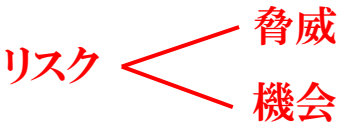
公認内部監査人(CIA)
Part Ⅰ／第6回

※アビタスCIA本講座講義資料のため、MUFG CIA受験対策講座の実施回と異なります。

5-1　内部監査におけるリスクの定義とリスクの分類



リスクとは

一般的にリスクという言葉は、企業にとって損失を与える要因としてとらえられることが多い。しかし、リスクは事業発展の機会にもなり得るビジネスの本質に関わるものであり、事業目標達成のために、企業は一定レベルのリスクを取る必要がある。

適切なリスクを取らない企業は、将来、適切なリスクを取って成長を実現した競合企業との競争に負けてしまうこともある。従って、ある種のリスクは回避すべきだが、事業を行っていくためのコストとして受け入れる必要のあるリスクがある。そしてこの受け入れたリスクのうちのある部分は内部統制システムによって軽減することができる。

リスクの定義

グローバル内部監査基準によれば、リスクは以下のように定義される。

定義 目標に対する不確実性がもたらす正又は負の影響

リスクの分類

リスクには様々な種類があり、それぞれが組織に異なる影響を与える。一義的な定義は存在しないが、代表的なリスクの種類について具体例を挙げて説明する。

戦略的リスク (Strategic risk)	経営体による基本的な意思決定が抱えるリスク。戦略項目、インフラが抱えるリスクは戦略的リスクである。
業務的リスク (Operational risk)	日常業務上のリスク。業務が抱えるリスク及び組織、体制、資産が抱えるリスクの多くは、業務リスクである。
財務的リスク (Financial risk)	企業の資金調達や運用に関するリスク。財務的リスクには、市場リスク（金利リスク、購買力リスク、為替リスク）と固有リスク（事業リスク、信用リスク、流動性リスク）がある。
コンプライアンスリスク (Compliance risk)	法律や規制、内部方針の遵守に関連するリスク。違反による罰金や制裁が発生するリスク。
評判リスク (Reputational risk)	法令違反、CSR情報開示における誤差脱漏、活動目標の未達、社会的な問題に対する無関心等の理由により、企業のブランド力や評判が損なわれてしまうリスク。

役員が全員親族、クレーム等

IR: 経営環境に関連するリスク、勘定そのものに内在するリスク
Gross Riskとも言われる。

環境リスク （Environmental risk）	環境や人間の健康、安全に影響を与える潜在的な危険を抱えるリスク。
持続可能性のリスク （Sustainability risk）	環境、社会、ガバナンス（Environmental, Social or Governance; ESG）に関わる事象又は状況であり、発生した場合、組織体に実際又は潜在的に重大な悪影響を及ぼすリスク。
社会的責任のリスク （Social Responsibility risk）	企業の事業活動が、人々、環境、社会に対して、直接的にも間接的にも損害を与えるリスク。社会的責任のリスクとして、評判、コンプライアンス、責任、オペレーション、株式市場、労働市場、販売市場、外部取引関係にかかわるものがある。
モデルリスク （Model Risk）	経営者の意思決定などにおいて、不適切な又は誤ったモデルを用いることにより、組織体へ損害を与えるリスク。
固有リスク （Inherent Risk）	経営管理措置がない場合に存在する内部及び外部のリスク要因が組み合わさったもの。
残余リスク （Residual Risk）	固有リスクのうち、経営管理措置を実施した後に残る部分。

RR: 正味リスク(Net Risk)とも言われる

リスクとコントロールの関係

経営者が、不利な事象の影響の大きさと発生可能性を軽減する措置(リスクに対応するコントロール活動を含む)を講じた後にさらに残るリスクを残余リスクと呼ぶ。

経営者は、適切なコントロールを導入することで残余リスクを許容リスクの範囲内に収めるよう管理する必要がある。

5-2　リスク・マネジメントの定義と基本概念

リスク・マネジメント

リスクを識別し、評価し、管理し、コントロールするリスク・マネジメントは経営者の重要な責任であり、内部監査の評価対象となるプロセスである。

論点　リスク・マネジメントの定義

グローバル内部監査基準によれば、リスク・マネジメントは以下のように定義される。

リスク管理

定義　組織体の目標達成に関し、合理的なアシュアランスを提供するために、発生する可能性のある事象や状況を、識別し、評価し、管理し、コントロールするプロセス。

リスク・マネジメントを、「リスクは悪である」という前提の下に、これを低減又は排除するためのプロセスである、と考えるのは適切ではない。

リスク・マネジメントは組織体が価値を創造するために、リスク選好(risk appetite)に沿って、「自社が抱えるべきリスクの種類と水準を主体的に選択するための方法に関わるプロセス」といえる。

組織体が、リスク・マネジメント・プロセスを構築するうえでグローバルに認められているフレームワークを活用することができる。

リスク・マネジメント・プロセスの用語

リスク選好 (risk appetite)	組織体が戦略や目標を追い求めて積極的に受容する、リスクの種類と量。
リスク評価 (risk assessment)	組織体の目標達成に関連するリスクを識別、分析すること。リスクの重大性は、通常、影響度と発生可能性に基づいて評価される。 $ %
リスク許容度 (risk tolerance)	目標の達成に当たり、パフォーマンスの変動が許容される範囲。パフォーマンス（成果物）の許容可能な差異
リスク対応 (risk response)	リスクを管理し、リスクに対して適切な行動を取るためのプロセス。
リスク・マネジメント・サイクルの諸要素 (elements of the risk management cycle)	リスク・マネジメント・サイクルにおける手続の諸要素。リスクの識別、分析、評価、優先順位付け、対応などが相当する。

5-3　リスク・マネジメント・プロセスに係る内部監査部門長の役割

リスク・マネジメント・プロセスに係るCAEの役割

基準9.1の後段部分では、CAEの役割として、リスク・マネジメント及びコントロールの各プロセスを理解しなければならない、としている。

基準

基準 9.1 ガバナンス、リスク・マネジメント及びコントロールの各プロセスの理解　要求事項の一部抜粋

リスク・マネジメント及びコントロールの各プロセスを理解するために、内部監査部門長は、組織がどのように重大なリスクを識別、評価し、適切なコントロール・プロセスを選択しているかを検討しなければならない。これには、組織体が次の重要なリスク分野をどのように識別、管理しているかを理解することが含まれる。

- 財務情報及び事業運営情報の信頼性及び完全性
- 事業運営及びプログラムの有効性及び効率性
- 資産の保全
- 法令や規制の遵守

リスク・マネジメント・プロセスの理解

CAEは、リスク・マネジメント・プロセスを理解するために、以下の活動を行う。

a) グローバルに受け入れられているリスク・マネジメントの原則、フレームワーク及びモデル、並びに組織体が活動する業界及びセクターに特有の専門職のガイダンスを理解すべきである。

b) 組織体のリスク・マネジメント・プロセスの成熟度を評価するために、組織体がリスク選好度を識別し、リスク・マネジメントの戦略やフレームワークを実施しているかどうかを確認することを含め、情報を収集すべきである。

c) 取締役会及び最高経営者との議論は、組織体のリスク・マネジメントに関する最高経営者及び取締役会の考え方や優先順位を理解するのに役立つ。

d) リスク情報を収集するために、最近完了したリスク評価、並びに最高経営者及び業務運営部門の経営管理者、リスク・マネジメントの担当者、外部監査人、規制当局、並びにその他の内部及び外部のアシュアランス業務のプロバイダが発した関連するコミュニケーションについてレビューすべきである。

5-4　リスク・マネジメント・プロセスに係るその他の関係者の役割

リスク・マネジメント・プロセスに係るその他の関係者の役割

原則8「取締役会による監督」において、リスク・マネジメント・プロセスを含む内部監査部門の全体的な有効性を可能にするには、取締役会によるモニタリングが不可欠である、としている。また基準8.1「取締役会による対話」では、あわせて最高経営者の役割についても言及されている。

本Unitにおいて、取締役会、最高経営者、CAEの役割を、協力的かつ双方向のコミュニケーションとして取り上げ、学習する。

a) リスク・マネジメント・プロセスに係る取締役会、最高経営者、内部監査部門の役割の概要は以下の通りである。

取締役会	適切なリスク・マネジメント・プロセスが整備され、それらのプロセスが妥当かつ有効であるかどうかを判断する監督者の役割を担う。この役割の中で、内部監査部門の監督と支援を行う。
最高経営者	適切なリスク・マネジメント・プロセスが整備され、かつ運用されていることを確実にする。
内部監査部門	経営管理者のリスク・マネジメント・プロセスの妥当性と有効性に関する検証・評価・報告・改善のための提言を行うことにより、最高経営者と取締役会を支援する。

RMの監視

RMの最終責任

RMプロセスの評価

b) リスク・マネジメント・プロセスを含む内部監査部門の全体的な有効性に係る取締役会、最高経営者の役割と、CAEによる取締役会及び最高経営者への報告事項は、以下の通りである。

内部監査機能の支援と監視

取締役会	CAEとコミュニケーションを図り、内部監査部門がその負託事項をどのように果たしているかを理解する。
	CAEが内部監査の優先順位を決定するのを支援するために組織体の戦略、目標及びリスクに関する取締役会の見解を伝える。
	CAEとの間で、以下の期待事項を設定する。 • CAEからコミュニケーションを受け取りたい頻度 • 取締役会の許容度を超える重大なリスクなど、どの問題を取締役会へ上申すべきかを決定する規準 • 重要事項を取締役会へ上申するためのプロセス
	内部監査の実施結果及び最高経営者との議論に基づいて、組織体のガバナンス、リスク・マネジメント及びコントロールの各プロセスの有効性を理解する。
	経営管理者又はその他のステークホルダーとの意見の相違についてCAEと協議し、CAEが内部監査の負託事項に記載された責任を果たすことができるよう、必要に応じて支援する。

最高経営者	組織体の戦略、目標及びリスクに関する最高経営者の見解を伝え、CAEが内部監査の優先順位を決定するのを支援する。
	取締役会がガバナンス、リスク・マネジメント及びコントロールの各プロセスの有効性を理解するのを支援する。
	重要事項を取締役会へ上申するためのプロセスについて、取締役会及びCAEと協力する。
CAE(報告事項)	内部監査の計画及び予算、並びに重大な修正。
	負託事項又は内部監査基本規程に影響を及ぼす可能性のある変更。
	独立性を侵害する可能性のある事項。
	結論、課題、アシュアランス、助言、インサイト、及びモニタリング結果を含む内部監査業務の結果。
	品質のアシュアランスと改善のプログラムの結果。

取締役会とCAEの支援

QA&IPの結果

5-6 COSO-ERM (1)

COSO全社的リスク・マネジメント(COSO-ERM)

米国のトレッドウェイ委員会支援組織委員会(COSO)は、大手監査法人と契約し、リスク管理についてのより深い理解と定義の研究に着手した。その結果、2004年に「全社的リスク・マネジメント―統合的フレームワーク」を発表した。(本テキストでは、以下で紹介する改訂版と区別するため「旧COSO-ERM」と呼ぶ。)

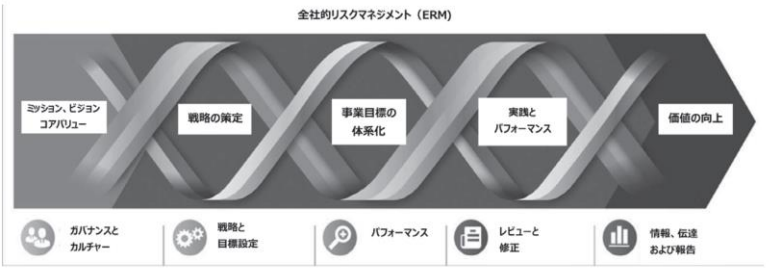
それから10年以上が経過し、情報技術の発展やグローバル化の進展により、企業を取り巻くリスクは多様化、複雑化し、新しいリスクが生じた。こうした経営環境の変化による経営者のリスクに対する関心の高まりに応じてCOSOは2017年に改訂版となる「全社的リスク・マネジメント―戦略及びパフォーマンスとの統合」(以下、COSO-ERM)を発表した。

論点 ERMの定義

COSO-ERMではERMを以下のように定義する。

RM自体を、企業の戦略や行動と整合させるべき

定義 組織が価値を創造し、維持し、及び実現する過程において、リスクを管理するために依拠する、戦略策定ならびにパフォーマンスと統合されたカルチャー、能力、実務。



出典：COSO『*Enterprise Risk Management – Integrating with Strategy and Performance*』を基にアビタスが翻訳

上図において、「戦略と目標設定」、「パフォーマンス」、「レビューと修正」をそれぞれ表す3つの細い帯が合わさったリボンが、事業体における共通のプロセスを表している。また、「ガバナンスとカルチャー」、「情報、伝達及び報告」をそれぞれ表す2つの細い帯が合わさったリボンが、ERMの支援的な側面を表している。

COSO-ERMの前提は、すべての事業体は、利害関係者に対して、何らかの価値を提供するために存在するということである。すべての事業体は価値を追求する上でリスクに直面する。

論点 COSO-ERMにおけるリスクの定義

定義 戦略と事業目標を達成しようとする全ての事業体には、不確実性が存在する。
ここで、リスクは以下のように定義できる。
リスクとは、事象が発生し、戦略と事業目標の達成に影響を及ぼす可能性である。

リスクは事業体が戦略と事業目標を達成する能力に影響を与える。どんな事業体であろうとも戦略を実行する上で不確実性に直面するのであって、経営者にとっての課題は、利害関係者のために価値を創造する過程において、事業体がどの程度のリスクの量を受け入れることができるかどうかを決定することである。COSO-ERMにおいて、リスクは重大性という観点から検討される場合が多い。

ERMの実施は事業体が、価値の創造、維持、実現を妨げる、あるいは既存の価値を破壊する可能性のあるリスクを識別し、優先順位をつけ、重点的に取り組むことを支援する。また同時に潜在的な機会を追求することも支援する。

COSO-ERMの便益

COSO-ERMにおいては、全社的リスクマネジメントを事業体の戦略策定及びパフォーマンス管理と一体化させることで、以下のような便益をもたらすとしている。

- 機会の範囲を増やす。
- プラスの成果と優位性を増進し、マイナスのサプライズを減らす。
- 全社的なリスクを識別し、管理する。
- パフォーマンスの変動を減らす。**成果物の品質の変動**
- 経営資源の配分を改善する。

すべての事業体に適用可能なアプローチは存在しないが、ERMを導入することによって、組織は成果と収益性を確保し、経営資源の損失を予防ないし低減することができる。

5-7 COSO-ERM (2)

COSO-ERMの構成要素

COSO-ERMでは、5つの相互に関連した構成要素と、各構成要素と結びついた基本概念である20の原則が設定されている。COSO-ERMは戦略の策定、目標の設定、そしてその導入とパフォーマンスと一体化した時に価値を増進するとしている。

COSO-ERMの５つの構成要素

RMに対する社風、価値観の形成

ガバナンスとカルチャー	ガバナンスとカルチャーはともに、全社的リスク・マネジメントの他のすべての構成要素の基礎となる。 ガバナンスは、全社的リスク・マネジメントの重要性を強調し、それに対する監督責任を確立する事業体の気風を醸成する。 カルチャーは、意思決定に反映される。
戦略と目標設定	全社的リスク・マネジメントは、戦略と事業目標の策定プロセスを通じて、事業体の戦略計画に統合される。事業環境を理解することにより、組織は、内外の要因とそれらがリスクに及ぼす影響についての知見を得ることができる。 組織は、戦略策定と合わせてリスク選好を設定する。事業目標は、戦略の実行を可能にし、事業体の日常活動とその優先順位を形づくる。
ERMの実行 パフォーマンス	組織は、戦略と事業目標を達成する事業体の能力に影響を及ぼすかもしれないリスクを識別し、評価する。 組織は、リスクの重大性に応じて、また事業体のリスク選好を考慮して、リスクを優先順位付けする。そして、組織は、リスクへの対応を選択し、パフォーマンスの変化の動向を監視する。 このように、組織は、戦略と全社レベルの事業目標を追求する中で受け入れたリスク量に対するポートフォリオの視点を構築する。

Takeしたリスクやパフォーマンスのレビュー

レビューと修正	全社的リスク・マネジメントの能力と実務、及びその目標に対する事業全体のパフォーマンスをレビューすることにより、組織は、全社的リスク・マネジメントの能力と実務が、どの程度まで長期的に価値を向上させられるかを検討できる。
情報、伝達及び報告	伝達は、事業全体を通して情報を収集し、共有する継続的で反復的なプロセスである。経営者は、全社的リスク・マネジメントを支援するために、内外の情報源から関連性のある情報を利用する。組織は、データと情報を入手し、処理し、管理するために、情報システムを活用する。すべての構成要素に関連する情報を利用して、組織は、リスク、カルチャー及びパフォーマンスについての報告を行う。

COSO-ERMの５つの構成要素は、構成要素と結びついた20の原則により支えられている。20の原則は以下のとおりである。

リスク・マネジメント原則（Risk Management Principles）

Key Point

構成要素	原則
ガバナンスとカルチャー	1. 取締役会によるリスク監視を行う
	2. 業務構造を確立する
	3. 望ましいカルチャーを定義づける
	4. コアバリューに対するコミットメントを表明する
	5. 有能な人材を惹きつけ、育成し、保持する
戦略と目標設定	6. 事業環境を分析する
	7. リスク選好を定義する
	8. 代替戦略を評価する
	9. 事業目標を組み立てる
パフォーマンス	10. リスクを識別する
	11. リスクの重大性を評価する
	12. リスクの優先順位をつける
	13. リスク対応を実施する
	14. ポートフォリオの視点を策定する

取締役会の監視・監督

行動規範の設定

社員の管理・育成

ERMの実行

レビューと修正	15. 重大な変化を評価する
	16. リスクとパフォーマンスを評価する
	17. 全社的リスク・マネジメントの改善を追求する
情報、伝達、及び報告	18. 情報とテクノロジーを有効活用する
	19. リスク情報を伝達する
	20. リスク、カルチャー及びパフォーマンスについて報告する

Takeしたリスク、成果物のレビュー

ERPパッケージの活用・導入

これらの原則を遵守することにより、経営者及び取締役会は、組織がその戦略及び事業目標に係るリスクを理解し、管理に取り組んでいるという合理的な期待を持つことができる。

5-8 COSO-ERM (3)

パフォーマンスに関連する原則

事業体の戦略と事業体の目標の達成に影響を及ぼす可能性のあるリスクを識別し、評価し、それに対応することによって、その事業体の価値をますます創造、維持、実現し、そして事業体の価値の下落を最小化することが可能となる。ここでは、COSO-ERMの20の原則のうち、パフォーマンスに関連する5つの原則を取り扱う。

a) 原則10：リスクを識別する

組織は、戦略及び事業目標のパフォーマンスに影響を及ぼすリスクを識別する。リスク一覧表の作成やリスク識別のアプローチとして以下の手法などが利用される。

- 過去の事象からのデータ追跡
- インタビュー
- 主要指標の活用
- プロセス分析
- ワークショップ

b) 原則11：リスクの重大性を評価する **リスク評価**

組織は、リスクの重大性を評価する。リスクの重大性は、影響を受ける可能性のある事業目標に沿って、複数の階層で（部門、機能及び業務ユニットにわたって）評価される。

経営者は、適切なリスク対応の選択、資源の配分を行うためにさまざまなリスクの重大性を決定し、そして、経営者の意思決定及びパフォーマンスを支援する。この測定基準は、影響度と発生可能性（定性的、定量的、頻度）が採用される。

リスク評価のアプローチは、定性的、定量的、又はその両方で行われる。またリスク評価の一部として、経営者は、固有リスク、ターゲットとする残余リスク、及び実際の残余リスクを考慮する。

c) 原則12：リスクの優先順位づけをする

組織は、リスク対応選択の基礎として、リスクの優先順位づけを行う。リスクの重大性、対応する事業目標の重大性、及び事業体のリスク選好を考慮したリスクの優先順位づけは、経営者の意思決定に役立つ。

優先順位づけは、同意された規準（適応性、速度、持続性、回復度）を適用することや、リスク選好を活用することで決定される。

d) 原則13：リスク対応を実施する

組織は、リスク対応を識別し、実施する。経営者は、リスクの重大性と優先順位づけ、事業環境と関連する事業目標を考慮する。

Key Point

論点 リスク対応

COSO-ERMでは、リスク対応を受容、回避、活用、低減、共有の5つに分類している。

リスク対応	定義	例
何もしない 受容	リスクの重大性を変更するための追加の対策を講じない。 この対応は戦略と事業目標に対するリスクが既にリスク選好の中に納まっている場合に適切である。	ある工場では従業員によりネジが盗難にあうリスクはあるが、金額が小さく発見可能性も低いため、ネジの容器に鍵をかけたり、ネジの数をカウントしたりはしないことにする。
やめる 回避	リスクを除去するための活動を行う。例えば、製品ラインの廃止や、事業部の売却等があげられる。	小切手の不正使用のリスクを回避するため、小切手による支払を停止する。

リスクテイク 活用 （追求）	より高いパフォーマンスを達成するため、より多くのリスクを受入れる活動を行う。積極的な成長戦略を選択することや新製品、サービスの開発などがあげられる。	国内トップシェアの製品を持つ会社が、更なる成長を目指して海外に販売子会社を設立し、海外市場に参入する。
%や$を下げる 低減	リスクの重大性を低減するための活動を行う。目標とするリスクプロファイルとリスク選好と整合するようにリスクを低減するために行う多種多様な日々の事業上の意思決定が含まれる。	地震による生産設備への損害を最小限とすべく、工場に耐震工事を行う。
共有 第3者に移し替える、シェアする	リスクの重大性を低減するために、リスクの一部を移転、又は共有するための活動を行う。外部専門家への外注や、保険商品の購入などがあげられる。	火災へのリスク対応として、建物に火災保険を掛ける。

e) 原則14：ポートフォリオの視点を策定する

組織は、リスクのポートフォリオの視点を策定し、評価する。経営者及び取締役会は、ポートフォリオの視点によって、リスクの種類、重大性及び相互関係を考慮することができる。そして、それがどのようにパフォーマンスに影響するかを考慮することができる。ポートフォリオの視点は、それぞれの組織上の機能、戦略そして事業目標に関する事業体のリスク選好と比較して、想定されたリスクの種類と量を示すように図示される。

事業体に対するリスクのポートフォリオの視点を策定することにより、リスクベースの意思決定が可能となり、パフォーマンス目標を設定し、パフォーマンス又はリスクプロファイルの変更を管理するのに役立つ。ポートフォリオの視点を使用してリスクとパフォーマンスの関係を理解することにより、組織は、事業体のリスク選好に基づいて、戦略及び事業目標の結果を評価することができる。

5-10 リスク・マネジメントの有効性の評価

リスク・マネジメントの有効性の評価

基準 13.2「個々の内部監査業務におけるリスク評価」は、内部監査人がリスクを評価するために、レビュー対象の活動を十分に理解し、信頼できる情報を収集する必要があるとしている。リスク評価には、活動の目標やリスク許容度、ガバナンス、リスク・マネジメント、コントロールの各プロセスが含まれ、不正リスクも考慮する。

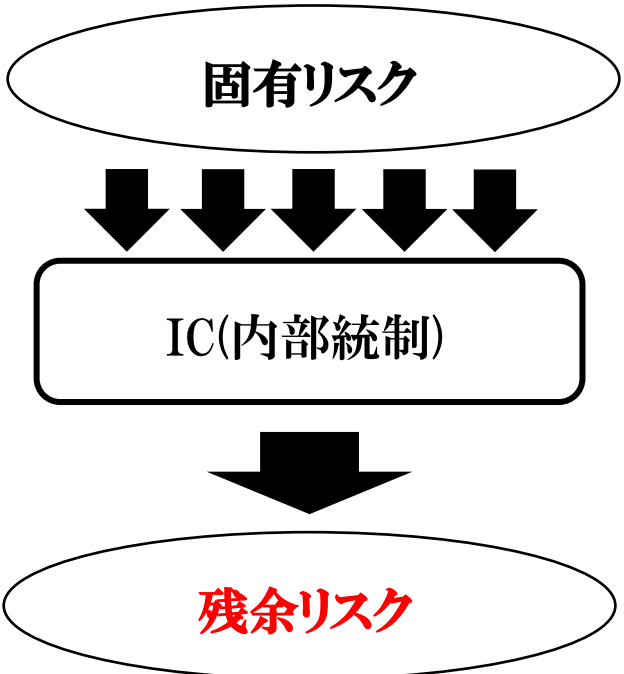
本 Unit では、個々の内部監査業務に関連するリスクとリスク・マネジメント・プロセスの有効性の評価について学習する。

内部監査人は、個々の内部監査業務に関連するリスクを評価するために、レビューの対象となる活動を理解しなければならない。

十分に理解するために、以下の事項について、信頼できる、関連性のある、十分な情報を識別、収集しなければならない。**証拠の収集**

- 内部監査部門、経営管理者又は外部のサービス・プロバイダが最近実施したリスク評価をレビューすること。検討される目標には、コンプライアンス、財務報告、業務運営又はパフォーマンス、不正、情報技術、戦略、及び内部監査の計画に関する目標を含めるべきである。
- 財務、環境、社会的責任及びガバナンスといった、内部監査部門及びその他のアシュアランス及びアドバイザリー業務のプロバイダが過去に実施した個々の内部監査業務に関するコミュニケーションをレビューすること。
- 過去に実施した個々の内部監査業務の調書をレビューすること。
- 参考資料をレビューすること — 参考資料には、IIA 及びその他の団体の権威あるガイダンス、法令、並びに組織体のセクター、業界及び法域に関連する規制を含む。

- 戦略、オペレーショナル、財務及びコンプライアンスなど、組織体の関連するリスク・カテゴリーを検討すること。
- リスク許容度が定義されている場合は、それを考慮すること。
- 組織図及び職務記述書を用いて、レビューの対象となる活動の関連情報、プロセス、及びその他の側面について誰が責任を有するかを決定すること。
- レビューの対象となる活動の物的資産を点検すること。
- 経営管理者の方針、手続、フローチャート及び報告書を含め、情報の所有者又は外部の情報源から入手した文書を調査すること。
- ウェブサイト、データベース及びシステムを調査すること。
- インタビュー、議論又はサーベイを通じて確認すること。
- 稼働中のプロセスを観察すること。
- 他のアシュアランス業務及びアドバイザリー業務のプロバイダと面談すること。


固有リスク
IC(内部統制)
残余リスク

リスク許容度(Risk Tolerance)

	ターゲット	リスク許容度(Risk Tolerance)
レストランの宅配サービス	40分以内の配達	30分～50分の配達時間
コールセンターの不在着信の最小化	着信全体の2%	着信全体の1%～5%

リスクインベントリー

組織体に影響を与えうる全てのリスクを書き出したもの

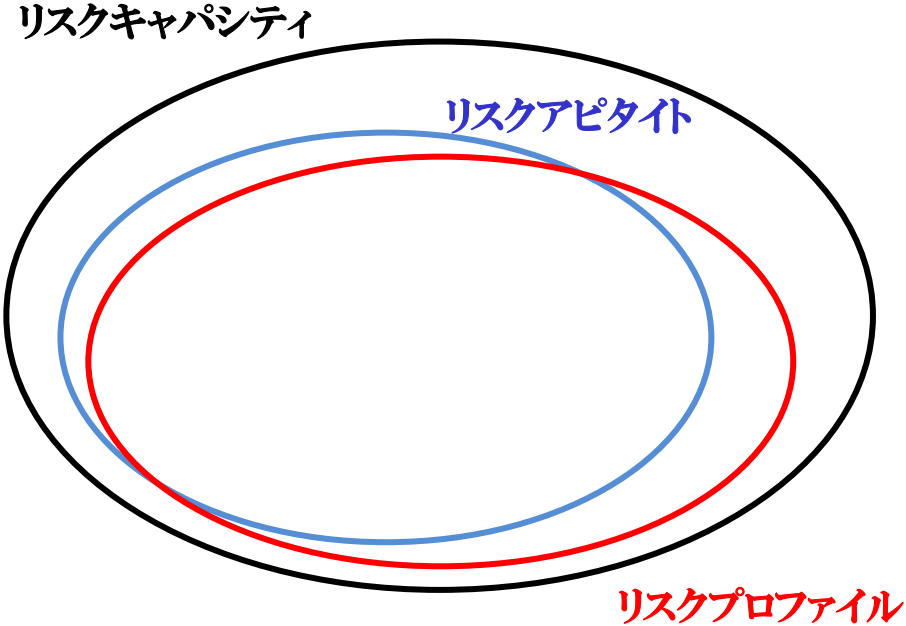
リスクプロファイル

組織が現時点で保有しているリスクの種類や量

リスクキャパシティ

組織が許容できるリスクの最大量

各リスクの関係性



原則14：ポートフォリオの視点を策定する

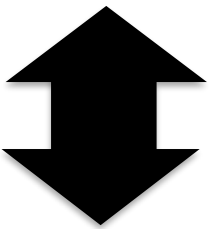
各部門長や事業部長が、各目標に関連するリスク評価を行う。それを経営者および取締役会が、ポートフォリオの視点（すなわち組織体全体の視点）によって、リスクの種類、重要度および相互関係を考慮する。

例：

ある事業部長は、新製品開発に必要な技術を入手するためのある企業買収案件はリスクが大きすぎる、と判断している。しかし全社レベル、すなわち組織体のリスクを、ポートフォリオの視点でみるCEOとCFOは、組織体全体ベースではリスクは許容範囲とみなして、その企業買収をすべき、という判断をする。

ERMが有効であるとは・・・

5つの構成要素が存在する



20の原則が機能する

本日の論点

- リスクやRMについて
- RMに係わる役割
- COSO-ERM
- ISO31000

Chapter 5

◎ 1, 2, 8, 11