protiviti®
Risk & Business Consulting.
Internal Audit.

The Bulletin

Volume 6, Issue 1

2016年度の監査委員会の議題（抜粋）

The Bulletinの本号では、2016度における多くの組織の監査委員会にとって適切な議題とすべき事項について解説します。これまでと同様、我々の所見は、クライアントの監査委員会との交流、当社が実施したラウンドテーブル、会議やその他のフォーラムでの取締役との討議、年次で実施するサーベイに基づいたものです。

本稿で議論する事項については、最初の５項目が全社、プロセス、テクノロジに関するリスク事項であり、残りの５項目が財務報告に関する事項です。我々が焦点を当てているのは、多くの組織における監査委員会が留意することが必要と考えられる重要な事項です。なお、包括的な監査委員会のベストプラクティスについては対象としていません。

全社、プロセス、テクノロジに関する事項

1. リスクプロファイルがビジネスの現状を反映したものであることを確かなものにする。

ほとんどの組織では、将来のリスク事象の影響度および発生可能性といった主観的な評価に基づいて、リスクマップやヒートマップ、リスクのランキング表を作成し、リスク評価を実施しています。このようなリスク評価を実施することで、会社のリスクの全体像が見えるようになります。しかし、問題は、リスクプロファイルが実際のビジネスの現状を適切に反映しているか、ということです。

これは重要な問題です。というのも、多くの監査委員会は、会社のリスク評価プロセスやリスクマネジメント能力に関して調査する責任を有しているからです。このような責任を特に有していない監査委員会においても、さまざまな理由で、組織の重要リスクの概要を理解したいと考えているケースが多くあります。

事業環境は絶えず変化しています。デジタル技術の進展、グローバル化の波、人口動態や社会全体の潮流の変化によって、ビジネスモデルの有効期間が短縮しつつあります。このような現状を踏まえて、取締役会は、少なくとも毎年１回は、会社のリスクプロファイルに目を通すべきです。リスクプロファイルの評価は、経営者が更新するリスク評価によって支援されるべきです。最も重要なリスクについて、監査委員会またはその他の取締役会委員会（どの委員会が主体になるかは、取締役会がリスク管理に対してどのような体制をとるかによる）は、適切な行動計画が、会社の重要なリスクを管理するために設定されていることを確認する必要があります。

2016年度における監査委員会が行うべき使命

全社、プロセス、テクノロジリスクに関する事項

1. **リスクプロファイルがビジネスの現状を反映したものであることを確かなものにする。**—組織のリスクプロファイルは新興リスクや既存リスクの変化を考慮しているか、また主要な全社リスクやリスク管理能力の妥当性に焦点を当てているか。
2. **ビジネスモデルを脅かすテクノロジ関連のリスクを理解する。**—サイバーセキュリティ、個人情報・身元情報管理、情報セキュリティ・システム保護ならびに潜在的な破壊リスクに関する事項に適切に対処しているか。
3. **組織におけるリスク文化やリスクに対する組織の姿勢に留意する。**—トップや中間管理者の気風ならびにそれらが統制環境に与える影響、リスク管理能力の有効性を考慮しているか。
4. **財務部門の能力を拡充させる必要性を検討する。**—財務部門の能力は会社のニーズと整合しているか。
5. **内部監査部門の能力を拡充させる必要性を検討する。**—内部監査部門は価値を生み出しているか、期待に応えるための人材を十分に配置しているか。

上記の表に、2016年におけるトップ10のリスクを挙げています。[1]

この表では、前年に実施したサーベイと比較して、各リスクの重要度が上がっている（↑）のか、下がっている（↓）のか、または変化がない（↔）のかを示しています。リストには、監査委員会が関与すべき、

1. このリストはノースカロライナ州立大学のERMのイニシアティブとプロティビティが行った上級役員および取締役により識別されたトップリスクについての年次調査の結果に基づいている。また、この結果は、2016年早期にはwww.protiviti.comに掲載予定。

いくつかの重要なリスクが示されています。特に、財務報告へ影響を持つ重要なリスクに関しては、監査委員会は、どのようにそれらが管理されているか、財務諸表に与える潜在的な影響はどの程度か、監査プロセスにおいて外部監査人によってどの程度検討されているか、を理解しておく必要があります。

監査委員会はまた、新たなリスクがタイムリーに、組織のリスク評価プロセスに組み込まれていることを知る必要があります。例えば、経営者は、組織の戦略や事業計画の基礎となる重要な前提条件に対する事業環境の変化の影響、警戒すべき早期の兆候を示す主要なリスク指標と傾向、そして組織とそのビジネスモデルに密接な関係があるリスクテーマを識別するためのリスク間の相関関係の分析に焦点を当てる必要があります。要約すると、企業のリスク評価プロセスは、既存のリスクの変化、新たなリスクの出現、リスクを管理するための組織体の能力の妥当性、および開示要件に対する最も重要なリスクの影響を考慮する必要があります。

2. ビジネスモデルを脅かすテクノロジ関連のリスクを理解する。

主要なテクノロジの変革や変更の過程において、多くの局面で危険が潜んでいます。インテリジェント機器および機械、バーチャルリアリティ、モバイル技術、クラウド・コンピューティング、ソーシャルビジネス、アプリを中心に据えたスマートグリッド、工場や都市のようなデジタル技術の進歩は、顧客体験を改善し、対象となるコミュニティに係わり、利便性を生成し、市場を拡大することで、確立されたビジネスモデルへの破壊的な変化を起こしています。これらの進歩はセキュリティと個人情報のリスクをも増大させています。サイバー侵入者は、本気で勝負してきており、組織のサイバーセキュリティの防御への脅威となりつつあります。それはすべてこの衰えることない変化のペースに対処することに対する最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）、事業ラインへの要請の増加につながっています。このことは、顕著な侵害の場合の潜在的な風評への影響の深刻さに鑑み、取締役会にとっても同じことです。

組織の「サイバードア」で狼たちを防ぎかつ自信を持って企業内変革を管理することはプロティビティの2015年度のITの優先順位項目[2]で強調表示された情報セキュリティのアプローチ、プロセス、ツール、スキルやコラボレーションの膨大な要素を展開する能力を必要とします。

今年の調査での上位２項目は次のとおりです。

- **セキュリティへの懸念が最重要である。**
  すべての調査回答者（CIOやあらゆる規模の会社）の間で、サイバーセキュリティへの対応および強化が重要優先事項となっています。

- **重要なITの変更や更新が継続している。**
  すべての組織の半分を優に越えるところが、一年もしくはそれ以上の時間をかけて重要なITの変更を行っており、IT部門には他の重要なビジネスニーズ（例えば、サイバーセキュリティ）に対応しつつ、これらの変更を正常に管理する要求が高まっています。

2016年のトップ10リスク[1]

		前年比較
1.	法規制の変更ならびに規制当局の監視強化が商品やサービスの納品、提供の方法に影響を与える可能性がある。	⇔
2.	会社の中核事業を著しく破壊し、ブランドを毀損しかねないサイバー攻撃の脅威を管理する準備が十分にできていない可能性がある。	↑
3.	現在、会社が商品やサービスを提供している市場の状況が会社にとっての成長機会を著しく妨げ可能性がある。	⇔
4.	後継者問題や有能な人材の引き留め、確保が事業目標の達成に対する能力を制限する可能性がある。	↓
5.	個人情報や身元情報の管理、情報セキュリティ・システム保護を確実にするために、著しい人数の投入を必要とする可能性がある。	↑
6.	変化に対する抵抗が会社のビジネスモデルや中核事業に対する必要な調整の妨げとなる可能性がある。	⇔
7.	破壊的な技術革新や業界内の新規テクノロジの急激な進展が会社の競争力やリスク管理能力を上回り、ビジネスモデルを大幅に変更することができない可能性がある。	↑
8.	会社の文化が、中核事業や戦略目標の達成に著しく影響を与えかねないリスク事項についての適時の識別や報告を促すものでない可能性がある。	↓
9.	世界的な金融市場及び通貨の予想されるボラティリティが組織が対処すべき重大な課題となる。	↑
10.	顧客のロイヤルティを継続的に保持することが、顧客の嗜好の進化や顧客の地理的移行により難しくなりつつある可能性がある。	↓

※ 2015年度のトップ10リスク項目であった「会社の評判に著しく影響を与えかねない想定外の危機を管理するのに十分な準備ができていない可能性がある。」は2016年度には入っていない。

IT担当役員や専門家は、数多くの差し迫った、量的にも意義的にも優先度が高い職務をかかえています。これらの課題に適宜に対処・管理するために、彼らはビジネスの価値を高める活動と組織の価値を保護する活動との間の適切なバランスをとるのに必要な専門知識とビジネスに対する判断力を向上、強化する必要があります。取締役会は、彼らとITが成功するために必要なリソースを持つことを

2. Today's Enterprise-Cyberthreats Lurk Amid Major Transformation: Assessing the Results of Protiviti's 2015 IT Priorities Survey. www.protiviti.comで取得可能。

確かなものにする必要があります。監査の可能性および開示の意味合いから、監査委員会は、この話に関心を持つ必要があります。

3. 組織におけるリスク文化やリスクに対する組織の気風に留意する。

監査委員会は、リスク管理および内部統制の観点から社会秩序を乱す行為の兆候を監視する必要があります。（たとえば、確立したリスク限度に留意することの失敗、反対意見の余波の恐れ、“不合理な非難を行う“環境、過度の組織の複雑さ、重要な取引の透明性の欠如、潜在的な利益相反、その他脆弱なリスク文化の兆候等）

一方で、戦略を実行し、業績を生み出すことを通じて企業価値を創造し、一方で、適切なリスク選好とリスク管理を通じて企業価値を保護するという必要不可欠なテンションのバランスをとることが肝要であるがゆえに、取締役にとって強力なリスク文化が重要です。監査委員会は、組織が有効なリスク文化を有していることを確実なものにする必要があり、その文化の中でユニットやプロセスの責任を担う管理者は、そのユニットとプロセスが作り出すリスクを管理する責任があります。強力なリスク文化は、これらのリスクを管理するため、トップの気風と整合した中間管理職の適切な気風を確立する必要があります。最後に、内部と外部の財務報告に係る統制環境への影響に鑑み、経営者はその文化を維持することが重要です。

監査委員会は、上級経営者が重要な事項が報告された場合、適時にリスク情報に基づいて対応すること、ならびに取締役会も同様に、必要に応じて適時に関与することを確実にする必要があります。

4. 財務部門の能力を拡充させる必要性を検討する。

財務部門は、監査委員会の監督の範疇にある情報の多くを取り扱っています。来年度は収益の維持、キャッシュフローの予測、新たな規制の遵守、およびサイバー脅威との戦いの中で、財務部門は、レーダーとして監視することが多々あります。2016年度の財務優先度調査の結果は、最高財務責任者（CFO）と財務専門家は拡大する優先項目に対処しながら、レーダー役の観点からボラティリティの高まりを警告しつづけています。

調査結果の中で上位３項目は下記のとおりです。

- **マーケットシェアではなく、収益を重視する。**
  財務部門は、マージンを維持することに焦点を当て、運転資本管理や収益を重視しています。

- **サイバーセキュリティの懸念が財務部門に拡大する。**
  今日、ITセキュリティと個人情報が単なるIT事項以上のものであることは、ほとんど疑いがありません。それらは戦略的な組織に関するリスクであり、かつ一驚くことではありませんが、私たちの他の調査と同様、財務部門の優先順位の最上位にランクされているリスクです。効果的なサイバーセキュリティは、精力的な取締役会の関与、適切な方針、企業の最も貴重な機密データを理解する必要があります。

- **セグメント毎、リアルタイムの実態の把握が求められる。**
  全体的な業績や戦略的計画を強化するために、また、組織内の財務データから価値を導き出すために、財務部門は、顧客、製品、事業単位、地域に結びつく収益分析を可能にするより正確でタイムリーなデータ収集、データ分析、報告、予算策定・先見能力を望んでいます。財務部門の優先度は、組織の業種、構造、文化、業績上の問題、内部および公的報告要件に応じて異なります。監査委員会は、財務部門が組織の具体的な期待に応えられるように、適正なリソースがなされていることを確かなものにする必要があります。

5. 内部監査部門の能力を拡充させる必要性を検討する

監査部門長（CAEs）と内部監査部門は、より将来を見据えた、変革志向の高い適応力を持つことへの期待の高まりに直面しています。CIO組織ならびに財務部門と同様、内部監査人は、サイバーセキュリティが監査計画において十分に考慮されることを確保するために、上級経営者や職能部門長と密接に連携することにより、組織を守る上で極めて重要な役割を果たしています。

今年の内部監査能力とニーズの調査結果は、サイバーセキュリティが、内部監査上のいくつかの課題の一つであることを示しています。

調査結果のうち、主な項目は下記のとおりです。

- **取締役会の関与と監査計画は、効果的なサイバーセキュリティにとって重要である。**
  業績上位の組織は高度の取締役会の関与と年次監査計画における設定されたサイバーセキュリティの評価の両方を有しています。

- **内部監査の優先度の高い項目は増加し続けている。**
  サイバーセキュリティの課題に加えて、新技術（例えば、ソーシャルメディア、クラウド・コンピューティング、モバイルアプリケーション）に関連するリスク、コンプライアンス要件の増加、およびIIA、ISOとCOSOからの新たな指針や基準があります。これらおよび他の優先事項は、組織が急速に変化している要求に対処するのを支援するために、内部監査人は鋭敏性ならびに適応力を持つことが求められています。

- **テクノロジを活用した監査が増加しつつある。**
  数多くの優先項目の緊急性に対応するために、テクノロジを活用した監査手法やツールへの投資および利用が増加しつつあります。

- **内部監査機能のPRおよび協調に重点を置くことが増加している。**
  CAEは、内部監査のミッションや価値とリスクに関連するリスクを、他部門に対し伝達することをこれまで以上に重視するようになっています。彼らはまた、組織がリスクを理解し、戦略的目標を達成するのを支援するために、戦略パートナーとして、上級経営者、他の部門長、取締役会との協調関係を高めようと努めています。

監査委員会は内部監査が、そのリスクベースの監査計画を実行し、そして、状況変化にあわせて期待に応える上で成功するために必要なサポートを受けていることを確かなものにする必要があります。

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、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。

Powerful Insights. Proven Delivery.®

protiviti®
Risk & Business Consulting.
Internal Audit.