内部監査人協会（ＩＩＡ）情報／ＣＯＳＯ

2015年７月公表

ＣＯＳＯ――ガバナンスと内部統制

３つのディフェンスライン全体でのＣＯＳＯの活用

内部監査人協会（ＩＩＡ）

著者：ダグラス J. アンダーソン（CIA，CPA，CRMA，CMA）
ＩＩＡ Audit Executive Centerコンサルタント

ジーナ・ユーバンクス（CIA，CISA，CRMA，CCSA）
ＩＩＡ　プロフェッショナルサービス担当ヴァイスプレジデント

訳者：堺　　咲子
内部監査人協会（ＩＩＡ）国際本部　理事
内部監査人協会（ＩＩＡ）調査研究財団　理事・評議員
インフィニティコンサルティング　代表
公認内部監査人（ＣＩＡ）　内部統制評価指導士（ＣＣＳＡ）
公認金融監査人（ＣＦＳＡ）　公認リスク管理監査人（ＣＲＭＡ）
米国公認会計士（ＣＰＡ（ＵＳＡ））

目次

はじめに

本文書は、トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）と内部監査人協会（ＩＩＡ）が共同で作成したものである。本文書は、ＣＯＳＯの『内部統制の統合的フレームワーク』[1]と３つのディフェンスラインモデル[2]を結びつけて内部統制に関する具体的な役割と責任の説明や割り当て方法のガイダンスを示すことにより、組織の全般的なガバナンス体制向上に役立つことを目的としている。

エグゼクティブサマリー

あらゆる組織には達成に向けて努力している目的があるが、それらを追及する中で、組織は目的の達成を脅かし得る事象や状況に遭遇する。そのような潜在的事象や状況は、組織が識別し分析し定義し対処しなければならないさまざまなリスクを生み出す。（全体的にまたは部分的に）受け入れるリスクもあれば、組織が受容可能な水準にまで完全にまたは部分的に低減するリスクもある。リスクを低減する方法は多数あるが、１つの重要な方法は有効な内部統制を整備し運用することである。

ＣＯＳＯの『内部統制の統合的フレームワーク』（以下、『フレームワーク』）は、組織が内部統制の運用を通じてリスクを有効に管理するために必要な構成要素、原則、要素を概説している。しかし『フレームワーク』は、概説している具体的な職務の責任を誰が負うかについてはほとんど述べていない。各当事者がリスクとコントロールに対処する際の役割、説明責任を負う状況、互いの業務を連携する方法を理解するためには、責任が明確に定められなければならない。リスクとコントロールに対処する際の「ギャップ」や不要または意図せず重複した業務のいずれも、あってはならない。

３つのディフェンスラインモデル（以下、モデル）は、組織の規模や複雑性を問わず、リスクとコントロールに関する具体的な職務を組織内で割り当てて連携する方法を検討している。取締役と経営者は、これらの職務の役割と責任の決定的な違いを理解すべきであり、さらに、組織目的の達成可能性を高めるために役割と責任を最適に割り当てる方法を理解すべきである。特にこのモデルでは、明確に定義しないと誤解が生じ得る、組織のアシュアランス活動と他のモニタリング活動の相違点と関係性を明らかにしている。

先に進むにあたっては、読者が既に『フレームワーク』の基本を理解しているという前提で『フレームワーク』とモデルの両方を引用する。『フレームワーク』に馴染みのない方は、ＣＯＳＯのホームページの詳しい情報を参照していただきたい。モデルについては、本文書の第１章で詳しく述べている。

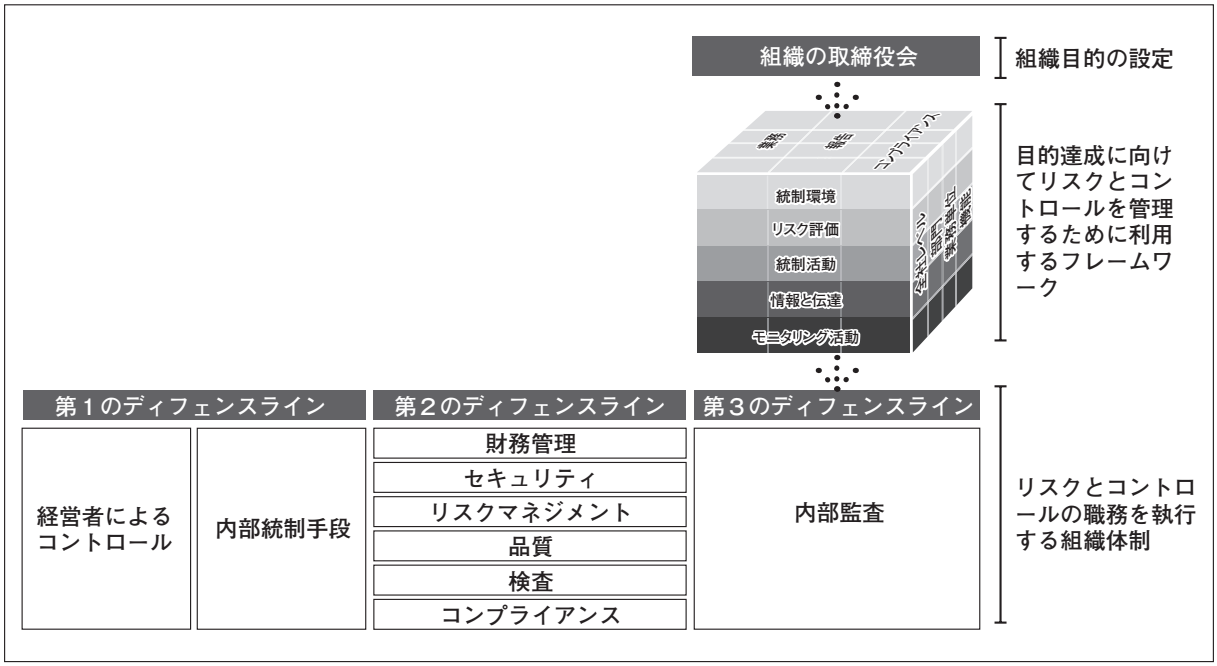
Ⅰ．３つのディフェンスラインモデル

このモデルは、役割と職務を明確にすることにより、リスクマネジメントとコントロールへの理解を深めている。基本的な前提となっているのは、リスクとコントロールの有効な管理のためには上級経営者と取締役会[3]の監督と指揮の下で３つの別々のグループ（またはディフェンスライン）が必要だという考

[1] *Internal Control – Integrated Framework*, Committee of Sponsoring Organization of the Treadway Commission (Jersey City, NJ: American Institute of Certified Public Accountants. May 2013. Available at coso.org.（訳者注：同書の邦訳書は、八田進二・箱田順哉監訳『内部統制の統合的フレームワーク』日本公認会計士協会出版局、2014年２月。）

[2] The Three Lines of Defense in Effective Risk Management and Control.（Altamonte Springs, FL: The Institutes of Internal Auditors, Inc., January 2013）. Available at: 3Lines of Defensein Effective Risk Management and Control.

＜図１＞目的、フレームワーク、モデルの関係



え方である。各グループ（または「ライン」）の責任は、以下の通りである。

1．リスクとコントロールを**所有し管理する**（現業部門の経営者）。
2．経営者を支援してリスクとコントロールを**モニターする**（経営者が整備するリスク、コントロール、コンプライアンス機能）。
3．リスクマネジメントとコントロールの有効性に関して取締役会と上級経営者に**独立的なアシュアランスを提供する**（内部監査）。

３つの各ディフェンスラインは、組織の広範なガバナンスフレームワークの中で異なる役割を担うが、それぞれが割り当てられた役割を有効に果たすと、組織の全般的な目的達成に成功する可能性が高まる。

組織の誰もが内部統制について何らかの責任を負っているが、必要不可欠な職務が意図したとおりに確実に行われるようにするために、モデルは具体的な役割と責任を明確にしている。組織が３つのディフェンスラインを適切に構築しそれらを有効に運営すれば、網羅すべき範囲にギャップはなく不要に重複した業務もなく、リスクとコントロールが有効に管理される可能性が高まる。取締役会は、組織の最も重要なリスクとそれらのリスクに対する経営者の対応に関して偏見のない情報を受け取る機会が増える。

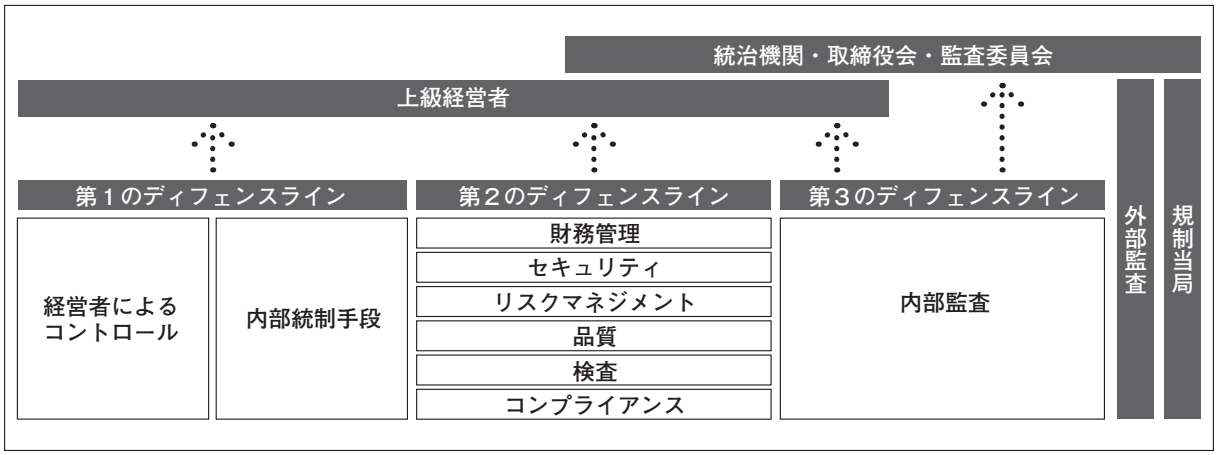
モデルは、『フレームワーク』を支持する形で運用できるように柔軟性のある構造になっている。各ディフェンスライン内の機能は組織によって異なり、ディフェンスラインをまたがったり分割したりする機能があり得る。例えば、第２のディフェンスラインの中のコンプライアンス機能の一部が第１のディフェンスラインのためにコントロールの設計に関与する一方で、第２のディフェンスラインの他の機能がそれらのコントロールのモニタリングに主眼を置いているという組織もある。

組織が３つのディフェンスラインをどのように構築するかに関係なく、モデルにはいくつか重要な原則が内在する。

[3] ＣＯＳＯの出版物と同様に、本文書で「取締役会」という用語は、取締役会、評議員会、無限責任パートナー、所有者、監督機関のような統治機関を指している。

＜図２＞３つのディフェンスラインモデル

The Three Lines of Defense in Effective Risk Management and Control, The Institute of Internal Auditors, January, 2013



１．第１のディフェンスラインは、ビジネスやプロセスの所有者が担当する。彼らは組織の目的達成を促進または抑止し得るリスクを、生み出したり管理したりする。彼らの業務には、適切なリスクを取ることが含まれる。第１のディフェンスラインはリスクを所有し、それらのリスクに対応するために組織のコントロールを設計し遂行する。

２．第２のディフェンスラインは、リスクとコントロールが有効に管理されることを確実にするために、専門知識、優れたプロセス、第１のディフェンスラインと並行したマネジメントモニタリングの提供によって、経営者を支援するために整備される。第２のディフェンスライン機能は第１のディフェンスラインから分離されているものの上級経営者の監督・指揮下にあり、通常ある程度の経営機能を果たしている。第２のディフェンスラインは基本的に、リスク管理の多くの側面を担う経営や監督の機能である。

３．第３のディフェンスラインは上級経営者と取締役会に対して、彼らの期待に一致するように第１と第２のディフェンスライン両方が行った業務に関するアシュアランスを提供する。第３のディフェンスラインは、自らの客観性と組織上の独立性を守るために、経営機能を担うことは通常許されていない。さらに第３のディフェンスラインは、取締役会に対する直接的報告経路がある。このように、第３のディフェンスラインは経営機能ではなくアシュアランス機能であり、第２のディフェンスラインから切り離れている。

どのような組織でも、ゴールは目的を達成することである。これらの目的の追求には、機会の活用、成長の追求、リスクテイク、それらのリスクの管理が関わるが、それらすべては組織の発展のためのものである。適切なリスクテイクや取ったリスクの適正な管理に失敗すると、組織の目的達成を妨げかねない。企業価値を生み出す活動と守る活動との間には、常に緊張がある。『フレームワーク』は、リスクとコントロールが妥当であり適切に管理されることを確実にするように、それらを検討するための仕組みを示している。モデルは、導入する組織体制と、リスクとコントロールの有効な管理をより成功させるような役割と責任の割り当てについて、ガイダンスを示している。

３つのディフェンスラインモデルにおける上級経営者と取締役会の役割

上級経営者と取締役会は、モデルの中で不可欠な役割を担っている。上級経営者は、取締役会の監督の下、内部統制システムの選択、整備、評価に説明責任を負っている。上級経営者と取締役会のいずれも３つのディフェンスラインの一部であるとは考えられていないが、両者は、組織目的の設定、それらの目的達成のためのハイレベルな戦略の決定、リスクを最善に管理するためのガバナンス体制の構築に共同で責任を負っている。上級経営者と取締役会はまた、リスクとコントロールに関する最適な組織体制を確立するのに最良な立場にある。上級経営者は、強固なガバナンス、リスクマネジメント、コントロールを全面的に支援しなければならない。さらに彼らは、第１と第２のディフェンスラインの活動に最終的な責任を負っている。彼らの関与はこのモデル全体の成功に不可欠である。

『フレームワーク』は、取締役会と上級経営者のこのような責任を明らかにするのに役立つ。図３に示す通り、上級経営者と取締役会は、組織のトップの気風を確立する５つの原則によって支えられる組織の統制環境に一義的な責任を負っている。

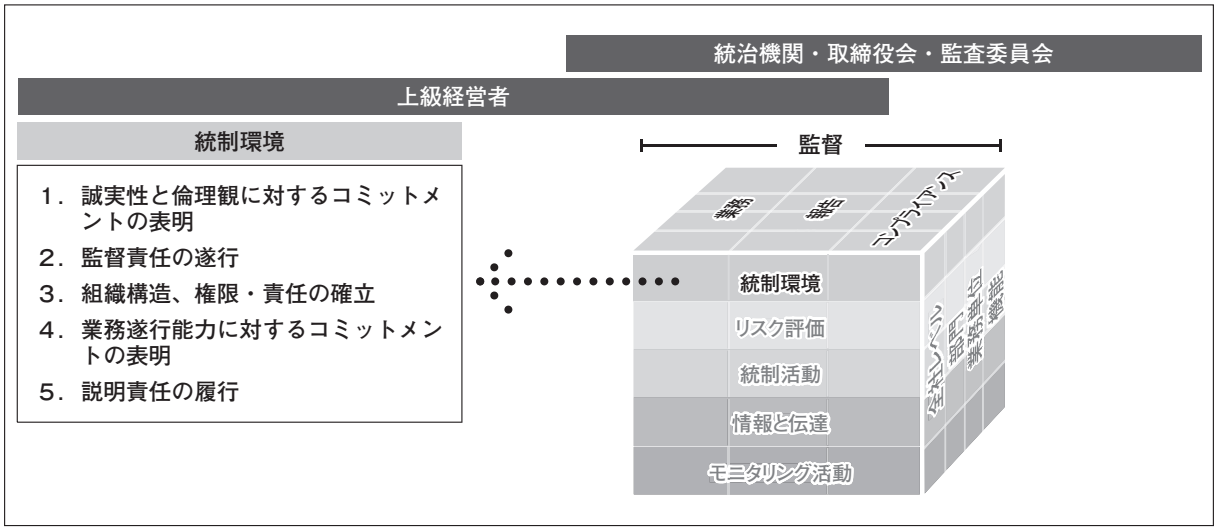
モデルは、『フレームワーク』の下での体制で、役割と責任をどのように割り当てるかを詳しく示している。この体制は、取締役会と上級経営者の積極的な支援とガイダンスがあれば最適に実施される。

第１のディフェンスライン：業務部門の経営者

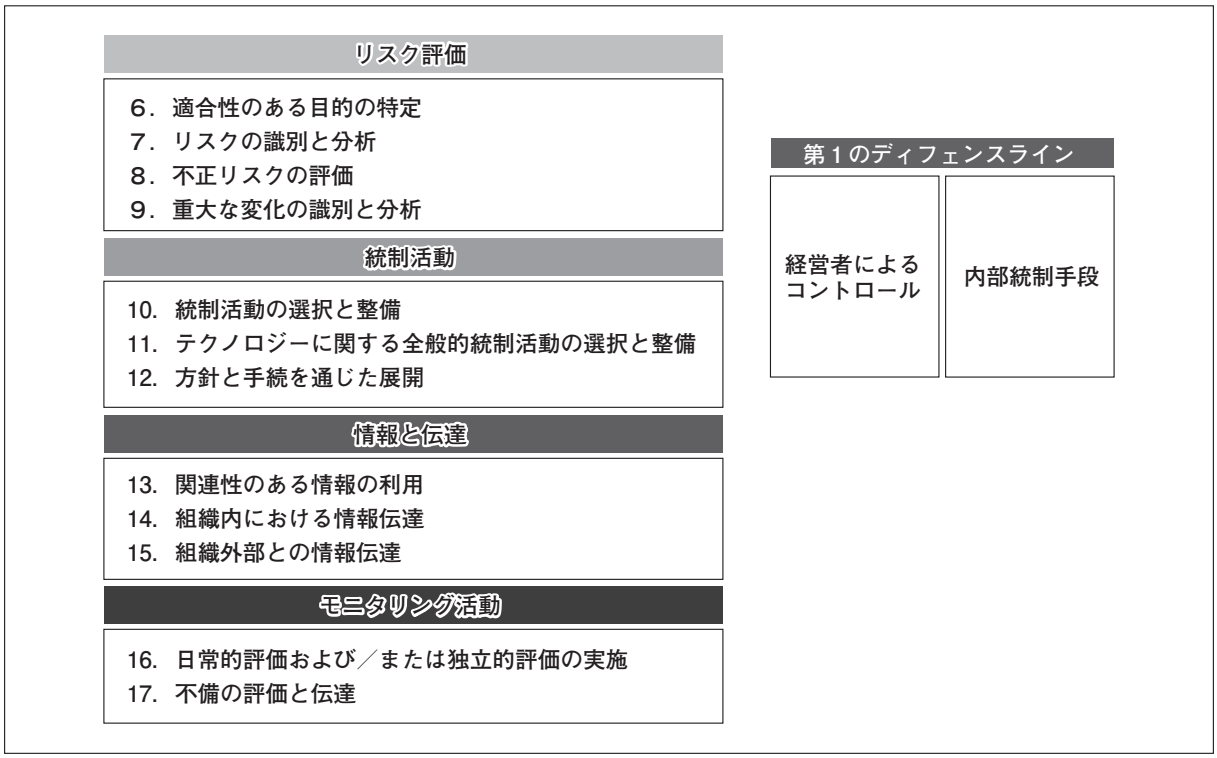
このモデルの第１のディフェンスラインは、リスクとコントロールを日常的に所有し管理する現業部門と間接部門の経営者が主として担当する。業務部門の経営者は、組織のコントロールとリスクマネジメントのプロセスを整備し実施する。これらには、重大なリスクの識別と評価、意図したとおりの業務遂行、不適切なプロセスの検出、コントロールの機能不全への対処、業務の主な利害関係者への伝達のために整備した内部統制プロセスが含まれる。業務部門の経営者は、自身が担当する業務分野でこれらの作業を実施するための適切なスキルを身につけていなければならない。

上級経営者は、第１のディフェンスラインのあらゆる業務の全般的な責任を負っている。上級経営者は自らが責任を負う第１のディフェンスラインの範囲であっても、特定の高リスク分野については、現業部門と間接部門の経営者に対して直接的な監督も行うこと

＜図３＞統制環境の監督責任



＜図４＞ＣＯＳＯと第１のディフェンスライン



がある。

第１のディフェンスラインの個々人は、『フレームワーク』の中のリスク評価、統制活動、情報と伝達に関する重大な責任を負っている。図４に示す通り、業務部門の経営者は、『フレームワーク』の中に示された残りの12の内部統制の原則に一義的な責任がある。

第２のディフェンスライン：内部のモニタリングと監督機能

第２のディフェンスラインは、第１のディフェンスラインが導入したコントロールとリスクマネジメントのプロセスが適切に設計され意図したとおりに運用されることを確実にするために、経営者が整備した各種のリスクマネジメントとコンプライアンスの機能である。第２のディフェンスラインは経営機能であり、業務部門の経営者である第１のディフェンスラインからは分離されているが上級経営者の監督・指揮下にある。第２のディフェンスラインに属する機能は、通常、コントロールとリスクの継続的モニタリングの責任を負っている。第２のディフェンスラインは業務部門の経営者と密接に連携することが多く、導入戦略の定義づけ、リスクの専門知識の提供、方針と手続の導入、リスクとコントロールの全社的視点を生み出すための情報の収集を支援する。

第２のディフェンスラインの構成は、組織の規模や業界により大きく異なることがある。大規模組織、株式公開会社、複雑な組織、規制が厳しい組織などは、第２のディフェンスラインの機能はすべて別々ではっきり分けられている。小規模組織、非公開会社、あまり複雑でない組織、規制が厳しくない組織などは、第２のディフェンスラインのいくつかの機能が統合されたり存在しないこともある。例えば、法務とコンプライアンスの機能を1つの部に統合したり、衛生・安全機能を環境機能と統合する組織がある。第２のディフェンスラインの職務の一部または全部を第１のディフェンスラインの経営者が担う組織もある。

代表的な第２のディフェンスライン機能に

は、以下のような専門的なグループがある。

- リスクマネジメント
- 情報セキュリティ
- 財務管理
- 物理的セキュリティ
- 品質
- 衛生・安全
- 検査
- コンプライアンス
- 法務
- 環境
- サプライチェーン
- その他（業界特有または企業特有のニーズによる）

経営者の監督の下、第２のディフェンスラインの構成員はコントロールが意図したとおりに機能しているかを判断するために特定のコントロールをモニターする。第２のディフェンスラインが行うモニタリング活動は、通常、『フレームワーク』で述べられている業務、報告、コンプライアンスの３つのすべての目的を網羅する。

第２のディフェンスラインの個々人の責任はさまざまであるが、通常、以下のようなものがある。

- リスクを管理するためのプロセスとコントロールを設計し整備して、経営者を補佐。
- モニターすべき活動および経営者の期待と比較した達成度の測定方法の決定。
- 内部統制活動の妥当性と有効性のモニタリング。
- 重大な問題、新たなリスク、異常値の上申。
- リスクマネジメントフレームワークの提供。
- 組織のリスクとコントロールに影響する既知および新たなリスクの識別とモニタリング。
- 組織の潜在的なリスク選好とリスク許容度の変化の識別。
- リスクマネジメントとコントロールプロセスに関するガイダンスと研修の提供。

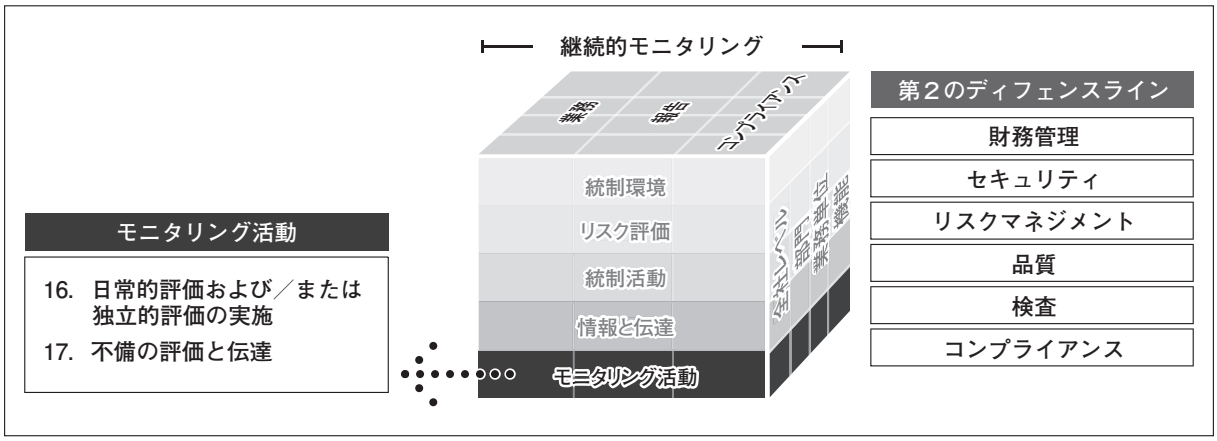
第２のディフェンスラインによるモニタリングは、組織の特定のニーズに合わせるべきである。通常、これらのモニタリング活動は、日常的な業務活動とは別のものである。多くの場合、モニタリング活動は組織中に分散しているが、モニタリング機能が１つまたはわずかな分野に限られている組織もある。

第２のディフェンスラインの各機能は、第１のディフェンスラインの業務からある程度独立しているものの、本来的には経営機能である。第２のディフェンスラインの機能は、組織の内部統制とリスクのプロセスを直接整備し実施し変更することがあり、また特定の業務活動について意思決定の役割を担うこともある。第２のディフェンスライン機能の役割が第１のディフェンスラインの業務への直接的な関与を必要とする限りは、第２のディフェンスライン機能は第１のディフェンスラインの業務から完全には独立していない。

第２のディフェンスラインの構成は、組織の規模や業界により大きく異なることがある。

独立的ではないものの、強力で有能な第２のディフェンスライン機能は言い表せないほど重要である。第２のディフェンスラインは、適度な客観性を持って業務を行うことと、第１のディフェンスラインによるリスクとコントロールの管理について上級経営者と取締役会に重要かつ有益な情報をもたらすことが期待されている。第２のディフェンスラインは全社的なリスクとコントロールの情報を上級経営者と取締役会に提供することもあるが、これは第１のディフェンスラインには期待されていないことである。ディフェンスラインとして有効であるためには、第２のディフェンスラインは組織各所のリーダーや業務部門の経営者を相手にするのに十分な地位がなければならないが、そのような地位は、敬意を

＜図５＞ＣＯＳＯと第２のディフェンスライン



払われる権限と直接的報告経路からもたらされる。

第３のディフェンスライン：内部監査

内部監査人は、組織の第３のディフェンスラインとしての機能を果たす。ＩＩＡは内部監査を次のように定義している。「組織体の運営に関し価値を付加し、また改善するために行われる、独立にして、客観的なアシュアランスとコンサルティング活動である。内部監査は、組織体の目標の達成に役立つことにある。このためにリスクマネジメント、コントロールおよびガバナンスの各プロセスの有効性の評価、改善を、内部監査の専門職として規律ある姿勢で体系的な手法をもって行う。」[4]

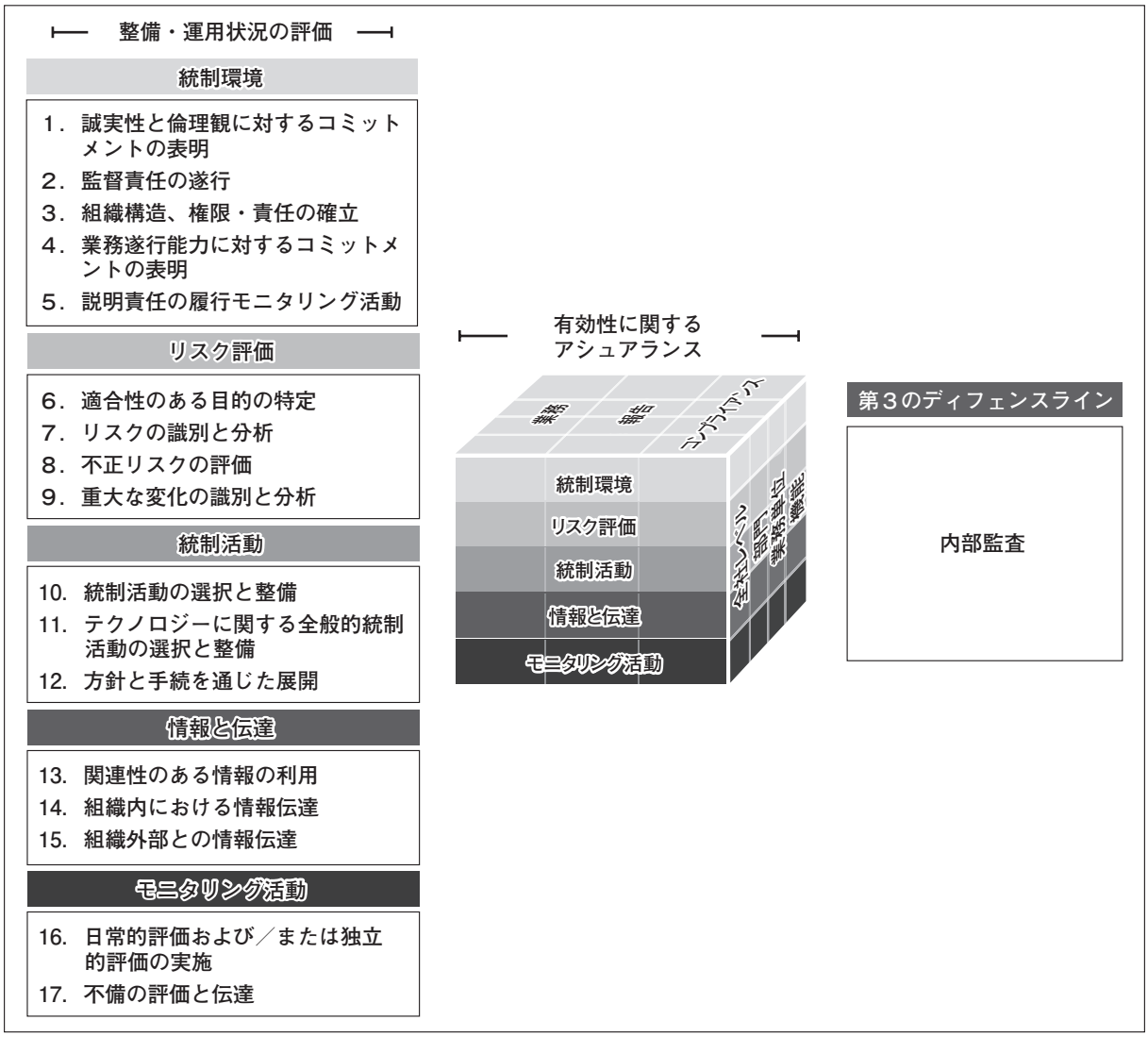
さまざまな役割の中でも内部監査は特に、ガバナンス、リスクマネジメント、内部統制の有効性と効率性のアシュアランスを提供する。内部監査の業務範囲は、組織の業務のあらゆる側面を網羅することができる。

内部監査を他の２つのディフェンスラインと区別しているのは、その高度な組織上の独立性と客観性である。内部監査人は通常の責任の一部としてコントロールの整備や運用はせず、組織の業務運営の責任も負っていない。多くの組織では、内部監査の独立性は内部監査部門長と取締役会の直接的報告関係によってさらに強化されている。この高度な組織上の独立性により、内部監査人はガバナンス、リスク、コントロールに関して取締役会と上級経営者に信頼性と客観性のあるアシュアランスを提供するのに最適に位置づけられている。

内部監査機能は、独立性と専門性を高める条件が整えば有効な組織的ガバナンスに貢献する。そのため、専門的な内部監査機能の確立はあらゆる組織にとって優先事項である。これは、大規模組織のみならず小規模企業にとっても重要である。やや非公式で強固でない体制の小規模組織がガバナンスとリスクマネジメントのプロセスの有効性を確保しようとすると、大規模組織と同様に複雑な環境に直面することがある。また小規模組織には、有効な第２のディフェンスラインが存在しないことがある。しかし、あらゆる組織が独立性、適切性、能力を備えた内部監査要員を確保すべきであり、内部監査は職務を独立的に遂行できるように組織内の十分高い地位に報告すべきであり、さらに（ＩＩＡの『専門職的実施の国際フレームワーク』のような）世界的に認められた適切な基準に従って業務を行うべきである。

[4] 専門職的実施の国際フレームワーク（IPPF）2013年版。

＜図６＞ＣＯＳＯと第３のディフェンスライン



外部監査人、規制当局、外部の関係者

外部の関係者は、正式には組織の３つのディフェンスラインの中にあるとは考えられていないが、外部監査人や規制当局などは、組織の全般的なガバナンスとコントロール体制に重要な役割を果たすことが多い。規制当局は、ガバナンスとコントロールを強化することを意図して規制を設けることがよくあり、規制対象組織について積極的にレビューし報告する。同様に、外部監査人は、組織の財務報告と関連リスクについて重要な発見事項と評価をもたらすことがある。

外部監査人、規制当局、その他組織外部の関係者が有効に連携すれば、追加的なディフェンスラインとして取締役会や上級経営者を含めた組織の利害関係者に重要な視点と見解をもたらし得る。しかし、そのような関係者による作業には、異なった目的や概してより焦点を絞った狭い目的があり、対象とする分野は組織内部のディフェンスラインによる評価ほど広範ではない。例えば、３つのディフェンスラインは、組織が直面する業務、報告、コンプライアンスのリスク全般に対応することを意図しているのに対して、特定の規制当局の監査は、コンプライアンス、安全またはその他の限られた範囲の問題だけに焦点を当てることがある。外部監査人や規制当局のような関係者は貴重な情報をもたらすが、組織

内部のディフェンスラインの代用と考えるべきではない。組織のリスクを管理することは組織の責任であって外部の関係者の責任ではない。

Ⅱ．３つのディフェンスラインの構築と連携

３つのディフェンスラインの構築

３つのディフェンスラインモデルは意図的に柔軟に設計されている。各組織は、自らの業界、規模、業務体制、リスクマネジメントに対するアプローチに合った方法でこのモデルを整備すべきである。しかし、３つに分かれ明確に定義されたディフェンスラインがある時に、通常、全般的なガバナンスと統制環境は最強となる。組織の規模や複雑性を問わず、何らかの形で３つのディフェンスラインすべてが存在するというこのモデルと一致するようなガバナンス体制を整備するように組織は努力すべきである。「ライン」は、別々の役割と責任、組織のしかるべき方針と手続への明記、一貫した「トップの気風」による裏付けを伴って、はっきりと区別されるべきである。

ディフェンスラインを引く場所は、各組織特有のニーズによって異なる。小規模会社や特定の機能が移行中の場合などは、ディフェンスラインが明確に分かれていないことがある。例えば、リスクマネジメント機能を立ち上げる時、整備を促すために他の機能を利用する組織もある。しかし、ディフェンスラインの機能がはっきりと分かれていない状況では、取締役会はその体制の潜在的影響を慎重に検討すべきである。可能であれば、そのような状況は短期のものとして、機能が成熟するにつれて適切に分離すべきである。もしそのような状況が短期や臨時でなく長期間であれば、３つの別々のディフェンスラインを維持できないために経営とアシュアランスの機能が分離されないことの影響を取締役会は理解すべきである。

モデル内の各グループの基本的な役割を覚えておくと、組織のさまざまなリスクとコントロールの機能内で具体的な職務を検討したり割り当てる際に役立つ。

組織上の独立性と客観性は第３のディフェンスラインの本質的な特徴であるため、組織が内部監査機能に第２のディフェンスラインの何らかの役割を統合する場合は特別な注意が必要である。内部監査機能が第２のディフェンスラインの何らかの職務を兼務する場合は、上級経営者と取締役会は、内部監査機能の組織上の独立性または客観性が損なわれないように統合または調整するよう十分確認すべきである。内部監査人は、本来は監査対象業務のいかなる経営上の責任も負うべきではない。内部監査が第２のディフェンスラインの業務に関与する組織では、相反する役割は他の者またはグループに割り当てて、このような関与は通常短期間にすべきである。内部監査による第２のディフェンスラインの職務への関与が短期間ではない場合は、上級経営者と取締役会は内部監査が独立的かつ客観的なアシュアランスを提供する能力には限界があることを認識する必要があり、影響を受ける特定の業務に関するアシュアランスの提供を外部の関係者に頼る必要もあり得る。

＜図７＞３つのディフェンスライン間の違い

経営機能		アシュアランス
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
業務部門の経営者	限定的な独立性 一義的には経営者に報告	内部監査 大きな独立性 統治機関へ報告

３つのディフェンスラインの連携

３つのディフェンスラインそれぞれが、リスクを有効に管理して組織の目的達成を支援するという同じ究極の目的を持っている。彼らは同じ最終的利害関係者のために働き、同じリスクとコントロール上の問題を扱うことが多い。上級経営者と取締役会は、３つのディフェンスラインが互いに情報を共有し業務の連携をすることを期待していると、明確に伝えるべきである。情報の共有と業務の連携は業務の全般的な有効性に役立ち、またどのディフェンスラインの主要機能も損ねない。例えば、多くの組織では、これらの期待を明示した取締役会レベルまたは経営者レベルのリスク方針を定めている。

連携と伝達を組織体制と混同してはならない。３つのディフェンスラインの目的は同じであっても、各ディフェンスラインは固有の役割と責任を負っている。しかし別々のディフェンスラインであっても縦割りで業務を行うべきではない。３つのディフェンスラインは、リスク、コントロール、ガバナンスについて情報を共有し業務の連携をすべきである。多くの場合、彼らはリスクとコントロールに関して共通した見方をしている可能性がある。

すべての重要なリスクに適切に対処しながらも業務の不要な重複を避けるために、慎重な調整が必要である。この調整は大変重要であり、『基準2050』は内部監査部門長に「適切な内部監査の業務範囲を確保し、業務の重複を最小限にするために、内部監査機能以外のアシュアランス業務やコンサルティング・サービスを行う組織体内部および外部の者と、情報を共有し活動の調整をすべきである。」[5]と求めている。

この調整を機能させるためには、最高リスク責任者、最高コンプライアンス責任者、内部監査部門長のような役員の主な役割を慎重にレビューし構築することが極めて重要である。それによりリスクとコントロールを担当する他の役員と連携し伝達しながら各自が固有の責任を果たせる。

第１のディフェンスラインは、リスクとその管理手法を一義的に所有している。第２のディフェンスラインは、リスクの専門知識を提供し、導入戦略の設定を助け、方針と手続の導入を支援する。これら２つのディフェンスラインはリスクとコントロールについて異なる役割を持つが、同じ用語を用い、組織のリスクに対する互いの評価を理解し、可能な限り共通のツールやプロセスを活用して、協働することが不可欠である。

第３のディフェンスラインである組織の内部監査機能は、組織の重要なリスクとコントロール活動を内部監査業務範囲に含めるべきである。第１と第２のディフェンスラインとのコミュニケーションは、内部監査が彼らと同様のリスク用語を用いることと、彼らのリスクに対する考えを理解することに役立つ。

内部監査は、第２のディフェンスラインと業務の連携もすべきである。この連携は、組織の性質、両者が行う具体的な業務、第２のディフェンスライン機能の組織上の独立性、上級経営者と取締役会の期待などにより、さまざまな形態をとり得る。内部監査は、第２のディフェンスラインが行った業務を内部監査の評価業務の一部の基礎にできる場合がある。この場合内部監査は、その業務が適切に設計、計画、監督、文書化、レビューされたかを確認すべきである。他の機能の業務の利用範囲と信頼度は、個々の状況により異なる。第２のディフェンスラインの業務を基礎として内部監査の評価業務を行うことを計画する場合は、第２のディフェンスラインの組織上の独立性についても慎重に注意を払うべきで

[5] 専門職的実施の国際フレームワーク（IPPF）2013年版。

ある。内部監査は偏見のない客観的な評価を提供するために組織上独立的に位置づけられているので、内部監査が依拠する業務を行う機能は、十分に高いレベルの組織上の独立性と客観性を示しているべきである。能力と効率性だけが規準なのではない。第１または第２のディフェンスラインが内部監査のために業務を行う能力があるということは、彼らが必要なレベルの独立性と客観性を提供することを意味するわけではない。同様に、内部監査が第１または第２のディフェンスラインの業務を行う能力があるということは、内部監査が第１または第２のディフェンスラインの業務を行う場合に組織上の独立性と客観性を必ずしも維持するものでないことを意味している。

業務を効率的に連携しやすくするために、内部監査には第２のディフェンスライン機能の業務または第三者が提供するあらゆる業務について成果と有効性を評価する責任があるということを、内部監査の基本規程に明記すべきである。

連携は、３つのディフェンスラインを超えて外部監査人のような外部の関係者を含めた範囲に広がることもある。内部監査人は、ガバナンス、リスクマネジメント、コントロールのアシュアランスを提供する際に、内部または外部者の業務に依拠したり利用することがある。ただしそれは、実施された業務、詳細な結果、外部者の独立性と能力を、内部監査が十分に理解した場合である。反対に、外部者の要請に合わせて内部監査業務が意図的に計画され実施されることもある。外部者との業務の連携は効率性の向上につなげることができるが、内部監査部門長と取締役会は、外部者の利益のために内部監査業務を設計することの費用と潜在的利益を検討すべきである。

Ⅲ．３つのディフェンスライン全体でのＣＯＳＯの活用

『フレームワーク』は、内部統制の５つの構成要素とそれらの構成要素に関連する基本概念を表した17の原則を定めている。ＣＯＳＯの出版物『内部統制の統合的フレームワーク』では、17の原則は５つの構成要素から直接導き出されることから、これらの各原則を適用することによって有効な内部統制を達成することができると述べている。経営者は17の原則に関連する不可欠な職務を割り当て、職務が意図したとおりに実施されていることを確認する責任を負っている。

付録は、17の原則についての責任を３つのディフェンスライン内で割り当てる方法を例示している。『内部統制の統合的フレームワーク』は、17の各原則に関連する各種の「着眼点」も示している。着眼点の多くは３つのディフェンスライン内の個々人の主な責任を表しているため、『内部統制の統合的フレームワーク』に馴染みのある読者は、着眼点の多くが付録の至る所に反映されていることに気付くだろう。

付録の情報は、３つのディフェンスライン内での職務の配分例を示すことを意図している。組織は皆それぞれ独特であるため、付録の例とは異なる役割や責任を定める合理的な理由があり得る。組織内での職務の割り当て方法に関わらず、内部統制の対象範囲のギャップを減らし不要な業務の重複をなくすために、17の原則すべてに関する具体的な役割と責任を明確に定めて関係者全員に伝えるべきである。

結論

あらゆる組織は、コントロールの「ギャップ」およびリスクとコントロールに関する職務分担の不要な重複を最小にするように、ガ

バナンス、リスク、コントロールに関する責任を明確に定めるべきである。３つのディフェンスラインモデルは、不可欠な役割と職務を明確にすることにより、リスクとコントロールに関するコミュニケーションを深めるための有効な方法を示している。モデルは、リスクとコントロールに関する責任について組織全体で連携する方法を明らかにするために利用することができる。

このモデルの基本的前提は、リスクとコントロールの有効な管理のためには、上級経営者と取締役会の監督と指揮の下で３つの別々のグループ（ディフェンスライン）が必要だということである。３つのグループは、以下のとおりである。

- リスクとコントロールを**所有し管理する**（業務部門の経営者）。
- 経営者を支援するためにリスクとコントロールを**モニターする**（経営者が整備するリスク、コントロール、コンプライアンス機能）。
- リスクマネジメントとコントロールの有効性に関して取締役会と上級経営者に**独立的なアシュアランスを提供する**（内部監査）。

３つの各「ライン」は組織の広範なガバナンスフレームワークの中で異なる役割を担うが、それぞれが割り当てられた役割を有効に果たせば、重大なコントロールの機能不全に陥る可能性が低くなる。この体制はまた、組織の最も重要なリスクとそれらのリスクに対する経営者の対応方法について、取締役会が偏見のない情報を受け取る裏付けになる。

モデルは、各ディフェンスライン内の個々人がリスクとコントロールに関する自らの完全な責任範囲および自らの職務が組織の全般的なリスクとコントロールの体制にどう当てはまるかを確実に理解するために、ＣＯＳＯの『内部統制の統合的フレームワーク』と併せて利用することができる。

キーポイント

1．上級経営者と取締役会は、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の効率性と有効性を確実にする最終的責任を負っている。
2．３つに分かれ明確に定義されたディフェンスラインがあれば、リスクマネジメントは最強となる。組織の規模や複雑性を問わず、どのような組織にも何らかの形で３つのディフェンスラインすべてが存在すべきである。
3．３つのディフェンスライン内の各グループは、適切な方針、手続、報告経路に裏付けられて明確に定められた役割と責任を持つべきである。
4．すべての重要なリスクに適切に対処しつつ効率性を向上し重複業務を避けるために、各ディフェンスラインは情報を共有し業務の連携をすべきである。
5．ディフェンスラインは有効性を損なうような形で統合または連携すべきではない。各ディフェンスラインは、組織内で固有の位置づけと責任がある。組織が３つのディフェンスラインを横切って機能を統合する場合は、特別な注意を払うべきである。第２または第３のディフェンスラインの統合がそのディフェンスラインの独自性を損なうようなものであると、有効性に悪影響が生じ得る。能力と効率性だけが規準なのではなく、独立性と客観性もまた検討すべき不可欠の要素である。

付録

原則１．組織は、誠実性と倫理観に対するコミットメントを表明する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
すべてのディフェンスラインは、誠実性と倫理観の重要性を自らの指示、行動、態度で示すことが期待される。			
●組織の価値観、哲学、業務の姿勢を構築するに当たり、模範を示して指導する。 ●倫理関連の目的、プログラム、活動を構築する。 ●期待される行動基準に照らして個々人とチームの遵守状況を評価するプロセスを整備し運用する。	●第２のディフェンスラインの特定の者は、コンプライアンス・ホットラインの支援、潜在的不正行為の調査、誠実性と倫理観に関連する特定業務などを行うよう要請されることがある。	●組織の倫理風土および法律と倫理の望ましい遵守水準を達成するための戦略、戦術、コミュニケーション、その他のプロセスを評価する。 ●組織の倫理関連の目的、プログラム、活動の整備、運用、有効性を評価する。 ●倫理プログラムが定めた目的を達成しており、主要なリスクが有効に管理されており、コントロールが有効に機能し続けているというアシュアランスを提供する。 ●組織が強固な倫理プログラムを確立し、望ましい遵守水準にプログラムを向上するのを支援するために、コンサルティング・サービスを提供する。	●取締役会は倫理風土を監督し、経営者が妥当な倫理関連プログラムと目的を持つことを確実にする。 ●取締役会は、有効な「トップの気風」を確立する責任を負っている。この責任には、誠実性、倫理観、行動基準に関する期待を伝達することが含まれる。

原則２．取締役会は、経営者から独立していることを表明し、かつ、内部統制の整備および運用状況について監督を行う。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●取締役会が信認義務を果たせるように、内部統制の整備と運用に関する適切な情報を取締役会に提供する。	●取締役会の監督は、経営者が業務執行レベルで確立する体制とプロセスに裏付けされている。この裏付けは、第１または第２のディフェンスラインのいずれかが提供することがある。例えば、経営委員会または第２のディフェンスライングループのいずれかがＩＴやコンプライアンスといったテーマに焦点を当てることがある。	●内部統制の整備と運用に関してアシュアランスを提供し、コントロールが適切に整備され有効に運用され意図したとおりに機能しているかを評価する。 ●取締役会での議論のために、原則２に関する具体的な議題を提案することにより取締役会を支援することがある。	●取締役会は、経営者から独立しており客観的な評価と意思決定ができる十分な数の取締役を確保する責任を負う。 ●取締役会は、経営者が設計、適用、運用する内部統制の監督責任を保持する。 ✓**統制環境**：誠実性と倫理観、監督体制、権限と責任、期待される業務遂行能力、取締役会に対する説明責任の確立。 ✓**リスク評価**：経営者のリス

			ク選好設定への関与。目的達成に対するリスク（重大な変化、不正、経営者による内部統制の無効化による潜在的な影響を含む）に関する経営者の評価の監督。 ✓**統制活動**：統制活動の整備と運用について上級経営者を監督。 ✓**情報と伝達**：組織の目的達成に関する情報の分析と議論。 ✓**モニタリング活動**：モニタリング活動の性質と範囲および統制の不備に対する経営者の評価と改善策についての検討と監督。 ●取締役会は、内部監査および場合によっては経営者から独立した第２のディフェンスラインの関係者と会合を持つ。

原則３．経営者は、取締役会の監督の下、内部統制の目的を達成するに当たり、組織構造、報告経路および適切な権限と責任を確立する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●目的達成に当たり組織構造、報告経路、適切な権限と責任を確立する。 ●取締役会が監督責任を果たせるように、組織構造、報告経路、適切な権限と責任に関する情報を伝達する。	●経営者が責任を果たすために必要な組織構造、報告経路、適切な権限と責任の確立において、経営者を支援する。	●目的達成に当たり、組織の業務運営体制、報告経路、権限、責任について、適切性と有効性に関するアシュアランスを提供する。 ●適切な報告経路と権限を含めた内部監査の基本規程に従って業務を遂行するために、方針と実務慣行を導入する。 ●取締役会に対して定期的に内部監査の組織上の独立性と客観性を確認する。	●取締役会は、組織全体の目的を承認する。取締役会は、目的達成に当たり、組織構造と報告経路の構築と維持および適切な権限と責任の割り当てについて監督責任を負う。 ●取締役会は、監査委員会を含めた委員会を設置するために適切な基本規程を発表する。 ●監査委員会は、自らが責任を負うリスクとコントロールの機能（内部監査を含む）について、適切な基本規程を承認する。

原則４．組織は、内部統制の目的に合わせて、有能な個人を惹きつけ、育成し、かつ、維持することに対するコミットメントを表明する。			
第１のディフェンスライン（リスクの所有者・経営者）	**第２のディフェンスライン**（リスク、コントロール、コンプライアンス）	**第３のディフェンスライン**（内部監査）	**その他**
●目的に合わせて有能な人材を惹きつけ育成し維持する。	●目的達成のために有能な人材を惹きつけ育成する。 ●第２のディフェンスラインの構成員と業務が経営者と適切に調和することを確実にする。これには、人材を様々な経営機能にローテーションすることが含まれ得る。	●内部監査のミッションと基本規程を達成するために、能力とスキルのある人材を惹きつけ育成し維持する。 ●以下のような方針やプロセスの効率性と有効性を評価してアシュアランスを提供することがある。 ✓人事方針 ✓採用慣行 ✓研修・育成プログラム ✓業績評価システム ✓報酬制度 ✓後継者育成計画	●取締役会は、経営者が目的に合わせて有能な人材を惹きつけ育成し維持することに対するコミットメントを表明することを確実にするために監督する。 ●取締役会の委員会は、監督する機能が有能な人材を有することを確実にする。 ●取締役会の報酬委員会は、インセンティブや報酬制度が組織のリスク選好と長期目的に合ったものになることを確実にする。

原則５．組織は、内部統制の目的を達成するに当たり、内部統制に対する責任を個々人に持たせる。			
第１のディフェンスライン（リスクの所有者・経営者）	**第２のディフェンスライン**（リスク、コントロール、コンプライアンス）	**第３のディフェンスライン**（内部監査）	**その他**
●目的達成に当たり、内部統制に対する責任を個々人に持たせる。この責任には、具体的な責任の伝達、業績評価システムの実施、個々人の行動に責任を持たせるように設計した人事プロセスの実施が含まれる。	●経営者からの委任により、第２のディフェンスラインの個々人は内部統制の具体的な責任の遂行をモニターし報告する。	●内部統制の具体的な責任の遂行についてアシュアランスを提供する。 ●内部監査人は説明責任について改善提案をすることがあるが、通常は人事措置または内部統制に対して個々人に責任を持たせるように設計したプロセスについて意思決定する直接の権限はない。	●取締役会は、経営者が内部統制に対する責任を個々人に持たせることを確実にする責任を負う。 ●取締役会の報酬委員会は、インセンティブや報酬制度が組織の目的に合ったものになることを確実にする。

原則６．組織は、内部統制の目的に関連するリスクの識別と評価ができるように、十分な明確さを備えた内部統制の目的を明示する。			
第１のディフェンスライン（リスクの所有者・経営者）	**第２のディフェンスライン**（リスク、コントロール、コンプライアンス）	**第３のディフェンスライン**（内部監査）	**その他**
内部統制システムの一部であるすべての個々人は、組織が定めた全般的な戦略と目的を理解する必要がある。			
●目的の設定は、戦略計画に関連するプロセスの重要な部分である。 ●取締役会の監督の下、組織のミッション、ビジョン、	●事業体レベルの目的全体についての設定または承認には責任を負わない。しかし、コンプライアンスまたは品質コントロールのような専	●目的が設定されているか、またそれらが具体的で、測定可能または観測可能で、達成可能で、関連性があり、期限を定めたものであるか	●取締役会は、ハイレベルの目的が利害関係者のために価値を創造、維持、実現する方法に関する意思決定を反映したものとなるよう

戦略に合った事業体レベルの目的を設定する。 ●目的の達成に対するリスクが識別・評価できるような十分な詳細を備えた適切な目的を特定する。 ●個々のリスクに対して許容度を当てはめる。 ●事業体レベルの目的を、組織の管理体制を通して設定されるより具体的な下位目的とリンクさせる。 ●事業体レベルの目的と関連する下位目的の両方とも、具体的で、測定可能で、達成可能で、関連性があり、期限を定めたものとすべきである。	門的な特定分野に関連する目的または下位目的について、草稿、実施、モニター、報告を求められることがある。 ●適切なリスク選好と許容度が検討されたかを評価する。	を検証する。 ✓目的設定プロセスの全社的レビューは、単独の個別監査業務として実施することがある。 ✓個々の目的または下位目的は、他の内部監査業務中にレビューされることがある。 ●内部監査の組織上の独立性を維持するために、監査人は通常、（内部監査機能に関するもの以外の）目的は整備しない。	に、目的設定の監督に責任を負う。 ●取締役会は上級経営者とともに、適切なリスク選好とリスク許容度を確立し、それらが組織全体に伝達されることを確実にする。

原則７．組織は、自らの目的の達成に関連する事業体全体にわたるリスクを識別し、当該リスクの管理の仕方を決定するための基礎としてリスクを分析する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●目的達成に関連するリスクを識別し管理する。 ●取締役会の監督の下、組織のリスク選好とリスク許容度を決定し、リスク管理システムを構築し、個々のリスクの管理責任を定める。	●リスクとコントロールに関する重大な責任が、全社的リスク管理機能に移譲されることがある。代表的な業務には以下のようなものがある。 ✓リスクの共通語または用語集の作成。 ✓組織のリスク選好とリスク許容度の説明。 ✓「リスク棚卸表」の中のリスクの識別と説明。 ✓機能内および機能横断のリスクの優先順位付けをするためのリスク順位づけ方法の導入。 ✓他のリスク管理機能のしかるべき業務と連携するために、リスク委員会の設置または最高リスク責任者の任命。 ✓特定のリスクと対応の所有者の任命。	●組織のリスクフレームワークを考慮して、全組織的なリスクベースの監査計画を実施する。 ●独立性と客観性が侵害されない限り、しかるべき全社的リスク管理業務を手助けすることがある。 ●内部監査計画を策定するために、以下のようなものを検討する。 ✓固有リスクと残存リスクの識別と評価。 ✓リスク低減のためのコントロール、緊急時対応策、特定のリスクに結びついたモニタリング活動。 ✓リスク記録簿の正確性と完全性。 ✓経営者のリスクとコントロール活動に関する文書の妥当性。	●取締役会は、全般的な組織戦略および戦略に関連するリスクの理解を含めた組織目的を確立する。 ●取締役会は、目的達成に対するリスクを識別し管理するための責任を経営者に持たせ監督する。

	✓リスクが適切に管理されることを確実にするための行動計画の整備。 ✓各種利害関係者のための統合的な報告の作成。 ✓リスク低減のために講じた措置の結果のモニタリング。 ✓内部監査、コンサルティング・チーム、その他の評価者が対象とするリスク範囲の効率性の確保。 ✓第三者と遠隔地の従業員の参加を可能にするリスク管理フレームワークの整備。 ●セキュリティやコンプライアンス機能のような特定のグループは、組織の異なる業務や部署のために経営者が設定したリスク選好水準を考慮して、彼らの専門分野に関連するリスクの識別において経営者を支援することがある。		

原則８．組織は、内部統制の目的の達成に対するリスクの評価において、不正の可能性について検討する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●不正を識別、抑止、発見するプロセスを実施する。 ●組織の内部・外部監査人とともに、組織の不正エクスポージャーをレビューする。	●リスクとコントロールの評価に不正リスクの検討が含まれることを確実にする。 ●調査機能のようなグループが、不正の抑止と発見に重大な役割を果たすことがある。これらのグループは、不正に関する全社的な方針と手続の整備とモニタリングを担当することがある。	●『基準』は、監査中の分野において重大な不正の可能性を検討することにより、内部監査人が専門職としての正当な注意を払うことを求めている。 ●内部監査人は、不正リスクおよび経営者による不正リスクの管理方法を評価するために、十分な知識を持つことが求められている。しかし、主に不正の発見と調査に責任を負う者と同等の専門性を持つことは期待されていない。	●取締役会は、不正を抑止し発見するシステムとプロセスの監督に責任を負う。 ●取締役会と上級経営者は、不正の防止と発見のための気風を確立する。 ●取締役会は、財務報告不正を含めた組織の不正エクスポージャーに関する定期的な報告を受けるべきである。

原則９．組織は、内部統制システムに重大な影響を及ぼし得る変化を識別し、評価する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
変化は内部・外部のさまざまなところから起こり得るため、３つのディフェンスラインすべての個々人は内部統制システムに重大な影響を及ぼし得る新たな問題に警戒すべきである。			
●内部統制システムおよび内部統制システムに重大な影響を及ぼし得る変化を識別し評価する一義的な責任を負う。 ●取締役会が監督責任を果たすのに十分な詳細さで、内部統制システムに重大な影響を及ぼし得る変化に関する情報を、取締役会に伝達する。	●内部統制システムに重大な影響を及ぼし得る変化の影響の評価を支援するよう経営者から依頼されることがある。 ●変化に適応するために積極性が必要である。 ●組織の法務、規制、コンプライアンスのリスクに対する変化を定期的にモニターし検討する。	●定期的なリスク評価および内部監査業務を通じて、内部統制システムに重大な影響を及ぼし得る変化を識別し評価する。 ●組織のリスク評価に与える変化と影響を予測するために、経営者と定期的にコミュニケーションをとる。	●取締役会は、内部統制システムに重大な影響を及ぼし得る変化を識別し評価するプロセスを経営者が確立することを確実にする責任を負う。

原則10．組織は、内部統制の目的に対するリスクを許容可能な水準まで低減するのに役立つ統制活動を選択し、整備する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●日常的にリスクとコントロールの手続を実施するために、有効な内部統制を維持する。業務部門の経営者は、リスクを識別、評価、管理、低減し、内部の方針と手続を整備し運用するよう指導し、業務が設定されたゴールと目的に整合することを確実にする。組織の責任管理体制を通じて、中間層の経営者はコントロールとなる詳細な手続きを設計・導入し、従業員がそれらの手続を実行するのを監督する。 ●業務部門の経営者のガイダンスの下でコントロールはシステムとプロセスの中に組み込まれているため、必然的に第１のディフェンスラインとしての役目を果たす。コンプライアンスを確実にし、コントロールの機能不全、不適切なプロセス、予期せぬ事象を浮き彫りに	●第２のディフェンスライン内の機能は通常、経営者に代わって特定のコントロールのモニタリングに責任を負う。 ●第２のディフェンスラインの個々人は、経営者から任命されて特定のコントロールの選択と整備に参画することもある。しかしその場合でも、内部統制システムの責任は経営者が保持する。	●経営者によって整備されたコントロールについて、適切に整備され、効果的に運用され、目的達成に対するリスクが意図した許容水準まで低減されている、というアシュアランスを提供する。 ●内部統制の効率性と有効性の向上を意図して助言する。しかしその場合でも、内部統制システムの責任は経営者が保持する。	●取締役会は、経営者の内部統制システムが、目的達成に対するリスクを意図した許容水準まで低減していることを確実にするために、情報を評価し監督する。

するために、適切な管理監督的コントロールを整備すべきである。			

原則11. 組織は、内部統制の目的の達成を支援するテクノロジーに関する全般的統制活動を選択し、整備する。			
第１のディフェンスライン（リスクの所有者・経営者）	**第２のディフェンスライン**（リスク、コントロール、コンプライアンス）	**第３のディフェンスライン**（内部監査）	**その他**
●テクノロジーに関する統制活動を設計し適用する。これには、テクノロジーに関する方針と手続の策定と伝達、およびＩＴ統制が目的達成を支援するのに適切であることを確実にすることが含まれる。 ●新たなテクノロジーに関連するリスクエクスポージャーの変化をモニターし評価するプロセスを確立する。	●第２のディフェンスラインの個々人は、特定のテクノロジー統制のモニタリングに関連する職務を任されることが多い。 ●経営者の指名により、情報セキュリティ部のようなグループは、テクノロジーに係るコントロールの選択、整備、維持にも重要な役割を担うことがある。	●組織のＩＴガバナンスプロセスが組織の戦略と目的を支援しているかを評価する。 ●テクノロジー統制の効率性、有効性、網羅性についてアシュアランスを提供し、必要に応じて特定の統制活動の改善提案を行うこともある。 ●内部監査の独立性と客観性を維持するために、内部監査は通常はテクノロジーに関する全般的統制活動の選択や整備は行わない。しかしテクノロジー統制について提案を行うことがある。 ●内部監査人は業務遂行のために、ＩＴリスクとコントロールの十分な知識を持たなければならない。しかしＩＴ監査を主な職務とする監査人と同等の専門性を全監査人が持つよう期待されているわけではない。	●取締役会は、コントロールを指揮し評価しモニタリングする重大な監督責任を負っている。取締役会の監督責任は、ＩＴガバナンスに関する次のような側面も網羅すべきである。 ✓組織とガバナンスの体制。 ✓経営幹部のリーダーシップと支援。 ✓戦略的計画と業務運営面の計画。 ✓サービスの実施と測定。 ✓ＩＴ組織とリスクマネジメント。

原則12. 組織は、期待されていることを明確にした方針および方針を実行するための手続を通じて、統制活動を展開する。			
第１のディフェンスライン（リスクの所有者・経営者）	**第２のディフェンスライン**（リスク、コントロール、コンプライアンス）	**第３のディフェンスライン**（内部監査）	**その他**
●期待されていることを明確にした方針および行動を規定した関連性のある手続を通じて、ビジネスプロセスと従業員の日常業務に組み込まれる統制活動を設定する。 ●関連するリスクが存在するビジネスユニットまたは機	●経営者の指名により、特定の方針と手続への遵守状況をモニターする。 ●方針と手続の整備と伝達において、経営者を支援する。 ●組織が確立したリスク選好に関連してリスクがモニターされることを確実にする。	●方針、手続、コントロール手段の整備と運用についてアシュアランスを提供する。 ●方針と手続について改善提案を行う。しかし内部監査機能以外の業務の方針と手続の整備や運用については通常権限を持たない。	●取締役会は、業務を指導し目的達成を確かなものとするための強固な方針と手続のシステムが整備されるのを確実にするために監督を行う。

能の経営者（または任命された者）とともに、統制活動における行為責任と説明責任を明確にする。 ●十分な権限を有し、業務遂行能力のある構成員が、勤勉かつ常に集中して、方針と手続に示された通りに適時に統制活動を実施することを確実にする。 ●統制活動の結果として判明した問題点について、責任者が調査し対応することを確実にする。 ●継続して目的適合性があるかを判断するために統制活動を定期的にレビューし、必要に応じて更新する。			

原則13. 組織は、内部統制が機能することを支援する、関連性のある質の高い情報を入手または作成して利用する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●日常業務をモニタリングし組織中で情報を共有するために、データを作成して維持する。 ●伝達される情報の内容、品質、精度は目的達成にふさわしく目的達成を支援するものであるか、費用と便益を検討する。 ●情報の信頼性と完全性は経営者の責任である。この責任には、情報の保管方法に関係なく、組織のすべての重要情報が含まれる。情報の信頼性と完全性には、正確性、網羅性、セキュリティが含まれる。	●モニタリング活動に利用するために組織中からの情報を編集する。	●情報の信頼性と完全性および関連するリスクエクスポージャーについてアシュアランスを提供する。これには、内部と外部のリスクエクスポージャーと、組織外部の事業体との関係に関連するエクスポージャーが含まれる。 ●組織の情報の信頼性と完全性の実務について定期的に評価し、必要に応じて新たなコントロールの導入や安全対策の向上を提案する。このような評価は、単独の監査業務としてまたは内部監査計画の一部の業務としてのいずれかで行われ得る。 ●情報の信頼性と完全性が侵害されているか、また組織への脅威を示す状況が直ちに上級経営者、取締役会、内部監査へ知らされるか、を判断する。	●上級経営者と取締役会は、組織の成功をモニターし、リスクを予測し、投資家のような外部の利害関係者とコミュニケーションをとるための意思決定に、情報を活用する。 ●組織の内部統制システムの運用と有効性に関する報告を定期的に受け取る。

原則14. 組織は、内部統制が機能することを支援するために必要な、内部統制の目的と内部統制に対する責任を含む情報を組織内部に伝達する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●組織の全構成員が各自の内部統制の責任を理解し遂行するために必要な情報を伝達するプロセスを整備し維持する。 ●取締役会が事業体の目的に関する彼らの責任を果たせるように、取締役会に対して適切な情報を伝達する。 ●通常の伝達経路が機能しなかったり有効でない場合に、匿名または秘密の情報伝達ができるように二重の安全装置の役割を果たす、内部通報制度のような独立した伝達経路を確立する。	●特定のコントロールについてモニターし情報をまとめ、概要情報を第１のディフェンスライン、第３のディフェンスライン、取締役会に伝達する。 ●内部通報制度のような独立した伝達経路のモニタリングに責任を負うことがある。	●情報の網羅性、正確性、品質が取締役会と上級経営者のニーズに一致しているというアシュアランスを提供する。	●取締役会は、組織全体に期待する気風を伝達する。 ●取締役会と上級経営者は、各ディフェンスライン内の個々人から受け取ることを期待している情報の性質についてガイダンスを提供すべきである。

原則15. 組織は、内部統制が機能することに影響を及ぼす事項に関して、外部の関係者との間での情報伝達を行う。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●目的に適合する適時な情報を、株主、パートナー、所有者、規制当局、顧客、財務アナリスト、他の関係者等を含めた外部の関係者へ伝達するプロセスが整備されることを確実にする。 ●顧客、消費者、供給業者、外部監査人、規制当局、財務アナリスト等からの情報提供を可能にし、経営者と取締役会に対して目的に適合する情報を提供する、開かれた伝達経路を確立する。 ●外部の関係者による評価から得られた目的適合性をもった情報を、取締役会に伝達する。 ●適合性のある伝達方法を選択し、選択した伝達方法が伝達の時期、対象、性質お	●規制当局、外部監査人、その他特定グループへの一定のコミュニケーションの例外はあるが、第２のディフェンスラインは通常、内部統制機能に影響する事項に関して外部の関係者とコミュニケーションをとらない。 ●組織が外部に内部統制について報告する場合、第２のディフェンスライン機能は経営者の意見の裏付けとして自らの活動の結果を経営者に提供する。	●他者の重要なコミュニケーションが正確であるというアシュアランスを提供する。 ●内部監査機能は通常、内部統制の機能に影響する事項に関して外部の関係者とコミュニケーションをとらない。	●取締役会は外部者に伝達する前に、経営者から内部統制の機能と有効性および経営者の意見の根拠について、情報と報告を受け取るべきである。 ●取締役会は、組織の統制システムに関する外部報告に含まれる取締役会の意見について、外部監査人と協議すべきである。

よび法律、規則、受託責任に関する要件と期待を検討することを確実にする。 ●以下に関する適切な方針を制定する。 ✓組織外に情報を報告する際の承認要件。 ✓報告が許容される情報と許容されない情報に関するガイドライン。 ✓情報を受け取ることが承認される外部者と彼らが受け取れる情報の種類。 ✓組織外に情報を報告するためのプライバシー規制、規制要件、法的検討事項。 ✓組織外に伝達する情報に含まれ得るアシュアランス、助言、勧告、意見、ガイダンス、その他の情報の性質。			

原則16. 組織は、内部統制の構成要素が存在し、機能していることを確かめるために、日常的評価および／または独立的評価を選択し、整備および運用する。			
第１のディフェンスライン （リスクの所有者・経営者）	**第２のディフェンスライン** （リスク、コントロール、コンプライアンス）	**第３のディフェンスライン** （内部監査）	**その他**
●ビジネスとビジネスプロセスの変化の速度を検討し、リスクに応じて独立的評価の範囲と頻度を変えて、日常的および独立的評価のバランスを選択し整備する（これらの評価は、第２のディフェンスラインが行うことがある）。 ●日常的および独立的評価を実施する評価者が、評価対象を理解する十分な知識を持ち合わせていることを確実にする。 ●日常的および独立的評価の基準を確立するために、内部統制システムの設計と現状が使われることがある。 ●組織のリスクマネジメント活動の実績について、取締役会に定期的に報告する。	●経営者が指揮する内部統制システムの各種構成要素の状況をモニターするために、継続的および独立的評価を実施する。 ●目的の達成が定められたリスク許容度内であるかをモニターするために、継続的および独立的評価を実施する。	●経営者の日常的評価がビジネスプロセスに組み込まれており、状況の変化に応じて調整されているというアシュアランスを提供する。 ●経営者の評価からもたらされる情報が、公正かつ正確に示されているというアシュアランスを提供する。 ●内部統制システムが期待通りに運用されており、リスクが組織のリスク選好と許容度の範囲内で管理されているというアシュアランスを提供する。	●取締役会は経営者に、内部統制の構成要素の評価を選択、整備、運用する責任を持たせ、監督する。 ●組織のリスクおよびリスク管理活動の有効性に関する定期的な報告を受け取る。

原則17. 組織は、適時に内部統制の不備を評価し、必要に応じて、それを適時に上級経営者および取締役会を含む、是正措置を講じる責任を負う者に対して伝達する。			
第１のディフェンスライン（リスクの所有者・経営者）	**第２のディフェンスライン**（リスク、コントロール、コンプライアンス）	**第３のディフェンスライン**（内部監査）	**その他**
●内部統制の不備についての情報を、是正措置を講じる責任者および必要に応じて上級経営者と取締役会に伝達する。 ●不備が適時に是正されていることを追跡管理する。	●第２のディフェンスラインの個々人は、特定の種類の内部統制の不備のモニタリングと報告の責任を移譲されることがある。	●内部監査人は、経営者へ伝達した内部監査の検出事項および改善勧告について、解決状況をモニターするシステムを確立し維持する。このシステムは、通常以下を検討する。 ✓監査検出事項と改善勧告への対応に経営者が必要とする時間。 ✓経営者の対応の評価。 ✓（適切な場合）経営者の対応の検証。 ✓（適切な場合）フォローアップ監査の実施。 ✓リスクの前提を含め不満足な対応や措置を上級経営者または取締役会へ上申するプロセス。	●取締役会は、内部統制の不備に関する情報を適時に受領し、重大な統制の不備に対する是正措置が適時かつ適切であることを確実にすべきである。 ●経営者と取締役会は、必要に応じて日常的および独立的評価の結果を検討する。

著者について

ダグラス J. アンダーソン氏は、公認内部監査人、公認会計士、公認リスク管理監査人、公認管理会計士の資格を持ち、ＩＩＡのAudit Executive Center©のコンサルタントであり、サギノー・バレー州立大学客員講師であり、ガバナンス、リスク、コントロールに重点を置いたコンサルティング・サービスを行っている。内部監査、外部監査、会計、ファイナンスの分野で30年以上の経験があり、その職責は世界中の多様な組織に及んだ。ＩＩＡでインストラクター、プロフェッショナルガイダンス委員会の委員長および委員、理事会のプロフェッショナルガイダンス担当副会長などの多くのボランティアを務め、また、公開会社会計監督委員会（ＰＣＡＯＢ）の常任アドバイザリーグループおよびＣＯＳＯの２つのプロジェクトの監督グループのメンバーも務めた。

ジーナ・ユーバンクス氏は、公認内部監査人、公認情報システム監査人、公認リスク管理監査人、内部統制評価指導士の資格を持ち、ＩＩＡのプロフェッショナルサービス担当ヴァイスプレジデントとして品質評価、内部監査部門長サービス、業種別サービスなどのプログラムを統括している。彼女は、４大監査法人の１つでグローバル・エンタープライズ・リスク・サービスの業務を15年間担当したのを含めて20年以上の内部監査経験があり、その経歴は米国内外におよび、特にインドに長く滞在した。小売業と金融サービス分野で実務家およびディレクターも経験し、地元の金融機関の監査委員会の委員も務めており、また、ＩＩＡのボランティア・リーダーも15年近く務めた。

ＣＯＳＯについて

1985年に創立されたＣＯＳＯは、５つの民間組織の共同体であり、全社的リスクマネジメント、内部統制および不正抑止に関するフレームワークとガイダンスの開発を通じて先導的な考え方を提供することに取り組んでいる。ＣＯＳＯを構成している組織は、内部監査人協会（ＩＩＡ）、米国会計学会（ＡＡＡ）、米国公認会計士協会（ＡＩＣＰＡ）、国際財務担当経営者協会（ＦＥＩ）および管理会計士協会（ＩＭＡ）である。

ＩＩＡについて

内部監査人協会（ＩＩＡ）は、内部監査の専門職の提唱者、教育者および基準、ガイダンス、公認資格の提供者として最も広く認められている。1941年に創立されたＩＩＡは、今日では170か国の18万人以上の会員にサービスを提供している。ＩＩＡの本部所在地は、米国フロリダ州アルタモンテ・プリングスである。ＩＩＡに関する詳しい情報は、ＩＩＡのホームページを参照いただきたい。

ＩＩＡのAudit Executive Center©は、内部監査部門長（ＣＡＥ）の一層の成功を支援するための重要なリソースである。同センターの情報、商品、サービスは、専門職に特有な課題や新たなリスクにＣＡＥが対応できるようにするためのものである。センターに関する詳しい情報は、ＩＩＡのホーム―ページ内を参照いただきたい。