protiviti®
Risk & Business Consulting.
Internal Audit.

Risk Oversight vol.76
取締役会のリスク監視

COSO 2013：何を学んだか?

改訂COSO内部統制の統合的フレームワークは、2013年5月に発行されました。発行以来、いくつか重要な学びがありました。その一部を本資料の中で考察します。

3年前、トレッドウェイ委員会組織委員会(“COSO”)は、改訂内部統制—統合的フレームワーク(フレームワーク)を発表しました。以来、米国証券取引所に上場している多くの企業にとって、米国SOX法404条(以下US-SOX法)に準拠すべく、改訂フレームワークの実施は重要な業務となりました。背景としては、US-SOX法の要請として、米国証券取引委員会(SEC)は、財務報告に係る内部統制(ICFR)の評価の基準として、各企業が「適切なフレームワーク」を使用することを求めているからです。　COSOのフレームワークはSECの唱える適切性基準を満たしており、結果として、ほとんどの企業が旧フレームワークから改訂フレームワークへ移行しました。

財務報告に係る内部統制を効果的に維持する上でUS-SOX法への準拠が大切であることは言うまでもありません。しかし、一方で同様に、取締役会がリスク監視のために内部統制をどう位置づけるかを考える上で学ぶべき重要なポイントがあります。以下、このポイントについて概説します。

統制環境は組織のレピュテーション、ブランドイメージを守るために重要である。— COSOフレームワークの当初発表以後(1992年)、多くのオペレーション、コンプライアンス、報告書に関する企業の不祥事がありました。それを特定しませんが(いくつかは有名な話ですが)、それらの会社のほとんど全ての取締役の方々には、過去残念ながら不祥事等で責め立てられた記憶があることでしょう。これらの会社には問題となった危機に対する統制環境が乏しかったものと思われます。

内部統制の重要な要素として、統制環境は、内部統制に係わる強い組織カルチャー形成のための基盤となります。統制環境とは、ポリシー、基準、手続そして組織全体に対し効果的な内部統制を行える仕組みなどで成り立っています。取締役や上級経営者たちは、自分の行動、意思決定、コミュニケーションを通じて、内部統制の重要性に関する「トップの姿勢」を示します。経営者は中層部にトップの姿勢を浸透させる努力を行うことによって、企業内の様々な層の意識を高めることができます。

COSOフレームワークによると、統制環境とは下記で成り立っています:

- 組織としての誠実性と倫理観に対するコミットメントの表明
- 取締役が、監視を通じてガバナンスに対する責任を遂行すること
- 組織構造と、責任・権限の委譲
- 有能な人材の採用、育成、維持
- 個人の業績、報酬、各種のインセンティブなどの評価基準の厳正化(パフォーマンス評価の説明責任を果たす。)

しっかりした企業文化と内部統制に対する効果的なマネジメントの支援がなければ、企業は統制に亀裂を生じ、評判とブラン

ドイメージを傷つけることになります。おそらくこれらの問題が最近大ニュースとなった不祥事の要因となっているでしょう。

統制環境は外注プロセスも対象となる ― 企業は自社内だけでなく、戦略的パートナーシップなどの関係により、外部と共に活動しています。「企業の内部統制責任」と「外注サービス提供者の内部統制への責任」の区別が不明確になる中、両社のコミュニケーションに対して高度の統制が必要となります。例えば、自社に代わってビジネスプロセスの一部を担当する外注業者から得る情報、または自社の業務遂行上依存せざるを得ない外部企業からの情報についても、自社の内部情報と同等の内部統制が求められます。

要するに、マネジメントは外注先に対しての統制においても責任があるということになります。従って、トップダウンのリスクアプローチで関連あるとされたものに対しては、オペレーション、コンプライアンス、報告に関する内部統制評価の際に、外部企業についても範囲対象に含めることとなります。外注先等で処理された情報に依拠する際の統制としては、下記があげられます。:

- 外注先デューデリジェンス
- 外注先等との契約に監査権限条項を入れること
- 同条項権限を行使すること
- 外注先等が実施する統制に対して独立的に評価できる権利を取得すること。（例：サービス・オーガニゼーション・コントロール・レポート＝SOC 1 レポート）
- 外注先とのやり取りに対する効果的なインプットとアウトプットへの統制

定期的なリスク評価は、具体的な不正の可能性を考慮して行わなければならない ― 継続的なリスク評価は、効果的な内部統制を保持するために必須とされるトップダウン・リスクベースアプローチの一部です。これらの評価を通して、取締役会は、経営陣が財務関連・非財務関連報告に不正がないか（例:内部統制報告書、サスティナビリティ報告書、規制当局への報告書）、資産の横領、違法行為などの可能性を適切に評価していることを確認すべきです。さらに、第三者による不正の可能性も多くの企業に該当する問題です。

COSOフレームワークは、不正リスクの要素として次のようなものがあげられます:会計方針の適用に関するマネジメントの偏見、報告書内での判断基準、業界でよくある不正スキーム、組織が活動する地域、不正を誘引する業績連動型報酬、財務・非財務領域における怪しげな情報の操作、異常なまたは複雑怪奇とも言える取引、わざと実態を見えにくくするストラクチャーの構築、マネジメントによる統制の逸脱（オペレーション、コンプライアンス、報告などに対する統制）など。

US-SOX法準拠から学んだ大切なこと ― 報告書の質は服の袖のような存在です。袖がきれいに洗濯されていると誰も気づきません。袖に泥や垢がついていたら皆が気づきます。このたとえは財務報告にもあてはまります。投資家は報告書の公平性を当たり前としているからです。しかし、上場会社が既に公開した財務諸表について、会計原則の適用上の誤りがあったために書き換えたり、重要事項の漏れ、不正使用などがあれば、投資家は気づきます。つまり、市場は報告書の質を額面でとらえています。一度企業が一般投資家からの報告書に対する信用を失うと、取り戻すのは難しいのです。US-SOX法への準拠は米国では重要です。ICFRにおける重要な欠陥は、投資家に対する報告書の不備への初期段階の警告となります。私達は、1992年版から2013年版COSOフレームワークへの移行作業の中で教訓を得ることができました。これらの学びの中で最も重要だったのは、「US-SOX法を守るためにはトップダウン・リスクベースアプローチが不可欠である」ということです。改訂フレームワークを使用して範囲と目的を決める際、企業はこのアプローチを忘れることがあります。その結果、統制テストや文書化をやりすぎてしまったりしています。2013年COSOフレームワークは、US-SOX法の遵守にトップダウン・リスクベースアプローチこそが必要という本質を変えていない、ということをいくら強調しても足りません。

他の学びとしては、下記があげられます:

- 早い段階に頻繁に外部監査人と会うことにより、改訂フレームワークへの移行を、監査人の考えに一致した方向性で適切な手続きにより進められること。
- フレームワークの着眼点に集中することで、COSOフレームワークであげられている原則にキーコントロールを関連づける効果的なマッピングアプローチが可能となること。現存する統制文書から始め、フレームワークの構成要素の本質を考える。
- 間接的統制（全社統制とよばれることが多い）をテストする

際、ICFRに密接に結びついた目標に焦点をあててテストの深度を調整しましょう。例えば、身元調査をする際、社員全員を対象とするのではなく、財務報告書に責任のある人のみを対象とする（経営者が財務報告の範囲を超えた範囲をもカバーしようと思っていない限り）など。

- 統制が求められているレベルに達しているかを確かめるために、間違いの発見や修正の履歴を調べながら、統制の詳細を理解し、文書化する。
- キーコントロールの実行をサポートするために、企業が作成した情報の網羅性と正確性を評価する。公開企業会計監視委員会の調査報告書では、監査人に対し、もっとシステムレポート、クエリやエクセルの検証に重点を置くよう促す。

2013COSOフレームワークのオペレーション、コンプライアンス、その他の報告目的への適用は新しい領域 — 改訂フレームワークを適用する上で、ほとんどの企業はICFRのみに注目しています。フレームワークはUS-SOX法に特化したものだと思っている企業さえありますが、これは誤った理解です。オペレーション、コンプライアンス、その他報告など他の目的においてもフレームワークを使う利点はありますが、これらの努力はUS-SOX法準拠とは分けて行われなければなりません。進んでいる企業はCOSOフレームワークを他の領域にも適用しています。例えばサスティナビリティ報告書、規制遵守や連邦補助金のコントロールなどです。

取締役会への質問

取締役は、自社の業務遂行における潜在リスクに関し、下記の問いについて検討するようお勧めします:

- 取締役は、自社の統制環境が有効に機能しているか、特に注目してきましたか。
- 自社は、定期的に不正リスクに関するアセスメントしていますか。取締役は、第三者による不正リスクが許容範囲内に収められていると考えますか。
- 企業のUS-SOX法準拠手続は、トップダウン・リスクベースアプローチで行われていますか。また、その手続の費用対効果は適正と考えますか。
- 経営者は、COSOフレームワークを非財務諸表報告に対する内部統制の向上に適用しようとしていますか。

プロティビティの支援

プロティビティは、取締役会や上級経営者に対して、企業戦略やビジネスプランに潜む潜在的リスクを、企業本体はもちろん、様々なオペレーションユニットを対象として評価し、それらのリスクを軽減する内部統制をはじめ、あらゆる方法の支援を行います。企業の評判やブランドイメージを損ね、企業戦略の成功を妨げかねないリスクを特定して、優先順位をつけ、対処する支援を提供します。プロティビティは、COSOフレームワーク（オペレーション、コンプライアンス、レポーティング）を適用した内部統制の実施を支援します。

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。

protiviti®
Risk & Business Consulting.
Internal Audit.