

第 114 回 月例研究会報告

1. タイトル

講演テーマ

「組織目標達成に役立つ COSO ERM」

講師

日本内部監査協会常務理事

淑徳大学兼任講師

JSSM コーポレート・ガバナンス研究会主査

山本 明知氏

会場 中央大学 駿河台記念館 285 号会議室

報告者 No. 6039 高井憲彦

2. はじめに

組織体のコントロールを確かめることが監査の役目だが、コントロールが適切であるためにはリスクを軽減するコントロールであるべきである。さらにそのリスクはビジネス目標達成に関連するものであるべきである。内部コントロールの定義として世界各国で採り入れられてきた COSO は COSO ERM に改訂され、さらに進化している。

COSO ERM は、組織体の使命、戦略目標、戦略、業務目標、リスク、コントロール、モニターリングの流れに沿った全社的取組みの枠組み（フレームワーク）を示している。

今回の月例研究会では、当分野でご活躍されている日本内部監査協会常務理事の山本明知氏から COSO ERM の最新動向について分かりやすくご紹介をいただいた。講演では「組織目標達成に役立つ COSO ERM」、「COSO ERM 統合的枠組み」、「ERM の実施状況」についてお話があり、質疑応答においても活発な討論が行われた。ここでは講演内容のポイントにつき報告する。以下の報告では講演で一部配布された資料から引用させていただきました。

* COSO : Committee Of Sponsoring Organization of the Treadway Commission

(米国のトレッドウエイ委員会組織委員会)

* COSO ERM : COSO Enterprise Risk Management Framework

3. 組織目標達成に役立つ COSO ERM

(1) COSO ERM に至る経緯

1987 年ガルフカナダ社で C S A (コントロール・セルフ・アセスメント) が開始されたことに端を発する。その後、米国で研究が進められ、1992 年 COSO レポートが発表され COSO コントロールモデルが銀行を中心に世界各国へ普及した。さらにこれが発展し、2000 年頃から ERM が提唱され 2004 年には「COSO ERM 統合的枠組み」が発表された。

(2) コントロールの存在価値

・経営者は業務目標と規程を設定し、監査対象のビジネスプロセス（現場）へ指示する。現場は本業について経営者へ報告をする一方、規程を遵守してい

るかには内部監査を受ける。内部監査人は監査報告を経営者および取締役会（監査委員会）へ報告する。

・ここでの規程は、外部の法律や規則をベースに自社のポリシー、スタンダード、ガイドラインなどであるが、監査対象の中には、これらが業務目標を達成するブレーキになっていると思っている人も多い。

・最近、内部監査人にはアシュアランスだけでなくコンサルテーションも求められている。後者については、リスク評価のワークショップを立ち上げることも必要である。これを継続するために「リスク管理室」や C R O (リスク管理担当役員) の設置に進む。

(3) COSO ERM の論理的必然性

2004 年「COSO ERM 統合的枠組み」では、下記のような展開で最終的にはステークホルダーに価値を提供することを目標にする。

・監査は内部コントロールの有効性をエンシュアする。組織体の中にあるコントロール目標（皆が納得した規程類）が基準であった。

↓

・内部コントロールが有効であるためにはリスクを軽減する内部コントロールでなければならない。リスクを評価してコントロール活動を進める、

↓

・組織体の目標達成に影響するリスクでなければならない。リスクは機会にもなりうるからリスクをマネージすることが重要である。目標とリスクおよびコントロールの関係を明らかにするのが ERM である。

(4) COSO ERM の要素について

1992 年発表された COSO IC-IF では 5 つの要素であったが 2004 年発表された COSO ERM -IF で下記の 8 要素になった。

1. 内部環境
2. 目標設定
3. 事象識別
4. リスク評価
5. リスク対応
6. コントロール活動
7. 情報およびコミュニケーション
8. モニターリング

ここでの「3.事象識別」は、将来どのようなことが起こるかを識別することであり、「5.リスク対応」においては経営判断が入る。つまり、リスク・マネジメントが重視されていることを示す。なお、「8.モニターリング」は監査を含む。

(5) ERM におけるマネジメントプロセス

下記のようなトップダウン・アプローチでリスク・マネジメントを重要視する。

1. 組織体の戦略にそって達成すべき全社的および下位レベルの業務目標を設定する。

2. 目標設定のためのリスクをマネージし、必要ならコントロール活動へ繋げる。
3. 内部監査は、リスク・マネジメントとコントロールのプロセスが適切かどうかを検証する。

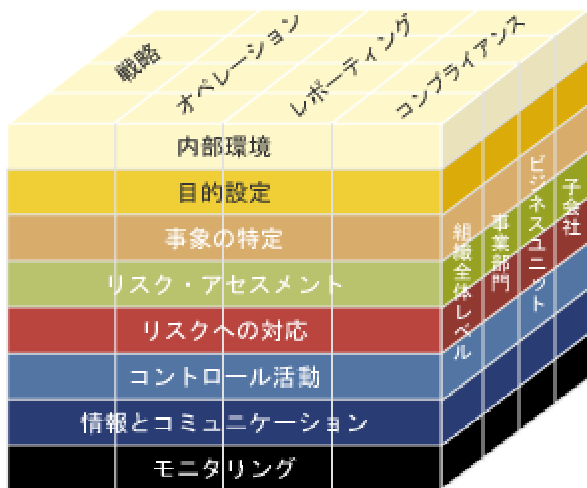
(6)内部監査パラダイムの変化

旧パラダイム→新パラダイムの変化を示すと以下のとおり、「コントロール」重視から「リスク」重視に移行していることがわかる。

- ・ 着眼点：内部コントロール→ビジネス・リスク
- ・ リスク評価：リスク要素→シナリオ計画（よい報告への展開、悪い報告への展開）
- ・ 内部監査テスト：重要なコントロール→重要なリスク
- ・ 内部監査方法：詳細テストの完全性を強調→広範なビジネス・リスク網羅を強調
- ・ 内部監査勧告：内部コントロール→リスク・マネジメント

4. COSO ERM 統合的枠組み

COSO ERM では ERM を図に示すように3つの基礎概念で整理して3次元マトリックスで表している。



出展：COSO Enterprise Risk Management Framework

上面の「目的カテゴリー」は戦略、オペレーション（業務）、レポート、コンプライアンスの4分類とし、側面の「事業組織」では組織全体、事業部門、ビジネスユニット、子会社の4部類としている。表面の「構成要素」は3.(4)に示すように8分類としている。

それぞれの活動はこのマトリックスのどこに位置するかを確認しその意義を把握することができる。なお、この枠組みの内容は下記 COSO のホームページが参考文献を参照されたい。

URL : <http://www.coso.org/publications.htm>

5. まとめ

(1) なぜ ERM は必要か

(John Lewise VP Chief Audit Executive
WalMart Stores Inc 2002.6 発表から)

- ・ ビジネスが直面するリスクが増加
- ・ 監査委員がリスク・マネジメントを監視
- ・ ミスマネジメントは株主利益を損なう
- ・ リスク評価に体系的アプローチ
- ・ リスクを価値創造につなげる

(2) COSO ERM の定義

(Enterprise Risk Management-Integrated
Executive Summary Framework Sep.2004)

ERM は組織体の取締役、経営管理者、その他の要員によってもたらされるプロセスである。ERM は戦略策定においてその企業全体に適用される。そのゴールは組織体に影響する可能性のある事象を識別し、その組織体のリスク選好内にあるリスクをマネージすることによって、組織目標達成に関する合理的なアシュアランスを備えることである。

6. 感想

最近では企業の不祥事が続発しリスク・マネジメントの必要性が叫ばれているが、今回の講演で認識を新たにしました。3.(6)で内部監査パラダイムの変化で監査の着眼点が「コントロール」から「ビジネス・リスク」へ移っているのもシステム監査を行なう上で留意すべき点と思う。つまり、この監査の目的は何かということを常に検証しながら進めることが必要でしょうか。また、監査人にも「アシュアランス」と共に「コンサルテーション」が求められるとのお話があったが「助言型監査」の重要性が示されていると思う。

米国でも COSO ERM の普及は大企業を中心だとのことだが、わが国でもこの手法は徐々に大企業から中小企業へと進展していくものと考えられる。われわれもこの動向に注目し、システム監査能力を高めていきたいと思う。

以上