CCSA

ドメインⅤ
リスクの識別および評価

2008年4月

CIAフォーラム　CSA研究会（No. 6）

ドメインⅤ：増田・碓井・斉藤

ドメインⅤ　リスクの識別および評価

ドメイン Ⅰ ～Ⅲ CSAの設計・導入・運用の要素
ドメインⅣ～Ⅵ CSAを適用するコンテンツの知識

リスクマネジメントは、

目的の設定	ドメインⅣ
∨	
リスクの識別	ドメインⅤ
∨	
リスクの評価	ドメインⅤ
∨	
リスクへの対応	ドメインⅤ
∨	
統制活動	ドメインⅥ

「内部監査の専門的実施の国際基準」において、リスクを明確かつ網羅的に取り上げ、監査プロセスに組み入れることが要請されている。

ドメインV　リスクの識別および評価

－　リスク及びリスクマネジメントに関する基礎知識

（　）:テキストページ

A. リスクに関する理論（p.95-102）

B. リスクモデル／フレームワーク（p.102-111）

C. 一般的な事業プロセスに伴う固有リスクの理解（p.111-117）

D. リスクの識別および評価手法の適用（p.117-120）

E. リスクマネジメント手法／費用対効果分析（p.120-123）

F. 結論（p.123）

※　テキストでは、リスクマネジメント、リスクベース監査に関する内容がA～Eに分散して記載されています。セミナーでは、リスクマネジメントの説明を A. でまとめて行います。また、最後（B.の後）に、リスクベース監査の説明をまとめて行います。スライドの中にテキストの 該当箇所（A～E）を表示しましたので、適宜、ご参照下さい。 なお、理解の一助とする ためテキストには記載がない図表、事例を追加しています（【参考】と表示）。

V-A. リスクに関する理論

リスクの定義 （V-A.1.）

- 組織の目標・目的の達成に（マイナスの）影響を与える事象の発生可能性。
- 影響の大きさと発生の可能性に基づいて測定される。

（留意点）

- リスクは全ての事業活動に内在し、リスクと報酬は一般的に正の関係にある。（V-A.2.）
- リスク発生のタイミングおよび影響の継続期間により影響の大きさが異なる場合がある。（V-E.）

V-A.リスクに関する理論

固有リスク　（V-C.）

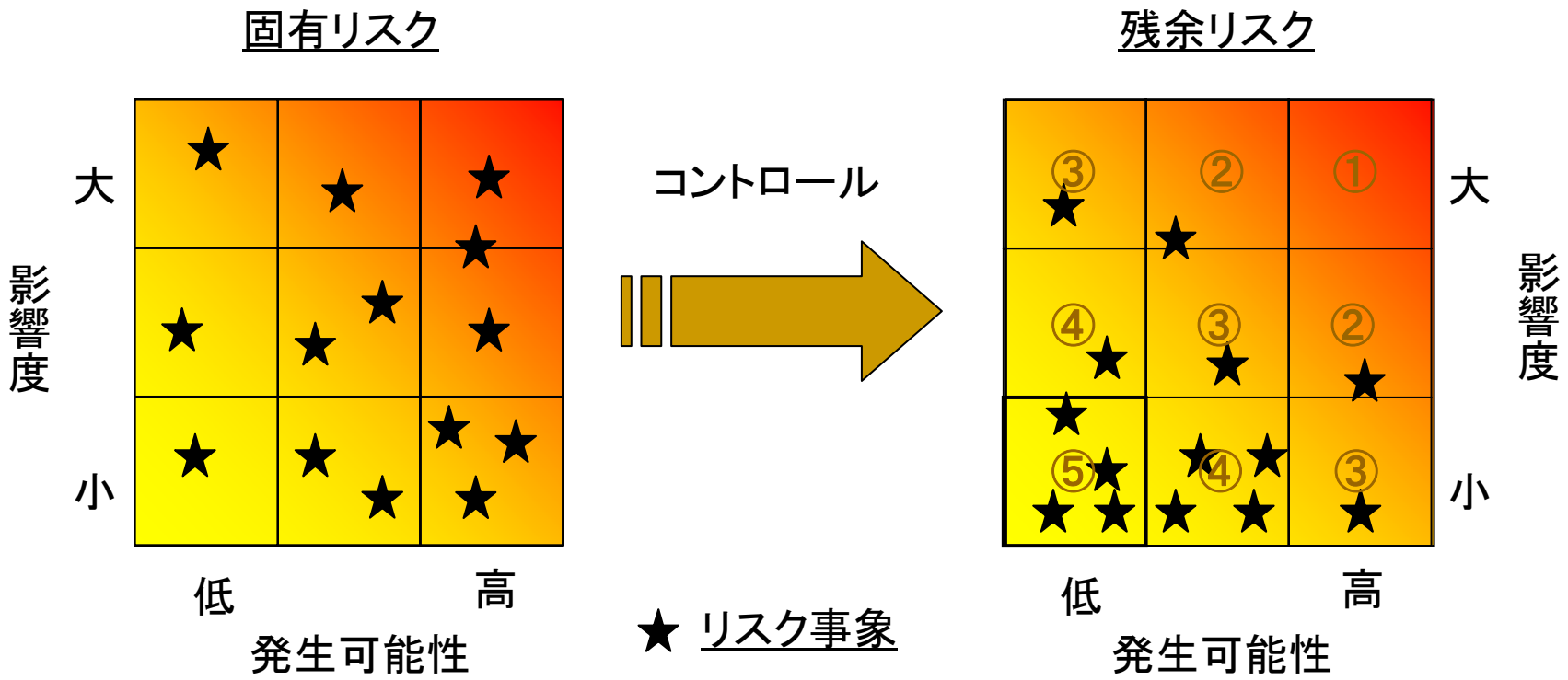
- コントロール等が全く整備されていないと仮定した場合に存在するリスク

残余リスク　（V-A.1.）

- 不利な事象の影響と発生の可能性を軽減する措置（コントロール等）を講じた後にさらに残るリスク

V-A. リスクに関する理論

【参考】リスクマップでみた固有リスクと残余リスクの関係



V-A.リスクに関する理論

統制リスク/脆弱性 （V-A.3.）

- マネジメントプロセスに固有のリスク、または機能しないコントロール手続への依存に関連するリスク

統制リスク	小さい	大きい
脆弱性	低い	高い
コントロール	強い （有効である）	弱い （有効でない）

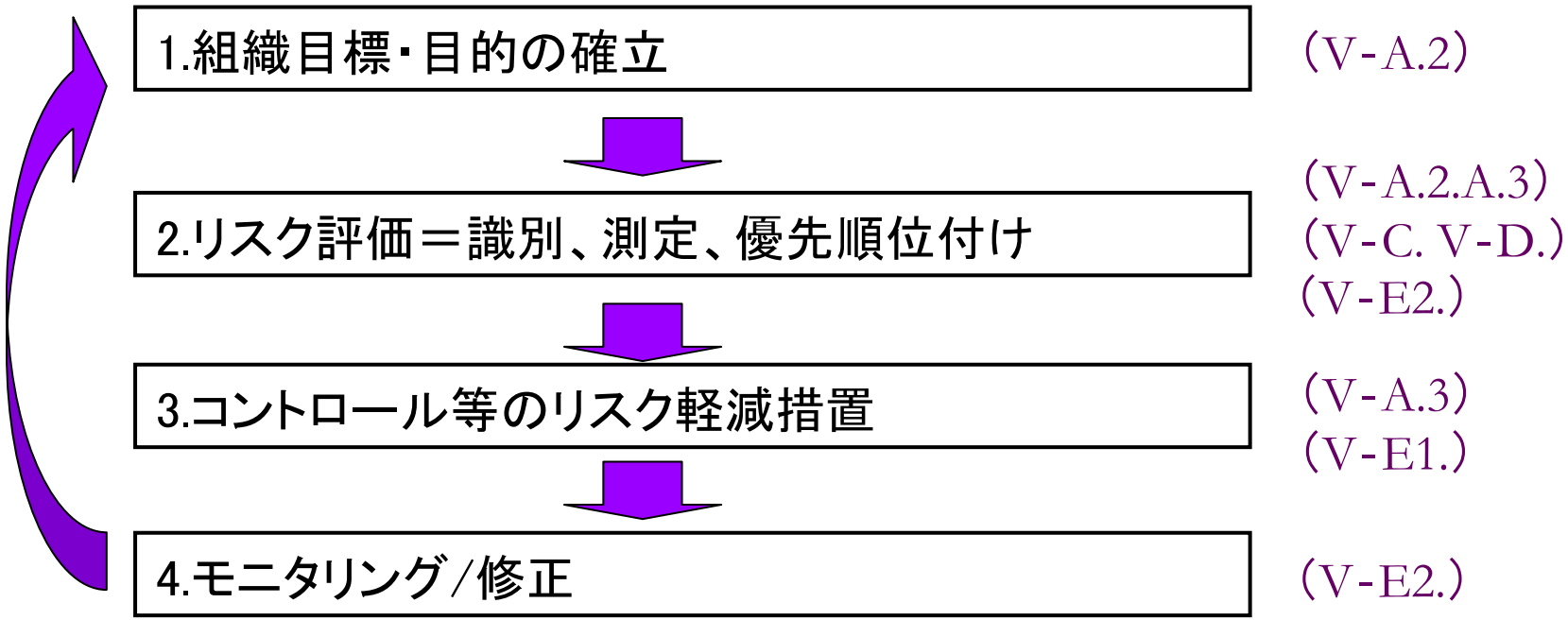
（V-C.）

- 残余リスクが小さくても、統制リスクが大きい（＝脆弱性が高い）場合、そのコントロールは改善を要すると判断されることがある。

V-A. リスクに関する理論

リスクマネジメントの定義 （V-A.1.）

- 組織の目標・目的の達成に関して合理的保証を提供するため、発生する可能性のある事象や状況を識別、評価、管理およびコントロールするプロセス



V-A. リスクに関する理論

リスクマネジメント・プロセスの5つの目的 （V-A.4）

（1）事業戦略および活動から生じるリスクを識別・測定し、優先順位付けすること
（2）組織にとって受け入れ可能なリスクレベルを決定すること
（3）許容可能なレベルまでリスクを軽減する活動（リスクの回避、リスクの共有・移転、リスクのコントロール）をデザインし実施すること
（4）リスクおよびリスク・コントロールの有効性を評価する継続的なモニタリング活動を実施すること
（5）取締役会および経営者が、リスク・マネジメント・プロセスの結果に関する報告書を定期的に受け取ること

固有リスク － コントロールによるリスク軽減
＝ 残余リスク ≦ 組織にとって許容可能なリスク

V-A. リスクに関する理論

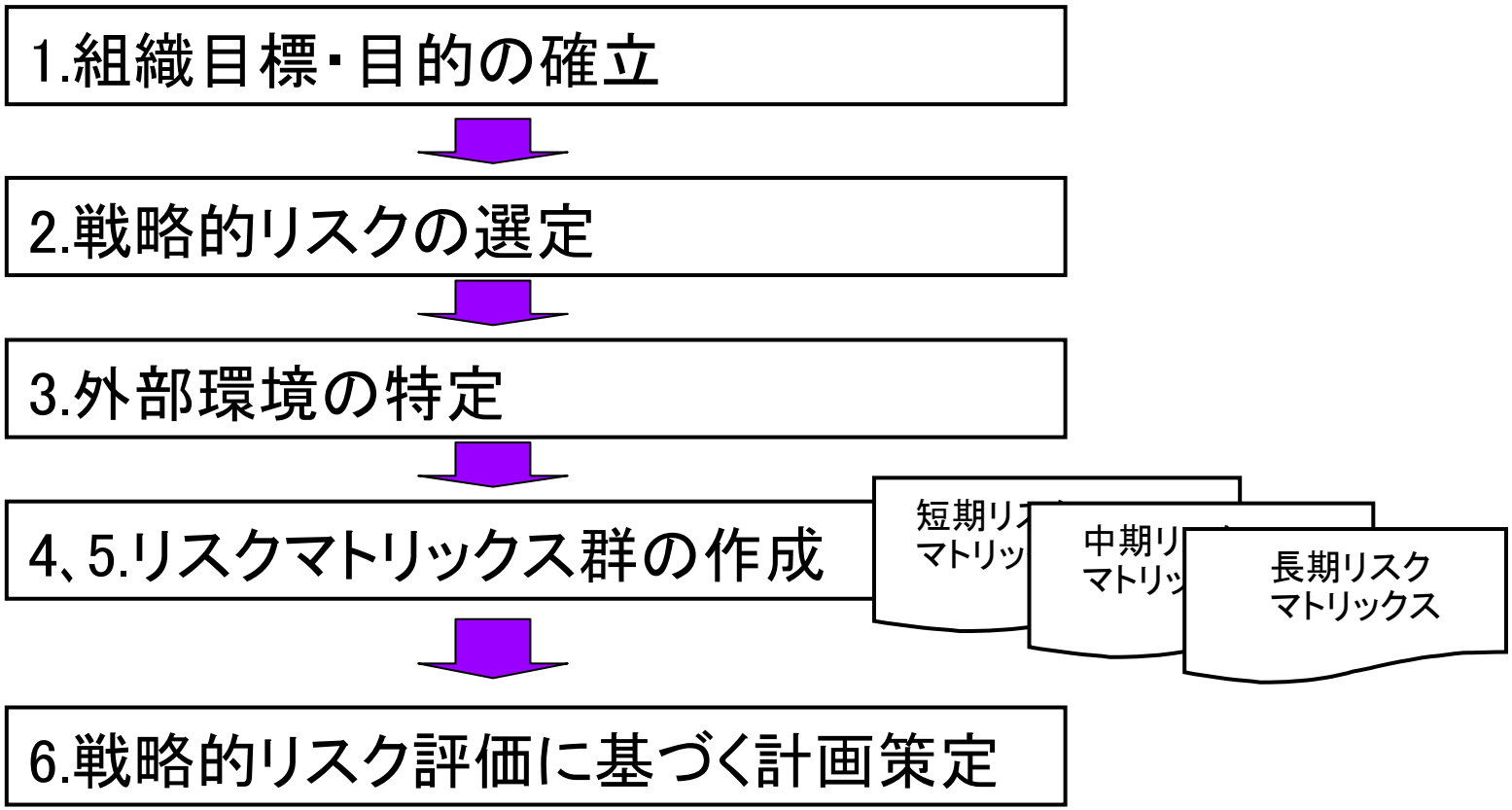
リスク評価・マネジメントの3つのレベル （V-A.2）

- 戦略:
  中長期（5～10年）
  取締役会・経営者レベル
- プロセス（/プログラム/プロジェクト）
  各期（ ～1年）
  部門管理者レベル
- オペレーショナル（日常的業務）
  日常的
  現場管理者レベル
  ― リスク評価というより、個別リスク事象の管理が中心

（David McNamee, *Business Risk Assessment*より）

V-A. リスクに関する理論

（1）戦略的リスク評価に基づく計画策定プロセス（V-A.2）



（David McNamee，*Business Risk Assessment*より）

V-A. リスクに関する理論

＜マトリックスフォーム＞ （V-A.2）

目標／目的（　　）　時間軸　短期・中期・長期

戦略的リスク ／ 外部環境	オペレーショナルリスク	財務リスク	評判リスク	×××リスク
政治／政府				
テクノロジー				
法規制				
競争相手				
顧客／利害関係者				
物理的環境				
市場				
サプライヤー				
経済／金融環境				

各セルに機会／リスクシナリオを記入

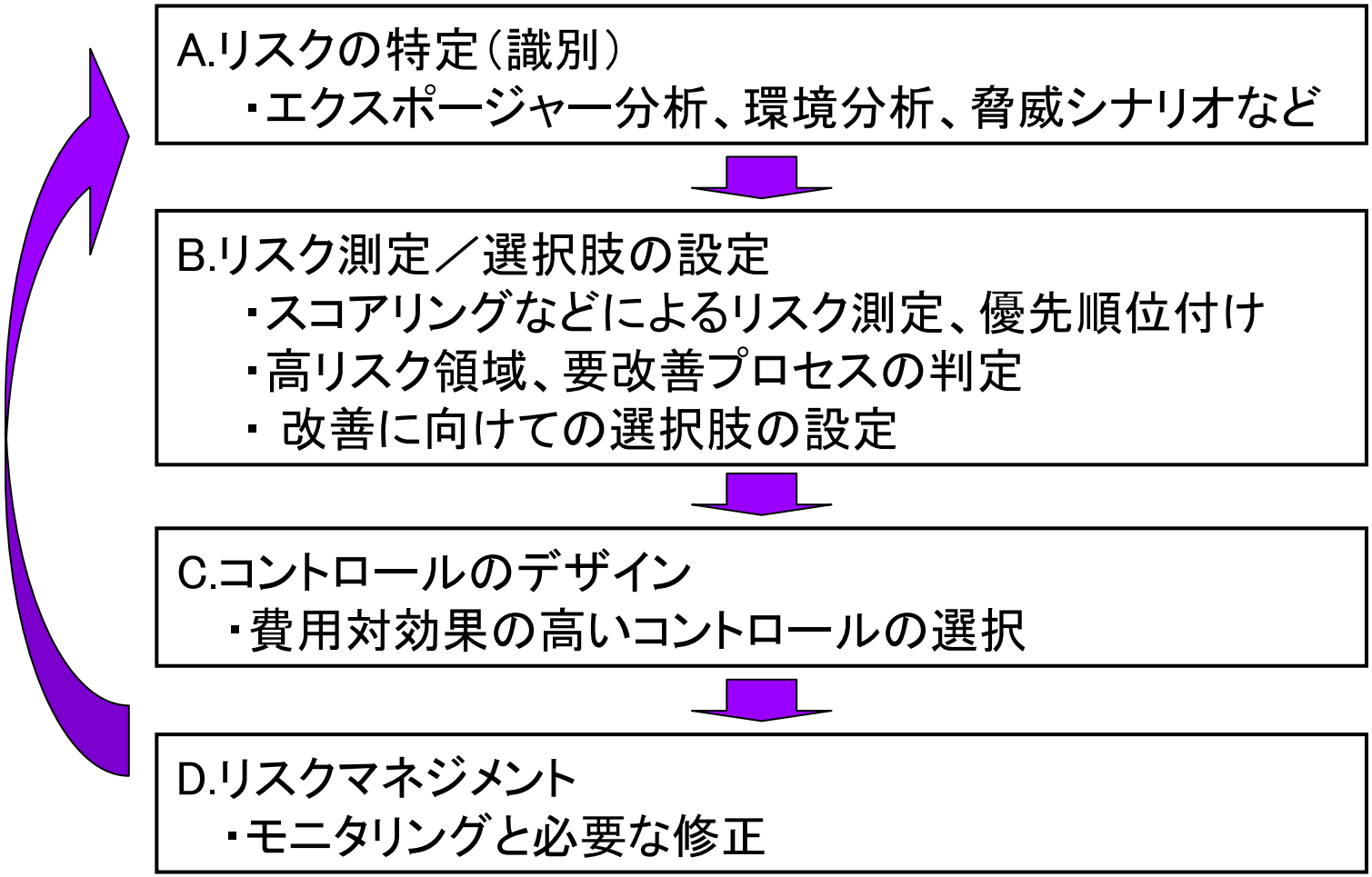
・全てのセルを記入する必要はない

・重要な機会／リスクに絞って記入

（David McNamee，*Business Risk Assessment*より）

V-A. リスクに関する理論

（2）プロセスレベルのリスクマネジメント（V-A.2）



（David McNamee, *Business Risk Assessment*より）

V-A. リスクに関する理論

A. リスクの特定（識別） （V-A.2）

①エクスポージャー分析
曝されているリスクの大きさ（事業資産の価額、取引規模など）に注目したアプローチ

②環境分析
事業の目標達成に影響を与える外部環境とその変化に注目したアプローチ

③脅威（リスク）シナリオ
事業の目標達成に影響を与えうるリスクシナリオ（不正、災害など）を網羅的に記述していくアプローチ

※ リスクの特定（識別）には、上記以外にも様々な手法がある。それぞれに長所・短所があり、複数のアプローチを組み合わせて使用することで、重要なリスクの洗い出し漏れがないようにすることが望ましい

V-A. リスクに関する理論

B. リスク測定／選択肢の設定 （V-A.2）

① 固有リスクとコントロールの有効性を評価し、残余リスクの測定、優先順位付けを行う。

⇒ リスクコントロール・マトリックスの作成
リスクおよびコントロールの有効性のスコアリング
影響金額・発生頻度の直接見積もり　など

※ 実務的には、上記以外にも様々な手法、バリエーションがある。

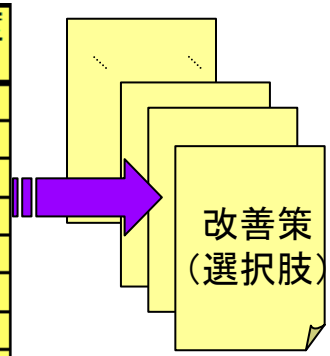
② 高リスク領域（要改善プロセス）を判定する。

③ 改善に向けての選択肢を設定する。

V-A. リスクに関する理論

【参考1】リスクコントロール・マトリックス（例）

プロセス・コード	リスクの内容	リスク分類	固有リスクの評価		コントロールの内容	種類	評価	残余リスクの評価		優先度
			影響度	発生頻度				影響度	発生頻度	
123－001		事務ミス	大	大		予防的	有効	大	大	①
123－004		システム障害	中	中		発見的	概ね有効	中	中	②
123－016		規程違反	小	小			不十分	小	小	③
123－021		内部不正					コントロール無			④
123－022		外部不正								⑤
123－067		自然災害								
		人為的災害								



【参考2】スコアリングによる残余リスクの測定（例）

残余リスク（評点A×B×C）

＝影響度（評点A）×発生可能性（評点B）×コントロールの有効性（評点C）

V-A. リスクに関する理論

C. コントロールのデザイン

費用対効果の分析に基づく改善策の策定

- リスク許容度の範囲内で、最も費用対効果の高いコントロールを選択する。（V-A.2）

- 識別したリスクを軽減するためのコントロールの実施は、潜在的損失よりも少なくなくてはならない。（V-E2.）

- 残余リスクが高過ぎる場合、その業務を行うべきではない。
- 残余リスクがそれほど高くない場合、そのリスクの受け入れを選択することがある。（V-A.3）

V-A. リスクに関する理論

D. リスクマネジメント（モニタリングと修正）

- 経営者は、リスクの状況をモニタリングして変化する状況に適合させるため、必要な修正を行う （V-A.2）

- 経営者は、リスクマネジメントおよびコントロールプロセスに対して責任を負う。 （V-A4.）

  ⇒ 有効なリスクマネジメントの構築は経営者の責任

- 内部監査人は、リスクマネジメントおよびコントロールプロセスの妥当性および有効性について、検査、評価、報告し、また改善提案を行うことで、経営者を支援する。 （V-A4.）

V-B. リスクモデル／フレームワーク

- COSO「内部統制の統合的枠組み」（1992年）は、内部統制を定義し、その構成要素を説明し、統制システムの評価を可能にする基準を提供。（V-B.）
  - COSO「内部統制の統合的枠組み」は、内部統制のフレームワークのデファクト・スタンダードとなった。
- COSO「ERMフレームワーク」（2004年）は内部統制のフレームワークとして、コントロール重視からリスク重視へと進展したものと言われている。
  - ERMは、経営者がリスクに満ちた環境の中でより効果的に事業を運営することを可能にする。（V-B.）
  - ERMは、事業体のミッション/ビジョンに合わせた目的を設定するためのプロセスを整備し、また、その目的が事業体のリスク選好に合致していることを確実にする。（V-B.）

V-B. リスクモデル／フレームワーク

COSO「内部統制の統合的枠組み」

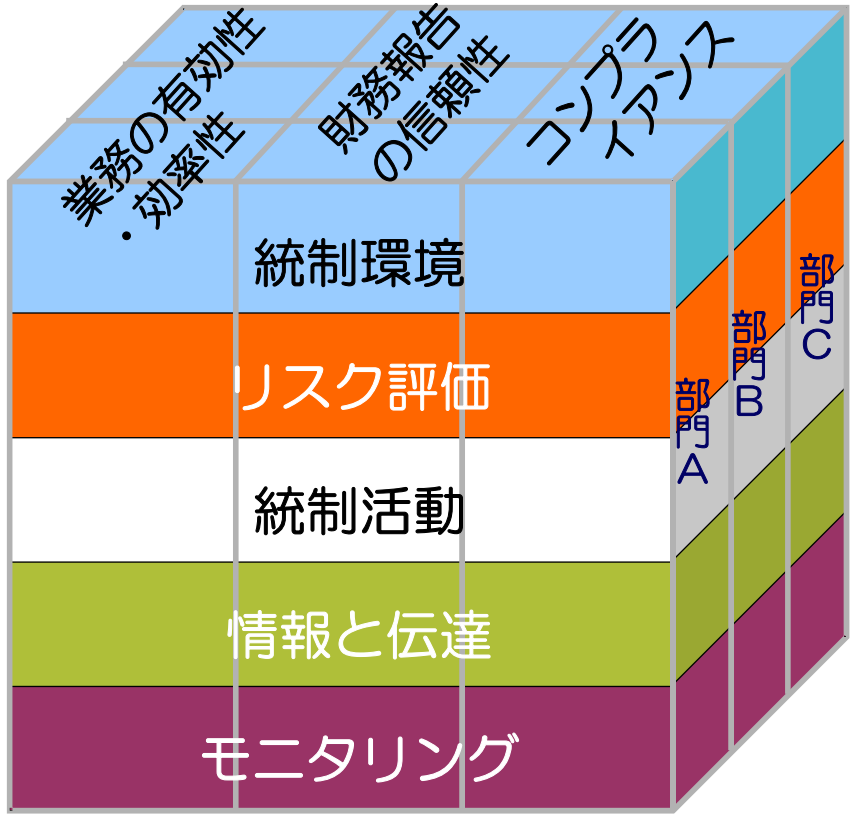
（COSO：The Committee of Sponsoring Organizations of the Treadway Commission <トレッドウェイ委員会組織支援委員会>）

内部統制の目的

1. 業務の有効性・効率性
2. 財務報告の信頼性
3. コンプライアンス

内部統制の構成要素

1. 統制環境
2. リスク評価
3. 統制活動
4. 情報と伝達
5. モニタリング（監視活動）



V-B. リスクモデル／フレームワーク

COSOの全社的リスクマネジメント(ERM)フレームワーク

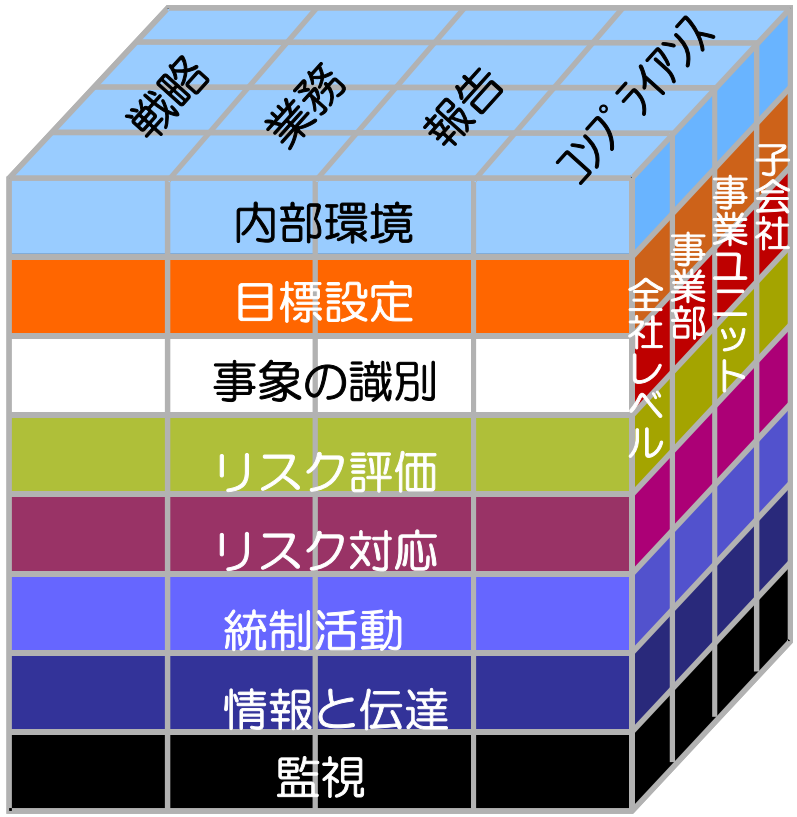
（ERM：Enterprise Risk Manegement）

事業体の目的

1.戦略目的
2.業務目的
3.報告目的
4.コンプライアンス

内部統制の構成要素

1.内部環境
2.目的の設定
3.事象の識別
4.リスク評価
5.リスクへの対応
6.統制活動
7.情報と伝達
8.モニタリング（監視活動）



V-B. リスクモデル／フレームワーク

（V-A.C.D.E.）

内部監査のパラダイムの変化

（V-C.）

統制／コントロールベースの監査からリスクベースの監査へ

特性	旧	新
内部監査の重点	内部統制	事業リスク
内部監査の対応	受動的、事後的、非継続的、戦略策定のオブザーバー	協力的、同時的、継続的モニタリング、戦略策定への参加者
リスクアセスメント	リスク要因	シナリオ計画
内部監査テストの対象	重要なコントロール	重要なリスク
内部監査の方法	細かいコントロールのテストの完全性に重点	対象とする全社的事業リスクの重要性に重点
内部監査	内部統制	リスクマネジメント
改善提言	強化 費用対効果 効率的／効果的	リスクの回避／多様化 リスクの共有／移転 リスクのコントロール／許容
内部監査報告書	機能のコントロールに言及	プロセスリスクに言及
組織における内部監査の役割	独立した評価の機能	統合リスクマネジメントおよびコーポレートガバナンスの検査・評価・改善の機能

CSAの活用①：リスクマネジメント　（V-A.）

- CSAは、経営者（管理者）および内部監査人が、組織のリスクマネジメントおよびコントロール・プロセスの妥当性を評価するために利用可能な手法である。

- CSAを定期的に更新することで、現在のリスクを適切に処理し、新たなリスクを的確に識別・検討することができる。（V-C.）
- 急速な変化が進行し、または新たなリスク・エクスポージャーに直面している分野において、CSAはリスクの識別に 重要な役割を果たす。（V-A4.）
- CSAは、内部統制の強化を求める新たな法令・規則への対応にも役立ちうる。（V-C.）
- CSAは、従業員と管理者間のコミュニケーションを向上させる手段となる。（V-A4.）

CSAの活用②:リスクベース監査 （V-A.C.D.E.）

リスクベース監査

（V-D.）

- リスクベース監査では、業務・プロセスの目的とリスクの関係を勘案して、リスクの高い領域（業務・部門）にフォーカスする。
- リスクにフォーカスすることで、限られた監査資源の下で、監査の効率性および有効性を高めることを目的とする。
- コントロールにフォーカスすると被監査部署との間で対立関係が生じがちであるが、リスクにフォーカスすることにより、対立関係が緩和される。
- リスクにフォーカスすることで、監査目的の設定から、予備調査、実査、監査報告書の作成までの監査プロセスが一貫性を持つ。
- 業務・プロセスの目的やリスクの観点から、経営者と同じ目線で、監査を行うため、監査報告書や改善提案がより有用なものとなる

CSAの活用②:リスクベース監査

【参考】内部監査におけるCSAの活用ポイント(例)