protiviti®
Risk & Business Consulting.
Internal Audit.

Risk Oversight vol.71
取締役会のリスク監視

リスクマネジメント能力の成熟度を考える

「自社のリスクマネジメントの成熟度はどの程度か」、という質問を投げかけられたことはあるでしょうか。少なくとも、この質問を聞いたことはあるのではないでしょうか。我々もこの質問をよく耳にします。プロセスの成熟度が高まれば、有効性がより高まることが推定されます。しかし、これが実際に意味するところは何でしょうか。そして、成熟度という考え方はリスクマネジメントにどのように適用されるのでしょうか。

効果的な全社的リスクマネジメント（ERM）は、最も重要なリスクへの適時の対応を可能にします。リスクマネジメントのインフラには以下の6つの要素があります：（1）戦略・方針、（2）プロセス、（3）人と組織、（4）レポート、（5）方法論と前提、および（6）システムとデータ。効果的なリスク対応は、これら全ての要素を考慮に入れます。

所与のリスク（または関連するリスクのグループ）に対してこれらの6要素を整備することにより、リスクマネジメントの成熟度向上に向けた道筋がつけられます。組織のリスクマネジメントがより成熟したものであればあるほど、戦略とパフォーマンス向上による企業価値の創造と、リスク選好フレームワークと有効なリスクマネジメント能力による企業価値の保護との間に生じる、避けがたい緊張のバランスを取る企業文化はより強いものになるでしょう。

主要な考慮事項

能力の成熟度フレームワークは、以下のような問いかけについて経営者がより明確に思考する上での助けとなります。

- 特定のリスクを管理する上で、場当たり的に数名の適任者に依拠しているか、それとも強固な能力を有し継続的な改善を行っているか。
- 優先順位の高いリスクのそれぞれに対してインフラの改善を行っていくにあたり、リスクマネジメント能力にどの程度の実効性を求めるのか。
- リスクの種類に応じて、リスク対応と関連するコントロール活動の厳格さと強固さを変える必要があるか。それとも、成熟したリスクマネジメント能力を適用する上で、全てのリスクを同じように取り扱ってよいか。

組織の能力と望まれるリスク対応を相互に整合させる上で、意識的な選択を行います。リソースは限られているため、予想されるコストとベネフィットを考慮し、リスクマネジメント能力を選択的に改善しなければなりません。ERMのゴールは、組織にとっての最も重要なエクスポージャーと不確実性を識別し、それらを管理するための能力の改善に焦点を当てることです。この理由のために、リスクマネジメントのインフラに力点を置くことが重要になります。

成熟度の5つの水準を以下に例示します。

- 成熟度の初期段階（Initial Stage）では、リスクマネジメントは断片的であり、場当たり的に行われています。個々のリス

クは縦割りで管理され、多くの場合、組織は事象に対して受け身となります。戦略・方針や正式なプロセスは概して存在しないため、組織のリスク管理は、自らのイニシアティブで行動する経験豊かなマネージャに依拠しています。
また、リスクオーナーが明確になっていないため、アカウンタビリティがほぼ存在しません。退職者が出た場合、彼らの仕事を引き継ぐことが困難です。重要性の低いリスクについては初期段階でも良いかもしれませんが、厳格さと規律がより求められる領域においては、方向性の欠如が危機の温床となります。

- 成熟度が連続・反復化の段階(Repeatable Stage)になると、所定の目的と要件を達成するために、リスク評価を含めたリスクマネジメント方針に関する基本的な仕組みとプロセスが整備されます。リスクマネジメントに人的リソースが割り当てられ、特定の個々人の責任と権限が定義されます。この段階では、結果に対する責任を特定の個々人に帰せられるほど報告の仕組みが厳格ではないため、アカウンタビリティに関する課題がまだ存在するかもしれません。このため、「留意すべき事項」について、依然として人に依拠するところが大きい状態にあります。しかし、プロセスの規律が高められ、リスク管理のガイドラインが確立することにより、「反復」があり、退職者によって生じる穴は初期段階ほど大きくはありません。

- 定義化の段階(Defined Stage)では、戦略・方針とプロセスはさらに精緻化され、文書化が行われることにより、事業部門や職能部門にわたって横断的により統一的なリスク低減活動とリスク監視が実施されます。例としては以下が挙げられます。

  - リスク委員会の仕組みが整備され、全社的リスクを総合し、部門・機能間の協調を確保することに責任を有する担当役員が指名されている。
  - 戦略・方針の遵守と意図したとおりのプロセスの実施を確実にするために、コントロールの文書化と検証を行う強固な仕組みが整備されている。
  - 役割と責任が明確に定義されている。精密な方法論に支えられた強固なマネジメント・レポートは、適切な主要業績指標と主要リスク指標を意思決定プロセスに組み入れることにより、より多くの価値を付加する。
  - テクノロジが他の全てのインフラ要素の基盤となり、機能が向上したシステムの安定性と拡張性が増している。
  - 例外事項や「ニアミス」が適時に報告され、教訓や統制の不備に基づく改善活動が行われており、「リスク感度とリスク認識の高い意思決定」が行われていることが明らかである。

- 定義化の段階にある組織は、強固なリスク・ガバナンスとリスク文化の基礎を構築する途上にあります。管理化の段階(Managed Stage)では、新たなリスクを識別し破壊的な変化が生じる可能性を検知するための予測、シナリオ・プランニング、およびトレンド分析など、より高度な定量化手法や信頼性が実証されたモデル、データ・アナリティクスによる意思決定の支援が見られます。正式なディフェンスライン・フレームワークが導入され、リスクの測定がパフォーマンス・ゴールと紐付けられ、早期警戒システムが整備され、資本配分手法の効果的な採用が行われます。
リスク選好（アペタイト）フレームワークも確立され、事業部門に配分されるリスク許容度への切り分けが行われます。所定のリスク許容度を超過しそうになる、あるいは超過した際には、状況評価が行われ、必要に応じて是正措置が取られます。目標、ターゲットおよび業績指標はダッシュボードレポーティングやドリル・ダウン能力備えた全社的システムに組み込まれます。これらの強化された能力により、リスクに関する考察の戦略設定、事業計画および業績管理への組み込みが促進されます。また、これらの能力によって、組織は他に先んじて新たなリスク（および機会）を捉え、行動することができます。

- 最適化の段階(Optimizing Stage)は能力が最も高い水準であり、組織は管理化の段階にある能力の継続的改善にコミットしており、事業環境が変化する中でリスクマネジメント・インフラの全ての要素が完全に合致した状態に維持されます。リスクとリウォードの望まれるバランスを達成し、複数のリスクにわたる分散化の効果を理解し利用するために、会社全体を視野にリスク戦略・方針が評価・見直しされます。
最適化の段階では、ベストプラクティスが日常的に識別され、組織にわたって共有され、リスクマネジメント能力の強化は、外部および内部の状況が変化する中で、継続的に行われていくことが示されます。全社的に構築、適用された改善

活動（例えば、シックス・シグマ）は、リスクマネジメントとの統合・連携が確立されます。

以上が成熟度フレームワークにおける5つの段階です。上記の各段階で例示した基準は、それぞれの連続する成熟度の段階が、リスク管理の更なる強化を反映していることを示しています。企業の能力の成熟度が高まると、リスク管理が成功する見込みがより高まり、リスク管理が失敗する可能性はより低くなります。成熟度フレームワークをリスクオーナーが一貫性を持ち、かつ事実に基づいて活用することにより、組織全体のリスクマネジメント能力の現状と目標とする状態を的確に理解し、明確にすることが可能になります。

成熟度フレームワークの利用例としては以下が挙げられます。

- それぞれのリスク（例えば、規制、安全衛生、あるいはサプライチェーン・リスク）について、企業のリスクマネジメント能力の現状を評価します。現状とは、一般的には、存在し機能している能力を意味しますが、能力を改善するために計画されているイニシアティブのうち予算が確保され着手済みのものも考慮に入れます（これを改善後の状態ともいいます）。

- 適切なリスク対応を達成するためにどの程度の能力を追加する必要があるのかを判断します。これを目標とする状態といいます。目標とする状態を評価するにあたっては、可能な限り現実的であることが求められます。その目的は、企業がビジネスモデルを実行する上で、中核的コンピテンシーに最も合致した合理的に期待される能力を選択することにあります。

- 目標とする状態はリスクによって変わることを認識する必要があります。例えば、外国為替レートの変動に対する著しいエクスポージャーについては、少なくとも管理化の段階における能力が求められます。原子力発電所の操業などに伴う業務リスクについては、誤謬を許容する余地がほとんどないため、経営者は最適化の段階を選択するでしょう。暴風、洪水、その他の災害リスクについては、定期的な分析実施と保険付保のみを必要とし、複雑なリスク・レポーティングの必要性はほとんどないため、連続・反復化の段階における能力が求められます。最も重要な情報資産とシステムに関するサイバーセキュリティ・リスクについては、管理化の段階が目標とするでしょう。

- 現状と目標とする状態との間のギャップを識別した上で、ギャップを埋めるための能力強化に伴う予想コストとベネフィットの評価を行います。ギャップ分析の結果として策定される行動ステップは、ビジネスプランに統合されます。

多くの場合、能力の改善は段階的に行われます。例えば、ある会社の信用リスク管理能力の現状が、連続・反復化の段階にあるとします。また、経営者が、これらの能力は管理化の段階にあるべきとの決定を行ったとします。このギャップを埋める上で、ギャップを一度に埋めるのではなく、能力改善の設計と実施に対して段階的なアプローチを活用し、まずは定義化の段階に進み、その後管理化の段階に進むことが望ましいかもしれません。

このアプローチは、従業員の変革に対する準備の度合いにより沿っている可能性があり、成功の見込みを高める可能性もありますので、このアプローチは組織における混乱を低減します。能力の成熟度フレームワークは、現状から目標とする将来の状態への組織の移行のスピードを計画し、決定する上で、知識を有する人員による慎重な検討と判断を促します。

全ての組織に当てはまるアプローチは存在しません。ある会社における特定のリスクを管理する上での「ベストプラクティス」は、別の会社において同じリスクを管理する上で、不十分もしくは過度であるかもしれません。例えば、洗練されたモデルの適用は、売買取引を行っている組織では市場リスク管理におけるベストプラクティスでしょう。しかし、価格変動リスクにさらされている取引が数えるほどしかない企業においては、エクスポージャーは無視し得るほどのものであるため、そのような洗練されたモデルは不要でしょう。全てのリスクについて最先端の手法を採用する必要はありません。それができるほどのリソースを持つ組織はなく、そうする事業上の合理的な理由もありません。このように、能力の成熟度という観点で思考することにより、リソース配分プロセスが円滑なものとなります。

取締役会の考慮事項

以下は、事業体の活動に内在するリスクに関連して取締役会が考慮すべき事項です。

- 組織全体および最も重要なリスクのそれぞれについて、組織のリスクマネジメントにおける能力はどの成熟度段階にあるか。
- 個々のリスクへの組織のリスク対応は、リスクを許容水準に低減するために必要とされる適切な能力についての慎重な評価を反映したものになっているか。
- リスクマネジメント能力の改善が求められる場合、能力を次の成熟度レベルに高めるための計画を持っているか。
- 重要なリスクを管理するのに、過度に従業員に依存していないか、予期せぬ退職や解雇が起こった場合に重要なリスクにさらされることにならないか。

プロティビティの支援

プロティビティは、上場および非上場企業の取締役が組織の重要なリスクを識別し、管理するのを支援しています。プロティビティは、リスクマネジメント能力の成熟度評価において、企業の内側からの視点とは異なる、経験に基づいた偏りのない見解を提供しています。

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.