公認内部監査人(CIA)
Part I／第5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。

6-1　内部監査におけるリスクの定義

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インターナル・コントロール・システムによって軽減することができる。

論点　リスクの定義

IPPFによれば、リスクは以下のように定義される。

定義　目標の達成に影響を与える事象発生の可能性。リスクは影響の大きさと発生可能性とに基づいて測定される。

$

%

リスクの定義は、各種の基準書や組織体によって様々であり、絶対的な定義はない。しかしながら、全ての組織体は明確な定義を持つべきである。

リスクの分類

内部監査に係わるリスクは以下の５つに分類することができる。

1	ビジネス・リスク	事業や取引などが成功しないリスク
	ハザード・リスク	事象の発生により損失が発生するリスク
2	行動するリスク	行動の結果による失敗等、行動したことによるリスク
	行動しないリスク	機会の喪失等、行動しなかったことによるリスク
3	戦略的リスク	経営体による基本的な意思決定が抱えるリスク
	業務的リスク	日常業務上のリスク
4	全社的リスク	全社的な信頼性に関わるリスク
	個別的リスク	特定業務、手続き等の信頼性に関わるリスク
5	現在のリスク	現在の業務や組織が抱えているリスク
	将来のリスク	将来の業務や組織が抱えるであろうリスク

参考文献：実践的内部監査の実務（日本内部監査協会編）

リスクやコントロールに関する用語について、絶対的な定義は存在しないものが多いが、以下は、内部監査人が理解しておくべき代表的な用語である。ただしその全てを網羅することを意図したものではない。

リスクとコントロールに関する用語

AR: 監査失敗のリスク

妥当なコントロール (Adequate control)	組織体のリスクが有効に管理されており、組織体のゴールや目標が効率的かつ経済的に達成されるとの、合理的なアシュアランスを提供するに相応しい方法で、経営管理者がコントロールを計画し整備(設計)しているときに、妥当なコントロールが存在する。
監査リスク (Audit risk)	内部監査における監査リスクとは、実施した業務に基づいて誤った結論もしくは意見を表明することである。
コントロール (Control)	経営管理者、取締役会およびその他の者が、リスクを管理するために、また、設定した目標やゴールが達成される可能性を高めるために行うすべての措置。経営管理者は、設定した目標やゴールが達成されるとの合理的なアシュアランスを得るのに十分な措置の遂行を、計画し、準備し、指揮する。

CR: ICがうまく働かないリスク

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。

コントロール・プロセス (Control process)	コントロールのフレームワークの一部としての、方針、手続(手動のものも自動化されたものも含む)および活動であって、リスクが確実に組織体の受容しようとしている水準以内にあるように、設計され、運用されているもの。
コントロール・リスク (Control risk)	コントロール活動がコントロール可能なリスクを許容可能なレベルまで低減することに失敗する可能性。
固有リスク (Inherent risk)	インターナル・コントロールが全く整備されていないと仮定した場合に存在するリスク。
残余リスク (Residual risk)	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。

RR: 正味リスク(Net Risk)とも言われる

リスク (Risk)	目標の達成に影響を与える事象発生の可能性。リスクは影響の大きさと発生可能性に基づいて測定される。 リスクのうち、目標の達成にマイナスの影響を与えるリスクを脅威(threat)、プラスの影響を与えるリスクを機会(opportu- を含む。
リスク選好 (Risk appetite)	組織体が積極的に受容するリスクのレベル。
リスク評価 (Risk assessment/ Risk Analysis)	リスクを識別し、測定する、また優先順位をつけるプロセス。
リスクの識別 (Risk identification)	目標の達成に対して影響を与えうる潜在的な脅威と機会を識別する手法。

企業価値増大のために

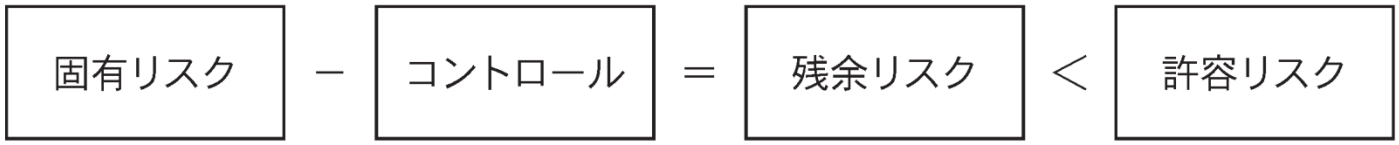
リスク・マネジメント （Risk management）	組織体の目標達成に関し、合理的なアシュアランスを提供するために、発生する可能性のある事象や状況を、識別し、評価し、管理し、コントロールするプロセス。
リスク対応 （Risk response/ Risk treatment）	リスクを管理するために行う活動。
リスク許容度 （Risk tolerance）	目標達成に関し、許容できるリスクの変動水準。

RT: パフォーマンス(成果物)の許容可能な差異

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。



6-2　リスク・マネジメントの定義

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。

リスク・マネジメントの定義　リスク管理

IPPF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。

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。

6-3　リスク・マネジメント・プロセスに係る内部監査部門の役割

リスク・マネジメント・プロセスに係る内部監査部門の役割

「基準」2120では、内部監査部門の役割として、リスク・マネジメント・プロセスの有効性の評価と改善への貢献を規定し、解釈指針において有効性の判断基準を示している。

基準　「基準」2120：リスク・マネジメント；「基準」2120.A1

内部監査部門はリスク・マネジメント・プロセスの有効性を評価し、リスク・マネジメント・プロセスの改善に貢献しなければならない。(2120)

内部監査部門は、以下の各事項に関わる組織体のガバナンス、業務および情報システムに関するリスク・エクスポージャー(リスクに曝されている度合い)を評価しなければならない。

- 組織体の戦略目標の達成状況
- 財務および業務に関する情報の、信頼性とインテグリティ
- 業務とプログラムの有効性と効率性
- 資産の保全
- 法令、方針、定められた手続および契約の遵守(2120.A1)

完全性

6-4　リスク・マネジメント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

リスク・マネジメントは、最高経営者と取締役会の重要な責任の１つである。

a) リスク・マネジメント・プロセスに係る役割については以下の通りである。

最高経営者	強固なリスク・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。
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負う。この役割の中で、内部監査部門の監督を行う。
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の最終責任

RMの監視

RMプロセスの評価

6-5　リスク・マネジメントの評価と既存のフレームワーク

a） CAEは、組織体のガバナンス、リスク・マネジメントおよびコントロールの各プロセスを評価するための適切な戦略を立てるために、通常次の2つの事項を考慮する。

1） ガバナンス、リスク・マネジメントおよびコントロールの各プロセスの成熟度の水準

2） 組織体の文化および1)の各プロセスに責任をもつ個人の職位の序列

その後で、CAEは、上記の3つのプロセスに関連したリスクを評価する。CAEは、最高経営者が採用した既存のフレームワーク（例：トレッドウェイ委員会支援組織委員会（COSO）の内部統制（インターナル・コントロール）および全社的リスク・マネジメントのフレームワーク、コーポレート・ガバナンスに関するKingレポート、またはISO 31000）をこの評価のガイダンスとするために使用してもよい。この評価の間、CAEは、関連する発見事項および結論があればそれを文書化し最高経営者と協議する。CAEはまた、この各プロセスを強化するために改善のための提言を作成する。

トレッドウェイ委員会支援組織委員会

e) COSOの設立とCOSOフレームワークの確立

海外腐敗行為防止法成立の後も、1980年代の米国では外部監査人によって無限定意見が提出された直後にその企業が経営破綻するということが相次いだ。内部統制に関連する5つの団体は、1985年、不正な財務報告の発生を減少させることを主たる目的として、COSOを共同で設立し、1992年9月“Internal Control-Integrated Framework”という報告書(COSOレポート)を公表し、内部統制の定義のフレームワークを確立した。COSOフレームワークは事実上内部統制の世界標準となった。

b） 既存のフレームワークが当該組織体のガバナンス、リスク・マネジメントおよびコントロールの各プロセスをガイドするのに採用されていない場合には、CAEは、最高経営者がこの各プロセスを向上させようとするのを導くための適切なフレームワークを推奨することを検討してもよい。

次のUnit以降で、国際的に認められているリスク・マネジメント・フレームワークから代表的なものを学習する。

6-6 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。）

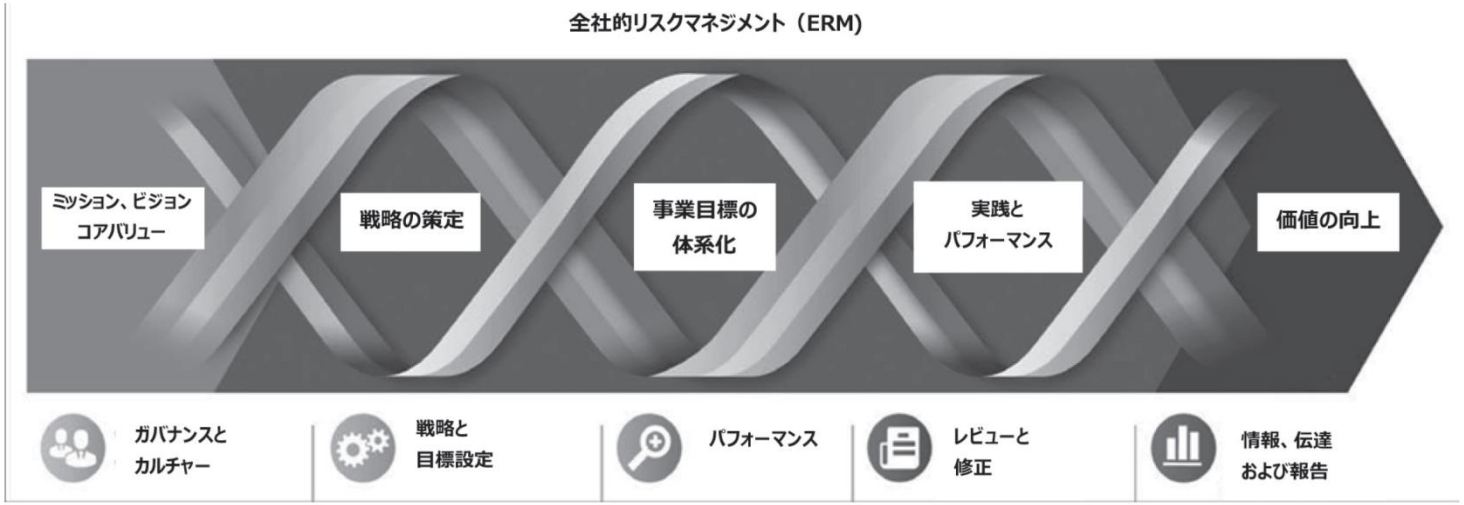
それから10年以上が経過し、情報技術の発展やグローバル化の進展により、企業を取り巻くリスクは多様化、複雑化し、新しいリスクが生じた。こうした経営環境の変化による経営者のリスクに対する関心の高まりに応じてCOSOは2017年に改訂版となる「全社的リスクマネジメント－戦略およびパフォーマンスとの統合」（以下「COSO-ERM」）を公表した。

論点 COSO-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、およ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*』を元にアビタスが翻訳

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。全ての事業体は価値を追求する上でリスクに直面する。

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。

論点　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。
- 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。

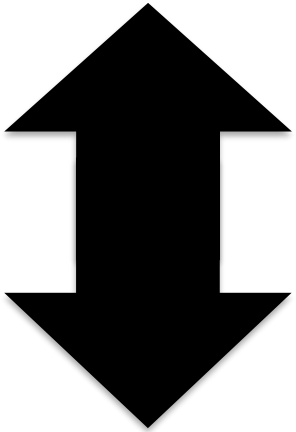
6-7 COSO-ERM（2）

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。

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

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、リスクを優先順位づけする。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。
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、およびその目標に対する事業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てきたのか、さらに、大きな変化に直面した場合でも価値を向上させられるかを検討できる。

情報、伝達および報告	伝達は、事業体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、カルチャーおよ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。

Key Point

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

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

取締役会の監視・監督

行動規範の設定

社員の管理・育成

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 **ERMの実行**	10. リスクを識別する
	11. リスクの重大性を評価する
	12. リスクの優先順位づけをする
	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

Takeしたリスク、 成果物のレビュー

レビューと修正	15 化を評価する
	16. リスクとパフォーマンスをレビューする
	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、および報告	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、カルチャーおよびパフォーマンスについて報告する

これらの原則を遵守することにより、経営者および取締役会は、組織がその戦略およ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。

6-8 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つの原則を取扱う。

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。

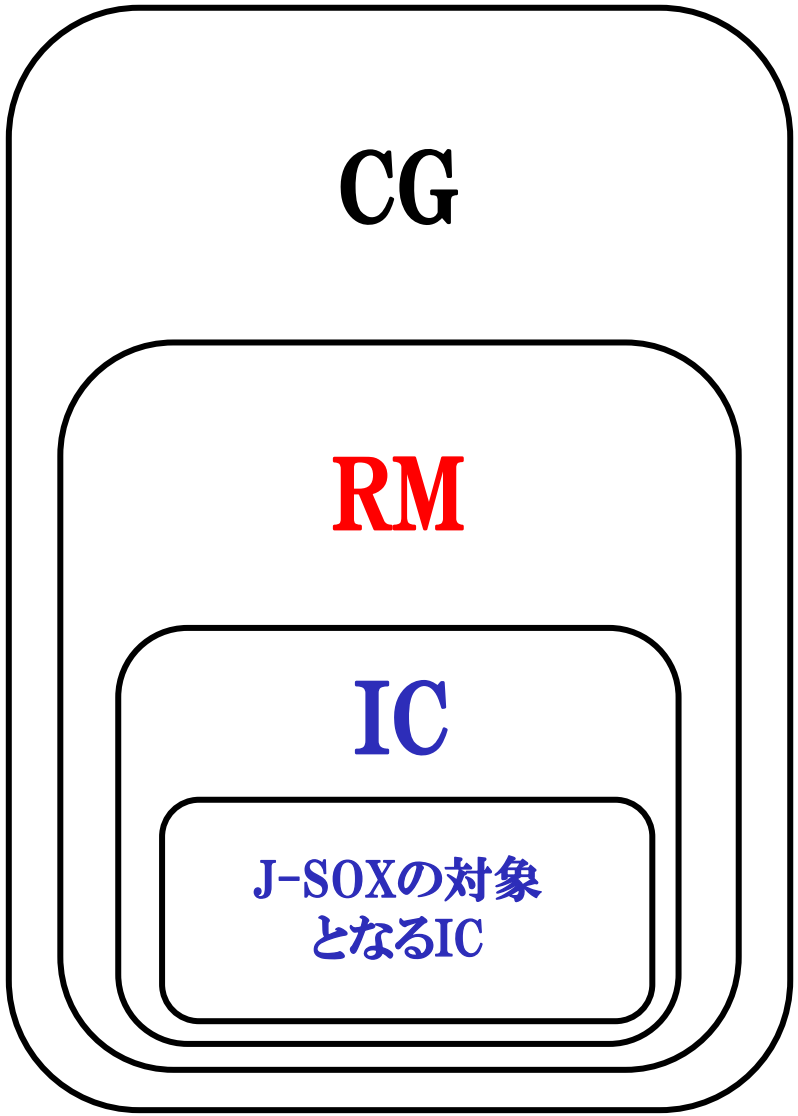
リスク対応	定義	例
何もしない 受容	リスクの重大性を変更するための追加の対策を講じない。 この対応は戦略と事業目標に対するリスクが既にリスク選好の中に納まっている場合に適切である。	ある工場では従業員によりネジが盗難にあうリスクはあるが、金額が小さく発見可能性も低いため、ネジの容器に鍵をかけたり、ネジの数をカウントしたりはしないことにする。

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	リスクの重大性を低減するために、リスクの一部を移転、また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。

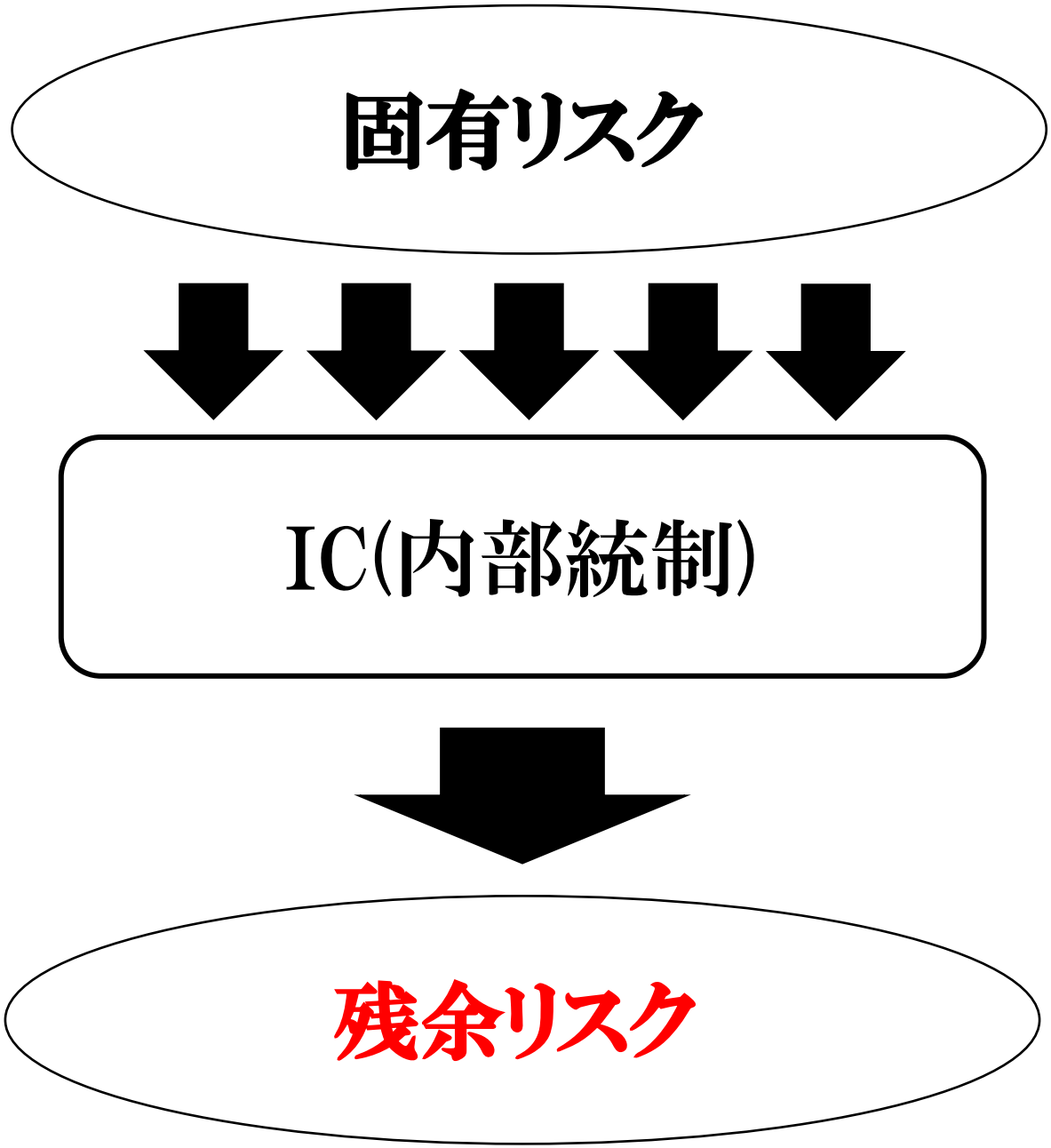
第3者に移し替える、シェアする



企業経営を規律するための仕組み

CGの目的の達成を支える手段

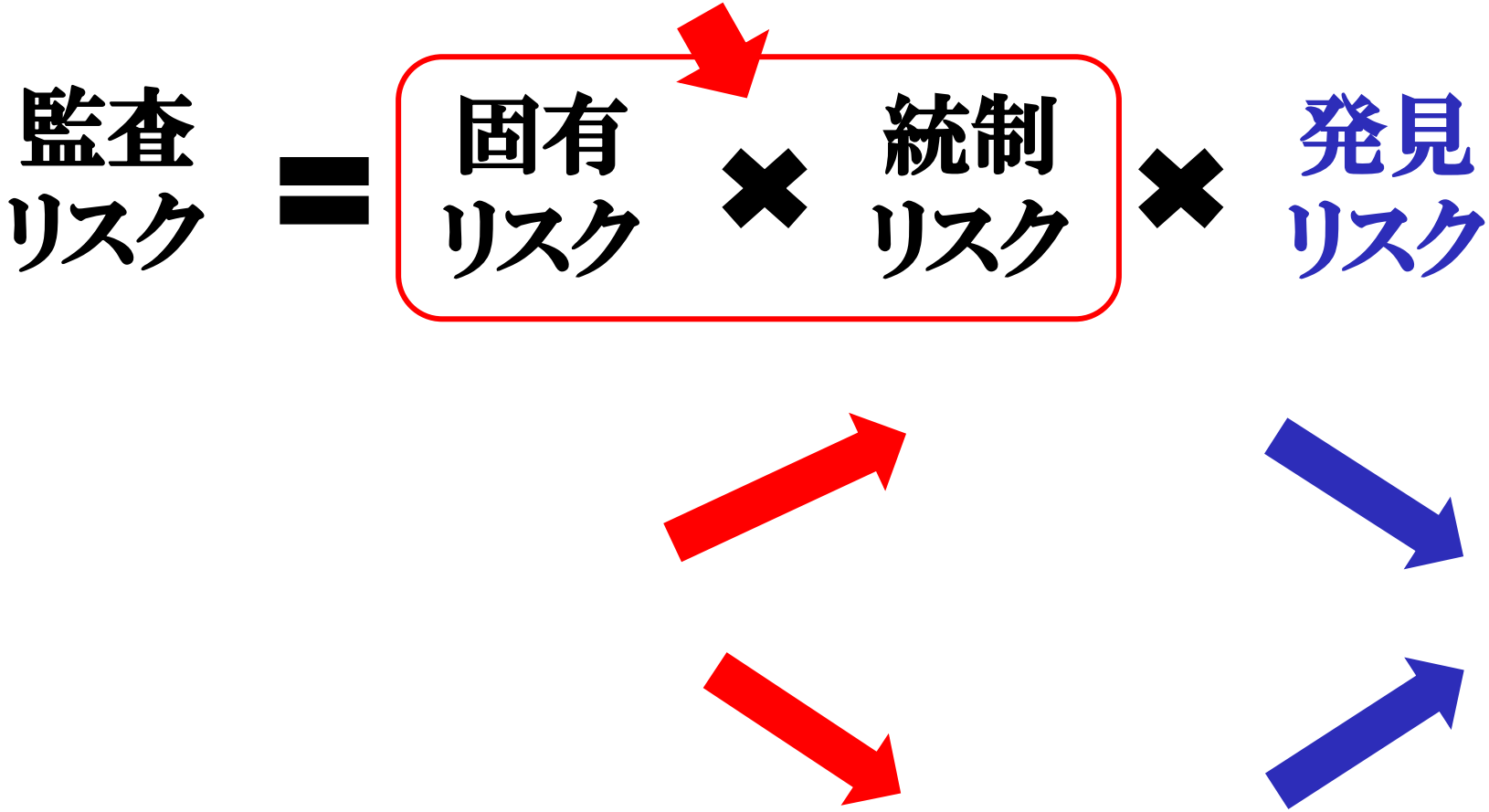
RMを機能させるために必要な
プロセスや措置


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%

監査人はコントロールできない



発見リスク(Detection Risk)

監査人の監査手続に問題のあるリスク

使命(Mission)

↓

目標

↓

戦略

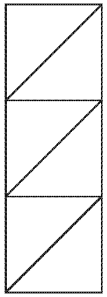
Key Point

MC 6-8-1

MC 6-8-7

多くの企業は、小切手の代わりに電子媒体による資金送金機能を利用して、仕入先への支払いを行なっている。この対応は、小切手等を発行することに伴うリスクについて、次のどのリスク管理手法を表しているか。

a. コントロールすること
b. 受容すること
c. 移転すること
d. 回避すること



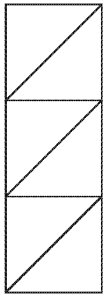
リスクへの対応についての問題。

「小切手を使用しない」ことにより、企業は小切手を使用することに伴うあらゆるリスクを回避している。
従って、正解はd。

a, b, cは誤り。いずれも本問には不適切である。

製造業などで、生産設備などが火災により損害を被るリスクに対応するために、火災保険に加入することが多い。これは以下のERMのリスク対応のうちどれに該当するか。

a. 回避
b. 低減
c. 共有
d. 受容



保険についての問題。

保険会社へ、保険料を支払い、それにより、保険事故発生時の損失を保険会社に補填してもらう。これは、リスクの一部を移転もしくは共有することである。
従って、正解はc。

aは誤り。回避とは、リスクを伴う活動を行わないことである。火災の原因をすべて回避することは現実的ではない。
bは誤り。低減とは、損害の発生可能性や影響を低下させることである。例えば消火設備を導入することで、火災の影響を軽減できる。
dは誤り。受容とは、リスクに対して対策を行わず、リスクを受け入れることである。火災は影響が大きく、人命にも関わるので、火災のリスクを完全に受容することはない。

Key Point

除雪作業を行う会社が、今期の積雪量は非常に多くなるだろうと予測している。これは以下のどのリスクに当てはまるか？

A: リスク選好
B: 残余リスク
C: 固有リスク
D: 統制リスク

本日の論点

- リスクやRMについて
- RMに係わる役割
- COSO-ERM

Chapter 6

◎ 1, 3, 7, 8,

9, 12