protiviti®
Global Business Consulting

THE BULLETIN

OUR VIEW ON CORPORATE GOVERNANCE MATTERS

VOLUME 8, ISSUE 9

2025年監査委員会の議題

次の12ヶ月も、監査委員会にとっては引き続き厳しい年になると予想されます。2025年に向けて私たちが取り上げた9つのトピックには、各監査委員会の憲章（基本方針）に記載されている公式の責任範囲を超えると考えられる分野が含まれる可能性があります。実は近年、多くの監査委員会が責任範囲の拡大を経験し、より広範なテーマを監督することが求められるようになっています。もしも以下に列挙した項目のいずれかについて別の委員会が正式な責任を負っている場合には、監査委員会は、これらの項目が及ぼす財務や報告、内部統制への影響について協力し、助言を提供すべきです。

2025年の監査委員会の考慮事項

1. サイバーセキュリティの脆弱性に関して、監査委員会が独立した保証を適切に受け取っているかを確認する
2. 生成AIへの投資と機会を、組織が責任を持って評価し活用しているかを判断する
3. 組織とサードパーティ（第三者）との関係に対するガバナンスの成熟度を検討する
4. 監査委員会が、テクノロジー関連のリスクを効果的に監視できるだけの専門知識を有しているかを検証する
5. 内部監査機能の戦略を評価し、組織に価値を付加し続けられるペースで進化しているかを評価する
6. 組織における不正リスクの程度と軽減に向けた戦略の有効性を再確認する
7. 気候変動リスクやその他のサステナビリティ開示要求事項に対する組織の対応状況を評価する
8. 全社的リスクの特定と管理プロセスの完全性や妥当性を確認する
9. 監査委員会に対する経営陣の報告の有効性を評価する

1. サイバーセキュリティの脆弱性に関して、監査委員会が独立した保証を適切に受け取っているかを確認する

監査委員会は、長年にわたり多くの組織で最重要リスクとみなされているサイバーセキュリティの管理責任者から、定期的に最新情報を受け取るべきです。このような基本的な期待は一般的に充足されているはずですが、監査委員会は、最高情報セキュリティ責任者（CISO）が組織の資産を保護するためにいかに積極的に行動しているかを強調して報告する内容を鵜呑みにしないよう留意する必要があります。

ガバナンスを有効に機能させるには、サイバーセキュリティリスクを管理するのに配分された人材やプロセス、技術が有効に機能しているかについて、通常、内部監査部門が独立した保証を提供するものです。実際には、多くの内部監査部門は、第2ラインによる対応やIT部門による外部評価者の起用に依拠し、範囲設定や課題のフォローアップに、あまり関与していない場合が見受けられます。多くの場合、内部監査部門がかかる評価を効果的に実施するための必要なスキルを有していないか、IT部門と連携して適切な保証レベルを確保するために必要な関係を構築していないことが原因です。取締役はこれらの状況を警戒すべき重大な問題として認識すべきです。

なぜそれが重要なのか：

サイバーセキュリティリスクを効果的に管理できないことによるコストは、広く知られています。IBM社の「データ侵害のコストに関する調査2024年」レポートによると、システムの複雑さとスキルの不足により、情報漏えいのコストは世界的に増大し、インシデント1件あたり平均500万ドル近くに達していることが判明しました[1]。

重要な質問

- 監査委員会は、サイバーセキュリティ関連のリスクについて、どのくらいの頻度で、誰から報告を受けていますか。
- 誰が独立した評価の範囲を決定し、評価結果の透明性を確保するためにどのような措置が取られていますか。
- 内部監査部門はサイバーセキュリティリスクに対してどのような範囲で対応し、その対応範囲の根拠は妥当ですか。
- サイバーセキュリティの評価は、高リスク環境全体における重要なテクノロジー・コントロールの整備と運用の両方をカバーしていますか。

2. 生成AIへの投資と機会を、組織が責任を持って評価し活用しているかを判断する

2024年の一年間に、個人と企業によるAIの利用が爆発的に拡大しています。全体的な導入率は高いものの、多くの組織でAIがどこでどのように利用されているかは大きく異なります。テクノロジー中心の組織は多額の投資を行い、従業員に独自の生成AIのテクノロジーを活用するよう促しています。他方、技術的な成熟度が低い組織では、広く利用可能で安全性の低いツールの活用を従業員任せにしているケースが散見されます。規制当局が対応方針に苦慮し、取締役会は適切な質問を把握するのに苦心する中、多くの組織で懸念すべきギャップが生じている可能性があります。

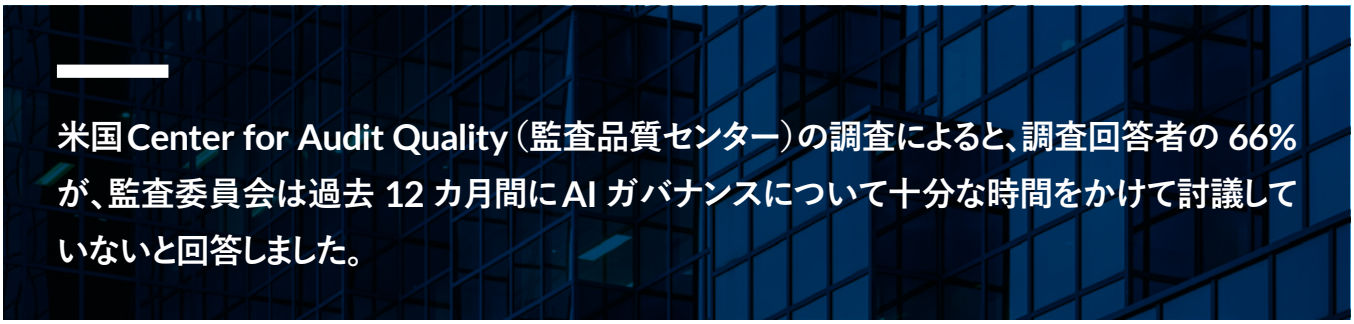
AIに積極的な企業は機会と影響を管理するのに適切なガバナンス態勢に投資しますが、これは所与のものではありません。同様に、AIに積極的でない組織が、従業員が引き起こすリスクを軽視することも的外れです。米国Center for Audit Quality（監査品質センター）の調査によると、調査回答者の66％が、監査委員会は過去12ヶ月間にAIガバナンスについて十分な時間をかけて討議していないと回答しました[2]。

1　2024年データ侵害のコストに関する調査、IBM: https://www.ibm.com/jp-ja/reports/data-breach

2　Audit Committee Oversight in the Age of Generative AI, CAQ, July 2024: https://www.thecaq.org/ac-oversight-in-the-age-of-genai

なぜそれが重要なのか：

AIの利用には、データプライバシーやセキュリティに係る数多くの懸念事項があり、規制当局はいずれ厳格に監視することになるでしょう。監査委員会は、責任あるAIの展開に向け、関連するリスク管理活動の有効性を検討しながら、組織のAIへの投資と利用の程度を理解する必要があります。



重要な質問

- 組織は、AIの責任ある利用を管理するための方針や枠組みを整備していますか。
- 組織は、各部門や組織全体にわたるAIの利用を追跡・監視するプロセスを定義し、そのための十分な能力を有していますか。
- 広く利用可能な生成AIツールを組織で活用することに関して、効果的なコミュニケーション戦略が確立されていますか。
- 主要な競合他社はAI関連テクノロジーの活用についてどのような投資を行っていますか。

3. 組織とサードパーティ（第三者）との関係に対するガバナンスの成熟度を検討する

プロティビティの2024グローバル・ファイナンス・トレンド・サーベイ[3]によると、売掛金や財務報告、財務計画と分析（FP&A）、総勘定元帳業務など、重要な財務・会計業務のほぼ半数は従業員以外が担っています。ITやその他の業務分野でも同様の傾向が見られ、各業務の執行責任が、十分に審査された従業員基盤の外側に移管されている割合が増加しています。スキルセットとキャパシティーの課題に対処するために、アメリカ国内で限りのあるパート労働者のプールやオフショア・アウトソーシングサービスのプロバイダー、その他のプロフェッショナル・サービス関係を活用することは、あらゆる産業で一般的に受け入れられつつあります。これらの人材モデルは、一般的なリスクと固有のリスクを考慮する必要があり、統制環境の範囲を確実に拡大させています。

サードパーティへの委託の利用が増えるのに伴い、組織のサードパーティリスク管理の成熟度も向上させる必要があります。さらに、業務上重要な機能であればあるほど、デューディリジェンスや契約、オンボーディング、モニタリング、オフボーディングの手順が堅牢であることがより重要になります。

なぜそれが重要なのか：

不適切なサードパーティを起用すると、財務報告プロセスだけでなく重要な業務プロセスにも深刻な影響を与える可能性が生じます。もしも適切な契約条件やサービス毎の約定、モニタリング機能を有しなければ、許容範囲をはるかに超える財務リスクが発現する恐れがあります。さらに、多くのサイバー関連のインシデントは、効果的なガバナンス構造に組み込まれていないサードパーティとの関係に起因しています。

3 Transform: Assessing CFO and Finance Leader Perspectives and Priorities for the Coming Year, Protiviti, 2024: https://www.protiviti.com/sites/default/files/2024-09/2024_global_finance_trends_survey_protiviti.pdf

重要な質問

– 主要な経営管理プロセスと統制にサードパーティを利用する組織上の傾向はどのように変化していますか。

– サードパーティに関連するオペレーショナルリスクやサイバーセキュリティ、レジリエンス、コンプライアンス、評判リスク、地政学的リスク、その他のリスクを管理するために、主要なガバナンス構造がどのように確立され、運用されていますか。

– ベンダーの管理活動は、各事業分野でどの程度一元化または分散化されていますか。また、新たな関係（SaaSプロバイダーなど）を特定するために、どのような監視機能が存在しますか。

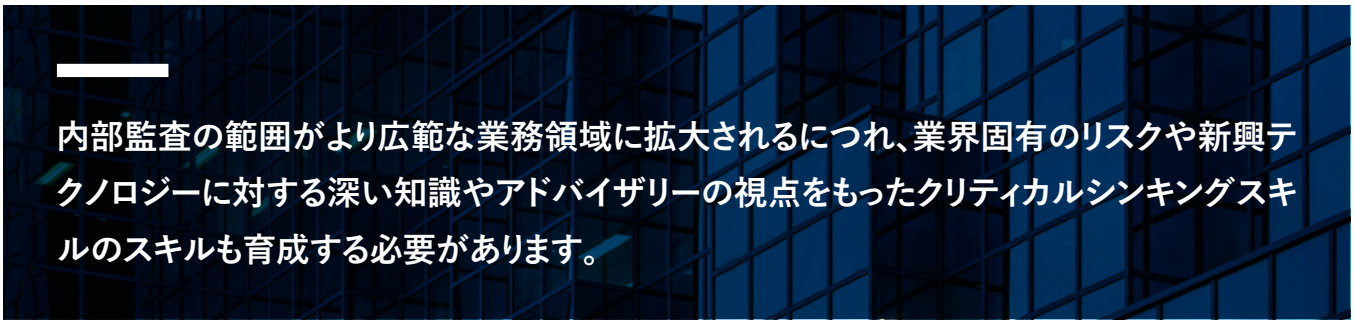
– 主要なサードパーティが業務を突然停止したり、長時間のシステム障害やランサムウェア被害が発生した場合に備えて、どのような危機対応計画が確立されていますか。

4. 監査委員会が、テクノロジー関連のリスクを効果的に監視できるだけの専門知識を有しているかを検証する

Corporate Governance Institute（コーポレートガバナンス研究所）によると、取締役の60％が、取締役会はテクノロジーの使用を効果的に監督するスキルや知識を有していないと考えています[4]。今日のデジタル社会では、すべての取締役が一定のテクノロジーリテラシーを備えるべきであり、近い将来、ビジネスや業界全体を変革するような重要なトレンドについて十分な知見を持つ取締役の存在が不可欠です。しかし、取締役会の半数未満しか各取締役の評価を実施していない現状を踏まえると、取締役会や監査委員会が取締役のテクノロジースキルの有無を厳しく見極め、必要があれば、効果的なガバナンスに向けて重要な変革を行う時期に来ているといえます。

なぜそれが重要なのか：

技術革新と変化が激しい時代において、取締役会は、投資やリスク管理手法の指南役として、ガバナンス体制全体にとって重要な要素です。クラウドインフラや生成AI、量子コンピューティングへの投資と適用は爆発的に増え続け、適切な対策が講じられなければ、経営陣と取締役会の間の知識格差は拡大する可能性があります。こうした大規模なテクノロジー投資の多くは、財務や会計プロセスの変革を支援し、業務プロセスに重大な影響を与えます。今進める投資は、将来的に業務効率や顧客体験を変える可能性があり、組織の業績に大きな影響を与えるかもしれないのです。



重要な質問

– 現在の委員会の構成はどのようなテクノロジーの専門知識を有し、どの委員会メンバーの経験がテクノロジー関連リスクの効果的な監視を可能にしますか。

– 委員会のテクノロジー関連の経験は、現在の業界動向や会社に影響を及ぼす将来の検討事項に適合していますか。

4 “Adapt or Perish: Boards and Technology,” by Dan Byrne, Corporate Governance Institute: https://www.thecorporategovernanceinstitute.com/insights/guides/boards-and-technology-adapt-or-perish/

– 委員会メンバーを交代させ、定期的に新しい知識と専門性を委員会にもたらすためにどのようなアプローチをとっていますか。

– 委員会は、必要に応じて特定の専門知識（サイバーセキュリティなど）に係る独立したアドバイザーを起用していますか。

5. 内部監査機能の戦略を評価し、組織に価値を付加し続けられるペースで進化しているかを評価する

監査委員会は、最高監査責任者（CAE）や最高リスク管理責任者（CRO）（またはそれに相当する者）と協働して、事業目標の達成に最も脅威を与えるリスクの特定を支援すべきです。内部監査部門は、例えばシェアードサービスへの移行の際やシステム導入期間中における内部統制に着目するなど、多くの組織の変革領域で支援できるポジションにあります。M&A活動が再び活発化する中、ディールの準備段階の支援など、必ずしも日頃は十分に活用されていないスキルを求められる領域があるかもしれません。独立性の確保を考慮すべき活動もありますが、内部監査がこうして貢献できる領域があることは否定できません。

内部監査の範囲が進化するにつれて、監査人に求められるスキルセットも進化します。継続的な学習と啓発を重視することで、チームはデータ分析やAIガバナンス、サイバーセキュリティなどの分野で必要な専門知識を獲得することができます。内部監査の範囲がより広範な業務領域に拡大されるにつれ、業界固有のリスクや新興テクノロジーに関するより深い知識やアドバイザリーの視点をもったクリティカルシンキングのスキルも育成する必要があります。

なぜそれが重要なのか：

監査委員達は、組織の全体的な戦略に即して内部監査部門の戦略を進化させるのを支援し、奨励することで多大に貢献することができます[5]。内部監査機能の戦略がこのように進化し続けなければ、提供できる価値は限られてしまいます。

重要な質問

– 現在の内部監査部門の戦略は、全体的な事業戦略や目標とどのように整合していますか。整合性はどのくらいの頻度で点検されていますか。

– サイバーセキュリティの脅威やテクノロジーの進歩、規制の変更、環境・社会・ガバナンス（ESG）への配慮をはじめとして新たなリスクに対処するために、監査戦略や監査計画に最近どのような変更が加えられましたか。

– 内部監査担当者が、進化するビジネスの複雑性とリスクに対処する必要なスキルを確保するために、どのような措置が講じられ、どのような継続研修プログラムが提供されていますか。

– 労働市場における困難が続く中、内部監査に必要な人材を確保していますか。それをどのように確認していますか。

6. 組織における不正リスクの程度と軽減に向けた戦略の有効性を再確認する

さまざまな要因によって、たとえば、従業員がリモートで複数の仕事に就いたり、いわゆる「静かな退職」（quiet quitting）をしたりする事例など、企業は新たな問題への対応を迫られています。消え去ることなく進化を続けている永続的な課題のひとつが、企業不正です。デジタル時代のリモートワークが従業員による不正の機会を増やしたとは言い切れませんが、いわゆる不正のトライアングルの要素の中で最も変化したのは正当化かもしれません[6]。企業は政治家やソーシャルメディア、アクティビストたちから頻繁に標的にされ、たとえ財務上の収益が限定的であっても、しばしば「貪欲な存在」とみなされがちです。今こそ、組織は自社の仮想空間（デジタル領域）と物理的空間における不

5 2024 Global Internal Audit Standards, The Institute of Internal Auditors: www.theiia.org/en/standards/2024-standards/global-internal-audit-standards.

6 “Fraud 101: What Is Fraud?” Association of Certified Fraud Examiners: https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

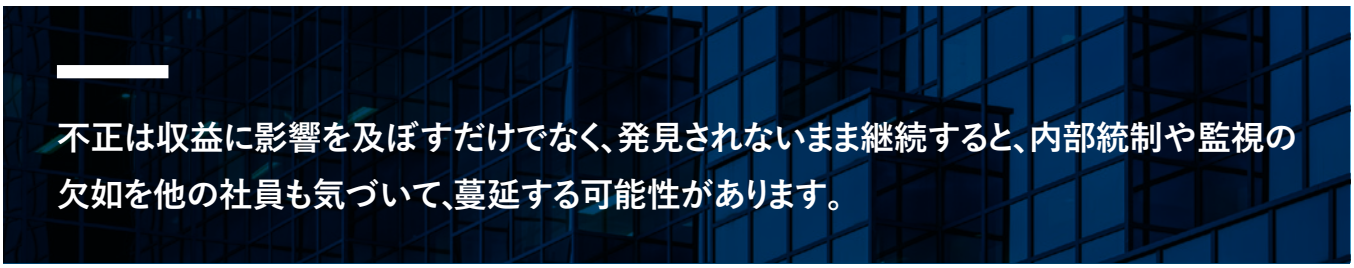
正の可能性を改めて徹底的に見直すべき時期に来ています。さらに、従業員だけでなく、業務の委託先やベンダー、顧客を含めたシナリオを積極的に検討することで、意外な結果が見えてくるかもしれません。

なぜそれが重要なのか：

不正は日常的に発生しており、あなたの組織でも今まさに起きている可能性があります。公認不正検査士協会が発表した『2024年版ネーションズレポート』によると、毎年何千件もの不正行為が行われ、企業は何十億ドルもの損失を被っています[7]。不正は収益に影響を及ぼすだけでなく、発見されないまま継続すると、内部統制や監視の欠如を他の社員も気づいて、蔓延する可能性があります。

重要な質問

- 経営陣は過去5年間に不正行為を特定しましたか。もしそうなら、これらの事例からどのような教訓が得られましたか。
- 組織は、一般的な不正のシナリオを特定するために、適切なリーダーを任命し、さまざまな業務領域が関与する、不正リスク評価を行っていますか。不正の影響を最も受けやすい分野がどこかを評価していますか。
- 従業員通報制度は有効に導入され、周知され、対応状況を監視していますか。監査委員会は、未加工で通報内容を見ていますか。
- 内部監査は不正行為を年度計画プロセスの一環で考慮するとともに、個別の監査の過程でも再度考慮していますか。



7. 気候変動リスクやその他のサステナビリティ開示要求事項に対する組織の対応状況を評価する

米国証券取引委員会（SEC）の規則案が施行されるかは不透明ですが、欧州持続可能性報告基準（ESRS）やEUの企業持続可能性報告指令（CSRD）、カリフォルニア州の法律など、既存の規制は、気候変動に関連する影響について、より詳細な情報を開示するよう企業に求めています。気候変動は、物理的リスク（異常気象など）や移行リスク（市場嗜好や規制環境の変化など）を含む新たな財務リスクをもたらします。ほとんどの規則は一定の保証（アシュアランス）を要求しており、報告された特定の項目について、将来的に監査対象となる可能性があることが示されています[8]。

前述の規制の要求事項が適用されるまでの期間が延長されたとしても、予想される開示を担保するプロセスを設計し、運用する必要があります。現行規制の直接の対象にはならない規模の組織であっても、顧客やベンダーから情報を求められるため、影響を受けます。重要なことは、この情報を自主的に報告している圧倒的多数の企業は、開示自体は義務付けられていないとしても、開示の正確性を担保する必要があるということです。

監査委員会は、経営陣が新しいマテリアリティ・アセスメントの要件に精通した有能な人材を今のうちに確保していることを確認することが重要です。特に、組織全体のカーボンフットプリントやエコシステムに存在する影響やリスクの分析を求める要件に対応するためです。このような人材は、報告する意味のあるデータを特定し、今後の比較基準とな

7 Occupational Fraud: A 2024 ACFE Report to the Nations®, Association of Certified Fraud Examiners: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

8 "GHG Emissions Reporting Considerations for Smaller Enterprises," by Mark Boheim and Jacob Chu, 2024, Protiviti: https://blog.protiviti.com/2024/08/29/ghg-emissions-reporting-considerations-for-smaller-enterprises/

る情報を収集するためのプロセスを設計することから始めるべきです。

なぜそれが重要なのか：

米国証券取引委員会(SEC)の規則案が施行されるかにかかわらず、EUやカリフォルニア州で事業を展開する企業は、それぞれの開示要件を遵守しなければなりません。進化する気候変動関連規制を遵守しないと、多額の法的処罰や風評被害につながる可能性があります。自主的な報告も不正確であれば、同じ結果を招く恐れがあります。投資家は、意思決定プロセスにおいて気候変動リスク基準を考慮するようになってきています。気候変動リスクの効果的な管理・開示責任の不履行は、投資家の信頼を失い、株価を低下させる可能性があるだけでなく、ブランドや評判の棄損や特定の市場における事業の認可を失う可能性があります。

重要な質問

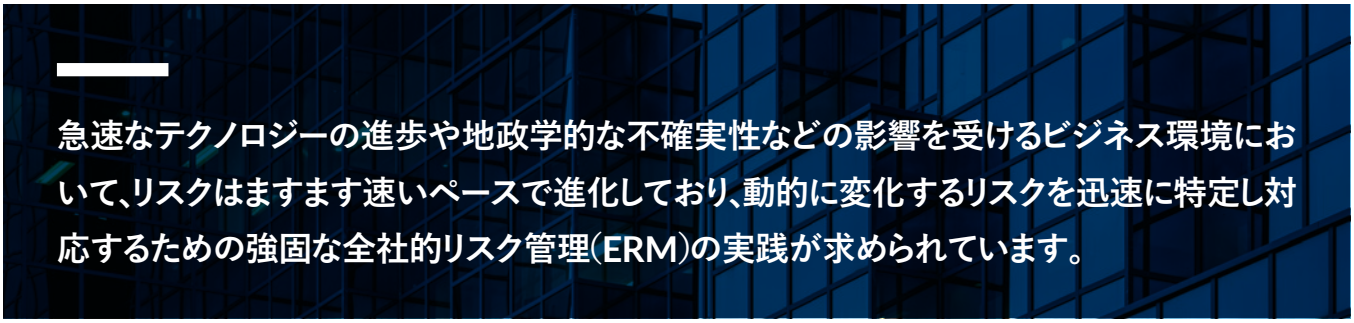
- 気候変動リスクに関連する新たな情報開示要求事項に対して、組織はどのように検討し、対応していますか。
- 組織は、追加の報告要件に対応し、変化するサステナビリティ報告の視点に対応するために、関連する専門知識を有する必要な人材を確保していますか。それをどのように確認しますか。
- 気候関連事象による潜在的な混乱に対処するために、事業継続計画は見直されていますか。
- 投資家、顧客、従業員を含むステークホルダーに対して、気候変動リスク管理戦略をどのように伝えていますか。組織の環境責任への取り組みに対するステークホルダーの認識を評価するために、どのようなフィードバック収集の仕組みを設けていますか。

8. 全社的リスクの特定と管理プロセスの完全性や妥当性を確認する

急速なテクノロジーの進歩や地政学的な不確実性などの影響を受けるビジネス環境において、リスクはますます速いペースで進化しており、動的に変化するリスクを迅速に特定し対応するための強固な全社的リスク管理（ERM）の実践が求められています。監査委員会は、経営陣のリスク評価プロセスを理解し、対応策がリスクを許容レベルまで軽減しているかどうかを判断する必要があります。リスクの複雑化と相互関連性の高まりにより、一層包括的なリスク管理と監視が優先されています。今日では多くの（あるいはほとんどの）監査委員会が、サイバーセキュリティやESG、法規制コンプライアンスリスクなど本来の責務を超えた重要なリスク課題やその監視責任、さらには経営陣が構築・運用するERMのシステムやプロセス全体またはその一部を監視する責任を担っています[9]。

なぜそれが重要なのか：

監査委員会が、単独かまたは取締役会の他の委員会や取締役会と協働して、組織の全体的リスク管理を効果的に監視することは、他の分野に対する監督責任を果たす上での有効性を高めることができます。また、投資家や規制当局、顧客、従業員、その他のステークホルダーとの関係改善にもつながる可能性があります。



9 “2024 The State of Risk Oversight: An Overview of Enterprise Risk Management Practices — 15th Edition,” Enterprise Risk Management Initiative at NC State University, July 23, 2024: https://erm.ncsu.edu/resource-center/the-state-of-risk-oversight-an-overview-of-enterprise-risk-management-practices-15th-edition/

重要な質問

- 拡大し続けるリスクに対応するために、ERMのプロセスに十分なリソースを投入していますか。

- 個々の監査委員は、経営陣によるリスク管理プロセスについて首尾一貫した説明ができますか。

- 監査委員会や他の取締役会委員会、取締役会全体は、会社の主要リスクに関する経営陣による評価の完全性を、外部の情報源と照らし、どのように評価していますか。

- 最近予期せぬ出来事があった場合、事後検証において、組織のERMプロセスを更新する必要性を特定できましたか。

9. 監査委員会に対する経営陣の報告の有効性を評価する

経営陣と内部監査部門が、監査委員会に提供する情報は、単なるデータの羅列ではなく、適切な文脈を持った、質の高い簡潔な情報であることが極めて重要です。監査委員会がその役割を十分に果たすためには、潜在的なリスクや死角を見落とさないためにも、部門単位や縦割り（サイロ化）された報告ではなく、全社的で大局的な視点が求められます[10]。監査委員会は、経営陣と内部監査部門が協力するよう求め、委員会が受け取る報告が簡潔で、戦略的に関連性があり、行動に結びつくものにするべきです。取締役会資料が、取締役に不必要な調整や読み解きを強いるようなものであってはなりません。

なぜそれが重要なのか：

多くの監査委員会にとって、監督責任は拡大し続けており、効果的なガバナンスを担保する適切で消化しやすい情報が必要です。内部と外部のアシュアランスの提供者が特定した共通テーマを監査委員会に包括的に報告すれば、監査委員会がその責任を果たすうえで役立ちます。変化のペースがますます速まる中、経営陣の報告が効果的かつ焦点を絞った監査委員会の監督を支援し、組織と内部監査の人材の継続的な連携を支援することが極めて重要です。

重要な質問

- 経営陣の報告は、思考を刺激し、学習を促進し、監査委員会から最善の助言を引き出していますか。そうでない場合、どのような改善が必要ですか。

- 財務やコンプライアンス、現場業務などの部門を横断して、監査委員会とのコミュニケーションを促進し、経営陣の報告が一貫性のある全体像を示すようにするにはどうすればよいですか。

- 必要に応じて、経営陣の報告は、組織のリスクに関する内部や外部のアシュアランスの情報を統合していますか。

- 取締役が受け取るコミュニケーションや報告の品質（文脈、データの視覚化、簡潔さなど）に関するフィードバックを収集するための仕組みは確立されていますか。

10「Risk Oversight 170：取締役会の盲点」, Board Perspectives, Issue 170, 2024, Protiviti: https://www.protiviti.com/jp-jp/newsletter/risk-oversight-vol-170

監査委員会の有効性の自己評価

監査委員会は、自らのパフォーマンスを定期的に自己評価することが推奨されます。監査委員会は、プロティビティが公表したhttps://www.protiviti.com/us-en/newsletter/bulletin-assessment-questions-audit-committeesで例示した質問を検討してみてはいかがでしょう。監査委員会の委員は、会社の業界や諸情勢、リスク、財務報告上の問題、現在の課題を考慮しつつ、監査委員会の構成や憲章、議題の焦点を定期的に評価する必要があります。

「監査委員会が検討すべき評価質問」に含まれるトピック

- 監査委員会の構成と力学
- 監査委員会の憲章と議題
- 内部統制と財務報告の監督
- 外部監査人の監督
- リスクの監視
- ビジネスの文脈
- 企業文化
- エグゼクティブセッション
- ESG報告
- 財務部門の監督
- 内部監査部門の監督
- 監査委員会の有効性
- 監査委員向けオリエンテーションと教育

謝辞

この記事に貢献されたプロティビティの専門家、Jim DeLoach, Chris Wright, Charlie Soranno, Rob Gouldに感謝いたします。