protiviti®
Risk & Business Consulting.
Internal Audit.

Risk Oversight vol.53
取締役会のリスク監視

ITリスク管理の監視

テクノロジが進歩し、私たちの生活、交流、仕事、遊びを変えたなどというのは、もはやあまりにもありふれた表現です。確かにコストの削減、ビジネスプロセスの改善、売上の拡大に向けたテクノロジの活用により事業のあり方は変化しています。ユーザーの高度な要請は、クラウドコンピューティング、ソーシャルネットワーク、モバイルテクノロジ、その他の実用化技術のトレンドとあいまって、テクノロジ分野における劇的な変化をもたらしています。

主要な考慮事項

このような環境変化は取締役会のリスク監視にどのような影響を与えるでしょうか。リスク監視が、投資予算承認の一部としての個別テクノロジプロジェクト評価や、場当たり的や受動的なベースでのITリスクの検討に限定されているのでは、不十分でありかつ焦点が狭すぎます。以下は取締役会がIT関連分野についてリスク監視を強化するに当たり検討すべき10の提案です。

1. **組織的にITリスク監視を実施する**：取締役会の多くは監査委員会にITに関する主たる監視役としての権限を委譲しています。しかしながら、監査委員会の関心は財務報告及び財務報告に関連する統制にとどまりがちです。選択肢としては、取締役会による戦略策定・実施の監視と併せて、戦略的なIT問題を別の戦略委員会や財務委員会のなかで評価することがあります。企業戦略全体の推進におけるテクノロジの重要性によっては、独立した技術委員会を設置することも必要でしょう。独立したリスク委員会があるのであれば、同委員会に委ねることも考えられます。要するに、監査委員会のみに限定して考えるべきではないということです。

2. **テクノロジがビジネスモデルにどのように組み込まれているかを理解する**：ITリスクの監視は多くの取締役会にとってある程度の学習が必要でしょう。テクノロジが戦略的サプライヤー、販売チャネルパートナー、カスタマーやアウトソース先との関係を築く手段となっている場合、取締役はITがビジネスにどのように統合されているかを理解することが必要です。取締役会は、またCEO、CIO、戦略責任者がこのような大局的視野をもつことを支援するように心がけなければなりません。

3. **的を射た質問からはじめる**：取締役会がリスク監視について問うべき概括的な質問は3つあります。自社のリスクは何か、どのようにリスクを管理しているか、リスクを管理していることをどのように確認しているか、です。これらの質問はITにも適用され、効果をあげるには独立した解析と評価が必要です。ITについて考える上で重要なのは、ITによって破壊的なビジネス変化がもたらされる可能性です。いかなる企業も業界の基盤を一変させる変化が生じた際、誤った側にはいたくはありません。

4. **ITを事業としてとらえる**：CIO部門がITを事業として管理します。すべての事業と同様に、IT事業にもカスタマーとサプライヤーが存在し、情報システムへの投資に対するリターンを最大化させる一方で、リスクを最小化させることを確実なものにしなければなりません。IT戦略を企業のニーズに合わせ、ITガバナンス、リスク管理、コンプライアンスを確立し、ITプロセスを効率的かつ効果的に管理しなければなりません。事業との一体化はCIOにとっていつも最重要課題ですが、いくつかの理由により実現されていません。例えば、多くの企業において目標、戦略、主たる成功要因が明確に伝達されていなかったり、IT部門が事業を十分に理解していなかったり、IT部門があまりに多くの課題を与えられて取り組みが細分化されてしまっている等があります。どのような要因があるにせよ、取締役会の監視により、上級経営者がIT戦略を事業ニーズとうまく一体化させるよう努めなければなりません。

5. **統合された全体的視点を持つ**：セキュリティ・機密情報漏洩が第一ではありますが、ITリスクにはそのほかにも取締役会が留意すべき重要リスクを含みます。ITリスクは多くのビジネスリスクの一要素であると同時に、評価しなければならないリスクの一分野でもあります。バーチャル組織やクラウドによりITインフラの責任は世界各地の拠点で事業を行っている数多くの事業体に分散されつつあります。ITを取締役会のリスク監視の議題のつけたしにするのではなく、監視プロセスにおいてITリスクを戦略・オペレーション・財務・コンプライアンスの各リスクと統合する必要があります。例えば、戦略リスク・財務リスクにはテクノロジの技術革新、リソースの配分、プロジェクト管理リスクが含まれます。オペレーションリスク・コンプライアンスリスクには重要情報の正確性や妥当性、セキュリティ・機密情報、ITリソースの可用性、ITサービスへの適切な費用配分、インフラストラクチャーリスクが含まれます。

6. **ITインフラの変化の影響に注意する**：企業が市場地位を拡大・縮小・現状維持しているかにかかわらず、今日のIT環境においては急激な変化が常であり、IT部門のポリシー、プロセス、人材、テクノロジを変化に合わせて進化させるべきと、取締役は認識しなければなりません。今日に必要なのは、機動性・柔軟性の高いITインフラです。インフラの変更にかかわる重要なリソースの意思決定については個々のIT機能より広い視点で評価する必要があります。（たとえば、クラウドによってもたらされるインソース、アウトソース、コソースの割合の変更など）　具体的には、クラウドは、アプリケーションを導入・設定する初期コストを抑えて、複数のユーザー（従業員、顧客、サプライヤー、委託者等）に対しソフトウェア、プラットフォームその他のリソースを提供する動的・拡張性のあるインフラです。また、クラウドは企業のファイヤウォールに対するリモートアクセスを要求しない、安全性の高いエクストラネット間の分散コンピューティングを提供します。ITにとっての課題は、これら変化する環境に適応し、迅速かつ効率的にユーザーの期待に応える一方、ITに対する投資の効果が十分に実現しないうちに次々と新規システム・アーキテクチャーに変えないようにすることにあります。

7. **主要なビジネスプロセスの継続性を保つ**：事業継続の計画、回復力、危機管理は全般的ITリスク管理プログラムの不可欠な要素です。取締役は経営者に危機管理や伝達、企業の主要システム（自社所有、第三者の活用にかかわらず）とビジネスプロセスの復旧能力について問い合わせることが重要です。

8. **ITセキュリティ・機密情報に注意を払う**：事業活動の相互依存性が増すにつれ、データは物理的または電子的に管理に失敗すると即、負債に転じてしまうような資産です。よって、情報セキュリティ・機密情報についてもビジネスにかかわる事項として考えることが重要です。セキュリティの脅威や脆弱性、機密情報のリスクは、気がついていようとなかろうとあらゆる企業にとって問題であり、理解し管理することが必要なリスクを生じさせます。企業が自社の直面するリスク

を把握できていないと、深刻な脅威が対応されないまま巨大な問題にふくれあがることがあります。取締役会は、経営者がセキュリティ・機密情報リスクを識別・管理するために効果的なプロセスを導入しているかを確認しなければなりません。

9. **ITリスクにはコンプライアンスの側面があることを理解する**：企業はITに関する特定のコンプライアンス上の要件があることもあれば、多くの法規制要件の遵守にはIT部門のサポートを必要とすることもあります。例えば、法令上の要件ごとに、下記の事項を確認する必要があります。
   - 当該法令は自社のデータのどの部分に影響し、当該データを必要に応じて取り出し、維持することができるのか。
   - 当該要件に従って、データをどのように分類し管理しているか。

   重要なことは、法令の要件（Eデイスカバリーを含む）を遵守しないと深刻な結果をもたらすおそれがあり、ITはコンプライアンス遵守に一定の役割を果たしているということです。

10. **先進的なテクノロジ監査手法を開発する**：2013年11月に発表されたプロティビティIT監査ベンチマークサーベイでは、460人以上の監査プロフェショナルからの情報を集計しています。このサーベイによると、多くの企業において必要とされるIT監査領域がカバーされておらず、IT監査リスクアセスメントに多くの問題点が残されています[1]。

要約すると、変化するビジネス目的に対してITが対応できなかったり、企業内のITの役割を理解できていなかったり、IT戦略とビジネス目標が合致していなかったり、ITインフラが陳腐化していたり、ITパフォーマンスについての明確な情報がなかったりすると、IT部門は効果的でなくなります。効果的な取締役会のリスク監視によりIT部門を強化することができ、ITが企業に与える価値を最大化することができます。

取締役会の考慮事項

以下は、企業の営む事業に内在するITリスクの性質に応じ、取締役会が考慮すべき事項です。

- 取締役会はITリスク及び自社がITリスクを管理するための能力・プロセスについて十分な時間を費やしているか。
- 自社は、競合他社や従業員による新規テクノロジの採用を含む破壊的変化を生じさせるテクノロジのイノベーションを注視しているか。
- 重要なITプロジェクトについて、取締役会は各プロジェクトがコストの削減、ビジネスプロセスの改善、戦略目標の達成をもたらす前提を理解し、その達成をどのように測定するかを理解しているか。各重要プロジェクトが想定された目標を達成できているかをフォローアップしているか。
- 取締役会は下記について、適切な情報を得ているか。
  - » 自社のITのトータルコスト
  - » 全プロジェクトに対するITの費用がROIの最適化を確実にし、コンプライアンスや契約上の要請を充たしていること。
- 取締役会は自社の直面する機密情報・セキュリティリスクを理解しているか。機密情報・セキュリティは全ての新規ビジネスプロセスの一部として考慮されているか。
- CIO部門は例えば以下のような変化するビジネス上の要請に効果的に対応しているか。
- CIO部門はコスト削減および機能改善の機会を識別するために、既存のアプリケーションポートフォリオを定期的にレビューしているか。
- 陳腐化したレガシーシステムが効率、機動性、イノベーションを阻害していないか。
- クラウドソリューションが利用されているか、もしされてい

※1 From Cybersecurity to IT Governance – Preparing Your 2014 Audit Plan, 2013年11月発表 www.protiviti.com

る場合、取締役会は関連するリスクを理解しているか。
- アウトソースプロバイダを利用している場合、取締役会はプロバイダとの関係が効果的に管理されているかを確認しているか。
- 取締役会は自社や業界に関連するIT問題についての知識や理解を維持するよう努めているか。

プロティビティの支援

プロティビティは、情報システム投資に対するリターンの最大化とITリスクの最小化を通じ、企業のITとビジネス戦略との一体化を支援します。

具体的にはITガバナンスやITインフラの強化、アプリケーション管理、セキュリティ管理、データ分析の支援やベンチマーキングなどのIT関連サービスをご用意しています。これらをご活用いただくことで、ビジネス上の要請とITの一体化ならびに費用効率のよいIT組織について、経営層がより一層理解を深めることが可能となります。

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。現在、世界の70を超える拠点で約3,500名のコンサルタントが活躍しています。

protiviti®
Risk & Business Consulting.
Internal Audit.