内部監査人協会（ＩＩＡ）情報

グローバルな視点と洞察

内部監査とコンプライアンス：ガバナンス強化のための明確化と協働

内部監査人協会（ＩＩＡ）

訳者：堺　　咲　子

内部監査人協会（ＩＩＡ）国際本部　理事　専門職資格担当
インフィニティコンサルティング　代表
プレミアアンチエイジング株式会社　社外取締役
ＣＩＡ，ＣＣＳＡ，ＣＦＳＡ，ＣＲＭＡ

目　次

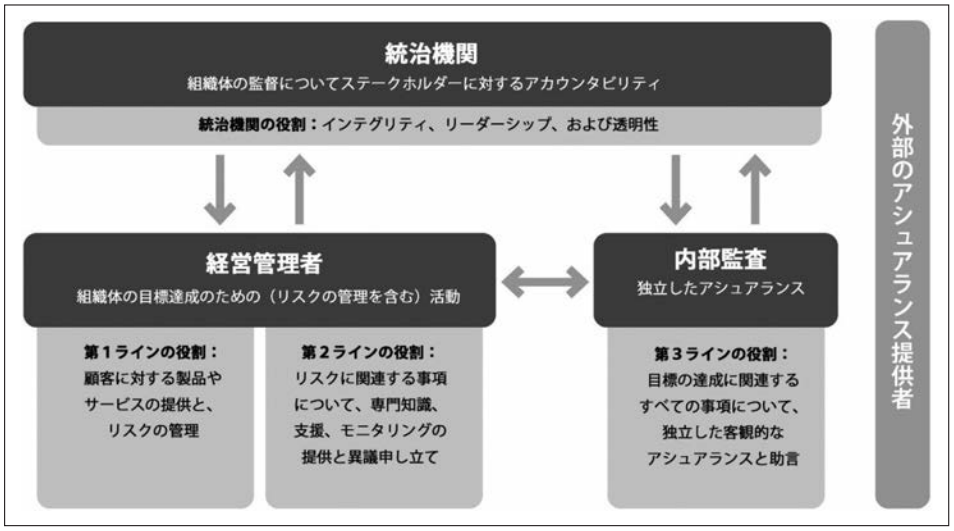
はじめに

内部監査とコンプライアンスの関係は不明確な場合があり、重要な疑問が生じている。内部監査は、コンプライアンスに責任を持つことができるか。コンプライアンス機能は、組織体全体のすべてのコンプライアンスに責任があるか。内部監査部門長（ＣＡＥ）として、コンプライアンスを担当しても良いのか。

本稿は、これらの複雑な問題を明確にし、混乱、ギャップ、および不要な重複を避けるための一助となることを目的としている。明確な理解が不可欠であり、協働が強く奨励されており、また、内部監査の独立性[1]が基本的に重要である。

本稿は、コンプライアンスを監査する方法に関する論文では**ない**。むしろ、取締役会、経営管理者、コンプライアンスの専門家、およびＣＡＥのためのツールであり、内部監査とコンプライアンスの関係を説明する方法として**３ラインモデル**[i]を使用している。**３ラインモデル**の「６つの原則」と、それらをコンプライアンスに適用する方法は、本稿の後半で詳しく検討する。

読者は、本稿を利用して、法域、業種、複雑さ、成熟度、または規模にかかわらずガバナンス構造内で、**３ラインモデル**に関連する様々な側面での効果的なコンプライアンスとコンプライアンス・リスク・マネジメントを明確に識別し、理解し、評価し、適用すべきである[2]。リスクやコンプライアンスの責任者と内部監査人が現場で直面しているコンプライアンス問題の実例は、**３ラインモデル**に従ってコンプライアンス活動の調整を評価する際に、モデルの「６つの原則」を実務に適用する上で有用である（27～34ページを参照）。



[1] 持続可能なガバナンスの一部としてコンプライアンスが不可欠であることは、B20イタリアが『B20イタリア：インテグリティとコンプライアンスの政策文書2021』（https://global.theiia.org/about/about-internal-auditing/Public%20Documents/B20-Italy-Integrity-and-Compliance-Report.pdf）におけるG20の中で、重要な焦点と政策行動として大臣に推奨している。特に、同文書11ページの政策行動2.1は、３ラインモデルで説明されている内部監査の役割に具体的に言及している。

[2] 特定の法域や業種では、コンプライアンスおよびコンプライアンス・リスク・マネジメントに関連する役割と責任が高度に定義されており、広範な法律、規制、判例、および学術研究の対象となっている。より詳細な研究が利用できるため、本稿の読者にはそれらを参照することをお勧めする。例えば、American Law Instituteの「Principles of the Law、Compliance、Risk Management、and Enforcement No.1 (https://www.ali.org/smedia/filer_private/85/7b/857b5fbb-2995-4146-b939-b14a79e93964/compliance_td_1_-_catalog.pdf)」および「Principles of the Law、Compliance and Enforcement No.2 (https://www.ali.org/smedia/filer_private/19/ec/19ecf7f3-594e-44c0-9773-595ae2f8ebe/compliance_td2_-_catalog.pdf)」を参照。

訳注[i] **３ラインモデル**の日本語訳は、月刊監査研究2020年８月号に掲載。

アカウンタビリティ、活動、およびアシュアランス

３ラインモデルは、統治機関のアカウンタビリティ、経営管理者による活動、および内部監査による独立したアシュアランスが、効果的なガバナンスの基盤となることを説明している。また、「６つの原則」が、組織体におけるそれぞれの役割と責任を評価する上で、どのように役立つかを示している。このモデルの中核となる要素と「６つの原則」の適用方法は、組織体の目標、資源、および状況によって異なる。このモデルは、組織体が目標の達成に最適な構造を特定し、プロセスを設計し、責任を割り当てるのに役立つ。これには、コンプライアンス・リスクの管理が含まれる。これは経営管理者の責任[3]であるが、協働によって達成される。

組織体が検討すべきコンプライアンス要件や期待の範囲は、法律、規則、規制などの外部から課せられるものと、方針、基準、手続、行動規範や行為規準などの内部から課せられるものがある。それらは、正式かつ明示的に定義されている場合もあれば、社会的、倫理的、文化的な期待などのように、より暗黙的な場合もある。この幅広く動的な範囲に及ぶ検討事項を、本稿では「要件や期待」と呼ぶ。

ステークホルダーは、組織体がその目的を果たし、合法的かつ倫理的に価値を最大化することを期待している。そのため、組織体は重要な領域のコンプライアンスを注視することに投資している。例えば、安全衛生、雇用、データ保護とプライバシー、法人・商業法規、業界規制、品質基準、贈収賄と汚職の防止、投資家と消費者の保護、財務報告と税務、および個人の行動規範などであり、数え上げればきりがない。コンプライアンスは、効果的なガバナンスに対する全体的なアプローチの一部として、**３ラインモデル**で説明されているように、アカウンタビリティ、活動、およびアシュアランスの文脈で理解して実施することができる。

コンプライアンスとは何か

組織体は、事業を行うための前提条件として、適用法令やその他の外部要件を遵守（または適合）しなければならない。これらのコンプライアンス要件は、従業員との関係から納税に至るまで、あらゆることを網羅している。特定の業種では、様々な規則設定機関、監督者、規制当局、および定義された要件があるが、外部から課せられる法規制上の限度や制約が少ない業種もある。とはいえ、公的部門でも民間部門でも、外部のコンプライアンス要件がない組織体を見つけるのは難しい。

同時に、組織体は、方針と手続の形で内部の期待を設計し、策定し、導入し、倫理的な行動や行為の基準を設定する。ある種の規制産業では、組織体は外部の要件に従って、内部の方針、基準、および行動規範を定めて遵守しなければならない。このように様々な要件が何層にも重なっているため、組織体の「コンプライアンス」の概念は様々な側面を持つようになる。したがって、コンプライアンスを、広範な側面、関連性のある側面、および異なる側面のそれぞれから考察し、組織体でどのように議論されているかを検討することは有用である。すなわち、成果としてのコンプライアンス、リスクのカテゴリー[4]としてのコンプライアンス、組織体の役割、部門、

[3] 本稿では、**経営管理者**は、統治機関または内部監査の責任ではない役割を特定するために広く使用されている。
[4] 組織体のコンプライアンス・リスクの幅広いカテゴリーのもとで、リスク分類法では、法律、規則、規制、方針、または行動に関する特定のリスクと関連するリスクの両方を扱うサブカテゴリーのカスケードが特定される。

機能等[5]としてのコンプライアンス、さらに、一連の活動としてのコンプライアンス、である。

これらのそれぞれについて、以下で説明する。

成果としてのコンプライアンス

組織体は、法律、規則、方針、規範などを遵守するために、または「遵守した状態である」ために、様々な活動に従事している。特定のコンプライアンス要件や期待を達成することは、多くの場合、事業を運営して戦略目標を追求するための必要条件である。

リスクのカテゴリーとしてのコンプライアンス

「専門職的実施の国際フレームワーク」は、リスクを、**組織体の目標の達成に影響を与える事象発生の可能性**と定義している。これらの影響は、好ましい場合と好ましくない場合がある。したがって、リスクを評価するときは、コンプライアンスの要件や期待を、コンプライアンス違反の可能性と、それが目標へ与える潜在的な影響とともに検討することが不可欠である。

組織体には、コンプライアンスとコンプライアンス違反の両方に関連するリスクがある。それらの影響は、有形または無形の報酬や罰則という形をとる場合がある。例えば、国際標準化機構（ＩＳＯ）規格の遵守は、業務効率やその他の利益、さらに自主的な規範に従うことで得られる好意的な注目を生み出すように設計されている。コンプライアンス違反は、これらのメリットをなくして直接的な損害をもたらすだけでなく、罰金の賦課、免許の取り消し、制裁措置、事業の終了、民事・刑事訴追、資金や支援の喪失などのペナルティが科せられる可能性がある。さらに、コンプライアンス違反は、潜在的なステークホルダーの不満、世間の批判、またはその他の損害の形で評判リスクを引き起こす可能性がある。

コンプライアンス・リスクの識別、測定、および評価、ならびにコンプライアンス・リスクのリスク選好と許容度の決定は、方針、手続、制限、およびコントロールを含む適切な対応を決定するのに役立つ[6]。

役割や組織体の部門としてのコンプライアンス

コンプライアンスは、特定の要件や期待に応えるために、あるいはコンプライアンス関連の問題に関する監督、専門知識、チェックと異議申し立て、モニタリング、テスト、またはアシュアランスを提供するために、設けられた役割や部門を指すことも多い。これらは、**３ラインモデル**で説明されているように、様々な第１ラインや第２ラインの役割の特徴であり、経営管理者の全体的な権限と責任の範囲内に存続し、その役割の特定の特性に応じて、第１ラインの役割を持つ人々と経営幹部に対して、専門家としての支援とリスク・マネジメントを提供することもある。

法規制の要件、ならびに組織体の業種、規模、および複雑さに従って、コンプライアンス上級職は、その具体的な責任に応じて、組織体内の様々な役割の中の１つに直属する場合がある。それらには、経営幹部（最高経営責任者（ＣＥＯ）、最高リスク管理責任者、最高執行責任者、法務顧問など）やそれらの

[5] 特定のリスクを担当する役割として、コンダクト・リスク責任者、データ保護リスク責任者などを定義することもできる。

[6] トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）は、リスク・マネジメントのためのフレームワークや、ＥＲＭリスクフレームワークをコンプライアンス・リスクの管理に適用するための新しいガイダンスなど、ソートリーダーシップを提供している。

直属者、あるいは統治機関や指定された小委員会への直属が含まれる。場合によっては、繰り返すが上記で明らかにした要因と内部監査部門の独立性を確保するための仕組みを条件として、コンプライアンスの役割や部門が、ＣＡＥまたはコンプライアンス部門と内部監査部門の両部門を監督する者に直属する場合もある。そのような場合は、**３ラインモデル**で説明されている「６つの原則」を適用して、コンプライアンスに関する各役割の責任が要件や期待に沿っているかを評価すべきである。このモデルで説明されているように、連携によって潜在的な利害の衝突や、客観性または独立性の侵害が見られる場合は、軽減措置を講じるべきである。客観性に対する潜在的または実際の衝突や侵害もまた、検討したり可能な措置を講じたりするために統治機関に報告すべきであり、必要に応じて規制当局にも報告すべきである。

一連の活動としてのコンプライアンス

コンプライアンスとは、コンプライアンスを達成、支援、モニター、監督、チェック、テスト、異議申し立て、または確認するために設計されたプロセスとコントロールを指すことがある。これらの手段の実施者は、組織体とその構成員が要件や期待を確実に遵守するための支援をする。

組織体内のコンプライアンスは、組織体のために働く、または組織体とともに働くすべての人が、それぞれの役割と年功に応じた活動や行為を行うことで達成される。

特定の要件や期待を一定のレベルで確実に満たすように設計された日常的なプロセス、手続、およびコントロールに対する責任は、組織体内の様々な場所にあり、また外部に委託する場合もある。**３ラインモデル**では、役割の調整を評価する際の重要な要素は、コンプライアンス活動に関連する意思決定権を特定することであるとしている（コンプライアンスを構成する詳細な役割と活動については、付録を参照）。

３ラインモデル

コンプライアンス

統治機関は、ガバナンスに対する最終的なアカウンタビリティを負っており、アカウンタビリティは、統治機関の活動と行為、および経営管理者と内部監査によって達成される[7]。

各組織体は、所定の外部要件に従って、自らの状況に応じてコンプライアンスの側面に関する責任を割り当てるので、組織体全体に割り当てられた特定の役割と責任が、**３ラインモデル**の「６つの原則」とどの程度整合しているかを分析しなければならない。評価によって、ある責任は統治機関の役割に、コンプライアンスとリスク・マネジメントを含むある責任は経営管理者の役割に、ある責任は内部監査の役割に整合することが示される場合がある。

第１ラインの役割には、クライアントや顧客に製品やサービスを提供することや、要件や期待を遵守して製品やサービスの提供を行うために必要な支援をすることが含まれる。第２ラインの役割は、専門家として監督と助言を行い、（特に総体で、またはポートフォリオベースで）リスクを評価し、（モニタリング、監督、およびテストを含む）リスク・マネジメント活動を実施し、第１ラインに信頼に足る異議を唱えることである。第３ライン

[7] 統治機関の構造は、法域、規制要件、および個々の機関設計によって異なる。統治機関という場合、様々な法域、業種、および公的部門と民間部門の両方で見られる幅広い統治機関の構造が含まれる。統治機関の責任には、次のようなものがある。組織体の方向性の設定。ビジョン、使命、価値観、およびリスク選好の定義。実際の、および期待される成果、ならびにリスクとリスク・マネジメントに関する経営管理者からの報告の受領。

の内部監査の役割は、第２ラインが第１ラインにどれだけうまく信頼に足る異議を唱えているかについてのアシュアランスを含む、独立したアシュアランスを提供することである。これらの役割の活動が、過度な重複やギャップがなく、また、矛盾や不整合がないように的確に調整されるようにするために、適切な連携、コミュニケーション、および協働を通じて効果的に取り組む必要がある。

このモデルを表すために使用された図は、コンプライアンスの役割や部門、あるいは特定の第２ラインの役割、部門、または責任を特定するものではない。この図は、所定の組織構造ではなく、ガバナンスの中心的な役割間の関係を示している。

コンプライアンスの役割と活動に対する責任の決定

アカウンタビリティ、活動、およびアシュアランスは、ガバナンスに不可欠な要素である。 リスク・マネジメント、コンプライアンス、倫理、サステナビリティ、セキュリティ、データプライバシー、法務、財務管理などの専門部署の設置や特性は、多くの要因に左右される。 それらには、組織体の複雑さ、規模、業種、資源、規制、法律とカルチャー、統治機関のリスク許容度とリスク選好などがあり、そして重要なのは、各専門部署内の役割の目標と責任である。

一部の業種では特定の規制によって、単独では所定のコンプライアンス部門を持たない組織体もある。また、コンプライアンスに関連した肩書きや職務記述書を持つ人がいない組織体も多い。

しかし、たとえコンプライアンスに関する役割や部門が定められていない場合でも、組織体は効果的なガバナンスを発揮して要件や期待を遵守することができる。ただし、該当する要件や期待を遵守するために組織体に応じた役割と責任を割り当て、さらに、定められた役割を個人が遵守することが条件である。

通常、組織が大きくなり、より複雑になり、資源が豊富になり、あるいは規制が厳しくなると、コンプライアンスの様々な側面について、個々の役割や部門に別々の責任や資源を割り当てることを決定したり要求したりする場合がある。

さらに、１人の従業員が複数の役割を担当する場合もある。この場合、これらの複数の役割の両立性を適切に評価して、各役割の責任と、それらの役割の遂行に対する監督とアシュアランスを明確に定義すべきである。場合によっては、統治機関や規制当局による承認が必要になることもある。

複数の役割を担うと、両立不能性や利害の衝突というリスクが増し、また、アカウンタビリティと責任の明確さが損なわれる可能性がある。リスク選好の範囲内に収めるためには、リスクの軽減措置が必要となる場合があり、また、該当する場合には統治機関や規制当局に報告する必要がある。

コンプライアンスを達成するための共同の取り組み

コンプライアンスに関する役割や部門が定められている場合でも、すべてのコンプライアンス活動が組織体内の１か所にのみ存在するわけではないことを認識することが重要である。すべてのレベルの従業員、および業務執行役員と非業務執行役員は、コンプライアンスの取り組みに共同で貢献することが求められる。コンプライアンスを達成し、コンプライアンス・リスクを軽減し、要件や期待の遵守をモニターするために、責任とアカウンタビリティは、組織体の階層、定義された役割、およびライン・マネジメント構造全体に分散されている。

外部と内部の要件や期待に対するコンプライアンスは、専門部署や所定のコンプライアンス部門外の個人が対処することが多い。そ

れぞれの役割と責任は、業種に対する規制によって、または特定の個人や一連の要件や期待によって、より狭く定義される場合がある。例としては、人事部門が担当する人事関連の法規制の遵守、財務部門が担当する財務報告や税務上の要件の遵守などがある。

上述のように、様々な役割や部門が、コンプライアンスの達成、ならびにコンプライアンス面の監督、モニタリング、およびテストを担当する場合がある。そのため、個々の役割とその責任のコンプライアンス関連の特性を明らかにする際には、「６つの原則」を適用することが明らかに重要である。

効果的なガバナンスは、正式なコミュニケーション、連携、および協働からだけでなく非公式のコミュニケーションからも恩恵を受け、透明性を高める。ただし、ガバナンス構造やコントロール構造における非公式の交流が、コンプライアンス上の問題の適切な識別、上申、および軽減を妨げる場合、正式なガバナンス構造やコントロール構造の有効性が損なわれ、アカウンタビリティと責任の決定が曖昧になる可能性がある。

ガバナンスモデルの有効性を評価する際には、コンプライアンスを達成するために設計し構築した正式なガバナンス構造を評価するだけでなく、非公式なコミュニケーション、意思決定、および行動について組織体を調査して、非公式なガバナンス構造が正式なガバナンス構造を弱めたり台無しにしたりしないか、どこで、いつ、そうなり得るかを特定することが不可欠である。**３ラインモデル**では、コミュニケーション、連携、および協働を促進するために、強力な公式・非公式な交流が奨励されている。しかし、非公式なガバナンス構造は、コンプライアンスを妨げ、コントロールを回避し、効果的でないコンプライアンス・リスク・マネジメントをもたらし、責任とアカウンタビリティの明確さを曖昧にする可能性がある。**３ラインモデル**を適用して役割、責任、および活動を特定することで、組織体は、コンプライアンスの失敗につながり得る非公式なガバナンス、意思決定、および活動のリスクを軽減するためのセーフガードの策定を含む、効果的なガバナンス・フレームワークを設計できる。

効果的なコンプライアンス・プログラムは、文書化された正式なガバナンス構造とコントロール構造の採用と遵守を促進するだけでなく、コンプライアンスとコントロールのカルチャーの展開と維持のための重要な要素となり、**３ラインモデル**の有効性を高める。

６つの原則の適用

３ラインモデルは、コンプライアンスに関する特定の要件や期待などの組織体の状況を考慮しながら、原則ベースのアプローチで役割と責任を評価して調整することを奨励している。このモデルの「６つの原則」は、成果としてのコンプライアンス、リスクのカテゴリーとしてのコンプライアンス、役割や部門としてのコンプライアンス、および一連の活動としてのコンプライアンスについて、また、ガバナンス・フレームワークを成功させるためのコンプライアンスの貢献について、理解を深めるために利用することができる（「６つの原則」の全文は、**３ラインモデル**を参照）。

原則１：ガバナンスの要件を定める

原則１は、ガバナンスの最低要件を以下のように述べている。

- アカウンタビリティ（統治機関がステークホルダーに対して成功のために）
- 活動と資源の適用（リスクとコンプライアンスの管理を含め、経営管理者が目標達成のために）
- アシュアランスと助言（効果的な監督と透明性を可能にし、信頼と継続的な改善を促進するために、独立した内部監査機

能がすべての側面に関して）

統治機関は、組織体が一般に認められた基準や社会規範に従って行動することを確実にする最終的なアカウンタビリティを負っている。経営管理者は、統治機関が表明したリスク選好に従って、コンプライアンスとコンプライアンス違反に関連するリスクを管理しなければならない。これには、コンプライアンスの側面に特に焦点を当てた個々の役割やチームを定めることや、リスクを所有する第１ラインと信頼に足る異議を唱えて第１ラインがリスク選好に適合するように促す第２ラインとの間の意思決定権を明確に定義することが含まれる。内部監査は、経営管理者と統治機関に対して、コンプライアンスに関するコントロールの適切性と有効性についてのアシュアランスと、継続的な改善と革新のための助言を提供する。

現場の実例

「医療は規制の厳しい業種なので、ほぼすべてのサービスの提供には、何らかの規則、規制、または基準の遵守が伴う。看護師、医師、およびその他の医療従事者は、提供するすべてのサービスが適切に承認され文書化されるようにしなければならない。コンプライアンスの担当者（個人の役割や部門）は、特定の手続の文書化と承認の要件について臨床部門に助言することができるが、最終的には、第１ラインの医療従事者がプロセスとコントロールを実施し、これらの要件を確実に遵守する責任がある。

―米国、

コンプライアンス・内部監査責任者」

「私の業界の例では、組織体や規制要件に対するコンプライアンス・リスクの上位をランク付けし、規制要件を遵守するための活動、コントロール、モニタリング、および責任を、これらのリスクに応じて調整することが挙げられる。例えば、ある組織体には、規制要件に従って、マネーロンダリング防止コンプライアンス責任者、プライバシー責任者、贈収賄防止責任者などがいる場合があり、これらの主要なリスク領域のコンプライアンスと管理の達成を支援するために、製品、情報開示、雇用、苦情等について責任と特定の資源を持つ場合がある。統治機関には定期的な報告が行われ、すべての活動は独立した内部監査の対象となる。

―英国、最高コンプライアンス責任者」

「組織体が現在直面している課題の好例として、“環境、社会、ガバナンス”すなわち“ＥＳＧ”基準の採用と活用の推進が挙げられる。統治機関は、統治機関が定めた戦略、基準、および社会規範に従って組織体が行動するように、経営管理者にアカウンタビリティを負わせる責任がある。ＥＳＧは、組織体の隅々まで、そしてすべての従業員、サプライヤー、および顧客に及ぶため、統治機関は、組織体に当てはまるＥＳＧリスク、外部の法律や規制、内部の方針と手続、関連する業績指標、およびそれらの内部の要件や期待に対するコンプライアンスの達成を反映するための信頼できる真正で比較可能なデータが、経営管理者によって明確にされていることを確認しなければならない。さらに、経営管理者と統治機関の双方が、ＥＳＧコンプライアンス目標の達成に関するアシュアランスを望んでいる、または必要としている。ＥＳＧを活用して、コンプライアンスを実証するために必要なそれぞれの役割と部門、およびそれらの活動を把握するためには、組織体全体の責任とアカウンタビリティを複雑にマッピングする必要がある。

―米国、最高コンプライアンス責任者」

原則２：適切なガバナンスの監督を継続する

原則２は、統治機関の役割を以下のように定めている。

- ガバナンス
- 経営管理者の監督
- 有能な内部監査機能の確立と監督

統治機関は、ガバナンスに最終的な責任を持ち、適切な構造とプロセスがあることを確認する。これには、コンプライアンスに関する取り決めや、内部監査の役割の監督も含まれる。

統治機関は、リスクへのエクスポージャーのレベルや、戦略目標に影響を与える可能性に関連する要件や期待の遵守について、どの程度信頼し、要求するかを判断しなければならない。統治機関は、コンプライアンス・リスクのリスク選好や許容度の決定にあたり、リスク選好や関連する許容度に従ってコンプライアンスの成果を達成するための、経営管理者の活動の遂行と、所定の役割や部門による責任の遂行を監督する。

統治機関は、内部監査がコンプライアンスに関して独立した効果的なアシュアランスと助言を提供できるように、適切に位置付けられ資源が確保されるようにすべきである。ＣＡＥは、その権限と独立した地位を確保するために、統治機関、独立監査委員会、または統治機関が指定した同等の委員会に対してアカウンタビリティを負わなければならない。

現場の実例

「有能な統治機関は、組織体全体に変化をもたらし、影響力を持つことができる。上申や報告が当然のように行われる場合もあるが、過去のデータに基づいた遡及的な対応ではなく、“現在”において効果的な監督と指示を行うためには、統治機関がどれだけ最新の情報を持っているかと、その情報の質とにかかっている。内部監査は、統治機関が、リスクに関する予測、監督、および指示を行うために、管理されているリスクについて明確な見通しを入手しているかを検証すべきである。コンプライアンスは、コンプライアンスとコントロールの有効性に関して経営管理者に異議を唱え、また、リスク選好内でのコンプライアンス・リスク・マネジメントの有効性に関して統治機関に洞察を提供するという、重要な第２ラインの役割を果たす。

―シンガポール、
コンプライアンス責任者」

「医療をはじめとする多くの業種では、コンプライアンス部門が、研修と教育、ホットラインのモニタリング、倫理規定の周知、身元調査の実施など、コンプライアンス・プログラムの一定の要素に対して日常的な責任を負う場合がある。これらの活動の中には、コンプライアンスを達成するためのものもあれば、方針を設定し、モニタリングし、またはコンプライアンスの有効性に関して経営管理者と統治機関へ報告するためのものもある。コンプライアンス部門がＣＡＥに直属している場合、内部監査部門は、コンプライアンス・プログラムの有効性について独立したアシュアランスを提供することはできない。ただし、そのような場合には、独立した第三者を雇うことによって統治機関にアシュアランスを提供することができる。

―米国、
コンプライアンス・内部監査責任者」

「統治機関は、内部監査の監査計画の中でコンプライアンス・リスクが徹底的に評価され検討されるようにし、主要な規制リスクと規制当局の重点領域に関する内部監査の複数年の対象範囲を理解し、また、コンプライアンス関連の報告や活動の結果をレビューするように努めるべきである。

―英国、ＣＡＥ」

「統治機関は、経営管理者と内部監査の双方に対して、コンプライアンス・リスク・マネジメントの方向性を示す。統治機関が効果的にコンプライアンスの監督をするためには、経営管理者と内部監査の双方が提供する、コンプライアンスの状態に関する適切な定量・定性情報について、十分に定期的かつ頻繁に調査しなければならない。統治機関は、違反、不履行、および是正に焦点を当てた単なる後ろ向きで場当たり的な対応をするのではなく、前向きなコンプライアンス・リスク・マネジメントに取り組むために、コンプライアンス・リスク・マネジメント活動の範囲を常設議題とすべきである。

―英国、最高コンプライアンス責任者」

原則３：第１ラインと第２ラインの経営管理者の役割を定義する

原則３は、経営管理者の役割（資源、目標、規制などに応じて組み合わせたり分けたりする場合がある、第１ラインと第２ラインの両方の役割）を述べている。

第１ラインと第２ラインの役割が、経営管理者を構成している。それらは、顧客に製品やサービスを提供するという第１ラインの責任と、専門家として監督し、（特に総体で、またはポートフォリオベースで）リスクを評価し、リスク・マネジメント活動を実施し、第１ラインに信頼に足る異議を唱えるという第２ラインの責任を反映している。

コンプライアンス部門などの独立した部門を設置する場合もあれば、部門長、または小規模で複雑でない組織体では個人を任命して、統治機関に直接または統治機関の委員会を介して報告する場合もある。部門長または個人は、ＣＥＯまたは経営管理者の中の指名された者に対して共同で報告する場合もある。このような統治機関への報告経路やアカウンタビリティは、コンプライアンス部門長や個人の独立性を高めるように見えるかもしれない。しかし、独立性の重要な点は、意思決定の責任がないことである。通常、コンプライアンスの役割を担う個人は、顧客の承諾、方針の例外適用の許可、新製品の承認など、ある程度の経営上の意思決定責任を保持している。したがって、統治機関や統治機関の委員会への報告経路があっても、そのような部門、部門長、または個人に真の独立性をもたらすものではない。内部監査とＣＡＥは、その報告経路が経営管理者から独立していることに加え、経営管理者の業務上の意思決定の責任を負っていないことも、さらなる独立性をもたらしている。

したがって、３ラインの役割の特徴は、以下のように明確に示すことができる。

- 第１ラインの役割：製品やサービスを提供する上で、法律、規制、行動規範、組織体の方針等を遵守すること。コンプライアンスは経営管理者の責任として存続する。
- 第２ラインの役割：個々のコンプライアンスの役割や部門は、フレームワークを構築し、監督を実施し、助言、モニタリング、および監視を行い、テストを実施し、経営管理者へ異議を唱え、また、一般的には経営管理者の業務上の意思決定やリスク所有の権限を持つことができる（例：顧客やクライアントの承諾、新製品やサービスの承認、取引の承認、限度額超過の承認、方針の例外適用などが含まれる場合がある）。
- 第３ラインの役割：内部監査は、コンプライアンス、コンプライアンスを達成するための経営管理者の取り組みの有効性、およびコンプライアンス・リスク・マネジメントの監督とコントロールをモニタリングして提供するためのコンプライアンス担当者や部門の作業について、独立したアシュアランスを提供するが、

その逆はない。内部監査は、経営管理者の意思決定の責任を持たず、独立した立場で統治機関に報告する。

３ラインモデルを用いることで、組織体は要件や期待に対するコンプライアンスを達成し、効果的で持続可能なガバナンスに貢献し、違法行為や腐敗に対抗することができる。コンプライアンスは、透明性を基盤として、組織体内の適切な基準を設定しなければならない。また、株主、政府機関、規制当局と取引所、サプライヤー、およびサプライチェーンなどの外部のステークホルダーにとっても、透明性を高める効果的なコンプライアンス・プログラムは、組織体に対する信頼性を高める。

現場の実例

「第１ラインと第２ラインの役割は、組織体のコンプライアンス・リスクを識別し、管理し、その軽減をモニタリングするために、効果的に協力すべきである。モニタリング、テスト、および発見を、内部監査に依存すべきではない。これは、第１ラインと第２ラインの役割によって行われ、所有されるべきである。

―米国、最高総務責任者」

「コンプライアンスの役割は、事業部門を支援し、プロセスとコントロールが明確に整合していることを確認すべきである。第２ラインとしてのコンプライアンスの役割が、事業部門に助言するケースは様々である。主要業績評価指標と主要リスク指標は、事業部門がコントロールの有効性に関するリスクを識別して管理するのを支援する。

―メキシコ、最高コンプライアンス責任者」

「多くの業種は、無数の複雑な規制の対象となっている。コンプライアンス部門は、各部門の規制要件や最近の規制変更について、専門知識と助言を提供する。例えば、医療機関では、臨床部門の経営管理者が、コンプライアンスを確保するために必要なコントロールを設計して実施する責任を負っている。コンプライアンス部門は、その専門性から、これらの要件に対するコンプライアンスを評価する上で理想的な立場にある。

―米国、最高コンプライアンス責任者」

「大企業ではよく管理されているが、重要な課題は、コンプライアンスの要件や期待の所有権と義務、およびコンプライアンスの役割やコンプライアンス部門がこれらを実施する方法である。そのためには、強固なガバナンスによる効果的な上申経路とともに、明確なアカウンタビリティや役割と責任を備えた、非常に明確なリスク・マネジメントとコントロールのフレームワークが必要である。これがなければ、コンプライアンスの監督は曖昧になり、実施が困難になる。

―英国、最高コンプライアンス責任者」

「コンプライアンスは、すべての人の責任である。医療のような規制の厳しい業種では、コンプライアンスの責任にはすべての医療従事者が含まれ、特定の手続の承認や文書化要件の遵守が含まれる場合がある。コンプライアンス部門が特定のプロセスや手続に関する方針、プロセス、およびコントロールを策定したり、その手続に対して日常的に責任を負ったりする場合、客観的なアシュアランスを提供することはできない。しかし、プロセスや手続に関連する規制要件について助言やコンサルティングを行うことは、必ずしもコンプライアンス部門の客観性を損ねるものではない。

―米国、コンプライアンス・内部監査責任者」

原則４：第３ラインの役割を定義する

原則４は、独立したアシュアランスと助言

の提供者としての内部監査の役割を述べている。

３ラインモデルは、ガバナンスの基本要素として、コントロールを含むリスク対応の適切性と有効性に対するアシュアランスを提供することの決定的な必要性を詳述している。リスク対応とコントロールには、コンプライアンスとコンプライアンス・リスク・マネジメントの達成、モニタリング、および監督に関するものが含まれる。これは、経営管理者から独立した組織体の唯一のアシュアランス提供者である内部監査が、体系的で規律あるプロセス、専門知識、および洞察を適切に適用することによって達成される。

コンプライアンスの役割と内部監査の役割の効果的な連携と協働は、それぞれの明確な役割を果たす上で有効性を損なうことなく、組織体の利益となるように達成することが可能である。

組織体には様々な役割とアカウンタビリティがあるため、アシュアランスの別の情報源が存在することもあり、それらを総合して、組織体に対する包括的で複合的な視点を提供することも可能である。しかし、そのようなアシュアランスの質と客観性を評価するためには、**３ラインモデル**に従って、具体的な役割とその調整を分析して評価することが重要である。

内部監査は、統治機関に対するアカウンタビリティと経営管理者の責任からの独立性を維持している。これは、アシュアランスの役割とガバナンス構造内での内部監査の明確な位置付けを理解する上で、非常に重要である。内部監査部門の独立性と内部監査人の客観性が脅かされた場合、ＣＡＥは是正措置のために、これを統治機関に報告しなければならない。

内部監査人は、コンプライアンスの役割と部門の有効性を評価する際に、**３ラインモデル**を効果的に適用してコンプライアンスとコントロールのカルチャーを促進するために、コミュニケーション、連携、および協働を進んで行うべきである。

現場の実例

「コンプライアンス・リスクの管理を評価する際に注意すべき重要な項目は、問題を軽減するために実施されている活動の有効性である。具体的なコンプライアンス・リスクの項目について確かなリスク評価を行い、そのリスクに見合った活動の調整をすることが重要である。そうでなければ、コンプライアンス違反のリスクから組織体を守るという利益を得られないまま、多くの活動が行われることになりかねない。

―南アフリカ、ＣＡＥ」

「内部監査人にとって特に重要な課題は、法規制、方針、基準、および行動規範の違反といったコンプライアンス違反の事例を明確に特定し、監査業務や監査報告書に反映させることである。このようなアシュアランスを提供するためには、適切なスキルを持つ資源を利用し、望ましいコンプライアンス成果の達成を効果的に評価して報告する必要がある。

―英国、ＣＡＥ」

原則５：第３ラインの独立性を維持する

原則５は、内部監査の独立性が重要であることを述べている。

第３ラインとしての内部監査には、その独立性を定義するのに役立ついくつかの特徴がある。これには、統治機関や統治機関の委員会への独立した職務上の報告経路、そして重要なこととして、経営管理者の意思決定からの独立性が含まれる。

リスク・マネジメント部門（コンプライアンス・リスク・マネジメント部門を含む）は、多くの場合、統治機関や統治機関の委員会に

職務上の報告経路を持つ一方で、通常は、それぞれの役割において、特にコンプライアンス・リスクを含むリスクの取得、管理、軽減、コントロール、および報告に関する経営管理者の意思決定の責任も負っている。

第２ラインは第１ラインに対して、効果的で信頼に足る異議を唱える責任を維持することができる。しかし、内部監査が経営管理者の意思決定から独立していることは、上記の原則３で詳述したように、第３ラインの役割と第２や第１ラインの役割との重要な差別化要因である。

現場の実例

「内部監査がジレンマに陥らないためには、内部監査人は、コントロールの設計や実施、または経営管理者の意思決定に参加してはならない。内部監査人が焦点を当てるのは、主要なリスクが意図したとおりに識別されてコントロールされているかを判断するための観察、テスト、および評価である。内部監査人は、偏見や先入観を持ってはならない。

―オーストラリア、ＣＡＥ」

「内部監査の主要なステークホルダーは統治機関であり、内部監査はその組織上の独立性により、フィルターのかかっていない結果と勧告を報告することができる。また、内部監査は組織上独立した存在であるため、コントロールの仕組みやその実施者が好意的に見られることを期待することもその必要性もない。内部監査は、真実を報告するという究極のアカウンタビリティを負っている。

―米国、
最高監査・コンプライアンス責任者」

「コンプライアンスの第２ラインの役割は、方針を定め、コントロールの設計に関して事業部門に助言し、事業リスクのリスク選好について助言してレビューし、アシュアランスを提供することである。コンプライアンスの担当者や部門は、第１ラインに代わって業務機能を実施する責任を負うことがある。このような場合、コンプライアンスの担当者や部門は、第１ラインから完全に独立してはいない。内部監査は、第１ラインと第２ラインの経営管理者の意思決定からの独立性により、唯一の完全に独立した活動である。

―米国、全社的リスク・内部監査責任者」

原則６：協働によって価値を創造し保全する

原則６は、これらすべての役割の連携と協働を確保することの重要性を述べている。

効果的なガバナンスには、適切な責任の分担だけでなく、連携、協働、およびコミュニケーションを通じて活動をしっかりと調整することも必要である。統治機関は、経営管理者や内部監査などからの報告に基づいて監督を行い、経営管理者に対して目標を達成し、リスクを管理し、価値を創造するよう指示を与える。統治機関の役割と、第１、第２、および第３ラインの役割は、互いが調整されて、ステークホルダーが優先する利益と整合している場合に、価値の創造と保全に共同で貢献する。したがって、組織体全体のコンプライアンス責任、意思決定権、報告義務、リスク選好、共通の分類法、明確に定義された評価主体や単位、要件や期待に照らしたパフォーマンスとリスクの報告、およびテストとアシュアランスのプログラムについて、明確に伝えることが連携と協働の向上に役立つ。

現場の実例

「連携と協働の例としては、データプライバシーがある。コンプライアンス、または組織体によっては法務部門と協働してコンプライアンスを行い、規制要件を明らかにして組織体に伝達し、適切なプロセスとコ

ントロールが実施されるようにする。事業チーム（オペレーション、ＩＴ、情報セキュリティ等）は、必要に応じて、モニタリング、上申、および情報の報告などの活動を実施する。情報セキュリティチームとコンプライアンスチームは、主要なリスク領域をモニタリングし、事業チームが手続に従って適切にモニタリングと報告を行っていることを確認する。内部監査は、コンプライアンス・リスクを含む関連リスクを管理するためのフレームワーク、および事業チームが実施する関連プロセスやコントロールを評価し、それらの領域を監査する。

―英国、最高コンプライアンス責任者」

「ＥＳＧは、要件や期待の遵守を達成するために、組織体全体が連携と協働を行った好例である。第１、第２、および第３ラインの役割は、それぞれの役割の中で、また統治機関の監督のもとで、望ましいＥＳＧの成果を達成するために協力しなければならない。コンプライアンスに様々な責任を持つ者は、組織体内の他者と協力して、組織体のＥＳＧ目標を達成する。

- 統治機関は、戦略とリスク選好を定め、カルチャーや行動の基調を示す。
- 経営管理者は、ＥＳＧの要件や期待を組織体のガバナンスと業務に統合する。
  - ＥＳＧに関連する戦略計画と業務計画、目標設定、データ収集、意思決定、および報告のための、適切な構造、システム、およびプロセスの、内容、設計、および導入に関して、助言、フレームワーク、および要件を提供する。
  - ＥＳＧの外部要件や基準、および社内方針やターゲットの遵守を達成するためのリスクを評価する。
  - ＥＳＧの成果を達成する上での影響を測定、モニタリング、および報告するために採用すべき基準、フレームワーク、原則、またはモデルを開発する。
  - サステナビリティ報告とＥＳＧ報告に利用するデータとデータ収集方法の正確性と一貫性を評価する。
  - 測定と評価プロセス、重要性の定義と関連指標（ＫＰＩ）のリスト、ならびに（社内外両方への）報告の方法、ガイドライン、およびツールの導入について定める。
- 内部監査は、統治機関に対して上記の活動と経営管理者によるＥＳＧ目標の達成について、また、経営管理者に対して要件や期待への適合の報告について、独立したアシュアランスを提供する。

―英国、最高コンプライアンス責任者」

コンプライアンスについての重要な事実

注意すべき重要な10項目

1．コンプライアンスに特化した資源、部門、管理者等が存在しない場合がある。すべての組織体がこのような方法で資源を配分できるわけでも、その必要があるわけでもない。組織体がより複雑になり、高度に、または特別に規制され、大規模になり、より厳しい監視の対象となり、急速に変化する環境（規制、商業等）で業務を行うようになり、また、類似の要因に対処するようになると、個人、チーム、システム、あるいはその他の資源を、労働力の振り分けや組織設計の正式な構成要素としてコンプライアンスに配分する必要性があると判断する場合が多い。このような資源は、組織体によっては、例えば、特定のコンプライアンスのモニタリングや専門家への外部委託などを通じて、外部に求めることもできる。

2．**３ラインモデル**の「６つの原則」を適用

してコンプライアンス関連の役割を評価する場合、その役割が責任を負う成果を検討することが有用である。

- 製品やサービスを提供する際に、法律、規制、契約、方針、手続、行動規範、またはその他の要件の遵守を達成すること。
- 専門家による監督を行うこと。（特に総体で、またはポートフォリオベースで）リスクを評価し、リスク・マネジメント活動を実施すること。適用される行動規範、または基準、要件、および期待に従って組織体全体のコンプライアンスを推進し達成するために、第１ラインへ信頼に足る異議を唱えること。
- コンプライアンス・プログラムの妥当性と有効性を評価すること。
- 組織体全体のコンプライアンス・プログラムとその構成要素の有効性について、専門家として異議を唱えること。

３．組織体内の単一のコンプライアンスの役割や部門が、その組織体のすべてのコンプライアンス関連事項を扱うわけではない場合がある[8]。このような場合、組織体は、コンプライアンスの役割や部門の範囲を明確に文書化し、どの役割が他の要件や期待に対して責任を持つかも明確にすべきである。このことは、一人の個人に複数の責任と役割が割り当てられ、一部の責任が外部に委託される可能性がある小規模な組織体にとっても、様々なコンプライアンス活動を担当する複数の役割や部門がある大規模な組織体にとっても、同様に重要である。

４．コンプライアンスの役割やコンプライアンス部門の責任者は、実際には、法律や規制の要件に従って、経営幹部（例：ＣＥＯ、最高リスク責任者、最高執行責任者、法務顧問など）や、統治機関やその委員会など、組織体内の多くの異なる役割のいずれかに直属することがある。場合によっては、コンプライアンスは、経営管理者の一部でありながら、ＣＡＥに直属することもある。報告経路の適切性は、**３ラインモデル**や各法規制要件に従って責任を評価する中で、部分的に判断される場合がある。

５．コンプライアンスの役割やコンプライアンス部門の責任者は、１つ以上の取締役会の委員会または１人以上の取締役会の委員会議長に対して、報告経路や報告に関するアカウンタビリティを持つ場合がある。しかし、これは経営管理者からの独立を意味するものではなく、内部監査による独立したアシュアランスの必要性に取って代わるものでもない。

６．個々のコンプライアンスの役割やコンプライアンス部門の責任には、広義のコンプライアンス・リスク・マネジメント、モニタリング、テスト、分析、評価、助言、アシュアランス、方針設定、システムやコントロールの開発と導入、経営判断、監督、および研修を含むが、これらに限定されない場合がある。

７．コンプライアンスの役割や部門には、製品やサービスの提供に密接または直接的に関連する責任が含まれる場合がある。この場合、その役割における責任、権限、およびアカウンタビリティを明確に文書化する必要がある（例えば、取引の禁止や経営判断による拒否権の行使により、製品やサー

[8] 倫理、サステナビリティ、財務報告、データプライバシー、人事、法的義務などを例に挙げると、コンプライアンスを達成するための独自の社内外の資源が存在したり、コンプライアンスの特定の要素に対して追加の監督やリスク・マネジメントを提供したりする場合がある。例えば、環境、社会、ガバナンス（ＥＳＧ）の進化により、様々な組織体において、ＥＳＧの幅広い側面のコンプライアンスに焦点を当てた新しい役割、責任、活動、および部門が見られるようになってきている。

ビスを提供する上でのコンプライアンス違反を防止する力)。

8．第１ラインと第２ラインの役割は分けるべきである。第１ラインの者は、自らが取るリスクを所有すべきであり、第２ラインの者は、第１ラインの意思決定や活動に対して信頼に足る異議を唱えながら、第１ラインが所有するリスクの管理を支援するフレームワークや基準を定めて監督すべきである。実際には、法域や業界の要件、ならびに組織体の規模、複雑さ、およびその他の要因によって、役割が混在する場合がある。その場合、それらの役割の両立性を評価して関連するリスクを軽減しなければならない。そのためには、役割の中で相容れない一連の活動から生じるリスクを効果的に軽減するために、役割の構成を調整する必要があるかもしれない。リスクを管理する責任は、第１ラインの役割の一部であり、経営管理者の範囲内に存続する。

9．組織体がコンプライアンスの義務に充てる資源をどのように構成するかにかかわらず、経営管理者は、組織体が統治機関の設定したリスク選好の設定値内で、その要件や期待を確実に満たすようにする責任を保持する。

10．第２ラインのコンプライアンスの役割の本質的な責任は、組織体のコンプライアンス・プログラムの有効性と組織体のコンプライアンス要件や期待を達成するために必要な取り組みを評価することである。

付録：コンプライアンスの役割と活動に対する責任の調整

コンプライアンス活動は、組織体のガバナンス、リスク・マネジメント、およびインターナル・コントロール活動にとって不可欠な要素である。コンプライアンスの達成、支援、チェック、および確認のために必要な行動とその実施の責任は、組織体の様々な部分に割り当てることができる。コンプライアンス活動の責任者は、コンプライアンスを構成する期待される成果を定義し、その成果の達成を実証するための適切な評価基準を定義する必要がある。

コンプライアンスを構成する活動には、以下が含まれるが、これらに限定されるものではない。

- 関連する外部の法律、規則、および規制、ならびに内部の方針、基準、手続、および行動規範と、組織体の目標に合致した許容される行動を特定する。
- 関連する外部の法律、規則、および規制、ならびに内部の方針、基準、手続、および行動規範と、組織体の目標に合致した許容される行動を、遵守しているか否かを判断するための適切なリスク評価基準を決定する。
- 関連する外部の法律、規則、および規制、ならびに内部の方針、基準、手続、および行動規範と、組織体の目標に合致した許容される行動を、遵守しているか判断するために、将来および新たに発生するリスクを含むリスク評価を実施する。
- 関連する外部の法律、規則、および規制、ならびに内部の方針、基準、手続、および行動規範と、組織体の目標に合致した許容される行動の、遵守を達成するためのプロセスとコントロールを設計し、策定して導入する。
- 関連する外部の法律、規則、および規制、ならびに内部の方針、基準、手続、および行動規範と、組織体の目標に合致した許容される行動の、遵守を達成するためのプロセスとコントロールを実施し、維持して管理する。
- 関連する外部の法律、規則、および規制、ならびに内部の方針、基準、手続、および行動規範と、組織体の目標に合致した

許容される行動を、遵守するためのプロセスとコントロールを評価し、テストしてモニタリングする。
- コンプライアンス・リスクに関して、経営管理者に対して信頼に足る異議を唱える。
- コンプライアンス・リスクを管理して軽減する。
- コンプライアンスとコンプライアンス違反の事例を判断する。
- コンプライアンス違反の事例を通知して上申する。
- 外部や内部の要件に従って、コンプライアンスとコンプライアンス違反の報告を行う。
- コンプライアンスを促進するカルチャーを育む。
- コミュニケーション、研修、プロモーション、および教育を通じて意識を向上させる。
- コンプライアンスに関する相談や助言を行う。
- 倫理プログラムや内部告発プログラムを確立して維持する。
- コンプライアンスに関する研修、教育、および意識向上策を策定して実施する。
- 規制当局と組織体の間の規制連絡役を務める。
- 専門機関や業界団体との関係を構築して維持し、組織体やその活動が遵守すべき、あるいは遵守することを選択できる関連基準、規範、またはガイドラインを特定するとともに、ベンチマーク情報の収集と報告を円滑に進める。
- インフラのユーザーや取引先に対して適合すべき要件や期待を定めて要求する可能性のある、業界のインフラ組織との連絡関係を確立して維持する。

各役割の責任と望ましい成果が明確であることが重要である。これらの役割や活動の中には、**３ラインモデル**で詳述されているように、取引の承認、顧客の承諾、または第３ラインの責任の範囲内で他の事業リスクについての意思決定を行うなど、他の役割と相容れないものもある。内部監査がこのような役割を担うよう求められる場合、統治機関や監査委員会の同意、影響を受ける領域で独立したアシュアランスを提供する第三者の利用、および必要に応じて規制当局の承認など、重要なセーフガードが必要とされる。

さらに、コンプライアンスに基づいて製品やサービスをクライアントに提供するという成果を達成しようとする最善の意図があっても、組織体は、製品やサービスを提供する際にコンプライアンスを達成し、監督と広範なコンプライアンス・リスク・マネジメントを提供するための役割を特定し、その責任を果たすように注意を払わなければならない。職務分離と独立性の基本原則を適用すれば、役割における相容れない活動が特定された場合に生じるリスクを軽減することが期待される。

同様に、製品やサービスの提供を支えるリスク・マネジメントやコントロール活動にギャップや不備があると判断した場合、監督の役割を担う者は、監督から実施へと自らの範囲を拡大しようとする誘惑に駆られることがある。その逆もまた真なりで、第１ラインは、監督やリスク・マネジメントの役割を担う者に過度の信頼を置くことがある。これでは、客観的な監督の効果が損なわれる。このような場合、ギャップや不備、および経営管理者の改善措置策を特定し、上申し、モニターすることが、監督役の責務となる。これらの要素は、定められたガバナンスの役割と責任に従って調整し、文書化しなければならない。