2025年版

EXECUTIVE PERSPECTIVES ON TOP RISKS

トップリスクに関するエグゼクティブの視点

短期的および長期的な展望

protiviti®
Global Business Consulting

CAE（最高監査責任者）はサイバー攻撃の脅威、人材管理、サードパーティーリスクを最大の懸念事項として捉えている

アンドリュー・ストルザース-ケネディ著

取締役会やシニアエグゼクティブは、複雑な不確実性に直面しています。これらは、戦略的優位性をもたらす機会を生み出すこともあれば、予期せぬ混乱や業績不振につながるリスクを生み出すこともあります。差し迫った事態になる前に、目前に迫っているかもしれないリスクを予測する能力があれば、リーダーは、特に制御不能な展開をうまく乗り切ることができ、それが組織の価値や成長目標に影響を与える可能性もあります。

第13回目となる「トップリスクに関するエグゼクティブの視点調査」は、世界中の1,215人の取締役メンバーおよび経営幹部が、短期的および長期的な視野で捉えたトップリスクに関する見解を提示しています。具体的には、本調査の世界各国の回答者グループは、以下の3つの側面の32のリスク問題について、短期的（2～3年先）および長期的（今後10年間）に及ぼす潜在的な影響に関する見解を示しました。

- 組織の成長機会に影響を与えそうなマクロ経済リスク
- 成長機会を追求する戦略の妥当性に影響を及ぼす可能性のある、組織が直面する戦略的リスク
- 戦略を実行する上で、組織の主要な業務に影響を及ぼす可能性のあるオペレーショナル・リスク

解説 – CAE（最高監査責任者）の視点

不確実性に満ちたダイナミックに変化するビジネス環境において、CAEは、組織が直面するマクロ経済リスク、戦略的リスク、オペレーショナル・リスクの大半を、CEO、CFO、その他の経営幹部の回答者と比べて、より重大な脅威であると認識しています。このため、内部監査リーダーは、企業のリーダーと緊密に協力し、リスクが十分に理解され、十分に対処されていることを確認する必要があります。

CAEにとって、世界的に（2～3年後を見据えた）短期的なリスクには、サイバーセキュリティ、人材管理、サードパーティーリスク、経済情勢、規制当局の監視強化などがあります。さらに、内部監査リーダーは、これら同じリスク懸念が、今後10年間、組織にとって重要な課題になると考えています。私たちは、この予想を次のような点で前向きに捉えています。それは、人材、テクノロジー、イノベーション、変革に対する今日の投資は、内部監査部門、そして組織全体が将来の課題に対してより良い準備をすることを示唆しているからです。

人材、テクノロジー、イノベーション、変革に対する今日の投資は、内部監査部門、そして組織全体が将来の課題に対してより良い準備をすることを示唆しているからです。

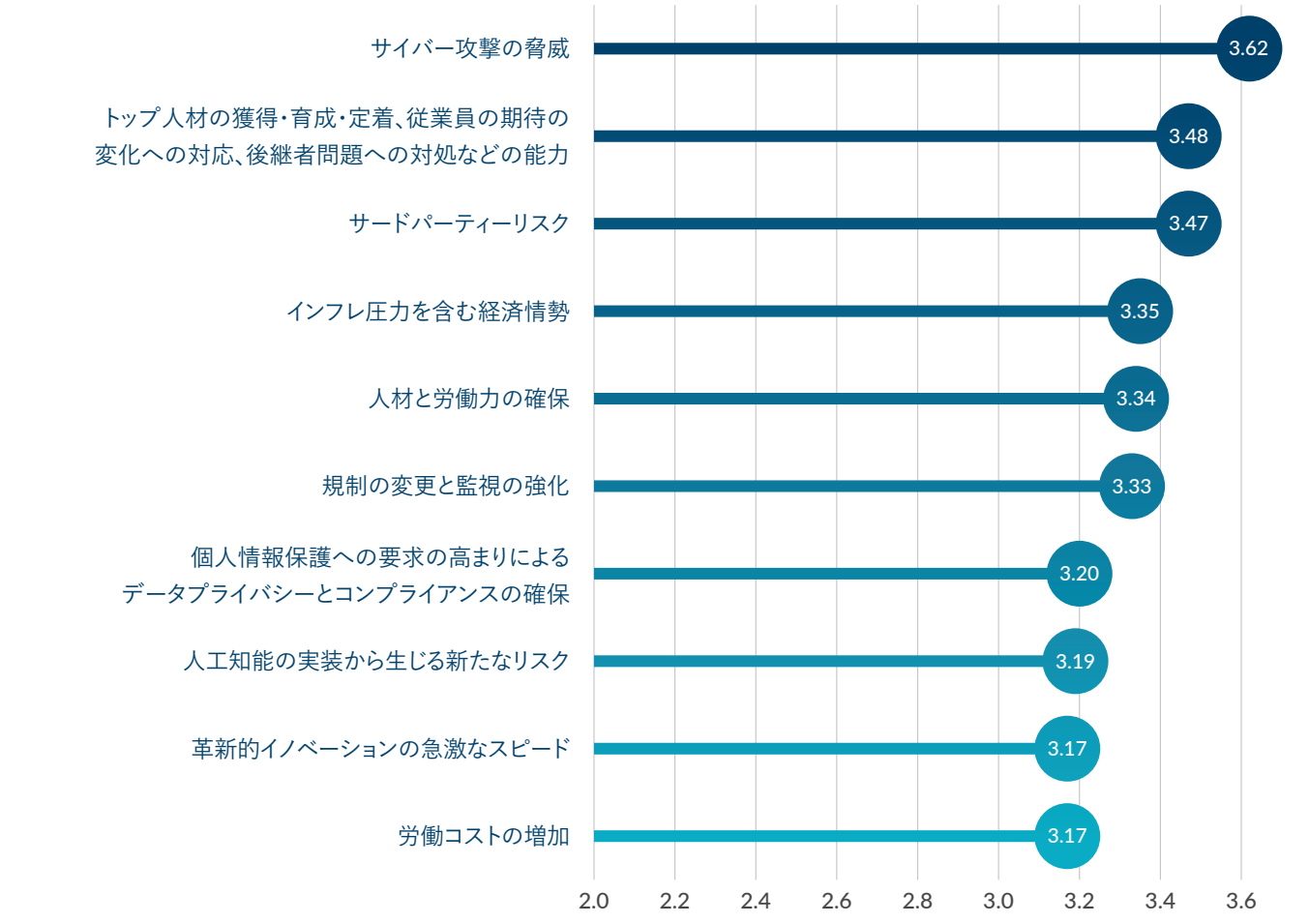
また、注目すべき点は、これらのリスクのうち3つが業務に関連する性質を持っているということです。これは、他のエグゼクティブとは異なり、内部監査は、組織の管理に関わり、監査が容易な業務分野に重点を置く傾向があるからと考えられます。加えて、目先のオペレーショナル・リスクの問題として、プライバシーコンプライアンスや人工知能（AI）の利用による新たなリスクなどが高く注目されています。さらに、内部監査リーダーにとって、マクロ経済や戦略的リスクの問題も見失わないことが重要です。

短期的なトップリスクの概要

CAEにとって、当面のリスク見通しは、サイバーセキュリティ、人材、サードパーティーに関する懸念、経済情勢、規制の変化と課題に焦点が絞られています。また、プライバシーとAIも非常に注目されています。CAEが直面するリスクについて幅広い見解を持っていること、また一般的に懐疑的でリスク回避的な傾向があることを踏まえると、CAEが、他の経営幹部や取締役会の回答者よりも、リスクをより重要視することは驚くことではないかもしれません。ただし、最高リスク管理責任者や取締役会のメンバーも、リスクの影響度に関する見解ではそれほど差はありません。内部監査リーダーにとって、これはまた、組織の真の残存リスクのレベル、リスク低減活動の有効性、経営陣のリスクに対する理解と対策に関して、より深いレベルの洞察力を持っていることの結果でもあります。

下のチャートは、CAEにとっての短期的なトップ10リスクを示しています。その後に、より高い評価を受けたリスクと、より広範なテーマについての私たちの見解を示しています。

CAE- 短期的な見通し



サイバー攻撃の脅威

サイバーセキュリティの脅威は、近い将来の見通しにおけるCAEのリスク懸念事項のリストのトップに挙げられています。さらに、リスクと統制を重視する考え方に基づき、内部監査リーダーは、サイバー攻撃の脅威を、経営幹部よりもはるかに高いリスクレベルと評価しています。これらの調査結果は、プロティビティと内部監査人協会（IIA）が実施した関連調査と一致しており、CAEとテクノロジー監査リーダーが直面するテクノロジーリスクのトップはサイバーセキュリティである、と指摘しています。注目すべきは、この共同調査によると、より頻繁に、かつより高度なテクノロジー監査を実施する内部監査チームは、サイバーセキュリティを重大な脅威と認識する可能性が高いということです。

進化し続ける脅威の状況や、攻撃や機密データ漏洩がもたらす潜在的な重大性といった要因に加え、サイバー攻撃の脅威に関するCAEの見解は、以下を含む多くの要因によって左右されています。

1. **継続的なサイバーリスクの監視** — 内部監査部門は、より頻繁かつ高度にサイバーリスク評価を実施しています（例えば、テクノロジー監査を強化するためにAIを使用している）。脅威をもたらす者はその能力を継続的に進化させています。これに対して経営陣は、内部監査チームがサイバーリスクを完全に把握し、サイバーリスク管理に対する経営陣の取り組みを評価できるように、管理体制、能力、ツールを強化する必要があります。

2. **内部監査の任務** — サイバーセキュリティリスクの評価は、組織価値を保護する義務と相まって、内部監査のリスクおよび監視の重点分野および責任の重要な部分です。特筆すべきは、IIAが最近、「サイバーセキュリティに関するトピック別要求事項」を発行したことです。このガイダンスは、サイバーセキュリティガバナンス、リスク管理および統制プロセスの設計と実施を評価するための一貫した包括的なアプローチを提供しています。この要件は、組織のサイバーセキュリティを評価するための最低限のベースラインを示しています[1]。

3. **増加する規制要件** — サイバーセキュリティの能力と必要な開示に関する規制要件は、世界中で増えています。例えば、米国証券取引委員会（SEC）のサイバーセキュリティ開示規則に加えて、企業は現在、欧州連合（EU）のネットワークおよび情報セキュリティに関する指令2（NIS2）を遵守しなければなりません。この指令は、EU全体でサイバーセキュリティをさらに強化することを目的とした共通の最低要件で各国の法律を統一する指令の適用範囲を拡大するものです。

悪質な脅威の深刻化とサイバー関連のコンプライアンス要求の高まりを受けて、内部監査部門は、データ漏洩、ランサムウェア、巧妙化するソーシャルエンジニアリング攻撃（その多くはAI技術によって可能になりつつある）、サードパーティーやサプライチェーンのリスク、クラウドサービスプロバイダのセキュリティ脆弱性に対する組織の防御策を精査しています。CAEがサードパーティーリスクを当面の重大な懸念事項として評価している理由は、こうしたサイバーセキュリティの重点分野にあります。

CAEが人材戦略を検討する際には、必要なスキルや知識を得るための選択肢を引き続き評価し、テクニカルな内容が多いサイバー関連の見直しをより幅広く実施する必要があります。

サイバーリスクへの備えを評価し、これらのサイバー関連トピックに対処するための「中核的な」サイバーセキュリティプログラムの見直しに加えて、CAEと内部監査部門は、データプライバシーとコンプライアンス、データガバナンスと整合性、AIテクノロジーの採用、技術的負債と老朽化したインフラ（および関連するテクノロジーの近代化への取り組み）、サードパーティーのセキュリティ管理、統合されたサイバーリスク報告の枠組み、データ分類スキームなど（ただし、これらに限定されない）その他のサイバー関連以外の分野についても、引き続き経営陣と連携して評価を行うべきです。

1 Cybersecurity Topical Requirement, The Institute of Internal Auditors, February 2025: www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement.pdf.

最後に、CAEが人材戦略を検討する際には、必要なスキルや知識を得るための選択肢を引き続き評価し、テクニカルな内容が多いサイバー関連の見直しを幅広く実施する必要があります。

人材の確保と管理

ほとんどの取締役および経営幹部が抱える懸念と同じように、人材は依然としてCAEにとって差し迫ったリスク課題です。そして、その多くは、自部門特有の人材ニーズや課題、組織全体が直面する人材関連のリスクという2つの側面からこの問題を捉えています。CAEは、組織全体および自らの部門が優秀な人材を惹きつけ、育成し、定着させる能力に懸念を抱いています。これは、オペレーショナル・リスクであり、組織によってある程度コントロール可能なものです。人材の確保や人件費に関連する広範なリスクは、組織のコントロールの及ばない部分が大きいですが、特に人材パイプラインに大きな課題がある場合は、こうした外部の状況や動向に柔軟に対応し、適応する必要があります。このような問題は、金融や会計の分野ではすでに顕在化しています[2]。

人材は依然としてCAEにとって差し迫ったリスク課題であり、多くのCAEはこれを2つの側面から捉えています。1つは自部門特有の人材ニーズや課題、もう1つは組織全体が直面する人材関連のリスクです。

優秀な人材、特にテクノロジー分野の優秀な人材の確保と定着は、その重要性が一層高まっています。この課題はCAEに直接影響を与え、CAEは、テクノロジーに重点を置いた分野の監査を実施するために必要なスキルを確保し、育成し、定着させることに苦慮しています。また、内部監査機能自体のデジタル変革も推進しなければなりません。さらに、AIの導入やより広範なテクノロジーの近代化の取り組みなど、組織全体のテクノロジーイニシアチブに関連する中核的な監査およびアドバイザリー活動を支援する、資格と経験のある専門家を必要としています。

サイバーセキュリティ、サードパーティーリスク、市場の混乱、AIの導入から生じるリスクに関するCAEの懸念を踏まえ、テクノロジー人材の管理(採用パイプラインから定着プログラムまで)は、内部監査戦略計画の一環として取り組むべきであり、内部監査戦略計画(グローバル内部監査基準、特に基準9.2で要件となっている)の中で明確に示されるべきです。また、経営陣のステークホルダーや監査委員会との議論においても、この問題を積極的に取り上げる必要があります。AIやその他の新興テクノロジーへのアクセスは(社内または外部パートナー経由)、これらのテクノロジーを利用し、効果的にリスクを管理し統制する企業の能力に直接関係します。これにより、競争優位性を維持または拡大し、関連リスクを管理することができます。CAEは、基盤となるテクノロジーに関する知識と洞察力が、すべてのチームメンバーに求められる基本レベルのスキルであるかどうかを検討すべきです。これらの分野における「マイナー」レベルの能力を身につけるためのスキルアッププログラムを作成することは、内部監査機能を発展させると強く主張されています。これにより、個人が「メジャー」レベルで持っている能力を補完することができます。

サードパーティーリスク

CAEは、複雑化および多次元化するサードパーティーのエコシステムがもたらす固有のリスクと課題を理解しています。サードパーティーの問題に起因する、さまざまな種類のビジネスの混乱が数多く発生しています。企業がテクノロジーソリューション、業務サポート、その他の重要な事業活動においてサードパーティーへの統合や依存を強める中で、強固なサードパーティーリスク管理プログラムの必要性がこれまで以上に高まっています。同時に、これらのプログラムやサードパーティ―リスク管理および統制プロセスに対する独立した監査の必要性はこれまでになく重要になっています。

サードパーティーリスクの監督および管理を担当するチームとの緊密な連携と協力は極めて重要であり、これは、CAEが組織内の他のリスクおよび保証チームを監督する担当者と連携することの必要性が高まっていることを示しています。

2 "Navigating the Accounting Pipeline Crisis," Anthony J. Tucci, LLM, JD, CPA, The CPA Journal, February 2025: www.cpajournal.com/2025/02/14/navigating-the-accounting-pipeline-crisis/

CAEは、データ共有およびシステムアクセス、セキュリティおよびプライバシー、契約、規制遵守、履行義務、保証報告などの分野におけるサードパーティーとの関係およびこれらのサードパーティーに関連するリスクを管理するための経営陣のアプローチ（第4者への配慮を含む）について、最新の包括的な見解を確実に把握しなければなりません。この分野では、サードパーティーリスクの監督および管理を担当するチーム（情報セキュリティ、事業継続、調達、サプライチェーンなど）との緊密な連携と協力が極めて重要であり、これは、CAEが組織内の他のリスクおよび保証チームを監督する担当者と連携することの必要性が高まっていることを示しています。

経済

米国やその他の国々の貿易および金融政策の変更、地政学的紛争、自然災害、その他のマクロ経済的要因に起因する世界的な不確実性の高まりの中で、インフレ圧力を含む経済情勢が、CAEの懸念するリスクのトップとなっています。マクロ経済的な要因は直接監査対象にはならないかもしれませんが、組織が、さまざまなシナリオにどのように計画を立て、それに対応するか、またサプライチェーンの回復力、組織の俊敏性、変化への対応力、混乱への対応といった基本的な業務プロセスは、定期的な評価と監査計画の検討対象となるリスクのリストに、確実に含める必要があります。

経済情勢の大幅な下降傾向の可能性に関して、内部監査は、組織の「景気後退プレイブック」を評価し、支出の削減、労働環境の激変（リスク管理および統制プロセスへの影響を含む）、および事業状況の悪化によってもたらされるその他の影響にどのように対応できるかを判断する立場にあります。また、テクノロジーの最新化戦略やプログラム、AIの導入と活用といった事業促進要因に関する監査およびアドバイザリー業務も実施します。このような取り組みは、さらなる能力を引き出し、業務効率と有効性の大幅な向上につながります。

2035年のトップリスクの概要

CAEの長期的な懸念は、いくつかの微妙な違いはあるものの、短期的なリスクの優先順位とほぼ一致しています。今後10年間で自社に最大の課題をもたらすと思われるリスクカテゴリー（マクロ経済、戦略、オペレーション）を2つ挙げてもらったところ、内部監査リーダーが最も多く挙げたのは次の通りです。

- 経済情勢と人材の確保（マクロ経済）
- 規制の変更と革新的イノベーションの急激なスピード（戦略）
- サイバーセキュリティとサードパーティーリスク（オペレーション）

これら6つの長期的リスク懸念は、いずれもCAEの短期的リスク懸念の上位10項目にも入っています。

CAE- 長期的展望

マクロ経済リスクの問題

リスク	パーセンテージ
インフレ圧力を含む経済情勢	43%
人材と労働力の確保	38%
地政学的シフト、地域紛争、不安定な政権体制	25%

戦略的リスクの問題

リスク	パーセンテージ
規制の変更と監視の強化	40%
革新的イノベーションの急激なスピード	32%
顧客ロイヤルティとリテンションの維持	24%

オペレーショナル・リスクの問題

リスク	パーセンテージ
サイバー攻撃の脅威	38%
サードパーティーリスク	31%
トップ人材の獲得・育成・定着、従業員の期待の変化への対応、後継者問題への対処などの能力	25%

注：回答者には、各カテゴリー（マクロ経済、戦略、オペレーション）の「上位2つ」のリスクを個別に特定してもらいました。つまり、回答者は6つのリスク（各カテゴリーで2つずつ）を「トップ2」のリスクとして特定しました。各カテゴリーについて、回答の多かった3つのリスク問題をパーセンテージで示しています。

このリスクが継続していることは、CAEが、これらのリスク脅威の規模が今後10年間にわたり続くか、拡大すると予想していることを表しています。また同時に、長期的な視点でリスクを考え、予測することの本質的な難しさを浮き彫りにしています。多くの主要国において、世界経済の不確実性は依然として存在おり、短期および長期的な経済予測についてコンセンサスが得られていない状態が続いています。ビジネスおよび広範な経済情勢は、事業支出や設備投資のペースや性質とともに、重点分野に大きな影響を与える傾向があります。特に、需要が拡大している分野では、人材の確保が引き続き制約要因となることが懸念されています。人材確保には、採用、スキルアップ、リスキリングに関連する効果的な戦略、急増するニーズや専門的知識を得るためのサードパーティーの活用、組織が必要な人材にアクセスするための方法が必要になるでしょう。

国および地方レベルのグローバルな規制当局は、今後も新たな要件を制定し、既存の規制を改正または撤廃するでしょう。規制環境の急速な変化に備え対応することが、効率的かつ効果的なコンプライアンスプログラムを確保する上で重要な鍵となります。

新しい技術は今後も継続的に登場し、導入されることで、競争上の差別化や顧客維持から、技術導入のリスク、人材、サイバー関連まで、幅広い分野に影響を及ぼすでしょう。また、継続的なサイバー攻撃の脅威とサードパーティーリスクは、引き続き多面的な課題をもたらすでしょう。

CAEおよび内部監査リーダーへの行動喚起

人材とテクノロジーは、CAEのトップリスクの上位を占めるテーマとなっています。不確実な経済情勢を除けば、CAEの上位5つのリスク懸念は、いずれもテクノロジー（サイバーセキュリティとサードパーティーリスク）または人材管理（優秀な人材を惹きつけ、育成し、定着させる組織の能力とその人材を確保する能力）に関連するものです。このようなリスクに対処するために、監査リーダーは様々な、以下を含む対応策を講じる必要があります。

経営幹部との連携 — CAEと経営幹部のリスクに関する懸念には、短期的および長期的な見通しにおいて、2つの点で違いがあります。第一に、これまで述べてきたように、内部監査のリーダーは、一般的に、ほとんどのリスクを経営幹部よりも重大であると評価しています。第二に、リスクに関する懸念の優先順位付けが異なります。これら2つの論点はいずれも、議論や建設的な意見の交換、そして意見の一致または調整に値します。評価や格付けに対する見方に影響を与えているかを理解することは重要であり、建設的な対話につながります。CAEと最高リスク管理責任者は、他の経営幹部とは異なり、リスクを特定・評価・報告する訓練を受け、経験を積みながら実務を行っています。彼らは、他の経営幹部とは異なるスキルセットと視点を持っています。そのため、プロとしての懐疑心やリスク回避の傾向が強いかもしれません。CAEが経営幹部や取締役会と明確で効果的かつ継続的な対話を続けることは、とても重要です。

グローバル市場を揺るがす地政学的、環境的、技術的な危機により、企業にこれまで以上の柔軟性、俊敏性、回復力を備えることが求められています。

監査が難しい分野への注目が高まる — グローバル市場を揺るがす地政学的、環境的、技術的な危機により、企業にこれまで以上の柔軟性、俊敏性、回復力を備えることが求められています。不安定な経済情勢やリスクは、その流動的な性質ゆえに監査が困難です。企業が備えるべき回復力、俊敏性、適応力についても同様で、これらはすべて事業機能全体にわたるものであり、絶えず進化し続けなければならなりません。長期的には、CAEは、こうした複雑なリスク、あるいは少なくともその根底にある組織的プロセス（戦略または、オペレーションに関連するもの）を監査する新たな方法を検討し、課題の特定と報告に役立てることが必要です。

サイバーセキュリティとテクノロジーの近代化 — CAEが最も懸念しているリスクは、直接的（サイバーセキュリティ、AIの導入、テクノロジーによる混乱など）にも間接的にもテクノロジーの進歩に関連する問題です。人材関連のリスクと人件費の上昇は、急速に進化するテクノロジースキルをめぐる激しい競争が主な原因となっています。また、サードパーティーリスク（データプライバシーやセキュリティなど）や規制リスク（サイバーセキュリティの開示やAIガバナンス要件など）も、テクノロジーの進歩が主な原因となっています。これらの問題は、CAEが優秀なテクノロジー人材を継続的に確保し、特にテクノロジーに焦点を当てた技術的な監査を実施するために必要なスキルを持つ人材を採用、育成、定着させる必要性を浮き彫りにしています。また、内部監査機能自体のデジタル変革も推進する必要があります。

人材関連のリスクと人件費の上昇は、急速に進化するテクノロジースキルをめぐる激しい競争が主な原因となっています。

AI — CAEは、AIの導入がCEOにとって最大のリスク懸念であることを再認識すべきです。新たなAI関連リスクへの対応に加えて（組織全体でのAIの導入・使用・進化、ならびに導入されるガバナンスの枠組みの監視による）、内部監査部門はAIトレーニングと導入を通じてチームを「補強」し、内部監査活動全体のライフサイクルにわたってAIの導入を受け入れ、活用する必要があります。

人材 — 組織の人材管理戦略および計画に対する監査に加えて、CAEは、自らの領域における人材とスキルの課題を評価し、対処する必要があります。内部監査部門において、AI、テクノロジー、サイバーセキュリティ、データガバナンス、データ分析、サードパーティー・リスクマネジメントの能力に対するニーズは高まり続けていますが、CAEは、バランスの取れた幅広い能力を持つ内部監査員を育成するためのスキル開発に投資する必要性を見過ごしてはなりません。具体的には、創造的思考、批判的思考、効果的なコミュニケーション、問題解決、革新的思考などの能力開発を支援する必要があります。

これからの内部監査機能 — AIをめぐる現在の過熱した状況を踏まえ、CAEはテクノロジーとデータ活用を基盤とした機能に重点的に取り組む必要があります。CAEは、自分自身やチームに「内部監査活動のテクノロジーとデータ活用に関して、理想的な状態はどのようなものか」、「将来の内部監査機能には、具体的にどのようなスキルや能力が必要なのか」といった問いかけを、自分自身やチームに投げかけ、深く考察することが求められています。これらの質問を熟考し、特定された課題に対処するための具体的な計画を策定することは、CAEが将来に備えた内部監査チームを持つための道筋となります。

「トップリスクに関するエグゼクティブの視点調査」について

私たちは、世界中のさまざまな業種の役員および経営幹部1,215人を対象として、今後2～3年間および今後10年間（2035年まで）における32の固有リスクが組織に及ぼす影響をどう評価するか調査しました。この調査は2024年11月中旬から12月中旬にかけてオンラインで実施されました。短期的な見通しについては、回答者は32 の個別リスクを5 段階で評価し、評価1は「まったく影響なし」、評価5は「広範囲にわたる影響」と位置づけました。32のリスクそれぞれについて、全回答者の平均スコアを算出し、スコアの大きいものから小さいものへとランク付けを行いました。

また、エグゼクティブの方々には、長期的なリスク（今後10年間、2035年まで）について、3つの側面（マクロ経済、戦略、オペレーション）からそれぞれ上位2つのリスクを挙げ、その見解を共有していただきました。32のリスクそれぞれについて、そのリスクを各側面の2つのトップリスクの1つとしてそのリスクを挙げた回答者の割合を算出しました。

「トップリスクに関するエグゼクティブの視点調査」に関する要約（エグゼクティブサマリー）および全レポートは、プロティビティまたは、NC State University ERM Initia- tive のウェブサイトをご覧ください。

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。25ヶ国、90を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、デジタル、オペレーション、人材・組織、データ分析におけるコンサルティングサービスを提供しています。プロティビティは、米国フォーチュン誌の働きがいのある会社ベスト100に10年連続で選出され、Fortune 100の80%以上、Fortune 500の約80%の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティはRobert Half（RHI）の100%子会社です。

© 2025 Protiviti Inc. All rights reserved. 複写禁、転載禁

protiviti®
Global Business Consulting