

www.pwc.com/jp

リスクアペタイト・フレームワークと 3線モデルの構築

PwCあらた有限責任監査法人
辻田 弘志

2018年7月11日

本資料の記載は、PwCあらた有限責任監査法人の見解を表しているものではありません

内容

1. リスクアペタイト・フレームワーク
2. 3つのディフェンスラインによるリスク管理能力の強化理
3. 参考資料

リスクアペタイト・フレームワーク

1

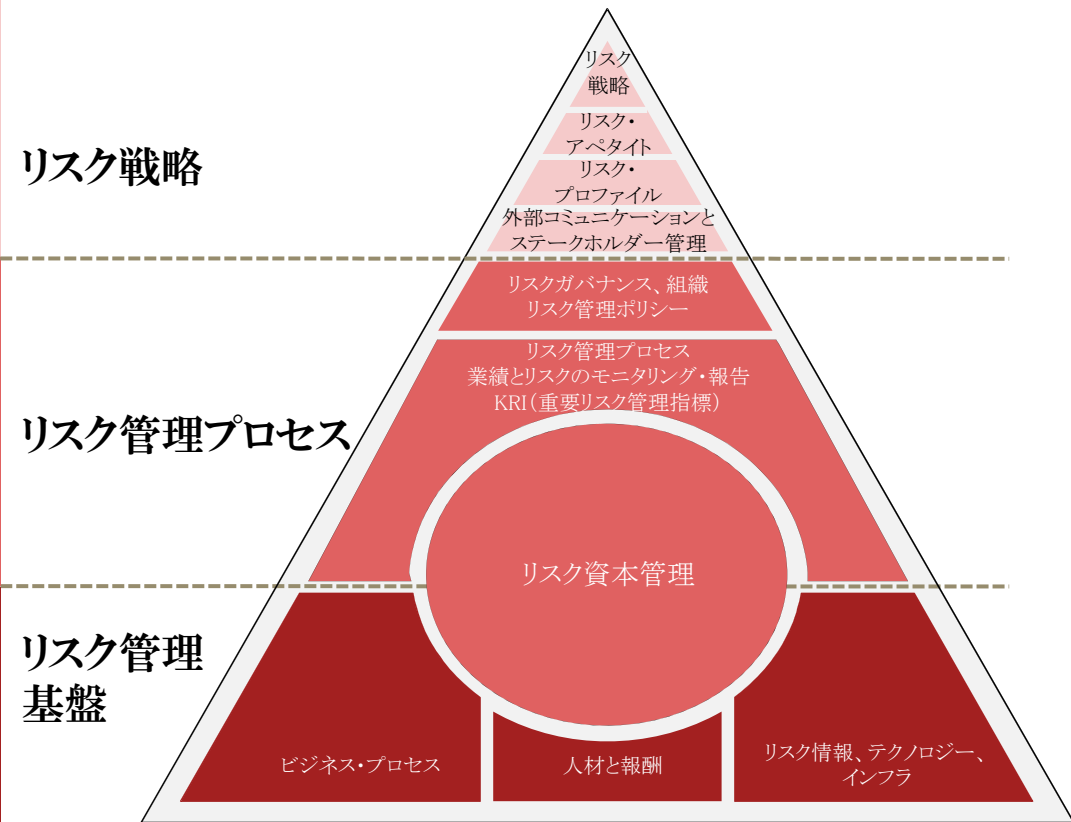
リスクガバナンスフレームワーク

以下は、PwCが考えるリスクガバナンスのフレームワークを表したもの。

リスクマネジメントにおいて達成すべき事項

- 01 リスク戦略
- 02 会社としてのコミットメント
- 03 リスク・アペタイト
- 04 リスク・プロファイル
- 05 ステークホルダー管理
- 06 リスク管理組織
- 07 リスク・ポリシー
- 08 モニタリングと報告
- 09 KRI(重要リスク評価指標)
- 10 リスク・モデリング
- 11 リスク分析
- 12 リスク管理プロセスのビジネス・プロセスへの統合
- 13 リスク・カルチャー
- 14 評価・報酬体系
- 15 トレーニング
- 16 情報システム

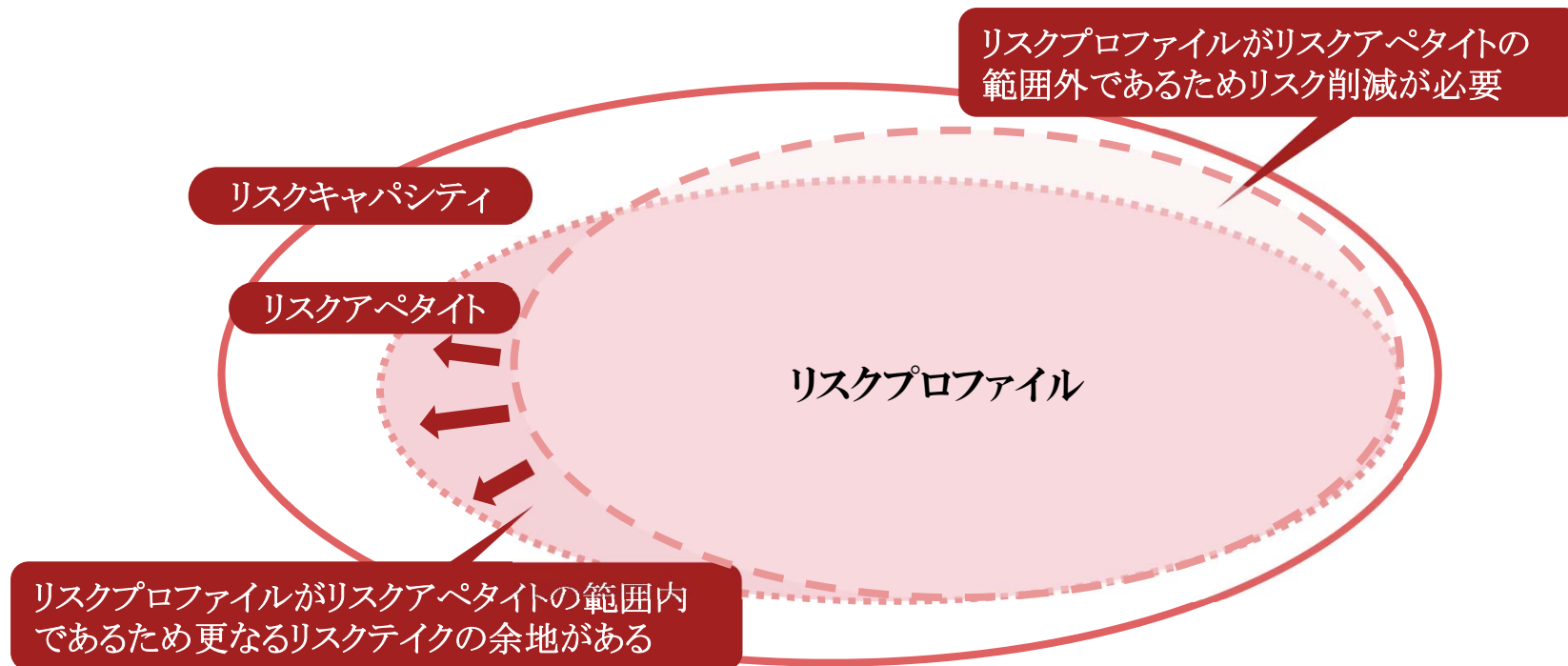
リスク管理態勢の全体像



リスクアペタイトとは

リスクアペタイトとは、組織の目的や事業計画を達成するために、進んで受け入れるリスクの種類・量を明示したものである。リスクアペタイトとは、リスクに対して受動的な対応ではなく、組織自らが望ましい形として能動的に定義していくものである。

【リスクアペタイトと他概念の関係整理】



リスクキャパシティ: 組織が許容できる最大リスク量

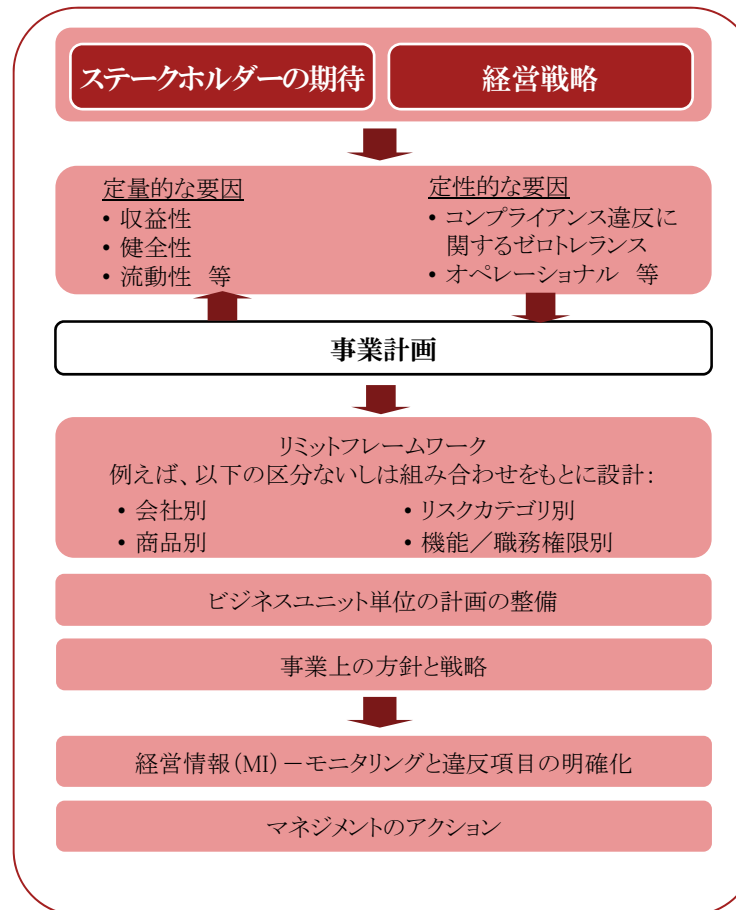
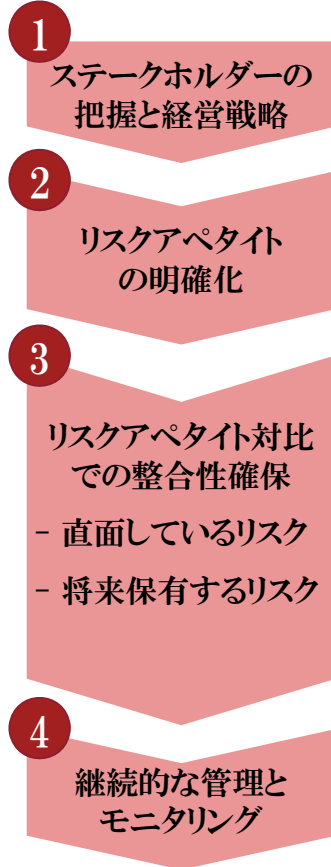
リスクアペタイト: 組織の目的や事業計画を達成するために、進んで受け入れるリスクの種類・量

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・量

リスクアペタイト・フレームワークとは

リスクアペタイト・フレームワーク(RAF)とは、リスクアペタイトを基本としたリスク認識の共有、モニタリングそしてアクションを実現することを目的とした一連の仕組みを指す。

【リスクアペタイト・フレームワーク】



- 主要なステークホルダーの特定と期待の明確化
➢ リスクの性質および程度の把握
- ステークホルダーの期待および経営戦略と整合した全社(グループ)レベルにおけるリスクアペタイトステートメントの設定
- リスクアペタイトの全社(グループ)および各部門別の計画への反映
- リスクアペタイトを各事業に展開するための適切なリミットフレームワークの構築
- 例えば、ゼロトレランス基準を組み込むための管理プロセスおよび方針の策定
- リスクアペタイトと整合的に設定した閾値やリミットに対するリスクの定期的なモニタリング
- ステートメントの抵触が起こる前に確実にマネジメントアクションがとられること

リスクアペタイト・フレームワークの整備

～①ステークホルダーの把握と経営戦略～

① ステークホルダーの把握と経営戦略

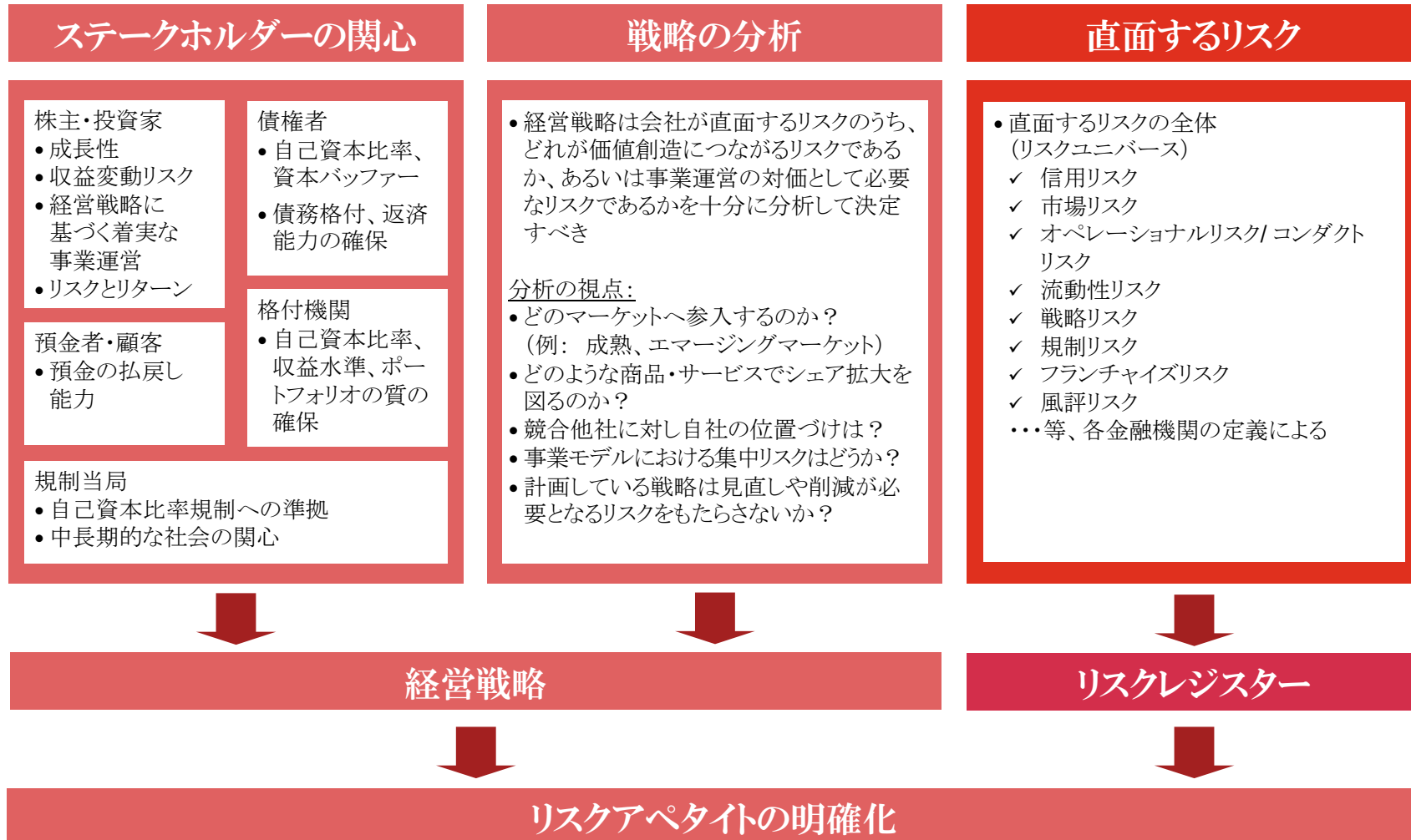
- ✓ リスクアペタイトとは、ステークホルダーの期待を分析し、対応する経営戦略を具現化・明確化したもの、つまり、リスクの観点からみた戦略目標の設定という側面を持つ。
- ✓ 自社を取り巻く主要なステークホルダーを特定し、彼らの要求・期待を明確にする

各ステークホルダーが互いに相反する要求や期待を持っていることに留意すべきである。
例えば、株主、債権者、監督当局、顧客、格付機関の要求・期待として次が挙げられる。

- 株主の期待:資本の効率性、成長・収益・収益の持続性、そして収益の変動に関するリミット
 - 債権者の期待:目標とする債務格付けの維持と債務弁済能力
 - 格付機関、監督当局、顧客(預金者)の期待:資本の充実性、預金払戻し・貸出能力 等
- ✓ 主要なステークホルダーにとって重要な指標を勘案し、戦略的にとるリスクを、自社が直面するリスクを洗い出した「リスクレジスター」をもとに把握し、リスクアペタイトとして整理する。
 - ✓ リスクアペタイトの設定は、平常時・危機時(ストレス時)の観点、短期(期間1年)・長期の観点で捉えることで、リスクに対する姿勢をより多面的に定義することが可能となる。

リスクアペタイト・フレームワークの整備 ～①ステークホルダーの把握と経営戦略～

【ステークホルダー、戦略、リスクアペタイトの関係】



リスクアペタイト・フレームワークの整備

～②リスクアペタイトの明確化と、リスクアペタイト・ステートメントの設定～

② リスクアペタイトの明確化と、リスクアペタイト・ステートメントの設定

- ✓ ステークホルダーからの要求・期待を踏まえ、自社のリスクアペタイトを、経営戦略と整合した全社(グループ)レベルで明確化する。
- ✓ リスクアペタイト・ステートメントは、組織としてのリスクに対する基本的な認識や原則とそれらに基づく主に定量的な指標によるリスクの受容の具体的な水準を定めたもので構成する
- ✓ 定性的な観点としては、オペレーショナルリスクや会社のブランドや評判に大きく影響を与える「コンダクトリスク」に言及する例が多い。
- ✓ グループの観点で設定することが重要である。その際は、全社、各事業部門、子会社・関連会社でのリスクアペタイトの設定及び全社戦略・事業計画との整合性の確保も求められる。
- ✓ 各リスクアペタイト・ステートメントのオーナーが、グループ／個社どちらの取締役会になるかも検討する必要がある。

リスクアペタイト・フレームワークの整備

～②リスクアペタイトの明確化と、リスクアペタイト・ステートメントの設定～

リスクアペタイト・ステートメントにおける定量的指標

- ✓ 全社的な経営戦略と統合的な定量的指標を用いる。
- ✓ 全社的な銀行経営戦略の観点と代表的な定量的指標を右表に記載している。
- ✓ これらの定量的指標に対して、リスクに対する経営のスタンスを明確化し、リスクアペタイト・ステートメントに記載する。
- ✓ リスクの受容の具体的水準を定量的に表現するための方法としては大きく分けると以下の2つのアプローチが考えられる。
 - 統計的手法:過去の定量的指標の変動分析から設定する。
 - ストレスシナリオ:ストレスシナリオが顕現化した場合においても定量的指標として維持する水準を設定する。

観点	定量的指標(代表例)
収益性	株主資本利益率(ROE) リスクアセット利益率(RORA) リスク調整後収益性指標(RAROC) 収益変動性(Earnings Volatility)
健全性	自己資本比率(普通株式等 Tier1比率等) 経済資本(EC) 規制資本(RC) リスクアセット(RWA) リスク量(VaR等) 期待損失/引当金額 与信集中度 外部格付
成長性	利益成長率(粗利、純利益等)
流動性	流動性カバレッジ比率

< HSBC 出典:HSBC「Annual Report and Accounts 2017」 >

Key risk appetite metrics	Component Measure	Risk appetite	2017
Returns	Return on average ordinary shareholders' equity	≥10.0%	5.9%
Capital	Common equity tier 1 ratio – CRD IV end point basis	≥11.5%	14.5%
Loan impairment charges	Loan impairment charges as % of advances: RBWM	≤0.50%	0.37%
	Loan impairment charges as % of advances: wholesale (CMB, GB&M and GPB)	≤0.45%	0.27%

リスクアペタイト・フレームワークの整備

～②リスクアペタイトの明確化と、リスクアペタイト・ステートメントの設定～

【リスクアペタイト・ステートメント例】

ステークホルダー と期待事項

株主

- 企業価値の向上
- 配当支払 等

債権者

- 債務履行の確実性
- 格付の維持・向上 等

顧客

- 預金の安全性
- 安定的な資金調達 等

監督当局

- 金融システムの安定
- 預金者保護 等

従業員

- 雇用の確保
- 報酬 等

ステーク
ホルダー
の期待の
反映

リスクに対する基本認識と原則

XXXフィナンシャルグループは、お客様に様々なサービス、金融商品の提供を通じて、当グループの戦略であるお客様中心主義の実現を図っています。

当グループは金融機関として社会において重要な役割を担っており、法令等の遵守にとどまらずすべての社外の利害関係者に対し公正かつ透明性を確保し期待に応え、当グループの評判を維持・向上していく責任があります。当グループは、確固たる金融基盤を堅持するために、金融ストレス時を含め設定された各種リスク制限の範囲内で業務運営を行う必要があります。また、株主に対しては、株主価値の最大化を目指し利益還元を実現します。また従業員に対しても、最も魅力的な職場となるように必要な投資と環境の整備を図っていきます。

これらを実現する上で、確固たるリスク文化の醸成、3つのディフェンスラインによる役割・責任の明確化と独立したリスク監視の実現、過度なリスクテイク、リスク集中の回避、リスクを的確に把握し管理可能な状態とすることが重要です。

当グループはリスクに対する基本原則として以下の通り定めます。

(資本)

- AA格以上の格付の維持
- 規制上求められる所要自己資本比率を超える資本の維持

(収益)

- 収益源の多様化と収益の安定性の確保
- リスクとリターンバランスの確保
- ストレス時の損失の回避を可能とするリスクテイク方針

(流動性)

- 流動性の確保

(その他)

- 法令等の遵守を含む、オペレーショナルリスクの管理
- 当グループの評判やブランドを棄損する恐れのあるリスクの管理
- 競合他社対比で過度なリスクテイクの回避

リスクアペタイト・フレームワークの整備

～③リスクリミットの設定、リスクアペタイト対比での整合性確保～

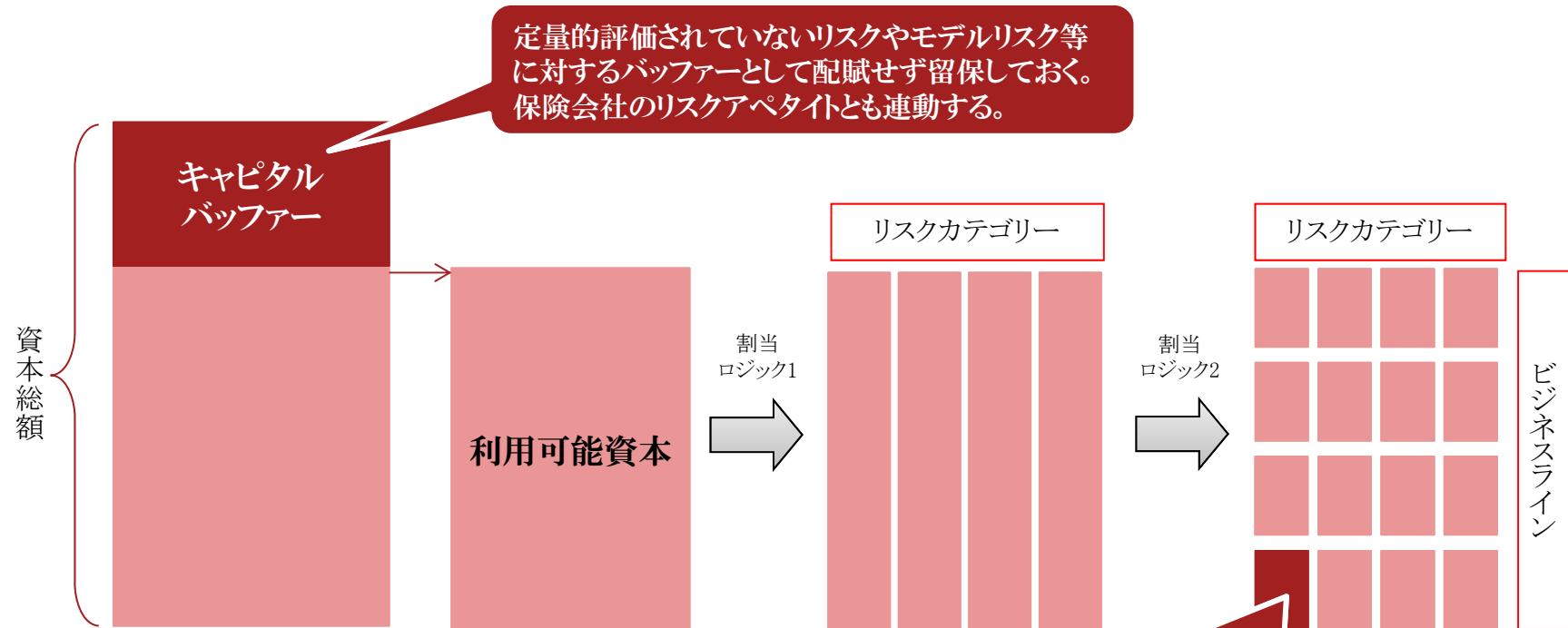
③ リスクリミットの設定、リスクアペタイト対比での整合性確保

- ✓ リスクリミットとは、リスクアペタイトの枠内で業務を運営するにあたり、各事業部門あるいは子会社・関連会社に配分された、各計測単位(リスクカテゴリ別、商品別等)で許容可能なリスク量を指す。
- ✓ リスクリミットは、会社が望む水準よりも多くのリスクを保有する状況を事前に防止するための事業上の統制となる。
- ✓ リスクリミット(定量／定性〔ゼロトレランス等〕)として、方針および手続きの策定、権限と責任部署の明確化、戦略的な計画プロセスへの組込が必要。
- ✓ リスクアペタイトを各事業に展開するため、リミット(およびフレームワーク)はどの単位で構築され定義されるかについて検討が求められる。例えば、会社別、ビジネスライン(事業ドメイン)別、リスクカテゴリー別、が挙げられる。

リスクアペタイト・フレームワークの整備

～③リスクリミットの設定、リスクアペタイト対比での整合性確保～

リスクアペタイトをリスクリミットに展開する際のプロセス概要



例えば、このセルがリスクカテゴリーとしては『信用リスク』、ビジネスラインとしては『法人』等のイメージ

リスクアペタイト・フレームワークの整備

～③リスクリミットの設定、リスクアペタイト対比での整合性確保～

【リスクリミットの設定イメージ】

リミットフレームワーク構築の観点

設定区分

- ビジネスモデル(分権的、集権的)を反映した設定
 - 会社形態/意思決定フレームワーク/マネジメント構造
- リスクの割当単位を所与
- 各リスクエクスポージャーを測定するために最適な指標(リスクの特性により異なる)
- 将来思考に基づく現実的なもの
- 例:
 - 資本
 - 収益
 - エクスポージャーリミット(特に、信用の集中リスク、カウンターパーティーリスク)

分散効果

- リスク間の分散効果の取り扱いについては、大きく3つのオプションが存在する
 - フルアロケーション
 - より低い信頼水準の設定
 - 資本保有会社

まとめ

- 各ラインがフレームワークの枠内に収まる場合には、ビジネス全体としてフレームワークの枠内に収まる

1. 定量的なリミット管理(例)

- 設定されたリミットフレームワークに基づく定量的なリスクアペタイトの展開
- 以下に示すようないくつかの単位にブレークダウンされ、管理
 - ビジネスライン(例: 割り当てられた資本の中での運営が可能な資本のレベル)
 - リスクカテゴリ(例: いくつかのビジネスラインがグループレベルで統合され管理される単位)
 - エンティティレベルでの自己資本比率規制
 - 与信集中リスク(国、業界、企業グループ 等)

2. 定性的なリミット管理(例)

- 定性的なステートメント部分についてはリスクアペタイトを以下のエリアに直接組み込むことで管理:
 - 事業方針/事業プロセス/ガバナンス構造
- 具体的な内容は以下のとおり:
 - 顧客を公平に扱わないことについてトレランスを持たない可能性
 - トレランスのレベルは、とりわけ、以下の方針およびプロセスに組み込まれる:
 - オペレーショナルリスク方針/コンプライアンス方針/オペレーショナルリスク委員会指示書/新規商品承認プロセス

リスクアペタイト・フレームワークの整備

～④継続的な管理とモニタリング～

④ 継続的な管理とモニタリング

- ✓ リスクアペタイトと整合的に設定した閾値やリミットの定期的なモニタリングはリスクアペタイトフレームワークが機能するために重要である。
- ✓ リスクアペタイト・フレームワークを実効的かつ効率的なものとして機能させるためには、日常の事業運営において、リスクアペタイト・ステートメントへの抵触が起こる前に確実にマネジメントアクションがとられることが重要である。
- ✓ モニタリングのためにリスク関連データを集計・捕捉することを「リスクデータアグリゲーション」と呼び、金融機関におけるリスク報告目的・要請に基づき、リスクアペタイトに関するパフォーマンスを計測するために、リスクデータの定義・収集・処理を行うことを指す。

(参考)トップリスクとエマージングリスクの例

重要なリスクを、トップリスクとエマージングリスクに区分して特定し、それぞれのリスクについて、必要な対応を検討している

Risk	Trend	Mitigants
Externally driven		
Economic outlook and capital flows (経済、資本市場)	▲	We actively monitor our wholesale credit and trading portfolios, including undertaking stress tests, to identify sectors and clients that may come under stress due to economic conditions in the eurozone, mainland China and in the UK as negotiations to exit from the EU continue.
Geopolitical risk (地政学リスク)	▲	We continually assess the impact of geopolitical events on our businesses and exposures, and take steps to mitigate them, where required, to help ensure we remain within our risk appetite. We have also strengthened physical security at our premises where the risk of terrorism is heightened.
● The credit cycle (信用(景気環境)サイクル)	▶	We continue to undertake detailed reviews of our portfolios and are proactively assessing customers and sectors likely to come under stress as a result of geopolitical or macroeconomic events, reducing limits where appropriate.
Cyber threat and unauthorised access to systems (サイバーセキュリティ)	▲	We continue to strengthen our cyber control framework and implement initiatives to improve our resilience and cybersecurity capabilities, including threat detection and analysis, access control, payment systems controls, data protection and backup and recovery.
● Regulatory, technological and sustainability developments including conduct, with adverse impact on business model and profitability	▶ (規制環境、テクノロジー、サステナビリティ、コンダクト)	We proactively engage with regulators wherever possible to help ensure new regulatory requirements are effectively implemented, and work with them in relation to their investigations into historical activities. We also engage with non-governmental organisations to help ensure our policies address environmental concerns.
Financial crime risk environment (金融犯罪、マネロン)	▶	We continue to develop and enhance the Financial Crime Risk function and augment our risk management capabilities to further improve our financial crime detection and compliance capabilities. We will continue to take steps to enhance our defences against financial crime across our operations globally to help ensure our Global Standards are sustainable over the long term.

Risk	Trend	Mitigants
Internally driven		
IT systems infrastructure and resilience (IT、BCP)	▶	We continue to monitor and improve service resilience across our technology infrastructure, enhancing our problem diagnosis/resolution and change execution capabilities, reducing service disruption to our customers.
Impact of organisational change and regulatory demands on employees (組織変更リスク)	▶	We continue to focus on resourcing and employee development to meet regulatory changes as well as to maintain and enhance our leadership succession strength.
Execution risk (戦略実行リスク)	▶	The Group Change Committee oversees the progress of the highest priority programmes, underpinning the implementation of our strategic actions to help ensure that we achieve a consistent on time, on budget and on quality delivery across these critical initiatives.
● Risks arising from the receipt of services from third parties (委託先管理リスク)	▶	We have strengthened essential governance processes and relevant policies relating to how we identify, assess, mitigate and manage risks across the range of third parties with which we do business. This includes control monitoring and assurance throughout the third-party lifecycle.
Enhanced model risk management expectations (モデルリスク)	▶	We have strengthened our model risk management framework by establishing an independent second line of defense Model Risk Management sub-function, and we continue to enhance our existing policy and standards in order to address evolving regulatory, external and internal requirements.
Data management (データ管理)	▲	We continue to improve our insights, consistency of data aggregation, reporting and decisions through ongoing enhancement of our data governance, data quality and architecture framework.

出典: HSBC 「Annual Report and Accounts 2017」

- ▲ Risk heightened during 2017
- ▶ Risk remained at the same level as 2016
- Thematic risk renamed during 2017

定性的なリスクに係るRAFの必要性

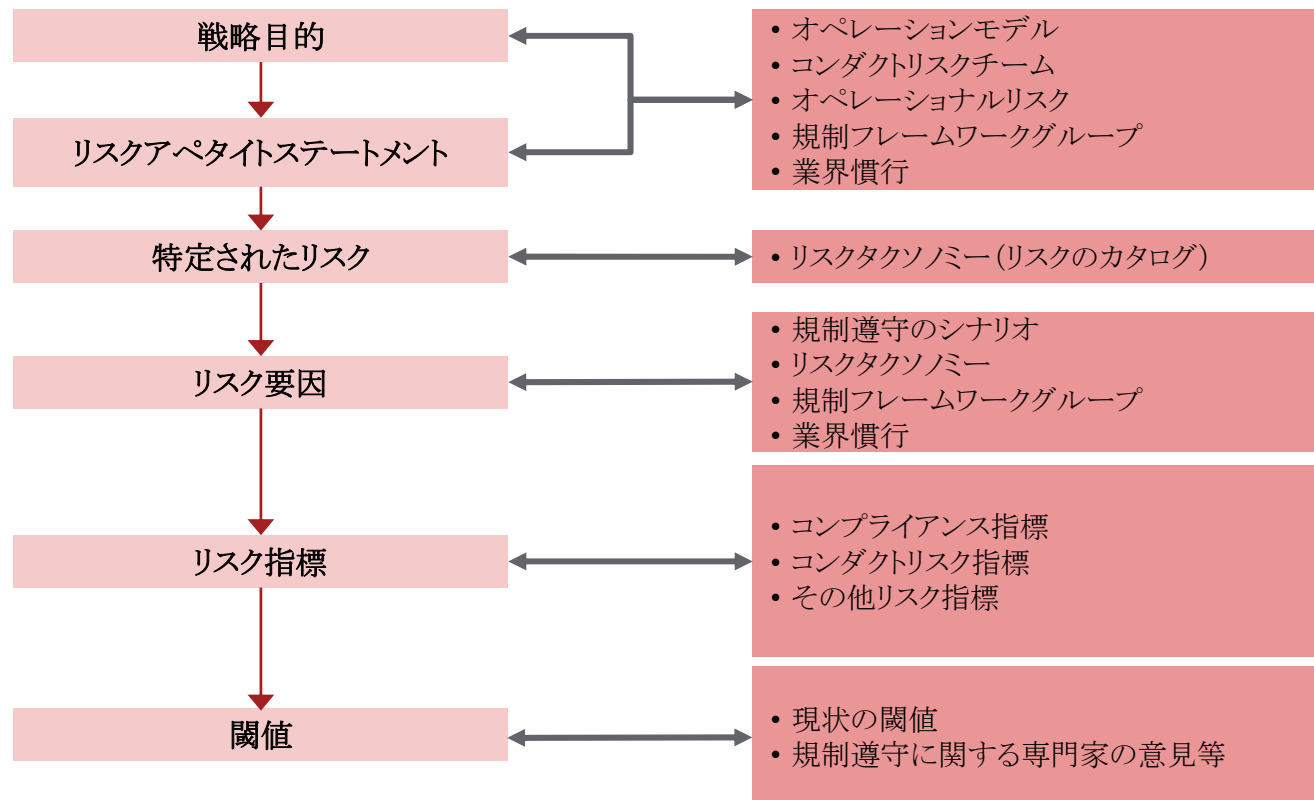
- ✓ バランスシート、収益、流動性の観点でのビジネスおよび付随するリスクについては先述の枠組みで一定程度対応できる。
- ✓ 一方、より広くリスクを捉えると定性的なリスクに係るリスクアペタイトを設定し管理する仕組みの構築が必要となる。
 - ビジネスモデルに係る組織や人の行為(コンダクト)に係るリスク
 - 銀行証券連携モデル、県域を超えた新たな顧客層の開拓モデル
 - オペレーティングモデルに係るオペレーショナルリスク
 - FinTechの取り込みに係る新たなリスクへの対応(サイバーリスク、委託先に係るリスク等)
- ✓ 上記は最終的にはカルチャー(企業風土)の問題に起因することが多い
 - リスクガバナンス、3LoDによる対応

定性リスクアペタイトフレームワークの例

最上位の構成要素である戦略目標や定性的なステートメントに基づき、特定されたリスク及びそれに関連するリスク要因、さらにはそれらを測定するための指標や閾値が設定されるような枠組みとなっている。

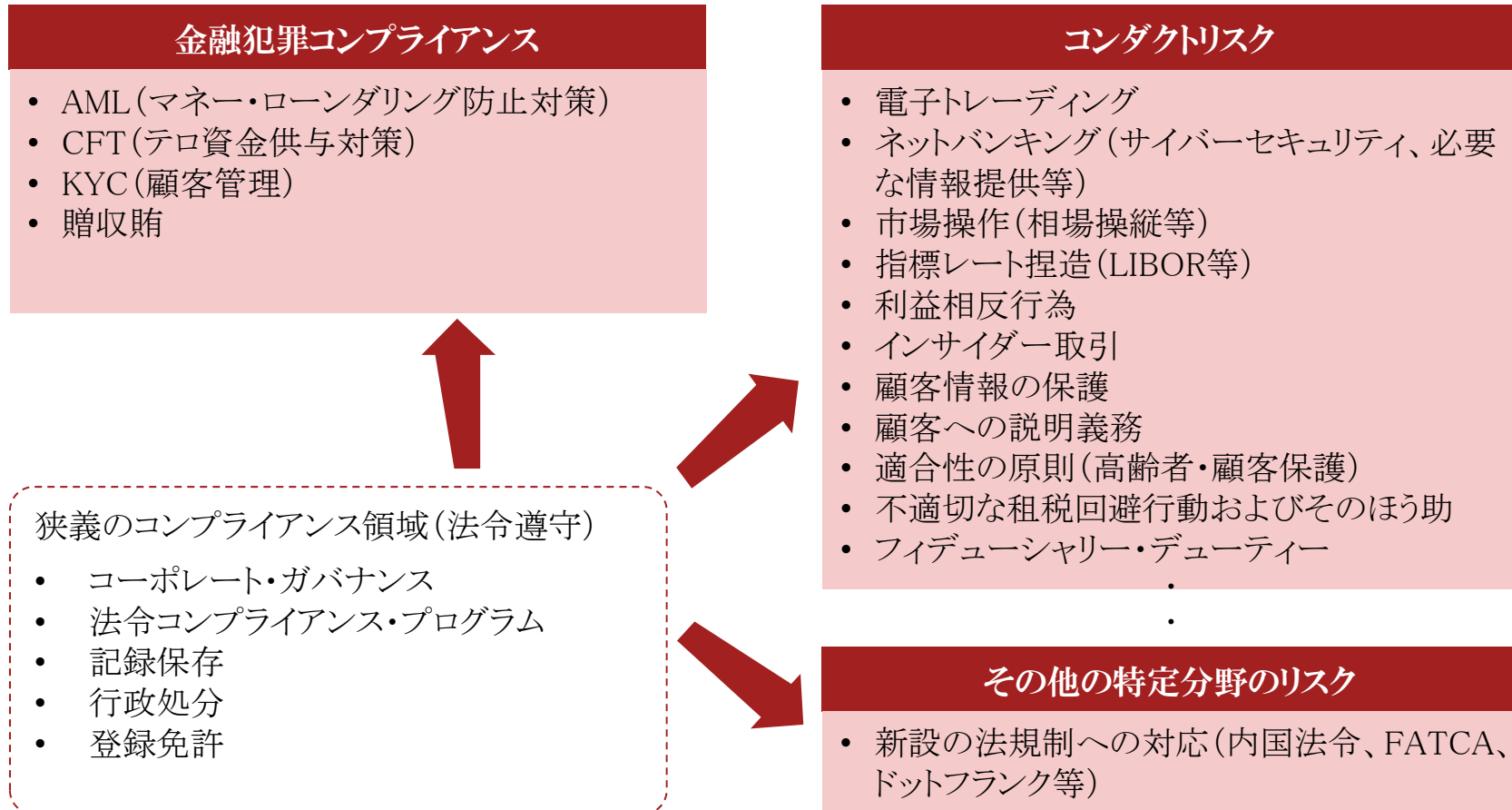
リスクアペタイト・フレームワークの構成要素

インプット



(参考) 金融機関における「コンダクトリスク」

【金融機関のリスク分類におけるコンダクトリスクの例】



定性的な管理指標

定性的なリスクアペタイトは、オペリスクやコンプライアンスに限らず、組織や人の行為に係るリスク(コンダクトリスク)までを考慮したものとして検討し位置づけるべきである。

- 事業拡大・収益獲得を目的とした企業行動(コンダクト)の結果として、自社のレピュテーション(評判)やブランド価値を毀損しうるリスクの考慮

近年の金融機関を取り巻く状況

- マイナス金利政策による収益悪化
- 手数料ビジネス収入への依存度の高まり

考えうるリスク顕在化の要因例

- 業績プレッシャーによる不正融資
- 顧客ニーズを無視した投信販売

必要となるリスクアペタイト

- 【定量】 投信販売の収益性に係るもの、特定顧客・特定商品の販売割合
- 【定性】 自社グループのガバナンスやカルチャーとの整合性、外部からの評判、等に関するもの

リスクアペタイト・フレームワークにおける役割・責任

リスクアペタイト・フレームワークが実効的に機能するためには、各レベルの担う役割・責任が明確に定義されることが重要である。この役割・責任については、金融安定理事会 (FSB) から原則案が示されており、金融機関における一つのモデルになると考えられる。

【各レベルが担う主要な役割・責任】

主要な役割・責任	取締役会	CEO	CRO	CFO	業務部門の長等	内部監査
リスクアペタイト・フレームワークの構築	●					
リスクアペタイト・ステートメントの承認	●					
リスクアペタイトと業務計画や報酬制度との整合性の確保	●					
リスクアペタイトの開発		●	●	●		
リスクアペタイト・フレームワークの健全性に関する取締役会への説明責任		●	●	●		
リスクアペタイトに関する基本姿勢の提示		●				
リスク・リミットの設定、モニタリング及び取締役会への報告			●			
リスク・プロファイルのモニタリング及び取締役会への報告				●		
計画、報酬、意思決定プロセスとリスクアペタイトとの整合性の確保					●	
リスクアペタイト・ステートメント、リスクリミットの業務活動への展開					●	
リスクアペタイト・フレームワークに対する独立した評価						●

3つのディフェンスラインによるリスク管理能力の強化

2

3つのディフェンスラインモデル(3LoD)に関する議論

3LoDは金融機関におけるデファクトスタンダードとして確立しつつある。

3LoDに関する主な動き

健全なオペレーショナル・リスク管理のための諸原則
(バーゼル銀行監督委員会 2011年6月)

“オペリスクに関する健全なガバナンスは、3LoDに依存”

銀行の内部監査機能
(バーゼル銀行監督委員会 2012年6月)

“ビジネスユニット、管理部門、内部監査部門の関係は3LoDモデルで説明可能”

有効なリスクマネジメントとコントロールにおける3つのディフェンスライン
(内部監査協会 2012年11月)

“上級経営者と取締役会を報告先として、経営者をリスクマネジメントにおける第1線、2線が監督、3線が独立した保証を提供する3LoDを提唱”

健全なオペレーショナル・リスク管理のための諸原則」の実施状況に関するピア・レビュー結果
(バーゼル銀行監督委員会 2014年10月)

“世界20地域・60金融機関中、55金融機関が3LoDに基づく体制を構築済と回答”

銀行のためのコーポレート・ガバナンス諸原則
(バーゼル銀行監督委員会 2015年7月)

“リスクガバナンスの枠組みには、3LoDに基づき定義された組織・責任が包含されていないといけない”

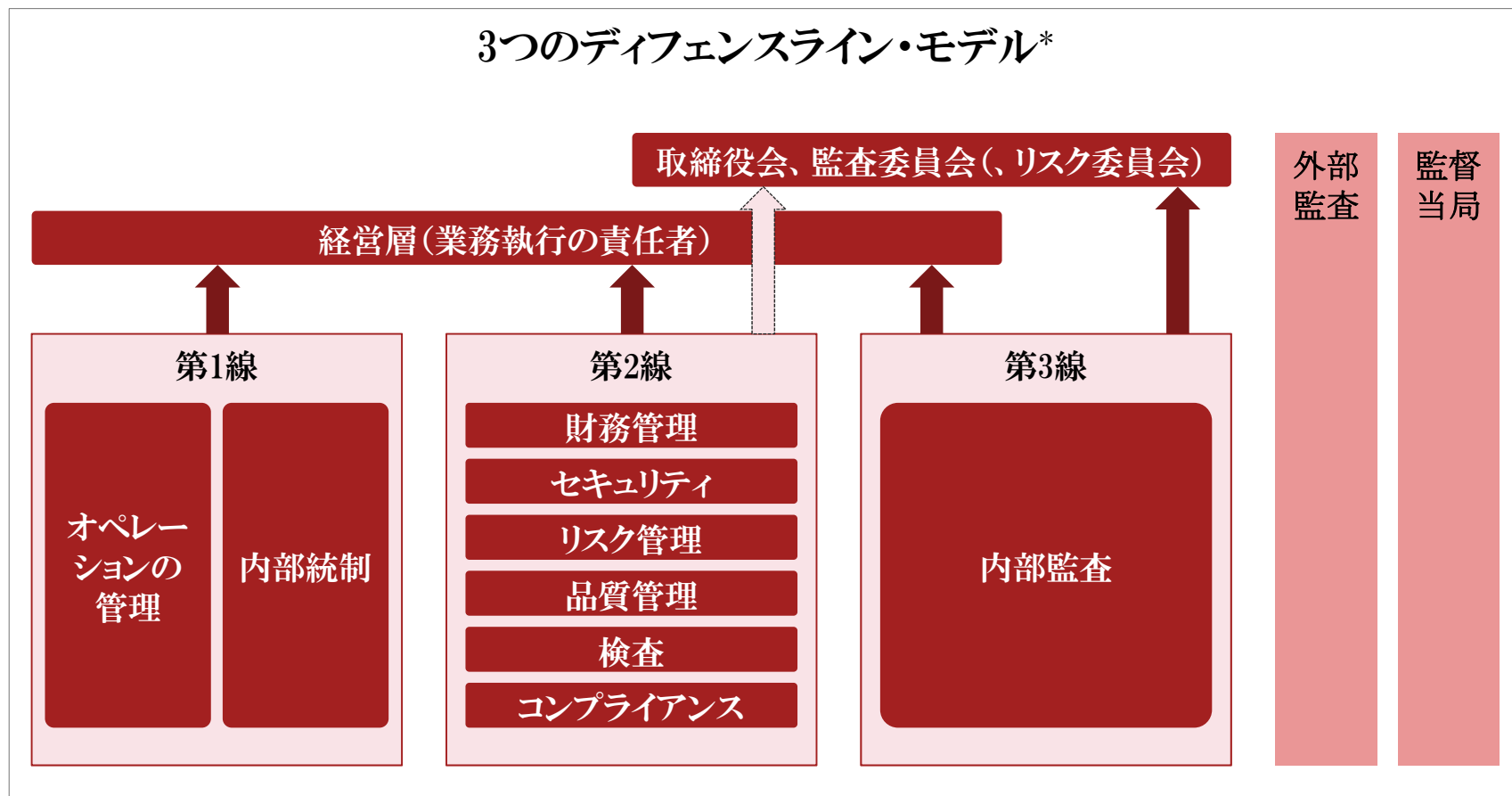
3つのディフェンスライン全体でのCOSOの活用
(内部監査協会&COSO 2015年7月)

“3LoDとCOSOの内部統制の統合的フレームワークを結び付けた内部統制に関する具体的な役割のガイダンスを提示”

特に金融分野では金融危機の反省も踏まえ、3つのディフェンスラインモデル(3LoD)は各国当局や主要機関において受け入れられてきている。

3つのディフェンスラインモデル(3LoD)とは

第1線(現場)、第2線(ミドルセクション)、第3線(内部監査)の3つのディフェンスラインに基づき組織体制を整備する考え方。3LoDに沿って組織体制を整備することで、リスク管理の複線化、牽制力の強化、および役割分担の明確化が達成される。



* 内部監査協会 (IIA) ポジションペーパー 「有効なリスクマネジメントとコントロールにおける3つのディフェンスライン(2013年1月)を基に作成

3LoDに一般的に期待される効果

3LoDの導入によりリスク管理の責任が明確化・前線化され、より適時かつ予防的なリスク管理が期待される。

テーマ	期待される効果
役割・責任	<ul style="list-style-type: none">・ リスクオーナーシップの明確化（一義的な責任は1線）・ 各ディフェンスライン（部門）のリスク・コントロールにおける役割・責任の明確化
牽制機能	<ul style="list-style-type: none">・ リスクオーナーに対する牽制機能の強化（第1線に対して1線内、2線、3線と3重に牽制）・ 主に第3線を通じた取締役会・監査委員会の牽制強化
リスクコミュニケーション	<ul style="list-style-type: none">・ 各ディフェンスラインからのリスク情報の伝達経路を確保（経営がリスク情報を認識できる選択肢・機会の増加）・ 第1線による自律的統制を通じたリスクの早期捕捉と対応
組織体制	<ul style="list-style-type: none">・ 内部統制機能に関して重複や漏れを排除した効率的・効果的な組織設計（アシュアランスマップの確立）

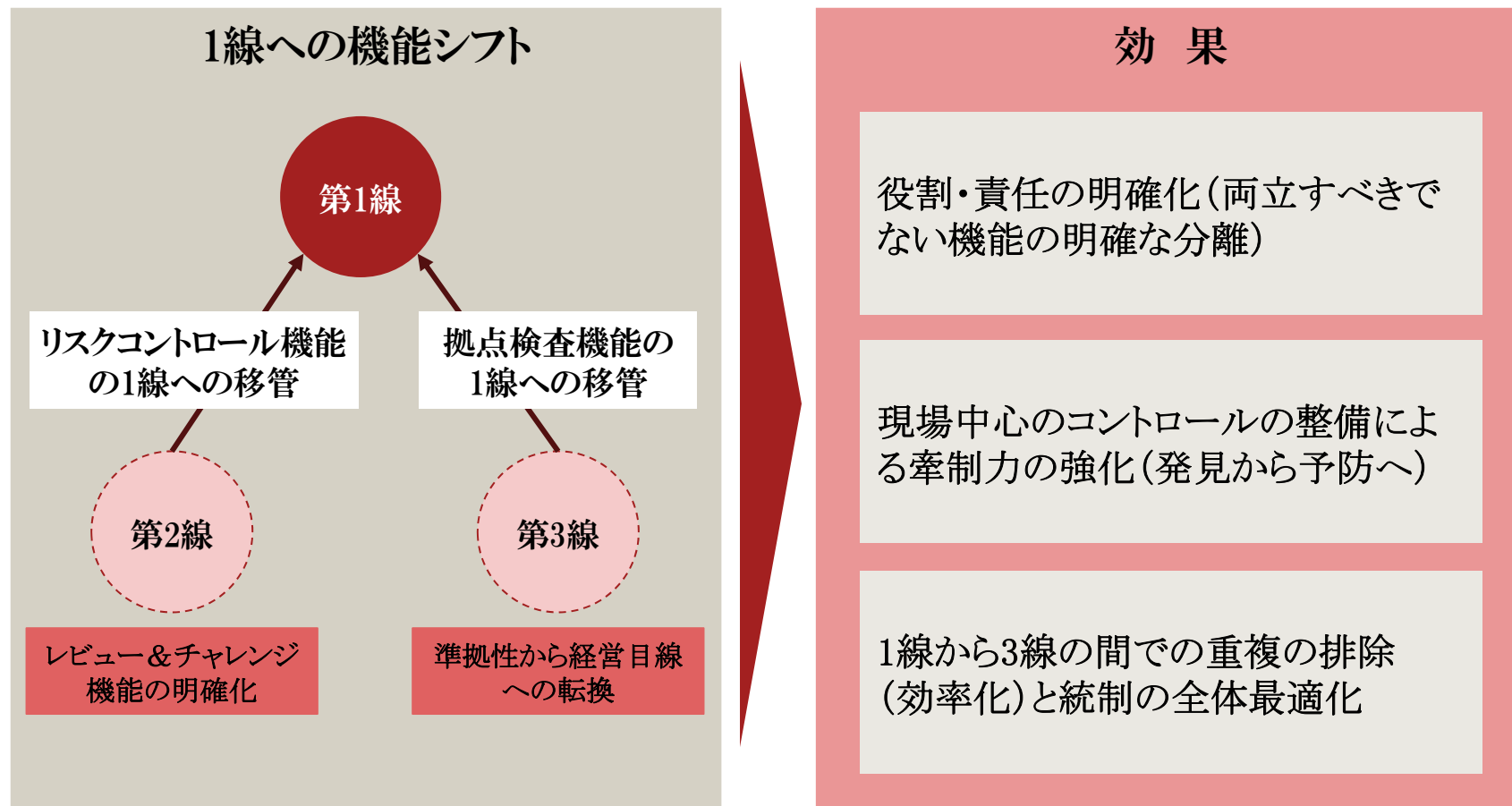
3LoDにおける1-3線の役割・責任

リスク管理の一義的な責任は第1線にあり、リスクオーナーとしての責任を自覚することが重要。

第1のディフェンスライン	第2のディフェンスライン	第3のディフェンスライン
リスクオーナーとして リスクコントロールを行う	リスクに対する監視を行う	合理的な保証を提供する
役割・責任 <ul style="list-style-type: none">日々の業務でリスクの特定及び必要な統制手続きを行う業務の方針や手続きの設計およびその維持、改善を行うリスク事象から生じた結果に対する責任を負う	役割・責任 <ul style="list-style-type: none">執行部門から独立した立場でリスクとその管理状況の監視を行う業務執行部門に対し、リスク管理上のアドバイスを提供するリスク管理フレームワークの設計およびその維持、改善を行う	役割・責任 <ul style="list-style-type: none">業務執行部門、リスク管理部門等から独立した立場から、リスク管理機能及び内部統制システムについて取締役会(監査委員会)に対し合理的な保証を与える
主たる部門 業務執行部門	主たる部門 リスク管理部門 コンプライアンス部門	主たる部門 内部監査部門
主たるレポート先 最高業務執行責任者 最高財務責任者	主たるレポート先 最高リスク管理責任者 最高コンプライアンス責任者	主たるレポート先 取締役会(監査委員会)

第1線への機能シフト(自律的統制)の効果

第1線への機能シフトにより組織全体の内部統制の強化(発見から予防的統制)が実現でき、2線と3線も本来担うべき役割・機能が明確になる。



1-3線の機能に関する大手金融機関の対応

(金融庁：金融モニタリングレポート2015年を参考)

第1線の自己評価や第2線によるモニタリング機能の強化等により、自律的統制を推進。従前、第3線が実施していた営業店に対する準拠性等検証を第1線、第2線に移行のうえ、第3線の監査資源を高リスク分野に重点配分。金融機関においては、複雑な業務から生じるリスクを従前のように各リスクカテゴリーの担当部門を中心に管理することの限界を認識。リスク管理に携わる各部門の役割・責任を見直す動きがみられる。

3LoDが有効に機能するための条件

3LoDが有効に機能するための条件は何か

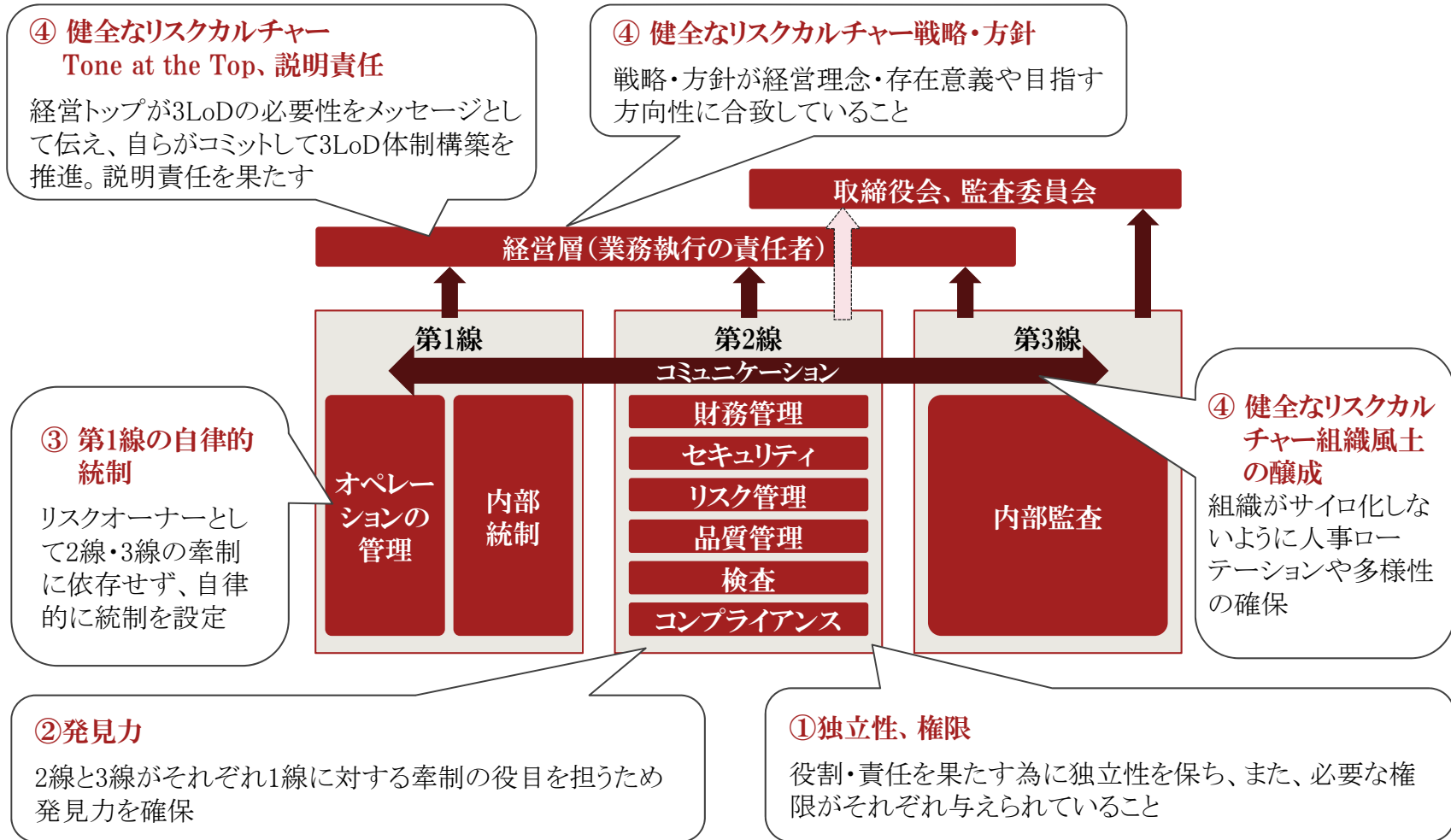
- ▶ 取締役会・監査委員会による監督
- ▶ 経営トップの基本理念 (Tone at the top)
- ▶ 説明責任
- ▶ 戦略・方針の適切な設定
- ▶ 役割・責任
- ▶ 牽制、独立性を担保する権限
- ▶ コミュニケーション、情報取得
- ▶ 報酬、評価

Wells Fargo (独立取締役による調査報告書より)

- ① Decentralized corporate structure (部門の経営は部門長任せ)になっていた。また、リスク管理および人事についても、現場中心の管理体制となっていた。
- ② 過度な業績プレッシャー、業績偏重の報酬・人事評価制度のもと、業績目標達成のために、350万近くの口座が顧客の同意なく開設された。
- ③ 経営陣は、2013年Los Angeles Times誌に報道されるまでに、適正販売における問題は重要リスクとして認識しなかった。(CEOは、1%の販売員が販売資格停止処分を受けたことについて、99%の販売員は適正販売を行っていると捉えていた。また、リテール部門の離職率は40%以上となっていたことについても、金融業界以外のリテール業界と比べて決して高くないことから、リテールビジネスの特性によるものと解釈した。)
- ④ 部門長は違う意見を聞かない独断的な人物であった。また、2線に対して情報を隠そうとしていた。
- ⑤ Chief Regional Risk Officerの報告ラインは部門長であり、Chief Operational Risk Officer (CORO) にドットラインを持っている。しかし、COROはセールスプロセスや報酬の問題は1線、及び人事部、法務部の所管であり、自分の所轄外だと認識していた。また、年間1000件の販売員資格停止が発生していることを知っていたにもかかわらず、それは大した数字ではないと思っていた。結果、セールス問題をA&E委員会 (Audit & Examination Committee) に報告しなかった。
- ⑥ CROや本社人事部は、現場に対して、直接的なレポートラインや、指令権を一切持っていなかった。そのため、セールスプロセスに問題があると気づいたとしても、それはどこまで蔓延しており、どれほど深刻な問題になっていたか分からなかった。2012年、CROは部門長にセールス品質や、離職率についてERMC (リスク委員会) で報告させようとしたが、結局拒否されたり、中身の無いプレゼンされたりして情報を把握できなかった。
- ⑦ 内部監査は、プロセスの実施状況のテストにフォーカスしており、リスクの根本原因についての調査は行っていない。リスクの真因の特定は1線で行うべきとの認識を持っていた。問題が発生した期間において、「セールスプラクティス」、「カルチャー」に関する監査成績は「良好」であった。

過去事案から見る3LoDが有効に機能するための条件

- ① 組織の独立性・権限、② 第2線・第3線の発見力、③ 第1線の自律的統制、④ 健全なリスクカルチャーが重要。



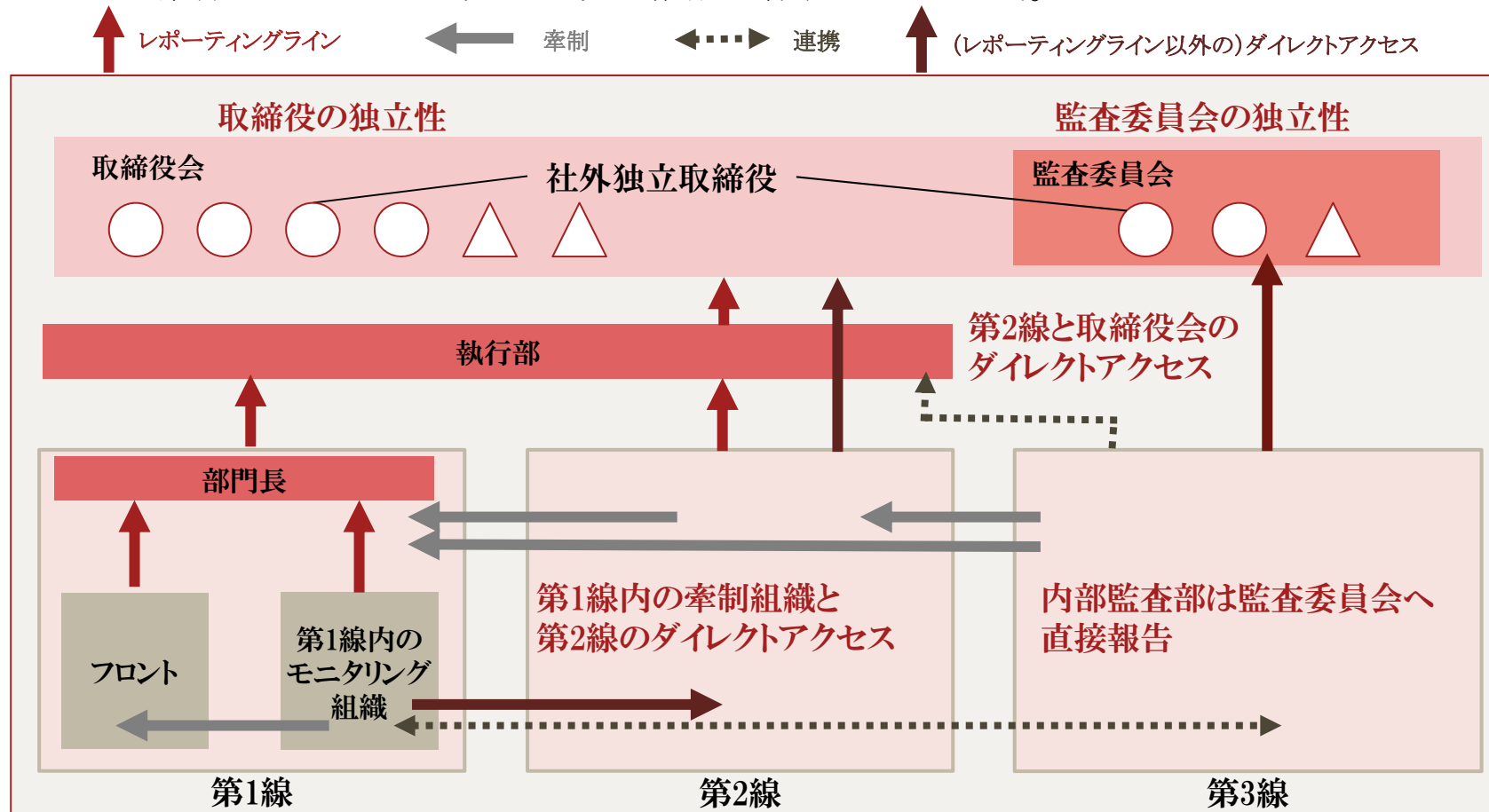
参考資料:3LoDが効果を発揮するための条件

3

3LoDが効果を発揮するための条件

① 組織の独立性・権限

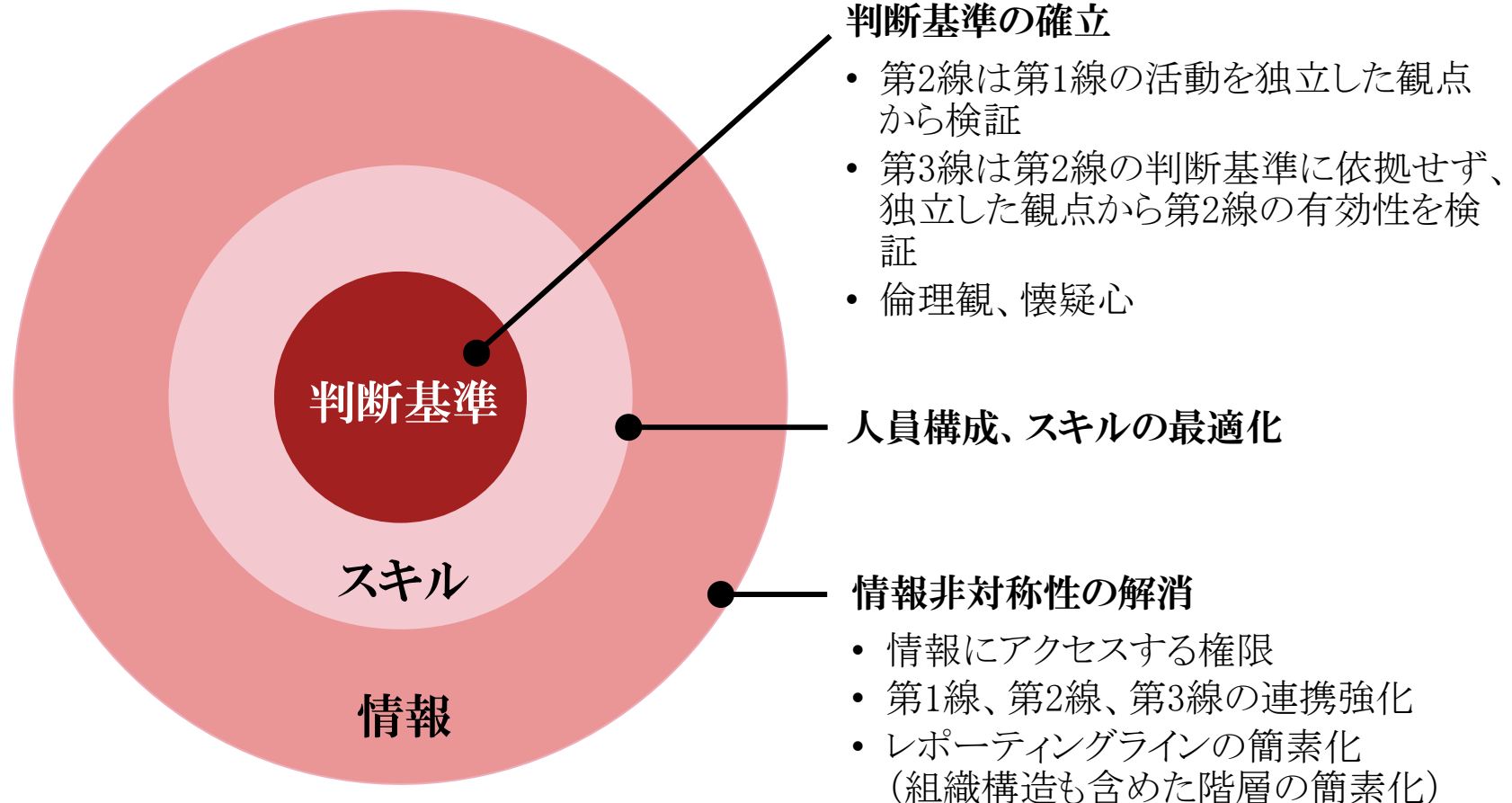
各機能の独立性を担保し牽制機能を発揮するためには、権限を有する先へのレポーティングラインの確保およびレポート先が適切な権限を有することが重要。



3LoDが効果を発揮するための条件

② 第2線・第3線の発見力

第2線、第3線が実効性ある発見力を具備するためには、判断基準、人員(質・量)、情報が充足される必要がある。



3LoDが効果を発揮するための条件

③ 第1線の自律的統制

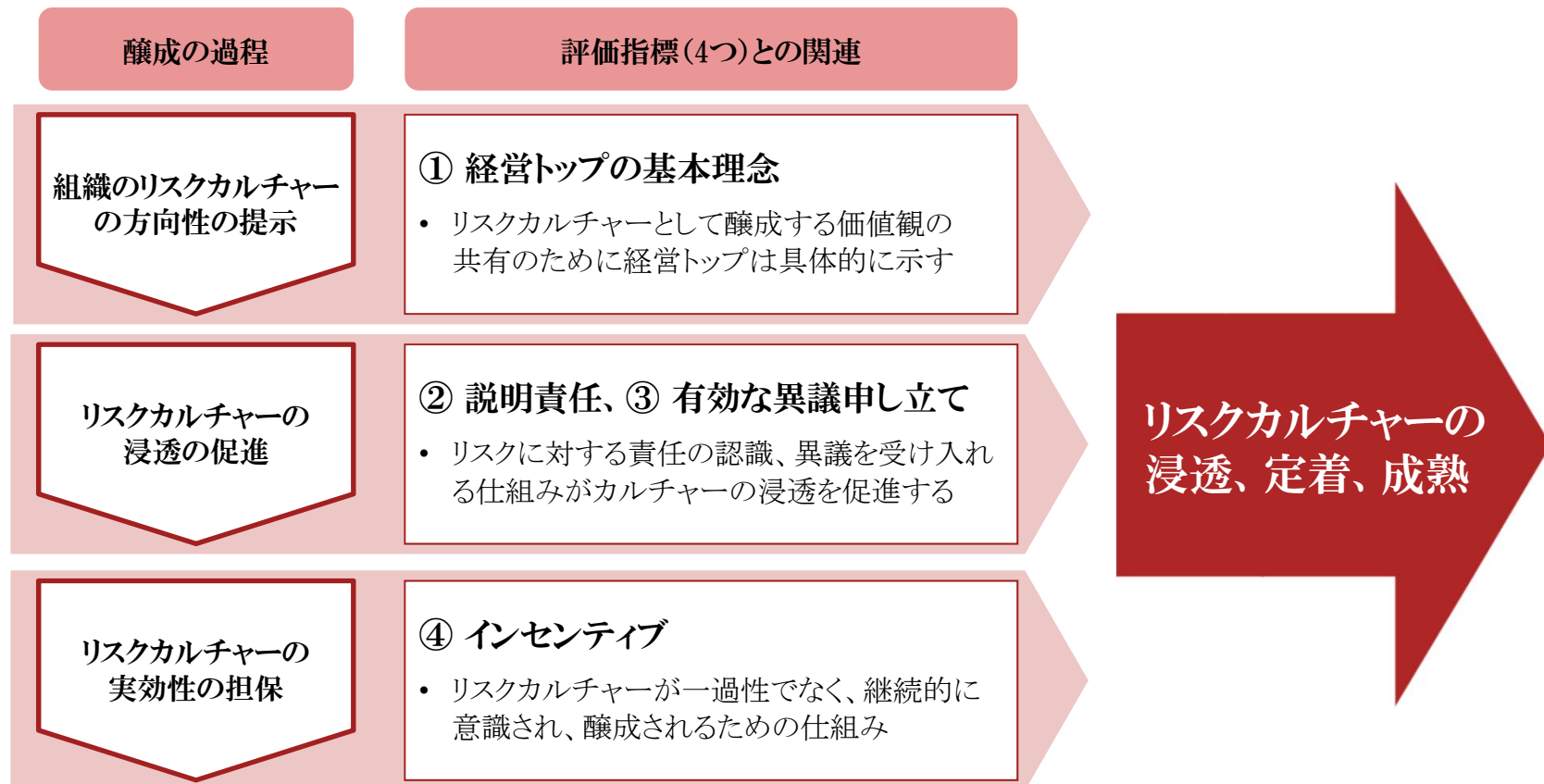
第1線の自律的統制を実現するためには、権限の付与、役割の明確化、およびリソースの確保が必要。

権限	第1線(広義)内の牽制機能を現場から分離させる。 分離した組織は業績目標や収益管理責任を負わない。
機能	第1線(広義)内牽制組織の役割機能の明確化 ✓ 現場の指導 ✓ オンサイトモニタリング
リソース	適切な人材配置 ✓ 量と質のバランス ✓ 2線(、3線)との一定の人材ローテーション

3LoDが効果を発揮するための条件

④ 健全なリスクカルチャー


リスクカルチャーの醸成に必要な要素について、金融安定理事会による「リスク文化に関する金融機関と監督当局の相互作用に関するガイダンス」で、以下4つの指標 (Indicator) が金融機関のリスクカルチャーを評価するための指標として示されている。



3LoDが効果を発揮するための条件

④ 健全なリスクカルチャー

先進的な金融機関においてはリスクカルチャーの強化要因を特定し強化策を講じ、その有効性のモニタリングを行っている

経営トップの役割	コミュニケーション	人事施策	パフォーマンス管理と表彰	組織体制	外部環境要因
 トップコミットメント	 コミュニケーションの進め方と計画	 人材の経験・能力の把握と適正配置	 パフォーマンス評価の仕組み	 組織体制の設計	 監督当局との関係
企業目的、ミッションビジョン、バリュー	双方向のコミュニケーション	採用時のチェックと入社後の意識付け	パフォーマンス評価の指標	リスクの管理、3線による防御	顧客重視の考え方と顧客との関係
現場への参画と近親感	従業員へのフィードバックの仕組み	昇進・昇格	パフォーマンスと表彰との関連付け	ガバナンス、意思決定体系	市場における行動
経験や能力の高さ	ポイントを絞った繰り返しのコミュニケーション	人材開発・教育	認識・価値観の把握	企業倫理綱領や行動規範	世間一般や社会との関係(評判への影響)
リーダーシップの一貫性とまとまり	多様なコミュニケーション手段	後継者・幹部候補の養成	人材の態度等の計測手法の検討	統制環境(企業風土)	外部委託先等

参考資料：リスクカルチャー

FSB:コンダクトリスクの抑制に最も重要なテーマ

テーマ	必要な措置
カルチャー ドライバー	経営陣がコンダクトリスクを抑制する目指すカルチャーについて明確に発信する。
	幅広い情報収集と複合的なテクノロジーの活用によって、コンダクトリスクをもたらす重要なリスクドライバーを特定する。
	非公式的及び公式な手段で行動規範を変革する。非公式な手段としてリーダーは過失に対して建設的に対応することによって、問題を隠さず報告しやすい職場環境を構築する。公式的な手段として内部通報者の保護措置の強化、報告手順の整備、報酬および人事評価制度の改善が考えられる。
個人の責任と アカウンタビリティ	コンダクトリスク抑制を含む重要な責任を定義し、誰がその責任を負うか明確にする。
	個人のアカウンタビリティを明確にする。
	重要な責任を負う個人に対して、その適合性を評価する。
「腐ったリンゴ」への 対処	採用過程において、あるべき行動・行為を早いタイミングで、首尾一貫した形で候補者に伝える。
	面接技術を強化する。
	採用前にできる限り多くの情報源を利用して調査する。
	定期的に社員の行動・行為を評価する。
	エグジットレビュー(退職者との面談)を実施する。

出典: FSB, Strengthening Governance Frameworks to Mitigate Misconduct Risk: A Toolkit for Firms and Supervisors, April 2018

コンダクトリスクをもたらす主なカルチャー要因

健全なカルチャーはガバナンスフレームワークを強化し、コンダクトリスクを削減することができる。一方、コンダクトリスクを容認、奨励するカルチャーはガバナンスフレームワークの有効性を毀損し、組織、顧客、市場に不利益を与える行為に繋がる。

リーダーシップ



- コンダクトリスクに対するアカウンタビリティの欠如
- コンダクトリスクに関する意識、スキル、知識の不足
- 支配的なリーダーシップスタイル
- リーダーの言行不一致
- 中間管理職が発信するメッセージと経営のメッセージの不整合
- 顧客、市場、社会等のステークホルダーを考慮しない理念／目標
- 従業員とのコミュニケーション、巻き込み不足
- 連携や情報共有に消極的な態度

意思決定



- 何を優先すべきかについての不適切な判断
- 異議申し立て、議論の欠如・不足
- 戦略やリスクアペタイトの不整合・矛盾
- マネジメント間の連携不足
- コミュニケーション不足
- 事業部門に支配される意思決定プロセス(2線の関与不足)
- 多様性の欠如による集団思考

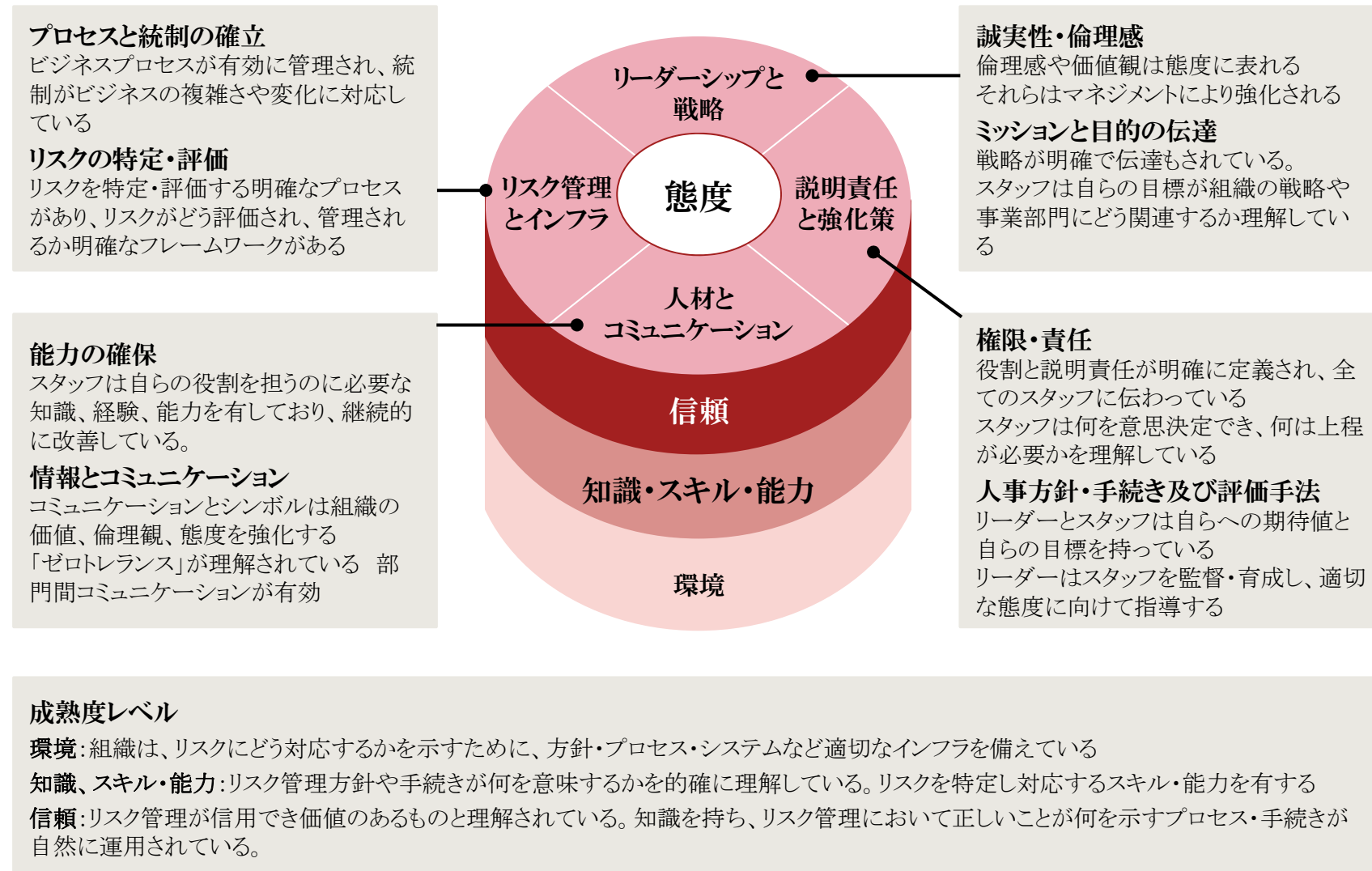
価値観、行動規範



- コンダクトリスクの常態化と受容
- 心理的安全性の低い職場環境
- 都合の悪い情報・事実を受け入れない風土
- コンダクトリスクに対する甘い懲罰措置
- エラーの検知、対応の不足
- 現場の透明性の欠如

出典：FSB, Strengthening Governance Frameworks to Mitigate Misconduct Risk: A Toolkit for Firms and Supervisors, April 2018

PwCの考えるリスクカルチャーのフレームワーク



PwCの考えるリスクカルチャーの寄与要因例

リーダーシップと戦略

- 組織およびチームの戦略は、効果的なリスク管理を前提とする短期および長期の目標を適切に考慮して策定される。
- 経営陣から現場に至るまで、すべての社員が行動できるよう、戦略を明確に示している。
- リーダーは自らの意見を述べ、自ら実践する。
- 許容可能なリスク行動に関するメッセージは、経営層から現場に至るまで、明確かつ一貫性がある。
- リーダーは、一貫してリスク対応のルールの導入を実施し、説明責任を負う。
- リーダーや経営層からのフィードバックとその対応を含む、問題と違反を報告するための明確なプロセスがある。
- リーダーは、技術面のスキルと対人面のスキルをバランスよく持っている。

PwCの考えるリスクカルチャーの寄与要因例

説明責任と強化策

- 報酬と昇進の意思決定は、戦略とリスクベースのKPIと整合的である。
- 明確に適切に期待が伝達され、それは必要なツールとスキル向上の機会に支えられている。
- インセンティブ・スキームは、戦略と望ましい行動と整合している。
- 報酬とリスク調整後のパフォーマンスは、互いに結びついている。
- リスク方針に違反した従業員は、自身の行為内容とその結果に応じた相応の処分がなされる。
- 明確な組織構造、報告ライン、説明責任の仕組みが整備されている。
- 組織、部門、チームは、ミスから学ぶことに重点を置いて改善を行う。

PwCの考えるリスクカルチャーの寄与要因例

人材とコミュニケーション

- 採用プロセスは、カルチャーへの明確な誘導と適切なリスク管理が含まれる。
- フロント・オフィスとバック・オフィスの連携を進めるために、リスク部門とビジネス部門間での処遇、インセンティブ、権限が整合しており極端な差がない。
- 望ましいリスク文化を促進し、維持するためのコミュニケーション戦略が存在する。これには、経営層、リーダー、現場間の双方向のコミュニケーションや、チーム間のコミュニケーションが含まれる。
- 支援と推進のためのメカニズムが整備されている。上程、迅速な対応、調査及び関連する意思決定委員会による注意が含まれる。
- 後継者育成のための助言を実施し、管理職への適切な登用に努めている。
- 適切なリスク管理行動は、技術面のスキルと対人面のスキルのバランスを含め、従業員のパフォーマンス計画において十分に考慮される。
- 教育研修と人材育成には、リスク管理の技術的側面と対人的側面の両方が含まれる。

PwCの考えるリスクカルチャーの寄与要因例

リスク管理とインフラ

- リスクの説明責任と意思決定権は、ビジネス全体で明確に定義されている。
- フロントオフィス/バックオフィス/ミドルオフィスの役割と責任が明確に規定されている。
- リスク管理におけるリーダーと経営層の役割と責任が明確に特定され、伝達されている。
- 不正行為、リスク、適切なチーム行動に関するトレーニングは、チームメンバー全員で一貫して行われます。
- 取引を適切に監視し、不正行為や取引の操作を防止するためのシステムや統制が導入されている。

PwC発出のレポートのご案内

下記リンク先よりレポートが入手可能です

- **リスクガバナンス、リスクアペタイト・フレームワーク、リスクカルチャー**

現在、金融機関におけるリスク管理のあり方は、業務執行レベルでの管理機能の問題に留まらず、取締役会を中心とするリスクガバナンスや、リスクアペタイト・フレームワーク、さらにはリスクカルチャーに係る問題であると捉えられています。本レポートでは、最近の規制動向も踏まえつつ、金融機関が抱えている課題やPwCが考える、あるべきフレームワークについて議論を展開しています。

<https://www.pwc.com/jp/ja/japan-knowledge/thoughtleadership/risk-governance-appetite-framework1502.html>

- **リスクカルチャーの醸成 -リスクカルチャーとコンダクトリスク管理**

本稿においては、コーポレートガバナンス／リスクガバナンスの仕組みが実効性を持つためのリスクカルチャーの醸成と、昨今のリスクプロファイルの変化に伴って高まっているコンダクトリスク管理について、最近の規制動向も踏まえつつ金融機関が抱えている課題やPwCが考えるあるべきフレームワークについて議論しています。

<https://www.pwc.com/jp/ja/japan-knowledge/thoughtleadership/risk-culture1611.html>

連絡先

本資料の詳しいご説明、提供サービスに関するお問い合わせは、下記担当者までお願いいたします。

本資料の記載は、PwCあらた有限責任監査法人の見解を表しているものではありません。

PwCあらた有限責任監査法人

ガバナンス・リスク・コンプライアンス アドバイザリー部

パートナー 辻田 弘志 090-1424-3247

hiroshi.tsujita@pwc.com



本資料は概略的な内容を紹介する目的で作成されたもので、プロフェッショナルとしてのアドバイスは含まれていません。個別にプロフェッショナルからのアドバイスを受けることなく、本資料の情報を基に判断し行動されないようお願いします。本資料に含まれる情報は正確性または完全性を、(明示的にも暗示的にも)表明あるいは保証するものではありません。また、本資料に含まれる情報に基づき、意思決定し何らかの行動を起こされたり、起こされなかったことによって発生した結果について、PwCあたら有限責任監査法人、およびメンバーファーム、職員、代理人は、法律によって認められる範囲においていかなる賠償責任、責任、義務も負いません。

© 2018 PricewaterhouseCoopers Aarata LLC. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Aarata, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.