指針を示す手続きにより対応計画が補完されているかを確認するために、事故対応計画の評価を支援することができます。

要約すると、監査気付き事項の含意により広く焦点を当て、監査計画の明示的あるいは暗示的な境界線を越えて思考することにより、内部監査は、取締役の求めに合致した、より堅固で実務的かつ強力な推奨事項を提示できるようになるでしょう。4つのCは、取締役会が目を向けるべき領域についての視点を提供するものです。

取締役会の考慮事項

以下は、事業体の活動に内在するリスクに関連して取締役会が考慮すべき事項です。

- 取締役は、事業環境や自社業務の変化を踏まえ、内部監査活動の範囲が十分であることを確認しているか。取締役会は、適切な領域において必要な保証を内部監査から得ているか。
- 内部監査担当役員は、取締役会と経営者に対して、組織の文化に関する潜在的な盲点やその他の課題についての洞察を提供しているか。
- 内部監査計画は、競争力、コンプライアンス、およびサイバーセキュリティにおける重要領域に対応する上で十分なリソースを配分しているか。

プロティビティの支援

プロティビティは、包括的な内部監査サービスの提供におけるグローバル・リーダーです。プロティビティは、上場・非上場両方の大小様々な企業において、内部監査の要請への対応を支援するために内部監査担当役員、経営者、および監査委員会と協働しています。そのような支援には、内部監査を完全にアウトソースし、一から内部監査活動を立ち上げる場合や、既存の内部監査部門が十分なスタッフやスキルを欠いている場合の補完的支援が含まれます。プロティビティが提供するサービスは、本資料で検討した4つの領域にお客様が焦点を当てるための支援を行います。

protiviti®