The Bulletin

protiviti
Independent Risk Consulting

VOLUME 2 ISSUE 6

エンタープライズリスクマネジメント（ERM－Enterprise Risk Management）：実践的な導入へのアドバイス

エンタープライズリスクマネジメント（ERM）の基盤となる概念の一つであるリスクに対するポートフォリオの視点は、以前から注目されてきている。この概念は、金融機関や世界の先進的な企業が、マーケットリスクと信用リスクの管理に、リスクの枠組み、資本配分及びバリューアットリスクなどの統合的リスク計測手法を適用するなかで生まれたものである。近年の市場の進化により、変動するのは今や通貨、利率、または株価だけではないことが明らかである。顧客の嗜好、競合の動向、労働市場、テクノロジーなどはすべて、より激しく金融市場のように変動している。企業のビジネスモデルの寿命が短くなるにつれ、変化の態様は単に直線的ではなく、幾何級数的なものとなってきている。つまり、覆されないビジネスモデルはこの世にはないといえるほどだ。成功を継続するには、企業は、常に革新を行い、顧客と市場のために新しい価値の源泉を創出しなければならない。さもなければ、より機敏で創造力のある競争相手に敗北を喫することになる。戦略設定は、流動的でダイナミックなプロセスだ。そのプロセスの価値をさらに増強するリスクマネジメントも、同様に流動的でダイナミックなプロセスである。

多くの経営幹部は、ERM の価値に気づいていない。一部の経営幹部と管理者は ERM を一時的な流行として話を合わせるだけで、そのうちなくなってくれればとさえ願っている。ERM に多くの経営者が踏み込めないのは、それが何なのかを直ちに理解するのが困難だからだ。この Bulletin では、ERM に関するそのような疑問に答えていく。

ERM とは何か？

ERM は、組織のリスクマネジメント能力を継続的に改善する目的をもって、戦略、人、プロセス、テクノロジー、知識を相互に深く連携させるものである。2004 年 9 月に発表された COSO の「エンタープライズリスクマネジメント（ERM）- 統合的枠組み（Enterprise Risk Management - Integrated Framework）」は、ERM を次のように定義している。

事業目的の達成について合理的な保証を提供するために、事業体の取締役会、経営者及びその他の構成員によって遂行される、戦略設定はもとより事業体のあらゆる領域に適用されるプロセスである。事業体に影響を及ぼす可能性のある潜在的事象を認識し、リスクをリスク選好の範囲内に収められるように策定される。

上記の定義が戦略設定に焦点をあてていることに留意すべきである。適用対象は企業全体であり、その基準は企業のリスク選好だ。
ERM は、優先的に対応すべきリスクに対する企業の管理能力を促進する。ERM のアプローチが戦略設定に効果的に統合されると、経営者の関心は企業の資産ポートフォリオ全体に影響する不確実性に向けられる。その資産ポートフォーリオには、顧客資産、従業員・サプライヤー資産、差別化戦略・固有のブランド・革新的なプロセスやシステムといった無形の組織的資産をも含む。このように広く捉えることは、時価総額がバランスシートの純資産価値をはるかに上回り、多くの企業が評判や信頼失墜のリスクを許容レベルにまで低減させたいと考えている今の時代にあっては極めて重要なことである。

なぜ ERM を導入するのか？

伝統的なリスクマネジメントのアプローチは、個々のリスクを個別に扱い、断片的になる傾向がある。このようなアプローチでは、しばしば有形資産や金融資産に関する不確実性に焦点が限定される。さらに伝統的アプローチは、企業価値の増大よりも損失回避に焦点を当てるため、急激に変化する事業環境におけるリスクマネジメントの価値を再定義するために多くの組織が必要としている枠組みを提供していない。

これに対して ERM は、組織がステークホルダーのために持続可能な価値を創出する際に直面する不確実性を評価・管理するにあたって、先見的で効果的なプロセスを企業に提供する。ERM は、企業価値を守り高めるためのリスクマネジメントに、以下の 3 つの要素をもって貢献する。

- 第一に、持続可能な競争優位の確立に焦点を当てる。ERM は、リスクに対する様々な視点を整合させ、統合し、変化する環境に企業が適切に対応できるよう支援することで、

分断的な組織行動を克服することに役立つ。ERM は、リスクマネジメントプロセスを有形資産や金融資産だけでなく、あらゆる企業価値の源泉に適用するよう焦点を広げることで、リスクマネジメントを戦略レベルにまで引き上げる。

- 第二に、リスクマネジメントのコストを最適化する。ERM を通じて、経営者はリスクの受け入れや移転などの意思決定を統合し、重複する活動を排除し、組織がビジネスモデルを実行する際に受け入れ可能なリスクのレベルが判断できるようになる。
- 第三に、経営者のビジネスパフォーマンスを改善することに役立つ。ERM は、(a) 大きな出来事の影響を予測し、(b) それらの出来事の発生を防ぐための対応をとり、それが発生した場合の組織への影響を管理することで、許容できない業績変動と損失発生を抑えることを支援する。ERMによって、リスクマネジメントは単なる「危険を回避し防止措置を講ずること」から、成長と収益の新しい機会の追求の中でよりよい意思決定を必要とする経営者のための、企業価値を守り高めるための差別化できる経営手法へと高められる。

ERM は、経営陣がリスクテイクしているリスクを真に理解し、そのリスクを管理する能力が組織内に備わっているという確信の支えとなり、事業機会追求の行動を活性化する。最近公表された "Protiviti U.S. Risk Barometer"（www.protiviti.com）など、長年にわたる当社の研究では、上級管理者の 6 割は、会社の現状のリスクマネジメント実施では潜在的に重要なすべてのビジネスリスクが特定され管理されていることに対して「強い確信を持てない」ことが一貫して示されている。ERM の焦点は、戦略設定とリスクマネジメントの統合にある。重要な点は、プラスの影響とマイナスの影響の両方を持ち得る将来の潜在的事象を特定し、その将来の事象に対する組織のエクスポージャーを管理するための効果的な戦略を評価することにある。ERM は、リスクマネジメントを、積極的・継続的で、企業価値の視点をもってより視野の広い、プロセスとしての活動に変えるものである。これは、ビジネスに対するリスクマネジメントの価値を再定義するものである。

ERM を導入するための 5 つのステップ

ERM の導入を選択する組織は、5 つの実践的ステップを実施すべきである。以下のステップは ERM 導入の作業を簡単に説明したものだが、導入プロセスは一夜でできるものではない。ERM は長い道のりであり、これらのステップは実践的な出発点となるものだ。

ステップ 1： 全社的リスク評価 － エンタープライズリスクアセスメント（ERA）を実施する

ERA は、ビジネス戦略を考慮して組織のリスクを特定し優先順位を決定し、優先的なリスクを管理する能力の現状についての情報など、効果的なリスク対応を設計するために必要な質の高いデータを提供する。組織がリスクの優先順位を決定していない場合、価値提示は抽象的なものとなり、ERM は説得力を欠いてしまう。組織の優先的リスクに関するギャップを把握することは、ERM の価値提示を具体化するための基礎になる。よって、ERM についての長々しい議論は避け、ビジネスモデルに内在するリスクを理解するために ERA を実施することから始める。

ステップ 2： 優先的リスクに係わるギャップをもとに ERM のビジョンと価値提示を明確にする

このステップは、取り組みを前進させるための経済合理性を提供する。ERM のビジョンとは、組織内でのリスクマネジメントの役割と、主要なリスクを管理するために必要な能力についての共通認識である。上級管理者からなるワーキンググループは、(a) 組織内のリスクマネジメントの役割を明確にし、(b) 企業全体及びその組織の関連目標を定める権限を与えられるべきである。

この作業を遂行するためには、経営者は、リスクマネジメントの有効性の維持向上のために必要な能力に支えられた、信頼できる事実の裏付けを必要とする。ここで、ギャップ分析が有用となり、次のように実施される。

A. まず、重大なリスクの優先順位付けを行い、そのリスクを管理するための能力の現状を評価する。これはステップ 1 で説明した ERA だ。その主要なリスクのそれぞれについて能力の現状を判断した後、目指すべき能力レベルを設定して、能力不足のギャップを把握し、そのギャップを埋めるようにリスクマネジメント能力を高めることを目標とする。「リスクマネジメント能力」要素には、組織のリスク対応に必要とされる方針、プロセス、組織構成、レポート、方法論、テクノロジーが含まれる。

B. ERM のインフラは、リスクマネジメント能力の維持向上

に必要な適切な監視、管理、規律を浸透させるための方針、プロセス、組織構成、レポートなどから構成される。ERM のインフラ要素の例としては、たとえば、全体的リスクマネジメント方針、全社レベルのリスク評価プロセス、リスクマネジメントに関しての取締役会の議題や CEO の検討事項リスト、正式なリスク管理委員会の設置、リスクマネジメントの役割と責任の明確性、ダッシュボードなどのリスク報告、及びリスクのポートフォリオ管理を可能にするツールなどがある。

つまり、組織のリスクマネジメント能力の現状と目指すべき状態とのギャップ（上記項目（A））が大きいほど、このリスクマネジメント能力向上を促進するための ERM のインフラ（上記項目（B））の必要性は大きくなる。

ステップ３： 優先順位の高い１つまたは２つのリスクについて組織のリスクマネジメント能力を高める

このステップは、経営者が改善の必要性を認識している分野のリスクマネジメント能力を改善することに焦点を当てる。他の優先項目と同様に、ERM はどこからか始めなければならない。例えば、可能な出発点には次のようなものがある。

- 内部統制評価・報告要請の遵守（米国企業改革法 404 条や日本の金融商品取引法による内部統制報告制度）
- 企業リスク評価の結果（ステップ１を参照）に基づく１つまたは２つの優先的な財務または業務リスク（例えば、金融機関のオペレーショナルリスク）
- 法規制遵守リスクやガバナンスの課題
- ERM と管理プロセスの統合（例えば、経営戦略、年度事業計画、製品計画または販路拡大、品質改善活動、設備投資計画、業績測定と評価等）

組織がその道のりをどこから始めるかにかかわらず、ERM の焦点は変わらない。組織としての優先順位の高いビジネスリスクに関するリスクマネジメント能力の成熟度を高めることである。

ステップ４： 既存の ERM インフラの能力を評価し、それを高めるための戦略を展開する

重要なリスクマネジメント能力を高めるためには監視、管理及び規律が必要だ。その監視、管理及び規律を浸透させる方針、プロセス、組織及びレポートが「ERM インフラ」と呼ばれるものだ。ERM インフラの目的は、主要なリスクを管理するために、組織のリスクマネジメント能力の現状と目指すべき状態と間の大きなギャップをなくすことである。前頁ステップ２において ERM インフラの例をいくつか提示した。その他の例としては、共通のリスク言語やその他のフレームワーク、ベストプラクティスの知識共有化、共通のトレーニング、チーフリスクオフィサー（あるいは同等の執行役員）の選任、リスク選好とリスク許容度の設定、リスク対応と事業計画の統合及び支援テクノロジーがあげられる。

ERM インフラは、ERM の導入における３つの重要なことを推進する。第一に、企業のリスクとそのマネジメント能力について事実に基づく理解を高める。第二に、重要なリスクについてのオーナーシップを確保する。最後に、容認できないリスクマネジメント能力のギャップを最小化する原動力となる。

ERM インフラは、すべての組織に画一的なものではない。ある組織で機能しても、他の組織で機能するとは限らない。ERM のインフラの要素は、ERM を導入するために用いられる方法やツール、対象とする目的の範囲、企業文化及び組織の事業単位のどこまでの範囲に横断的に適用したいかによって変わってくる。経営者はこのような要素に沿って必要とされる ERM インフラの要素を決定する必要がある。

ステップ５： その他の主要なリスクに対するリスクマネジメント能力を高める

前頁の４つのステップが完了した後、変化に合わせて ERA を更新することがしばしば必要になる。更新された ERA によって優先順位の高いリスクが再定義された場合、経営者は各リスクを管理する能力の現状を判断し、次に目指すべき状態を検討しなければならない。目的は、ステップ３で扱った１つまたは２つの優先順位の高いリスクの場合と同じだ。つまり、主要なリスクを管理する企業の能力の成熟度を高めることだ。このステップの実施により、経営者はその他の優先順位の高いリスクに焦点を広げることになる。

リスクマネジメント能力を高めることが目的

それぞれの優先的リスクについて、経営者は企業のリスクマネジメント能力の相対的な成熟度を評価する。つまり、経営者は

その評価に基づいて戦略的な決定をする必要がある。事業目的を継続的に達成するためにどの程度の能力がさらに必要になるかを評価する。

組織の有限な資源と予想される費用対効果に対する経営者の評価に沿って、リスクマネジメント能力を設計し、向上させなければならない。目的は、組織にとって最も緊急性の高い戦略上のリスクと不確実性を特定し、これらのリスクと不確実性を管理するための能力の改善に焦点を当てることだ。ERM インフラは、この目的に向かって進むことを促すものだ。
ERM インフラ構築の初期段階にある会社は、共通言語、リスクマネジメント管理体制及び全社リスク評価プロセスなどの基盤作りに取り組むことになる。会社によっては、ERM を特定の事業単位に適用することもある。また金融機関における市場リスクや与信リスクの管理、規制業界における法令遵守リスクの管理のように、より高い段階にまで進んでいる企業もある。

会社がリスクマネジメント実施のどのような段階にあろうとも、戦略を考慮して優先的なリスクそれぞれについて会社のリスクマネジメント能力がどの程度であるべきかを議論することは、取締役や経営者に多くの意思決定情報を提供する。

The Bulletin 第 2 部第 3 号（www.protiviti.com）で紹介された能力成熟度モデルは、組織のリスクマネジメント能力の成熟度を評価するための尺度を提供する。このモデルは、プロセス能力のレベルを「初期段階」から「最適化段階」までの 5 段階で示す。能力成熟度モデルは、戦略的に重要なリスク分野における企業の能力を評価するための強力なツールである。このモデルを活用して、経営者は特定の分野において目指すべき能力のレベルとのギャップを把握し、業務の評価指標からプロセスの成熟度へと議論を発展させることができる。ERM インフラは、評価プロセスが事実に基づき、関与するリスクオーナーによって適切に実施されることを確保する。

ERM の主要な成功要素

ERM へ向けて展開を図る会社は、それが旅の過程であって終着点ではないことに留意すべきである。ERM は、潜在的に組織の行動に大きな変革をもたらす可能性がある。自覚を促し、周囲に納得性を与え、究極的には組織全体を通してオーナーシップを植え付ける基本的なプロセスである。リスクに対する各人の視点は異なるため、変化への対応力は、ERM 推進の重要な側面となるのである。
ERM 導入を成功に導くためには、以下の「基本原則」に留意すべきである。

- ERM の計画を優先度の高いビジネスニーズに関連付け展開する。トップの支援を得て、マイルストーンに対して進捗状況を管理する。
- リスクマネジメントの目的と適切な ERM インフラについて同意を得る。関係する組織文化の課題を考慮し、全社レベルの適用に重点を置く。
- リスクマネジメントを戦略設定及び事業計画プロセスと統合し、有効な全社リスク評価プロセスをすみやかに実施する。
- (a) 目指すべきリスクマネジメント能力に関する決定を誰がするのか、(b) 重要なギャップを埋めるための能力向上の計画に誰が責任を負うのか、(c) 誰が進捗と業績を監視するのかなど、プロセスに対するオーナーシップの課題を明確にする。
- ERM インフラの目的は、リスクマネジメント能力を改善するにあたって適切な監督、管理及び規律を提供することであることを忘れないようにする。
- COSO の ERM フレームワークは、組織の ERM 能力をベンチマークする際の基準を提供する。

要約

ERM を適切に導入すれば、リスクテイクをその組織のコアコンピテンシーとリスク選好に整合させて、組織はより速いスピードとスキルと確信を持って、戦略的な成長の機会を追求することができる。市場は、戦略的に焦点を絞った企業に注目し、(真実または見かけの認識にかかわらず) リスクマネジメント能力の質と程度によってこれらの組織を識別していくことになるであろう。

確認のための主な質問項目

●取締役への主な質問

- リスクの受入れまたは拒否を決定するなどの戦略設定プロセスにおいて、執行陣は適時に取締役を関与させていますか？
  たとえば …
  — 「リスク選好」(つまり組織の戦略の選択肢をきめる執

行経営陣の「世界観」）に対して取締役会レベルの議論の内容に満足していますか？

— 取締役会の認識なしに会社は重大なリスクを取ることはないと確信できますか（例えば、競争相手よりも高い収益を生み出す事業は、競争相手よりもより大きなリスクをとっている結果ですか）？

・ 取締役会は優先的なビジネスリスク及びこれらのリスクへの対応を理解していますか？ リスクはリストに挙がっていますか？ それらを議論する十分な時間が取締役会において取られていますか？

・ 取締役会は受け取るレポートに満足していますか？

●執行役員・管理者向けの主な質問

・ 経営目標や業績目標を達成するための組織戦略に内在する重要な不確実性または弱点を理解しているか？ これらの不確実性を取締役会に伝えていますか？

・ 組織が潜在的に重要なすべてのビジネスリスクを管理できていると確信していますか？ リスクを特定し優先順位を決定する全社的プロセスがあるか？ 変化が生じているかどうかを判断するために定期的にリスク評価を行っていますか？

・ 以下を達成するための有効な監視組織が確立されていますか？

— リスクマネジメントに関する役割、責任及び実施義務を明確にする。

— リスクオーナーの行動をモニターする。

— リスクマネジメント能力の改善を計画に従って実施する。

エンタープライズリスクマネジメントについて詳細に知りたいという方のため、Protiviti では「エンタープライズリスクマネジメントのガイド：よくある質問（Guide to Enterprise Risk Management：Frequently Asked Questions）」という総合的リソースガイドを発行しています。これは www.protiviti.com で入手可能です。この新しい出版物には、ERM の基礎、COSO フレームワーク、役割と責任、リスクマネジメント監視組織、開始方法、リスクマネジメント能力の構築と強化、注目すべきビジネス実践例、及びその他多くのトピックに関する 160 項目を超える質問と回答が掲載されています。