2018 年 10 月 18 日開催　第 78 回 JIPDEC セミナー　講演レポート

ISO31000－2018 年版：リスクマネジメント－指針の経営への活用

東京海上日動リスクコンサルティング株式会社　主幹研究員
ISO31000国内WG委員　指田朝久　氏

2018 年 2 月に 9 年ぶりに改訂された「ISO31000:2018　リスクマネジメント－指針」の概要について、大きな変更点を中心に私見を述べる。なお、今回紹介する規格の項目や内容は正式の翻訳ではない。また、著作権の関係上、規格項目の詳細および関連図は掲載していないが、来春頃日本規格協会より JISQ31000 および解説が発行される予定なので参照していただきたい。

Ⅰ．ISO31000 とは

1．リスクマネジメントの国際標準

リスクマネジメントに関する国際標準規格は、2009 年に第 1 版が発行され 2018 年 2 月に 9 年ぶりに改定された「ISO31000」（以下、「本規格」という。）、「ISOGUIDE73;リスクマネジメント－用語」、「ISO/IEC31010;リスクアセスメント技術」の 3 つの規格が発行されている。

2．2009 年版との相違点

本規格は 2009 年版（以下、「旧規格」という。）と比べ、内容的にはさほどの変更は見られないが、経営を意識したリスクマネジメントを強調しており、経営そのものと統合が図られている。

本規格の主な変更点は以下のとおり。

①全体的に簡潔な記述となった。旧規格では「フレームワーク」と「プロセス」の項目に重複があったため、その整理がされるとともに、フレームワークについてはマネジメントシステムと整合性が図られた。

②企業全体のリスクマネジメント（ERM: Enterprise Risk Management）に適合させるため、活動主体に該当する場合の「監督機関の要求事項」が追加された。

③概要の簡潔化を目指したため、株主等ステークホルダーをも想定される外部／内部への「報告」が削除された。上場企業などの場合、コーポレートガバナンスコード等のさまざまな規制に委ねている。

④「第 4 章　原則」は「第 5 章　枠組み」、「第 6 章　プロセス」それぞれと関係性を持たせて「原則」を重視させるとともに、第 5 章、第 6 章間で相互の関係性を持たせた。

⑤用語の数は今後改定が予定されている「ISOGUIDE73」に収録させるため、収録数が大幅に減少した。なお本規格と現行の GUIDE73 では用語定義にずれがあるため、GUIDE 改定までは注意が必要である。

3．リスクの定義

本規格では、リスクを「目的に対する不確かさの影響」と定義し、3 つの注記が記されている。

注記 1）影響とは、期待されていることから乖離することを指し、好ましいもの（プラス）／好ましくないもの（マイナス）の両面が存在すること、機会または脅威を示したり、創り出したり、

もたらしたりすることがあり得る、と考える。

注記２）リスクの目的は、さまざまな側面を持ち、さまざまなレベルで適用されることがある。

注記 3）一般に、リスク源、起こりうる事象、およびそれらの結果ならびに起こりやすさ、として表される。

日本企業が ERM を行う場合は会社法を適用しなければならない。会社法で定義される「リスク」は内部統制の考え方である「組織目標の達成を阻害する要因」、いわゆるマイナスのリスクが対象なのに対し、本規格はプラスとマイナス両面のリスクを対象としており、一番広い範囲をカバーする定義となる。なお、実務においてはマイナスのリスクに対するリスクマネジメントを行うこととするのがわかりやすい。

4. ISO31000 のカバー範囲

日本の JIS Q 2001 はリスクマネジメントを時系列に捉えており、事前策（予防、防止策）から事故発生直後（クライシスポイント）、復旧までの一連の行動をカバー範囲としているのに対し、本規格は日常の（事前）のリスク対応までを対象としている。ただし、クライシスポイントの直後対応のための事前準備（災害対策や BCP 等）は本規格の範囲に含まれている。

国際規格では事前／事後で規格が分かれており、事後対応については「ISO22320;社会セキュリティ－危機事態管理－危機対応に関する要求事項」や「ISO22301;事業継続マネジメント（BCP）」が参考になる。

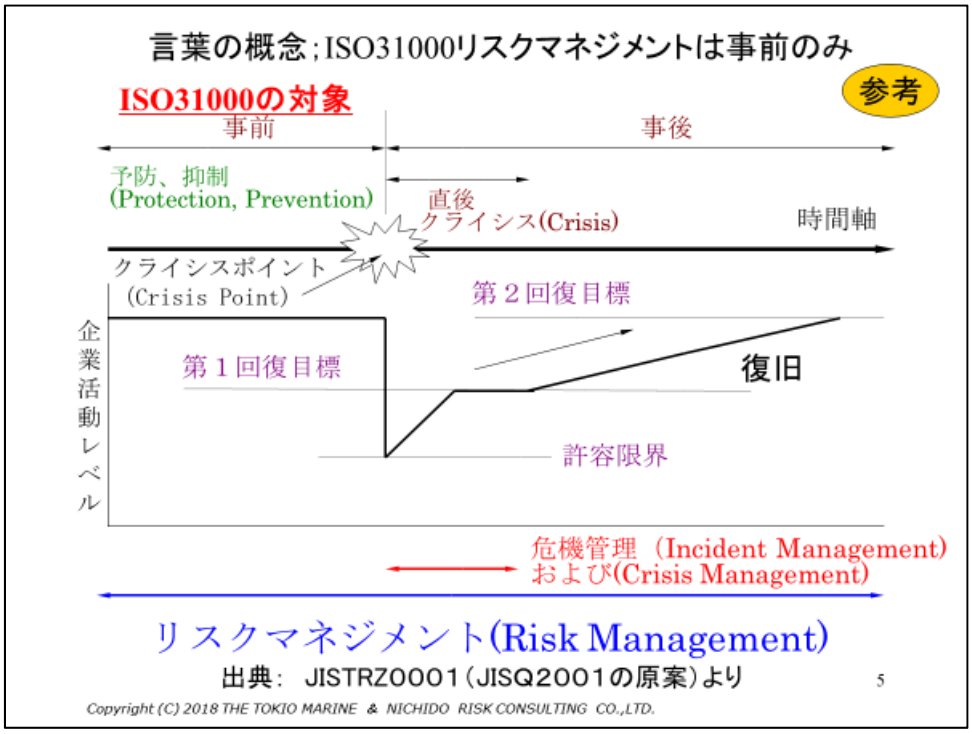


図 1.ISO31000:2018 のカバー範囲

Ⅱ． 規格の概要と主な変更点

ここでは、大きな変更点と、重要なポイントのみを紹介する。

1.「第４章　原則」の構成

リスクマネジメントの意義として「価値の創出および保護」を大原則として明確に打ち出した。リスクマネジメントはパフォーマンスを改善し、イノベーションを促進し、目的達成を支援するものである。

大原則の下、以下の８原則を設け、すべての階層で遵守させることで、会社経営そのものを支援するものと定義付けた。

①統合（本規格で新設された）
②体系化および包括
③組織への適合
④包含
⑤動的に繰り返し行う
⑥利用可能な最善の情報を使う
⑦人的および文化的要因を考慮する
⑧継続的改善の促進

2．リスクマネジメントプロセスの整理

リスクマネジメントの基本的な考え方を整理し、リスクの発見、リスク分析、リスク評価、リスク対応などの基本的なプロセスが標準化された。また、プロセスを円滑に実施するためのフレームワークも整理された。ただし、フレームワーク自体、品質管理、環境マネジメント、ISMS など他のマネジメントシステムとの差異が生じてしまい、わかりづらくなっているが、本規格でもその点は解消されていない。

3.「第５章　枠組み」　の構成と主な変更点

経営者の役割である「リーダーシップおよびコミットメント」を中央に置き、その周りを①統合→②設計→③実施→④評価→⑤改善→①統合...　という PDCA サイクルで回す形となった。

（1）5.2　リーダーシップおよびコミットメント

ここでは「統合」がキーワードとなる。本規格において、経営そのものを意識したリスクマネジメントとの統合が図られている。本章で最も重要な変更点は「5.2　リーダーシップおよびコミットメント」の新設であり、経営者の実施事項として、非常に重要な８項目が示されている。

・リスクマネジメント方針、計画、取り組み方を公開する。
・必要な資源がリスクマネジメントに配分されることを確実にする。
・アカウンタビリティ（説明責任）および責任を組織内の適切な階層に割り当てる（マネジメントシステムの基本的な考え方）。
・リスクマネジメントを組織の目的、戦略、文化と整合させる（企業経営と合わせる）。
・とることのできるリスク、できないリスクの種類と大きさを確定する（戦略系のリスクを意識した大きな改定点である）
　（(例）新規事業に投資をした際にどれだけ自社に体力があり、設備投資を含め、戦略が立てられるか、を見極めることが必要である。）。
・トップマネジメントはリスクマネジメントを行うことに責任を持つ。

・監督機関はリスクマネジメントを監視する責任がある。
・リスクおよび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。

（2）アカウンタビリティとレスポンシビリティ

トップマネジメントと監督機関は、関連する役割のアカウンタビリティ、責任、権限を各階層に割り当てて伝達することとなるが、アカウンタビリティとレスポンシビリティの区別が明確になっているのが本規格の特徴である。

アカウンタビリティは、組織の長（例：班長、課長、部長、担当役員等）にだけ付き、自分の権限において裁量権で行った行為に対して、各々のステークホルダー（上長）に対する説明と説明責任を持つ。この行為の善し悪しの判断はステークホルダーが行い、ステークホルダーが判断するための最低限の情報提供がアカウンタビリティを果たすことを意味する。たとえば社長の場合であれば、外部のステークホルダーに対し、説明責任を果たすこととなる。

一方、レスポンスビリティは、組織の全員が与えられた役割に責任を持つこととなる。

なお、旧規格では、リスクオーナーを定めることとし、すべての組織、人に対する責任や権限が割り振られていたが、本規格では廃止された。

4.「第 6 章　プロセス」の構成と主な変更点

旧規格でプロセス図に記載されていなかった「記録作成および報告」が追加された。プロセスの構成としては、「コミュニケーションおよび協議」「適用範囲、状況基準」「リスクアセスメント（①リスク特定→②リスク分析→③リスク評価）」「リスク対応」「モニタリングおよびレビュー」「記録作成および報告」のすべてを包括して PDCA を回すようになった。

「6.1　一般」での大きな変更点は、「戦略、事業活動、プログラム、プロジェクトに適用できる」「目的達成に併せて外部内部の状況に適応するために多数適用されている」ことが明示されたことである。

本規格で組織の中には PDCA が 1 つだけでなく、多数のサイクルが回っていることが明文化されたことは、非常に大きなポイントとなる。ERM に限らず、プログラム、プロジェクトなど、一過性のものにも本規格は適用できる。

（1）6.3.2　適用範囲の決定

「戦略、業務活動、プログラム、プロジェクトその他の活動で適用されるため、組織の目的との整合を明確にすること」、言い換えれば組織目的との紐付けが重要であることが明示された。企業全体の ERM の場合、全社の目的を達成するために支店や部門単位でそれぞれ定められた目的に対しリスクマネジメントを行い、さらにそこから情報セキュリティや製品安全、災害対策など、企業が行うべきサイクルを回すにあたり、細分化された一番最下層のところであっても、企業戦略などの組織目的、事業目的に紐付いていることが重要である。

（2）6.3.4　リスク基準の決定

「とってよいリスク、とってはならないリスク、大きさと種類を規定する」が追加された。「とってよいリスク」の例としては、新規事業の開発、新規ビジネスの開始にあたり、投資の規模を最初に決めておくことを示している。

（3）6.4　リスクアセスメント

リスクアセスメントは、①リスク特定②リスク分析③リスク評価を網羅するプロセスである。

旧規格では「ISO 31010」（リスクマネジメント実施のための 31 の技法を解説）を活用するよう示されていたが、本規格では削除された。

①6.4.2　リスクの特定

すでに説明しているように、リスク=悪いものではない。本規格では目的達成を助けるものも阻害するものも「リスク」と定義されているが、会社法では目的達成を阻害するものを「リスク」と定義付けているため、自社が直面しているリスクに見合った選択をすればよい。包括的なリスク一覧表を作成する必要があるが、本規格ではリスク発見のための考慮事項が記されている。

新たに「要素および要素間の関係を考慮」が追加され、有形無形のリスク源、原因および事象などの例が示された。

②6.4.3　リスク分析

リスク分析にあたっては、そのリスクの性質や特徴を理解し、一番対策に適切な手法を用いるべきである。なお、複数の専門家の意見に相違がある場合は、後々のためにそれぞれの意見を文書化して残しておくことが必要である。

③6.4.4　リスク評価

旧規格では、リスク評価はリスク基準とリスク分析で発見されたリスクレベル（頻度や影響）を比較し、その結果で対応の優先順位を付けることとしていたが、本基準で優先順位を付けることが削除され、「決定を裏付けること」と変更された。

（4）6.5　リスク対応

リスク対応の意義は「リスクに対処するために選択肢を選定し、実践すること」で、ここには反復的プロセスが含まれる。反復プロセスとは、リスク対応の選択肢を策定、選定、計画を立てて実施し、対応の有効性を評価することで、対策後の残存リスクへの対応後、さらに残ってしまった場合は再度対策を実施することとなる。このサイクルは「ISO27005;情報セキュリティマネジメント」のプロセス図に掲載されているが、本規格ではほとんど詳細説明はない。

（5）6.5.2　リスク対応の選択肢の選定

ここでは具体的な作業の内容が書かれているが、まず、目的達成のためとはいえ、コスト対効果を考えて実践する必要がある。そして、リスク対応には①リスク回避②リスクを取る・増加させる③リスク源の除去④起こり易さを変える⑤結果を変える⑥リスクの共有⑦リスクの保有、の選択肢が挙げられている。

JIS　Q 2001 には 4 つの対応項目があり、その中にリスクを損害保険会社に移転する「リスク移転」があるが、本規格ではこれが「リスクの共有」に変更された。このリスクの共有の仕組みは、会社と株主がメリット／デメリットを共有する株式会社制度の仕組みを該当させている。最も重要なのは、「リスクを取る・増加させる」ことが投資に該当し、新規ビジネス等への投資の影響でよりリスクが大きくなるため、リスクマネジメントの選択肢の 1 つに入れている。

（6）6.5.3　リスク対応計画の準備および実践

リスク対応の実施決定後、リスク対応計画の準備を行い、進捗をモニタリングできるように規定することとなる。この中で「不測の事態への対応を含む資源に関する要求事項」が挙げられているが、本規格のカバー範囲として、緊急時対応マニュアル、災害対策マニュアル、リコールマニュアルも含まれているが、具体的な行動までは含まれていない。内部統制において常に指摘される残留リスクの認識は削除された。

5. リスクマネジメント構築に向けての留意点

本規格構築上の留意点について以下に私見を述べる。

（1）ISO31000 の留意点

・規格自体は、ERM を意識して「監督機関」が設けられたが、一方で、コーポレートガバナンス関連の「報告」が限定的となっている。実際にはコーポレートガバナンスは各国が出しているガイドライン等が優先される。

・ERM を意識し、原則で価値の創出と保護が上位に位置付けられたことにより、ERM での利用が明確となった。

・戦略リスクを意識し、とってもよいリスク、とってはいけないリスクの大きさと種類を定めることが明示された。

・COSO－ERM が 2017 年に改定され、経営のパフォーマンスとリスクマネジメントの概念が明確化された。それに歩調を合わせ、フレームワークの評価がパフォーマンスに統一された。これにより、マネジメントシステムの方向性、COSO、ISO31000 の考え方の足並みが揃った。

・戦略、事業活動、プロジェクト等に活用できるようになり、企業内部の目標達成にあわせて多くのプロセスが適用されることが明確になり、より企業の実態に近づいた。

・その一方で、残留リスクやリスク評価におけるリスク対応の優先順位付けを行うことなど、リスクマネジメント実施上有効と思われる点が一部削除されてしまったため、個別に補う必要がでてきている。

・法令遵守、教育など、当たり前に行うことは省略された。

・個別リスクについてはそれぞれ該当する規格を適用する。

6.理想的なリスクマネジメントの進め方

企業の実状に即したリスクマネジメントを以下に紹介する（図 2 参照)。

経営者の役割は決まっており、リスクマネジメントの方針の提示、稟議書の承認、監査内容を承諾し、指摘に対する見直しを行うこととなる。

ERM の実務としてはフェーズが 3 つに分かれる。まず、企業全体のリスクマネジメントであるフェーズⅠで 1 年に 1 回、リスクの洗い出しから評価・選別までを行い、対応すべきリスクの優先順位を付けて、対応するリスクをフェーズⅡに落とし込む。フェーズⅡでは個別のリスクごとに PDCA を回し、リスク対応を行う。ここまでが日常行動となるが、万が一事件・事後が発生した場合は、フェーズⅢのとおり、緊急対応、復旧活動を行い、その結果をフェーズⅡにフィードバックし、反省して事後に活かすこととなる。有事の際に対応できるよう、フェーズⅢをシミュレーション訓練で補うことも必要である。

なお本規格のプロセスは汎用性が高く、全体像、または各フェーズそれぞれでの活用が可能である。

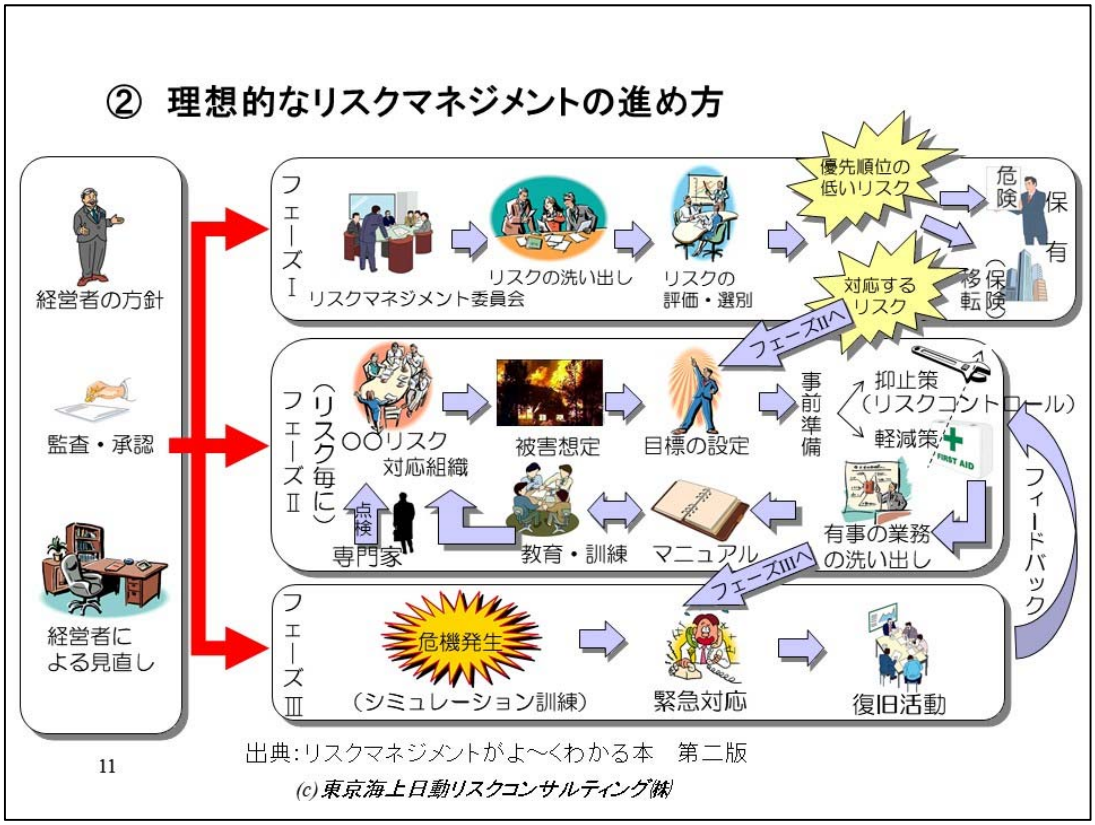


図 2. 理想的なリスクマネジメントの進め方

7．ERM で想定されるリスクの種類

ERM で想定されるリスクは、①戦略リスク（テイクするリスク）②財務リスク③ハザードリスク④オペレーショナルリスクの４つに分類される。本規格は戦略リスクにも対応することを念頭に置いて改訂されている。M&A、価格戦略など、経営者が決定しなければならない事項であり、発生直後からリスクが発生するため、経営者が逃れられないリスクとなる。

上場企業の場合、リスクの開示が義務付けられているが、対象とする一般的な主なリスク例としては、①戦略リスク②製品品質（欠品、リコール、苦情）③製品提供（災害、機械故障など）④コンプライアンス（データ偽造、談合）⑤従業員の安全（労働安全、ワークライフバランス）などが挙げられているが、ほとんどの企業では対応が行われている。とはいえときどき事件事故が発生する。アメリカのある調査結果では上場企業の株式価格下落要因の約 60%を戦略リスクが占めており、戦略リスクを含むリスクマネジメントが必要であることが言えよう。

8.マネジメントシステムへの活用上の留意点

ISO31000 は品質管理、環境、情報セキュリティマネジメント、BCP などのマネジメントシステムで２か所がリンクされている。

・「A６.計画」　リスクおよび機会を決定する

・「B８.運用」　リスクアセスメントは ISO31000 に準拠してできる　→　本規格の「プロセス」の適用が可能である。

ここで問題となるのが「リスクおよび機会」である。ISO31000 のリスクの定義は前述のとおり「目的に対する不確かさの影響」であり、プラス、マイナスのリスクの結末がないのに対し、内部統制では目的を阻害するものを「リスク」、プラス効果があるものは「機会」と定義付けている。マネジメントシステムの標準化（HLS）は、内部統制の考え方を取り入れてリスク＝マイナス、機会=プラスを対に捉えている。つまり、ISO31000 とリンクしながらも、リスクの定義が統一化されていないのだが、この点は割り切らざるを得ない状況である。

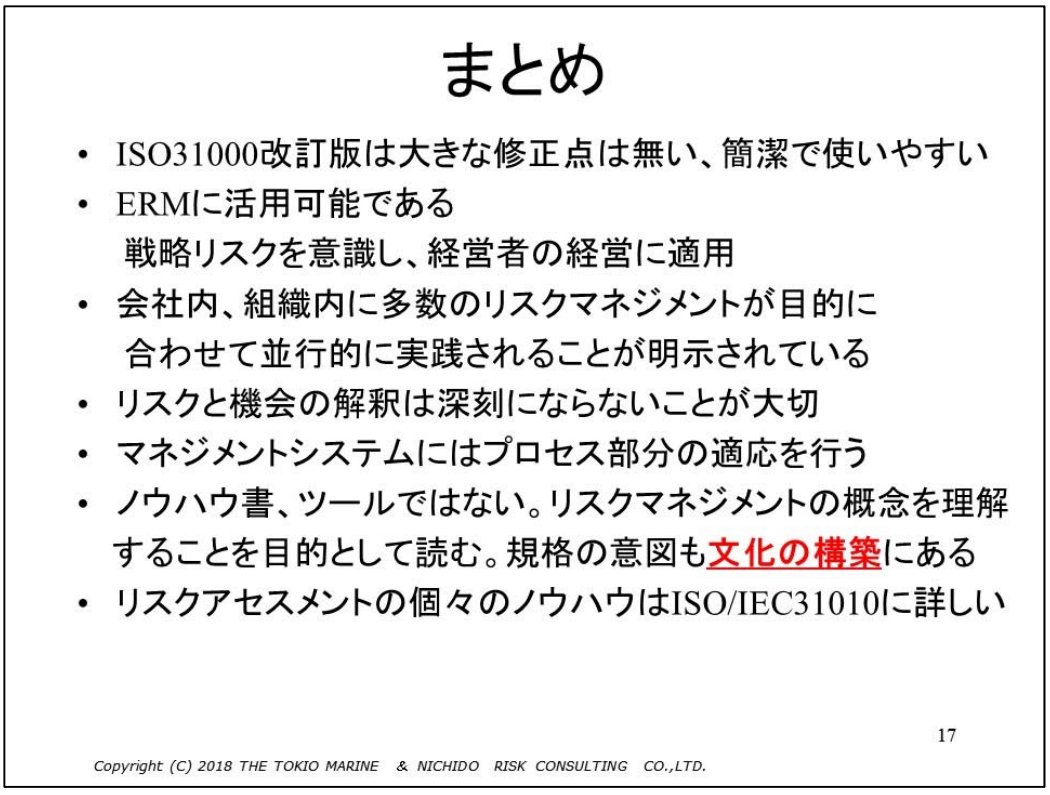
このほか、COSO－ERM:2004「全社的リスクマネジメント－統合的フレームワーク」では「リスク（マイナス）と機会（プラス）」の考え方が用いられ、会社法に内部統制にも採用されていたが、2017 年に COSO－ERM：全社的リスクマネジメント－戦略およびパフォーマンスとの統合」が新たに作成され、ここでは ISO31000 の定義に倣い、

・リスク：パフォーマンスの結果としてプラスとマイナスが生じる

・機会：現在の戦略を大きく変更するきっかけ

と示された。

現在、「リスクと機会」については内部統制、マネジメントシステム、ISO31000、COSO-ERM2004、2017 などそれぞれの規格により定義が異なっていることを理解し、自身が行うリスクマネジメントにおいてどの定義を適用するか判断の上利用してもらいたい。



以上