

ISO31000 箇条 5

5.1 一般

リスクマネジメントの枠組み(フレームワーク)の意義は、リスクマネジメントを組織の重要な活動及び機能に統合するときに組織を支援することである。リスクマネジメントの有効性は、意思決定を含む組織統治への統合にかかっている。そのためには、ステークホルダ、特にトップマネジメントの支援が必要である。枠組みの策定は、組織全体におけるリスクマネジメントの統合、設計、実施、評価及び改善を含む。図に枠組みの構成要素を示している。

組織は、既存のリスクマネジメントの方策及びプロセスを評価し、かい離を分析し、枠組みの中でこれらのかい離に取り組むことが望ましい。枠組みの構成要素と、それらの構成要素が共に機能する仕方は、組織の必要性に合わせて調整することが望ましい。

5.2 リーダーシップ及びコミットメント

トップマネジメント及び監督機関（該当する場合）は、リスクマネジメントが組織の全ての活動に統合されることを確実にすることが望ましい。



また、次の事項を通じて、リーダーシップ及びコミットメントを示すことが望ましい。

- 枠組みの全ての要素を組織に合わせて実施する。
- リスクマネジメントの取組み方、計画又は活動方針を

確定する声明又は方針を公表する。

- 必要な資源がリスクのマネジメントを行うことに配分されることを確実にする。
- 権限、責任及びアカウンタビリティを、組織内の適切な階層に割り当てる。

リーダーシップ及びコミットメントは、組織の次の事項を促進する。

- リスクマネジメントを、組織の目的、戦略及び文化と整合させる。設計
- 組織の全ての義務、及び組織の任意のコミットメントを認識し、これらに取り組む。
- リスク基準の策定の指針として組織が取ることができる、又は取ることができないリスクの大きさ及び種類を確定し、それらのリスクが組織及びステークホルダに伝達されることを確実にする。
- リスクマネジメントの価値を組織及び組織のステークホルダに伝達する。
- リスクの体系的モニタリングを推進する。
- リスクマネジメントの枠組みが組織の状況に対して常に適切であることを確実にする。

トップマネジメントはリスクのマネジメントを行うことに責任を負い、監督機関はリスクマネジメントを監視する責任を負う。監督機関は、しばしば次の事項を行うことを期待され又は必要とされる。

- 組織の目的を決定する際にリスクが十分に検討されることを確実にする。
- 組織が目的の追求に当たって直面するリスクを理解する。
- これらのリスクのマネジメントを行うためのシステムが実施され、有効に運用されることを確実にする。
- 組織の目的に照らして、それらのリスクが適切であることを確実にする。
- それらのリスク及びそれらのマネジメントに関する情報が適切に伝達されることを確実にする。

5.3 統合

リスクマネジメントの統合は、組織の体制及び状況の理解にかかっている。体制は、組織の意図、目標及び複雑さによって異なる。リスクは、組織の体制のあらゆる部分でマネジメントされる。組織の全員が、リスクのマネジメントを行うことに対する責任を負っている。

組織統治は、組織の意図を達成するために、組織の方向性、組織の外部関係及び内部関係、並びに規則、プロセス及び方策を導く。経営体制は、組織統治の方向性を、望ましいレベルの持続可能なパフォーマンス及び長期的な継続性を達成するために必要な

戦略及び関連する目的へと転換する。組織内部におけるアカウントビリティ及び監視の役割の決定は、組織の統治の不可欠な部分である。

リスクマネジメントと組織との統合は、動的かつ反復的なプロセスである。この統合は、組織の必要性及び文化に合わせることを望ましい。リスクマネジメントは、組織の意図、組織統治、リーダーシップ及びコミットメント、戦略、目的並びに業務活動の一部となり、これらと分離していないことが望ましい。

5.4 設計

5.4.1 組織及び組織の状況の理解

リスクのマネジメントを行うための枠組みを設計するに当たって、組織は、外部及び内部の状況を検証し、理解することが望ましい。

組織の外部状況の検証には、次の事項が含まれる場合がある。ただし、これらに限らない。

- 国際、国内、地方又は近隣地域を問わず、社会、文化、政治、法律、規制、金融、技術、経済及び環境に関する要因
- 組織の目的に影響を与える、鍵となる原動力及び傾向
- 外部ステークホルダとの関係、並びに外部ステークホルダの認知、価値観、必要性及び期待
- 契約上の関係及びコミットメント

- ネットワークの複雑さ，及び依存関係

組織の内部状況の検証には，次の事項が含まれる場合がある。ただし，これらに限らない。

- ビジョン，使命及び価値観

- 組織統治，組織体制，役割及びアカウンタビリティ

- 戦略，目的及び方針

- 組織の文化

- 組織が採用する規格，指針及びモデル

- 資源及び知識として理解される能力（例えば，資本，時間，人員，知的財産，プロセス，システム，技術）

- データ，情報システム及び情報の流れ

- 内部ステークホルダの認知及び価値観を考慮に入れた，内部ステークホルダとの関係

- 契約上の関係及びコミットメント

- 相互依存及び相互関連

5.4.2 リスクマネジメントに関するコミットメントの明示

トップマネジメント及び監督機関（該当する場合）は，リスクマネジメントに対する継続的なコミットメントを行動で示し，明示することが望ましい。これは，組織の目的及びリスクマネ

ジメントへのコミットメントを明確に伝える方針，声明又はその他の形式で行うことができる。

コミットメントには，次の事項を含めることが望ましい。ただし，これらに限らない。

– 組織がリスクのマネジメントを行う意義，並びに組織の目的及びその他の方針とのつながり、

– リスクマネジメントを組織全体の文化に統合する必要性を強めること

– リスクマネジメントと中核的事業活動及び意思決定との統合を主導すること

– 権限，責任及びアカウントビリティ

– 必要な資源を利用可能にすること

– 相反する目的への対処の仕方

– 組織のパフォーマンス指標の中での測定及び報告

– レビュー及び改善

リスクマネジメントに関するコミットメントを，必要に応じて，組織内及びステークホルダに伝達することが望ましい。

5.4.3 組織の役割，権限，責任及びアカウントビリティの割当て

トップマネジメント及び監督機関（該当する場合）は，リスクマネジメントに関して，関連する役割のアカウントビリティ，責任及び権限が組織のあらゆる階層で割り当てられ，伝達されることを確実にし，次の事項を行うことが望ましい。

– リスクマネジメントは，中核的な責務であることを強調する。

– リスクのマネジメントを行うためのアカウントビリティ及び権限をもつ個人（リスク所有者）を特定する。

5.4.4 資源の配分

トップマネジメント及び監督機関（該当する場合）は、リスクマネジメントのための適切な資源の割当てを確実にすることが望ましい。資源には、次の事項が含まれる場合がある。ただし、これらに限らない。

- 人員，技能，経験及び力量
- リスクのマネジメントを行うために使用する，組織のプロセス，方法及び手段
- 文書化されたプロセス及び手順
- 情報及び知識のマネジメントシステム
- 専門的な人材開発及び教育訓練の必要性

組織は、既存の資源の能力及び制約要因を考慮することが望ましい。

5.4.5 コミュニケーション及び協議の確立

組織は、枠組みを支え、リスクマネジメントの効果的な適用を促進するために、コミュニケーション及び協議に対する、認められた取組み方を確立することが望ましい。コミュニケーションは、対象者とする相手との情報共有を含む。また、協議は、意思決定又はその他の活動に寄与し、これらを形成することを期待してフィードバックを提供する参加者をも含む。関

連する場合、コミュニケーション及び協議の方法及び内容は、ステークホルダの期待を反映することが望ましい。

コミュニケーション及び協議は、適時に行うことが望ましい。また、関連する情報が適切に収集され、照合され、統合され、共有されること、及びフィードバックが提供され、改善がなされることを確実にすることが望ましい。

5.5 実施

組織は、次の事項を行うことによって、リスクマネジメントの枠組みを実施することが望ましい。

- 時間及び資源を含めた適切な計画を策定する。
- 様々な種類の決定が、組織全体のどこで、いつ、どのように、また、誰によって下されるのかを特定する。
- 必要に応じて、適用される意思決定プロセスを修正する。
- リスクのマネジメントを行うことに関する組織の取決めが明確に理解され、実施されることを確実にする。

枠組みの実施を成功させるためには、ステークホルダが参画し、自ら認識することが必要である。これによって、組織は、新たな不確かさ又は後続の不確かさが発生する都度、それらを考慮に入れることを可能にし、また、意思決定において不確かさに明確な形で取り組むことができる。

適切に設計され、実施されたリスクマネジメントの枠組みは、リスクマネジメントプロセスが、意思決定を含め、組織全体の全ての活動の一部になること、並びに外部及び内部の状況の変化が適切に取り入れられることを確実にする。

5.6 評価

リスクマネジメントの枠組みの有効性を評価するために、組織は、次の事項を行うことが望ましい。

– 意義、実施計画、指標及び期待される行動に照らして、リスクマネジメントの枠組みのパフォーマンスを定期的に測定する。

– リスクマネジメントの枠組みが組織の目的達成を支援するために適した状態か否かを明確にする。

5.7 改善

5.7.1 適応

組織は、外部及び内部の変化に対応できるように、リスクマネジメントの枠組みを継続的にモニタリングし、適応させることが望ましい。それによって、組織は自らの価値を高めることができる。

5.7.2 継続的改善

組織は、リスクマネジメントの枠組みの適切性、妥当性及び有効性、並びにリスクマネジメントプロセスを統合する方法を継続的に改善することが望ましい。

関連するかい離又は改善の機会が特定された時点で、組織は計画及び実施事項を策定し、実施に関してアカウントビリティをもつ人にそれらを割り当てることが望ましい。これらの改善は、実施された時点でリスクマネジメントの向上に寄与するはずである。

以上リーダーシップ及びコミットメントへのガイドライン。