GRCとセンターオブエクセレンス

小見門 恵
あずさ監査法人／KPMG
ビジネスアドバイザリー事業部パートナー
公認会計士

■はじめに

内部統制報告制度対応を終え、その後も相次ぎ発生する情報漏洩、不正等に対処する態勢を強化している企業の多くが、リスクマネジメント関連費用の増加に頭を悩ませている。本稿では企業のリスクマネジメントに係る取り組みの最近の傾向のひとつとして、GRC（ガバナンス、リスク、コンプライアンス）の取り組みについて紹介したい。

■GRCの意義

地震その他の災害、環境規格、品質規格、貸倒れ、政情不安、金利・為替・有価証券・商品相場等の市場変動、法令順守、財務報告、IT、人事、等々、法規制や規格が整備されるたびに、また、何らかの大きなリスク顕在化事例が話題になるごとに、企業はその種のリスクへの対処や低減にもっとも適すると考えられる方法で個別最適となるようにリスクに対処してきた。最高責任者や規程を定め、所管部署を置き、研修を行い、自己評価や内部監査機能を通じた統制テストを行う――このようなリスクマネジメントのアプローチを多くの企業はリスクの種類ごとに採用しているといえるだろう。

かかる状況下で、いくつかの企業が、それらの分断されたリスクマネジメント活動に費やされている経営資源の重複利用、現場負担、複雑な社内報告体系などを重要な経営課題と捉え、さまざまな種類のリスクマネジメント活動を体系立てて整理し、収斂させていくことにより、リスクマネジメント活動の最適化に向けて取り組み始めている。このような取り組みをGRCと呼んでいる。

ガバナンス（Governance）には、取締役会の活動等のいわゆる狭義のコーポレートガバナンスだけではなく、グループガバナンス等、企業グループを統治、統括するためのさまざまな活動が含まれる。ミッション、戦略、バリュー、ビジネスモデル、バリュードライバーなどを含み、企業の経営層の考え方がもっとも重要な要素となる。

リスク（Risk）には、リスクマネジメント関連活動すべてを含めている。自社が抱えるリスクにはどのようなものがあり、今どの程度なのか（リスクプロファイル）、それらリスクに対してどのような方針でいかなる態勢で取り組んでいるのか、今抱えている課題は何か、等についての利害関係者とのコミュニケーションもここでの検討範囲に入れる。

コンプライアンス（Compliance）として検討するのは、法規制等の遵守だけではなく、経営理念、社会通念、利害関係者の期待、等々を含む、いわゆる広義のコンプライアンス態勢である。

具体的にいえば、GRCの検討範囲には以下のような企業活動が含まれている。

- 会社の機関や組織設計、企業統治形態、活動
- 戦略や業績管理
- CSR関連活動、特に利害関係者との関係
- リスクマネジメント
- 内部統制関連活動
- 情報技術（IT）
- 企業倫理、法務コンプライアンス
- 環境マネジメント
- 品質マネジメント
- 人材（財）マネジメント
- 経理財務管理
- 監査その他のアシュアランス（保証）活動

GRCの取り組みを通じ、企業が利害関係者の期待を理解し優先順位付けを行い、バリューやリスクに応じた目標を設定し、リスクプロファイルを最適化し、企業価値を守りながら効率的、効果的にそれらの目標を達成することが可能となることが期待されている。企業はまた、法令

等の遵守のみならず社内外の期待に沿った企業運営を行い、利害関係者に適宜、適切な報告を行うことができる。

■センターオブエクセレンス（CoE）の活用

GRCの取り組みにはさまざまなケースがある。米国のある企業では、内部統制、コンプライアンス、個人情報保護、情報セキュリティ、ベンダーマネジメント等の各種リスクマネジメント関連活動の統合のためにセンターオブエクセレンス（CoE）を活用している。

当該企業では、いわゆる三層構造の防御ラインの中で、一次防御ラインである現場が、自部門の統制の自己点検／モニタリングを効果的に実施できていないため、二次や三次防御ラインである各種リスク所管部や内部監査部が評価作業を実施していた。そのため各種リスク所管部では、人員不足による負担過重や独立性が損なわれる恐れがあった。また、制度対応としての内部統制関連活動は比較的成熟しているものの、その他のリスクマネジメント活動の成熟度や評価精度にバラつきがあり、かつそれらの活動の調整が行われていないため、現場の負担も大きなものとなっていた。

そこで、各種活動の統合の第一歩として、リスク評価や統制の評価作業に係るCoEを設置することとした。CoEでは、以下のような機能を担っている。

一．年間の管理サイクルの調整

各種リスクマネジメント活動が現場に与える負荷を軽減するために、リスク評価、統制テスト、課題のフォローアップ、および研修を含む各種活動の実施時期を調整し、マスタースケジュールを作成。

二．所要スキルとナレッジ開発

従業員のスキル分析とそのデータベースの構築維持、リスクマネジメント関連研修カリキュラム作成支援、ベストプラクティスのツールと技法の取りまとめおよび共有。

リスクマネジメント活動のフレームワークや方法論、方針、標準的活動計画、展開ルール、データ収集や保管等に係る指針やガイダンスの作成。

三．統制テストの実施

テスト手続の策定、テストの作業計画、テストの実施、発見事項の分析、テスト結果の記録、傾向分析など。

特に例えば法令等の細かい知識を持たなくとも実施可能な部分は当該CoEにて協働実施（統制テストのシェアードサービスセンター化）。

まだまだCoEの取り組みは始まったばかりであり、その本格的効果はこれからであるが、これにより各種リスク所管部は、諸活動を展開する上では当該CoEを最大限に活用し、それぞれの活動を効率的に実施することができるようになりつつある。現場の統制テスト等への対応負担も軽減されてきている。さらに、現場による一次防御、各種リスク所管部による二次防御、内部監査部による三次防御という責任構造を明確化することで、各部門に求められるレベルの独立性を確保することが可能になっている。

GRCの取り組みは各社各様であるが、このようなCoEの活用は日本企業でもすぐに取り掛かれるのではないかと思われる。

■終わりに

世界経済フォーラムが二〇〇六年から公表している調査報告書第六版（「Global Risks 2011 Sixth Edition - An Initiative of the Risk Response Network」World Economic Forum）では、今後特に重要なリスクとして以下のようなものが挙げられている。

- 気候変動
- 財政危機
- 経済的不均衡
- グローバルガバナンスの失敗
- 極端なエネルギー価格変動性
- 地政学的紛争

多くの調査参加者たちが、今後十年内にこれらのリスクが顕在化し、私たちに大きな影響をもたらすものと予想している。

このようなリスクに対処していくためには、企業や国境の枠を超えた取り組みがますます必要になっていくものと思われる。今のうちに自社グループ内のリスク状況をしっかり「視える化」し、リスクマネジメント活動の最適化を図っておいた方がよいのかもしれない。