



The Institute of
Internal Auditors

意見書

全社的 リスク・マネジメント

における内部監査部門の役割

目次

エグゼクティブ・サマリー	3
第1部－原則ベースのフレームワーク	5
目的と背景	5
対象読者	6
ERM の定義	6
ガバナンス・システム内の ERM と内部監査部門	7
ERM における内部監査部門の役割	7
スキルと能力	7
ERM に関連する内部監査のアシュアランス	9
ERM に関連する内部監査の助言	9
ERM に関連する内部監査部門の管理業務	9
リスク・マネジメント部門	10
ERM 全体における内部監査部門の関与	11
独立性と客観性を維持するための防御措置	12
連携と依拠	13
第2部－実務における ERM での内部監査の役割	14
アシュアランスと助言のバランス	14
監督と重複する責任を伴うシナリオ	15
シナリオ A：内部監査部門が第2ラインの ERM 活動を実施する	15
シナリオ B：内部監査部門長がリスク・マネジメント部門を監督する	18
優れた取り組み：統合的アシュアランス	19
用語一覧	21

エグゼクティブ・サマリー

本「意見書」は、全社的リスク・マネジメント（ERM）における内部監査部門の役割を明確にするものである。組織体は、目標の達成と長期的な価値の維持のために、効果的なガバナンス、リスク・マネジメント、コンプライアンス及びコントロールのプロセスが必要である。ERM は、脅威と機会を識別、評価、管理、モニタリング及び報告するための、組織体全体での協調的なアプローチを提供し、レジリエンスの確保と戦略目標との整合を可能にする。データ主導型環境がますます進展する中、効果的な ERM は、取締役会と経営管理者による信頼性の高い意思決定を支えるものである。

ERM は、明確な説明責任を特徴とするガバナンスのフレームワークの中で機能する。

- 取締役会は期待事項を定め、最高経営者を監督する。
- 経営管理者は、リスクの管理と ERM プロセスの実施に責任を負う。
- 内部監査部門は、独立したリスクベースの客観的なアシュアランス、助言、インサイト及びフォーサイトを提供する。独立性と客観性は、内部監査部門の信頼性の基盤である。

内部監査部門は、相互に補完し合い強化し合うアシュアランス業務とアドバイザリー業務を提供することで、ERM を強化する。

- アシュアランス：ERM プロセスの設計と有効性を評価する。これには、リスク選好、リスク許容度、戦略及びガバナンス上の期待事項との整合性の評価が含まれる。
- アドバイザリー：ERM の実務を強化するためのインサイトとフォーサイトを提供する。これには、前提条件への異議申し立て、リスクに関する議論のファシリテーション、優良事例の共有などが含まれるが、経営責任は負わない。

アシュアランス業務とアドバイザリー業務のバランスは、ERM の成熟度、リスク環境、他部門の能力、及び取締役会からの指示など、組織体の状況によって決まる。ガバナンスや経営の体制は、変化する組織体のニーズや将来の目標に合わせて進化するため、これらの業務は、組織体全体の他のアシュアランスやアドバイザリーのプロバイダと連携や統合を図る場合、その効果がさらに高まる。内部監査部門は、連携を促進し、重複を削減し、ガバナンス、リスク・マネジメント、コンプライアンス及びコントロールの有効性について一貫した見解を取締役会と最高経営者に提供することで、統合的アシュアランスを支援する。

組織体の成熟度、資源の制約、関連スキル、あるいは他の要因により、ERM 活動の責任を内部監査部門長に任命する組織体もある。しかし、内部監査部門長が ERM 活動の責任を担う場合、以下の点を確保するための防御措置を講じなければならない。

- 責任が明確に定義され明記されていること。
- アシュアランスと助言の役割が適切に分離されていること。
- 侵害の可能性が取締役会に対して透明性をもって開示されていること。
- 内部監査部門が業務に関与している場合には、独立したアシュアランスが得られていること。
- 内部監査部門がリスク・マネジメント上の意思決定に対する責任を負わないこと。

第1部－原則ベースのフレームワーク

目的と背景

組織体は、目標の達成と長期的な価値の維持のために、効果的なガバナンス、リスク・マネジメント、コンプライアンス及びコントロールの構造とプロセスが必要である。取締役会は、組織体のガバナンスについてステークホルダーに対して説明責任を負う。これには、パフォーマンス、リスク及びコントロールに関する信頼性が高くバランスの取れた情報が必要となる。最高経営者は、目標の達成とリスクの管理のために、構造とプロセスを設計することについて、取締役会に対して説明責任を負う。全社的リスク・マネジメント（ERM）活動は、脅威や機会に関する考慮事項を戦略、意思決定及びパフォーマンスに統合することで、こうしたニーズを支援する。組織体が意思決定やパフォーマンスのモニタリングにおいてデータに依拠する度合いが高まるにつれて、リスク関連情報に対する独立性のあるインサイトとアシュアランスの重要性はますます高まっている。一方で、ERM 活動は、ガバナンス、リスク・マネジメント、コンプライアンス及びコントロールのプロセスを構築して整合させるのに役立ち、組織体全体での説明責任、実行責任及び連携の実現を可能にする。

本「意見書」において、「取締役会」という用語は、用語一覧で説明されている通り、様々な形態の統治機関とその委員会を指すものとする。

本「意見書」は、現代のガバナンス環境における ERM 内で、内部監査部門が果たす役割を明確にするものである。本「意見書」は、原則ベースの指針を提供し、内部監査部門にとっての独立性と客観性の重要性を強調しつつ、インサイト、フォーサイト、連携、及びアシュアランス活動と ERM 活動の統合が適切に構成された場合に、ガバナンスとリスク・マネジメントのプロセスを強化することを認識している。本「意見書」の根底にある原則はすべての組織体に当てはまるが、ガバナンス、リスク・マネジメント、コンプライアンス及びコントロールの構造やプロセスの実施方法は、組織体ごとに異なる。

内部監査人協会（IIA）は、「3ラインモデル—効果的なガバナンスを支援するためのアシュアランスと助言」¹という「意見書」と合わせて、組織体とそのステークホルダーのニーズを満たすために、組織体のガバナンスと ERM の役割と責任を支援する、一貫性があり柔軟なフレームワークを提供する。

¹ 訳注：日本語訳は、https://www.iiajapan.com/leg/pdf/data/iaa/SOP_ThreeLinesModel-Assurance_and_Advice_in_Support_of_Effective_Governance_Japanese%20.pdf

対象読者

本「意見書」の主な対象読者は、ERMに関連する期待に応える役割を担う内部監査部門長と内部監査人である。また、本「意見書」は、内部監査部門が、戦略上又は業務上の意思決定を行うという経営管理者の責任を引き受けることなく、ERMにどのように貢献できるかについての参考資料として、取締役会、監査・リスク委員会、最高リスク責任者、経営幹部、規制当局、及び他のアシュアランスや助言の部門と共有されることを意図して作成されている。

ERMの定義

ERMとは、リスク（脅威と機会）を識別、評価、管理、モニタリング及び報告するための、組織体全体で連携したアプローチである。ERMは、組織体内のガバナンス、リスク選好及びカルチャーの状況の下で、戦略目標、意思決定、持続可能な価値創造及びレジリエンスの実現を支援する。

この定義は、ERMを、定期的な取り組みや固定的なリスク登録簿ではなく、意思決定やパフォーマンスに組み込まれた継続的かつダイナミックな一連のプロセスとして捉える現代的な見方を反映している。この定義は、ERMが組織体全体で部門横断的に統合され、戦略、業務、財務、コンプライアンス及びカルチャーを結び付けていることを認識している。また、リスクには脅威と機会の両方が含まれているため、組織体が価値を創造、保全及び維持するための方法と直接結び付いていることも強調している。

ERMは拡張性があり、原則ベースである。組織体の状況、成熟度及び複雑性に合わせて設計して適用する一方で、取締役会の監督や最高経営者による管理と意思決定を支える一貫性のある全社的視点を提供し続けている。ただし、法律や規制上の要件により、特定の組織構造や責任分担が認められない場合がある。

ERMは、他の日常的なリスク・マネジメント活動を置き換えるものではない。業務、財務、コンプライアンス、テクノロジー及びその他のリスクの管理は、所定の目標を達成するためのコントロール・プロセスの設計と実施を支える具体的な役割とプロセスを通じて組織体全体で行われる。ERMは、こうしたリスク・マネジメント活動を組織体全体の視点へと昇華して結び付けるための基盤と統合メカニズムを提供し、経営幹部や取締役会レベルでの集約、上申、及び情報に基づいた選択を可能にする。これにより、ERMは組織体のリスク選好とリスク許容度の範囲内で業務を遂行できるよう支援し、リスクテイクがガバナンス上の期待事項や戦略的意図と整合した状態を確保する。

ガバナンス・システム内の ERM と内部監査部門

取締役会は、最高経営者によるリスク・マネジメントへの取り組みを監督する最終的な説明責任をステークホルダーに対して負う。取締役会は、組織体のリスク選好とリスク許容度を定め、リスク関連の報告が効果的な監督と意思決定を支えるようにする。最高経営者は、目標の達成とリスク・マネジメントを実現するための構造とプロセスを確立する責任を負う。これには、専門的支援、モニタリング、及び第1ラインによる意思決定へ異議申し立てを行うための第2ラインの部門や役割を創設することも含まれる。ERM 活動は、組織体の目標達成状況やリスク・マネジメントに関する意思決定に有用な情報を、取締役会と最高経営者が適時に受け取れるようにするのに役立つ。

第3ラインとしての内部監査部門は、取締役会から権限を付与され、独立したリスクベースの客観的なアシュアランス業務とアドバイザリー業務を提供する。独立性は孤立を意味するものではない。効果的なガバナンスは、説明責任と実行責任を明確に保ちつつ、連携したアシュアランスと助言を行うことに支えられている。

ERM における内部監査部門の役割

内部監査部門は、不可欠かつ相互に補完し合うアシュアランス業務、アドバイザリー業務、及び管理業務を通じて、ERM に貢献する。取締役会、最高経営者及びその他のステークホルダーは、内部監査部門に対して、ERM 活動が有効であるというアシュアランスを提供すると同時に、組織体が新たな不確実性を予測して対応する能力を強化するためのインサイトを提供することをますます期待している。この二重の貢献は、役割の境界が明確であり、適切な防御措置が講じられている場合に、内部監査部門の強みとなる。

スキルと能力

内部監査人は、組織体全体のリスク・マネジメント、コンプライアンス及びコントロールのプロセスを評価できる能力を備えているため、ERM 活動の実施や助言を行う上で特に適している。この能力には、リスクを戦略や目標と結び付ける専門知識、プロセス・レベルでリスク選好やリスク許容度が適用されているかを理解する能力、リスク・カルチャーがどのように現れているかを識別する能力、そしてリスク情報が意思決定にどのように反映されているかを評価する能力が含まれる。

内部監査人は、データ・アナリティクスや関連テクノロジーに関する強みを活用して、ERM 活動のスピードと範囲の拡大や、その客観的な裏付けの強化もできる。特別な分野やプロセスに関する専門知識が必要な場合に、その業務を行う際、内部監査部門は、内部又は外部からの支援によって、適切な能力を確保すべきである。

内部監査が提供するもの

独立したアシュアランス
ERMプロセスが効果的に設計され運用されているという信頼性を与える

助言的なインサイト
異議申し立て、ファシリテーション、優良事例の共有を通じて、ERMの実務を強化する

リスクベースの視点
リスク情報を活用してアシュアランス業務とアドバイザリー業務の優先順位を決定する

統合的アシュアランス
組織体全体でアシュアランスの視点を連携して調整する

組織体全体の視点
ガバナンス、リスク・マネジメント、コンプライアンス、コントロールについて、包括的な評価を行う

一般的な防御措置

責任の明確化
役割が明記され理解されている

取締役会による承認
拡大されたERMの役割が正式に承認されている

アシュアランスと助言の分離
アドバイザリー業務によって、アシュアランス業務が侵害されることはない

透明性
侵害の可能性が開示されている

外部によるアシュアランス
内部監査部門が実施する業務に対して、独立したアシュアランスが提供される



アシュアランス業務
ERMの有効性に関する独立した客観的なアシュアランス

アドバイザリー業務
ERMの実務を強化するためのインサイトと助言

内部監査の管理業務
リスクベースの監査計画と連携を支える業務

経営管理者による意思決定
リスクに関する意思決定と対応策についての経営管理者の責任。内部監査はこれらの業務を実施してはならない。

全社的リスク・マネジメント：識別・評価・管理・モニタリング・報告

ERMライフサイクル全体にわたり、ガバナンスの強化、価値の創出、及び情報に基づいた意思決定の支援を行う

ERM に関連する内部監査のアシュアランス

内部監査部門は、ERM プロセスが適切に設計され効果的に運用されていることについて、取締役会と最高経営者に対して独立した客観的なアシュアランスを提供する。これには、リスク選好とリスク許容度が設定され意思決定に組み込まれていること、信頼性が高く一貫した方法で脅威と機会が識別され評価されていること、重大なリスクが適切に上申され報告されていること、そして経営管理者の対応策がガバナンス上の期待事項に沿っていること、に対するアシュアランスが含まれる。

ERM に対するアシュアランスには、ERM が戦略目標やレジリエンスを支えているかの評価が含まれる。これには、意思決定においてリスク情報がどのように活用されているか、また、リスク・カルチャーがインセンティブや説明責任にどのような影響を与えているか、といった点も含まれる。内部監査部門は組織体全体を見渡す立場にあるため、単独の要素を評価するだけでなく、組織体全体のリスク・マネジメントの一貫性について統合的な結論が提供できる。また、内部監査部門は、アシュアランス・マップ作成への貢献や、リスク、コンプライアンス及びコントロールに関するテーマについて見解の整合を図る支援によって、各アシュアランス・プロバイダ間の連携強化の後押しもできる。

経営管理者が組織体のリスク選好やリスク許容度を超えるレベルのリスクを受け入れていると内部監査部門長が判断した場合、その問題は最高経営者と協議し、必要に応じて取締役会に上申しなければならない。

ERM に関連する内部監査の助言

内部監査部門は、組織体全体を見渡す視点を持つことから、ERM 活動を改善して強化するためのアドバイザリー業務も提供することがある。アドバイザリー業務には、リスクに関するワークショップや研修のファシリテーション、リスクに関する用語や手法の明確化や実用化に関する助言、リスクの評価や報告の根底にある前提条件やデータに対する異議申し立て、そして組織体内で確認された優良事例の共有などが含まれる。

重要なのは、内部監査部門による助言は、第 1 ラインや第 2 ラインの経営管理者の責任に代わるものではないということである。アドバイザリー業務は、理解を深め、より情報に基づいた意思決定を可能にすることでリスク・マネジメントを強化すべきであるが、一方で、内部監査部門が独立したアシュアランスを提供する能力は維持しなければならない。内部監査部門は、異議申し立てや助言を行うことはあっても、リスク対応に関する意思決定についての経営管理者の責任を免除するものではない。

ERM に関連する内部監査部門の管理業務

内部監査部門は、ダイナミックでリスクベースのアシュアランスと助言という役割を果たすために、様々な管理業務を行っている。こうした業務は、ERM の定義の構成要素と関連付けることができる。



内部監査の計画は、組織体の戦略、目標及びリスクの評価に基づいて策定されるが、これらは通常、監査対象領域となり得る単位の集合体として表される。内部監査の計画では、組織体の戦略に沿ったリスク評価に基づいて個々の内部監査業務の優先順位を決定する。個々の内部監査業務の目標も、関連するリスクの評価に基づいている。内部監査部門長は、組織体のパフォーマンスと新たに生じているリスクをモニタリングし、アシュアランス業務とアドバイザリー業務を、価値の創出、保全及び維持の可能性と整合させる。また、内部監査部門長は、経営管理者や他のアシュアランス・プロバイダと連携して、リスク報告書を統合する。

リスク・マネジメント部門

多くの組織体では、ERM プロセスの導入、運用及び改善を支援するために、リスク・マネジメント部門を設置している。こうした部門は通常、前述の内部監査部門と同様の業務を行うほか、さらに以下の業務を行う場合がある。

- 組織体の ERM フレームワークを維持する。
- リスク・マネジメント方針を策定する。
- 一般的な、あるいは特定分野の、リスク・マネジメントのツールや手法について専門的な助言を行う。
- 特定のリスクのモニタリングを行う。
- 組織体全体のリスクに関するポートフォリオの視点を形成して報告する。
- 経営管理者の意思決定に対して建設的な異議申し立てを行い、専門分野でのテーマ別レビューを行う。
- 内部監査部門と連携して、組織体のリスク・マネジメント・プロセスの改善を図る。

リスク・マネジメントの役割は、IIA の「3 ラインモデル」では第 2 ラインの業務に分類される。組織体によっては、リスク・マネジメント部門が内部監査部門長に報告する体制を取っている場合があるが、その場合は、内部監査部門の独立性を保護するための防御措置が必要となる。

専任の第 2 ラインの役割や部門を設けていない組織体では、経営管理者は、重大なリスクを識別してアシュアランスを提供するための、内部監査部門のプロセスに依拠することでメリットが得られる可能性がある。そのような状況では、内部監査部門長は、組織体の成長と成熟に伴い、経営管理者が ERM 活動を確立するのを支援できる。

経営管理者が第 2 ラインの業務を確立しているか否かにかかわらず、関係者間の協働、連携及び適切な依拠とともに、内部監査部門の独立性を確保するための十分な防御措置が組織体の成功に寄与する。

ERM 全体における内部監査部門の関与

ERM 活動は、ERM の定義における以下の要素、すなわち「識別」、「評価」、「管理」、「モニタリング」、「報告」に関連するものとして分類できる。この活動ベースの枠組みは、内部監査人が、自らの客観性を損なうことなく、また経営管理者の意思決定責任を引き受けることなく、ERM プロセスに協力や貢献ができる方法を示すのに役立つ。

- **識別**：内部監査部門は、リスクの分類体系や用語の統一性についての助言をすることや、リスクと目標との関連性を書面にすることはあっても、経営管理者によるアプローチを決定すべきではない。内部監査部門のアシュアランスの役割には、組織体のリスクの識別が十分に網羅的で、確立された分類体系と整合し、かつ戦略と整合しているかを評価することが含まれる。
- **評価**：内部監査部門は、組織体全体と特定のプロセスにおけるリスクを評価して内部監査業務の優先順位を決定するとともに、個々のアシュアランス業務では、経営管理者によるリスク対応策の残余の影響がリスク選好内やリスク許容度内にあるかを評価する。内部監査部門は、スコアリングや優先順位付けを含む経営管理者のリスク評価手法について一般的な助言や専門的な助言を行うことがあり、また、リスクプロファイルの根底にある前提条件に対して異議申し立てを行うこともある。ただし、後に監査対象となる継続的なリスク評価プロセスの責任を負うべきではない。ERM プロセスが効果的に機能している場合、内部監査部門は、内部監査の計画内の個々の内部監査業務の優先順位付けを行う際に、経営管理者による全社的リスク評価にある程度依拠できる。
- **管理**：内部監査部門は、方針やコントロールについて助言を行うことはあっても、最終的な方針やリスク対応の決定権を持つべきではない。経営管理者は、方針や決定に責任を負い、取締役会に対して説明責任を果たさなければならない。内部監査部門によるアシュアランス業務は、リスク・マネジメント、コンプライアンス及びコントロールのプロセスが効果的かつ効率的であるかに焦点を当てる。
- **モニタリング**：内部監査部門は、識別したギャップに対処するための改善措置の計画が導入されたかをモニタリングする。また、経営管理者が組織体のリスクプロファイルの変化を適切にモニタリングしているかも評価する。内部監査部門は、インシデント分析や重要なリスク指標について助言を行うこともあり、その際には、経営管理者のモニタリングが適時に行われ、意思決定を適切に支援しているかも含めて検討する。
- **報告**：内部監査部門は、リスクの報告と上申のプロセスの設計と実施についてアシュアランスを提供する。また、取締役会と最高経営者に提示されるリスク情報の明確性や一貫性について助言を行うこともある。内部監査部門がライン横断的なリスク報告の統合に寄与する場合、独立性を維持しつつ一貫性を高めるような方法で行うべきである。

独立性と客観性を維持するための防御措置

独立性と客観性は、内部監査部門の信頼性の基盤である。組織上の独立性は、内部監査人が客観性を維持し、不当な影響を受けることなくアシュアランスと助言を提供する能力を支援する。しかし、一部の組織体では、内部監査部門長が内部監査部門とリスク・マネジメント部門の両方を統括している。内部監査部門や内部監査部門長が ERM における役割を拡大している場合、防御措置は、慎重に検討され、適切で均衡が取れており、かつ内部監査基本規程の中で取締役会に明確に示されていないなければならない。内部監査部門長は、リスク対応策に関する意思決定を行ってはいならず、またその責任を負ってはならない。なぜならば、これらは経営管理者の責務であり、内部監査人の客観性を損なうおそれがある。

効果的な防御措置には、通常、以下が含まれる。

- **明確かつ書面にされた責任**

第 1 ラインの経営管理者、第 2 ライン、及び内部監査部門の役割は、業務レベルで明確に定義されるべきである（例えば、誰がリスク評価手法を策定し、誰がモニタリングを行い、誰がアシュアランスを提供するかなど）。曖昧さは、外観上の侵害が疑われるリスクを高める。

- **責任範囲の拡大に関する取締役会の正式な承認**

内部監査部門長を含む内部監査人が、ERM に関連する追加の責任を担う場合、取締役会は、例えば内部監査基本規程の中で、その体制を正式に承認し、関連するリスクとその低減策を認識すべきである。内部監査部門は、適切な防御措置を講じた上でこうした業務を行うために、取締役会と経営管理者による追加リソースの承認を必要とする場合がある。

- **アドバイザリー業務とアシュアランス業務の分離**

内部監査人がアドバイザリー支援（例えば、ファシリテーション型ワークショップや ERM の改善に関する助言など）を行う場合、それらの業務は、範囲を明確に定め、アドバイザリー業務として明記すべきである。その後のアシュアランス業務は、過去 12 か月以内に、対象となるプロセスの設計又は運用に責任を負わなかった者が実施しなければならない。

- **侵害の可能性に関する透明性のある開示**

客観性に対する実際の又は外観上のあらゆる侵害は、取締役会に報告しなければならない。透明性は信頼を強め、十分な情報に基づいた監督を可能にする。

- **ERM の責任分担に異議申し立てをする能力**

内部監査部門長は、内部監査部門の独立性を重大に侵害するおそれのある責任分担案に対して異議申し立てができるべきであり、また、取締役会と適切な防御措置について協議しなければならない。その責任分担を一時的なものとして経営管理者への責任移管計画を策定することで、生じ得る影響を低減できる可能性がある。

- **必要に応じて、代替の又は独立したアシュアランス措置を講じる**

内部監査人が ERM 活動を遂行又は監督する場合、当該分野に関するアシュアランスは、内部又は外部のいずれかを問わず、適切な資格を有する独立した第三者によって提供されなければならない。

- **外部による定期的なレビュー**

内部監査部門長が ERM 活動を監督する体制では、内部監査部門に対する定期的な品質の外部評価や、対象を絞った独立したレビューを行うことで、外観上のリスクを低減し、独立性と客観性が維持されていることが確認できる。

こうした防御措置により、組織体は自らの状況に適した体制を導入しつつ、アシュアランスの信頼性を確保し、リスク・マネジメント・プロセスの有効性に関する取締役会の信頼を維持できる。防御措置が慎重に適用される場合、監督機能の重複は、独立性、客観性及び説明責任を損なうことなく、連携とインサイトを高めることができる。

連携と依拠

ガバナンス、リスク・マネジメント、コンプライアンス及びコントロールのプロセスは、組織体内外のアシュアランスやアドバイザリーのプロバイダ間の連携と適切な依拠によってメリットが得られる。手法や証拠が十分であり、適切に記録されていれば、その依拠は適切である。アシュアランス・マップは、ギャップや重複を特定するのに役立つ可能性がある。内部監査部門が他のアシュアランスやアドバイザリーのプロバイダに依拠すること、あるいはその逆の場合も、説明責任の転嫁や、独立性や客観性の低下を招くことなく、効率性を高めるべきである。

内部監査部門長は、リスク評価とアシュアランスに対する統合的なアプローチを促進し、業務部門や支援の役割と連携して、対象範囲を最適化し、重複を削減し、インサイトを高めるべきである。取締役会は、依拠に関する決定について透明性を保つべきである。

第2部－実務における ERMでの内部監査の役割

アシュアランスと助言のバランス

アシュアランス業務とアドバイザリー業務は、いずれも内部監査部門の中核をなすものであるため、重要な課題は、それぞれの状況に応じて適切なバランスをいかに調整するかという点にある。両業務の配分にあたっては、以下を考慮すべきである。

- **ERMの成熟度とリソース配分**

ERM活動に対する内部監査部門のアシュアランス業務とアドバイザリー業務のバランスは、組織体の成熟度によって左右される可能性がある。ERMが発展段階や変革過程にある場合、将来的には独立した客観的なアシュアランスを提供する能力を維持しつつ、フレームワークやプロセスを強化するために、アドバイザリー業務による支援が一層重視されることがある。ERM活動が十分に確立されて組織体に定着している場合、内部監査部門は、その有効性、信頼性及び戦略との整合性についてアシュアランスを提供することに重点を置くことがある。しかし、ERM活動が最適化された状態に達してアシュアランスによってそれが確認された後も、戦略策定への貢献をさらに高めるためには、アドバイザリー業務が依然として適切な場合がある。

- **組織体の戦略とリスクを取り巻く状況**

急速な変化、変革、あるいは新たなリスクが浮上している時期には、アドバイザリーによるインサイトは、経営陣が不確実性やトレードオフを理解する上で役立つ。外部環境が比較的安定している時期には、たとえ内部で散発的なインシデントやガバナンス上の懸念があったとしても、リスク・マネジメントと報告に対する信頼を強化するために、アシュアランスが重視されることがある。

- **他のアシュアランスやアドバイザリーのプロバイダの強度と連携**

リスク・マネジメント部門などの有能な第2ライン部門が、効果的なモニタリングやテーマ別レビューを行っている場合、内部監査部門は、その依拠に透明性があり、かつ独立性や客観性を損なわない限り、連携したアシュアランスと適切な依拠をより重視できる。

- **取締役会からの継続的な指示と取締役会に対する透明性**

重大なアドバイザリー業務については、取締役会からの負託事項に沿ってその範囲を明確に定めて明記すべきであり、将来のアシュアランス業務に及ぼす影響については事前に協議すべきである。適切な防御措置が講じられていれば、アドバイザリー業務は、将来のアシュアランス業務に求められる客観性と信頼性を維持しつつ、大きな付加価値をもたらすことができる。



監督と重複する責任を伴うシナリオ

実際には、ガバナンスや経営の体制が常に明確に区分されているとは限らない。これらの体制は、将来像に関する明確なビジョンと、実際の制約や潜在的な影響への理解を指針として、変化する組織体のニーズや状況に応じて進化していくべきである。組織体の規模、資源の制約、規制上の期待事項、あるいは戦略的優先事項により、ERM に関連する責任が内部監査部門の責任と重複するような体制が生じることがある。監督機能の重複は、それ自体が問題となるわけではない。重要なのは、業務が適切なスキルを持つ担当者に任命されているか、リスク・マネジメントに関する経営管理者の責任が依然として明確か、内部監査人の独立性と客観性が維持されているか、そして取締役会がアシュアランスの質に対する信頼を維持しているか、という点である。

以下に説明する 2 つのシナリオが最も一般的であるが、別の組織構造もあり得る。これらは特定の体制を推奨するものではなく、一般的な体制を示すことを目的としており、法規制や専門職としての義務などの理由により、一部の法域やセクターでは適切でない場合もある。

シナリオ A：内部監査部門が第 2 ラインの ERM 活動を実施する

一部の組織体、特に小規模な組織体や発展途上の組織体では、通常はリスク・マネジメント部門に属する役割を内部監査部門が担うことがある。これは、現実的な必要性、構造設計、あるいは ERM の構築を加速させたいという意向を反映している場合がある。内部監査人は通常、リスク、コンプライアンス及びコントロールの識別、評価、モニタリング及び報告に関する適切な能力を備えている。こうしたスキルを活用することで、組織体の ERM への取り組みに体系と統合をもたらすことができる。しかし、内部監査部門の責任範囲が助言的支援にとどまらず、ERM の管理業務の運営にまで及ぶ場合、内部監査部門の独立性や、内部監査部門長を含む内部監査人の客観性が侵害されるおそれがある。



ERM サイクル全体で見ると、このシナリオは次のように見える可能性がある。

- **識別：**

内部監査部門は、自らの監査計画とアシュアランスの目的のために、リスクを適切に認識し、それらを組織体の目標と関連付ける。経営管理者が内部監査部門の業務に依拠し、独自のリスク分類体系を策定しない場合、内部監査部門の役割はさらに拡大する。内部監査部門は、経営管理者と連携して組織体全体のリスクの識別プロセスを調整し、重大なリスクについて共通認識を形成することもあるが、適切な対応策を決定する責任は依然として経営管理者にある。

- **評価：**

内部監査部門は、内部監査の計画を策定し、個々の内部監査業務の優先順位を決定するために、日常的にリスクを評価している。経営管理者による同様の正式なリスク評価活動が行われていない場合、あるいは内部監査部門が、全社的なリスク評価手法の策定、スコアリング規準の設定、全社的なリスク登録簿の管理、又は組織体全体のリスク評価の集約を求められた場合には、その役割の範囲が広がる。

- **管理：**

内部監査部門は、リスク選好やリスク許容度に合わせたコントロールを設計する方法を含め、ERM の方針やプロセスについて適切な助言を行う場合がある。内部監査部門が方針を起草したり、特定のリスク対応策を推奨したりする場合、その役割は、より業務執行的なものとなるが、リスクに関する意思決定に対する経営管理者の責任は、関係者全員が明確に理解すべきである。

- **モニタリング：**

内部監査部門は、組織体にとって重大なリスクについて常に最新の状況を把握し、それに基づいてアシュアランス業務とアドバイザリー業務の優先順位を決定する。また、アシュアランス業務で識別したリスクに対処するための経営管理者の措置の進捗状況をモニタリングする。内部監査部門が、経営管理者のためにリスク指標を策定してモニタリングすること、ERM 活動から生じるリスク低減策の進捗を追跡すること、あるいは継続的に第2ラインの支援業務を行うことを求められた場合、その役割はさらに拡大する。

- **報告：**

内部監査部門は、リスク・マネジメント、コンプライアンス及びコントロールのプロセスの有効性について、取締役会にアシュアランス報告を行う。内部監査部門が最高経営者に代わって全社的なリスク報告書を統合又は作成する場合、その役割はさらに広範なものとなる。



このシナリオは、内部監査人の役割の拡大が本質的に非効率的であるとか、望ましくないということを示唆するものではない。特定の状況下では、それらは実用的な措置であったり、過渡的な措置であったりする場合がある。ガバナンスや経営の体制が変化する中で、業務への関与が内部監査部門の独立性や客観性に与える影響を明確に把握することは、適切な防御措置を講じて将来のアシュアランスに対する信頼を維持するために不可欠である。

実際には、このシナリオには、以下を含むような明確なガバナンス上の防御措置が必要となる。

- 取締役会は、その範囲と根拠を明確に示した上で、責任範囲の拡大を正式に承認すべきである。
- 内部監査基本規程には、助言的なファシリテーションと業務上の責任を区別し、責任範囲を明記しなければならない。
- 内部監査人は、自身が設計、運営又は管理した業務については、その最後の業務又は責任から 12 か月が経過するまでは、アシュアランスを提供してはならない。
- 影響を受ける分野については、他の内部部門又は外部プロバイダによる、独立した客観的なアシュアランスを手配すべきである。
- この体制については、ERM の責任を経営管理者又は専任の第 2 ライン部門に完全に移行できるかを判断するために、定期的にレビューすべきである。

このシナリオは、恒久的なものではなく、過渡的又は例外的なものであるかもしれない。目標としては、リスク対応に関する意思決定の責任と、リスク・マネジメント及びコンプライアンスの業務に関する独立したアシュアランスとを明確に区分することを維持すべきである。

シナリオB：内部監査部門長がリスク・マネジメント部門を監督する

内部監査部門長は、内部監査部門とは組織上も業務上も独立した別のリスク・マネジメント部門の監督責任を負う場合がある。この体制では、内部監査部門長は、両部門が別々の目的を果たすことを確実にしつつ、両部門を管理するのに十分な知識とリーダーシップ能力を備えているとみなされる。

この体制は、連携を強化し、リスクとアシュアランスの視点を調整し、全社レベルで透明性を高めることができる。しかし、業務上の役割が明確に区分されている場合でも、報告体制が共有されていることから、客観性に対する外観上の懸念が生じる可能性がある。ガバナンス上の重要な課題は、内部監査部門の独立性と客観性が、実際に効果的に維持されているかである。

ERMサイクル全体で見ると、このシナリオは次のように見える可能性がある。

- **識別：**

リスク・マネジメント部門は、組織体全体のリスクの識別を主導し、リスク分類体系を維持する。内部監査部門は、監査計画の策定を目的として独自にリスクの識別を行うこともあれば、リスク・マネジメント部門の業務にある程度依拠することもある。業務の遂行、及びリスクの識別とリスク分類体系というフレームワークの活用は、別々に行われる場合もあるが、監督機能が共有されていることから、内部監査部門のリスクに対する見解が、リスク・マネジメント部門から完全に独立しているかについて疑問が生じる可能性がある。

- **評価：**

リスク・マネジメント部門は、リスク評価手法やスコアリング・モデルを策定して適用する。内部監査部門は、これらのプロセスを運用しないが、監査の優先順位を決定する際に、その成果を参考にする場合がある。ここでの懸念点は、第2ラインの業務が内部監査部門長の監督下にあるという事実にもかかわらず、ステークホルダーが監査計画の決定を十分に独立した客観的なものと捉えるかにある。

- **管理：**

経営管理者は、ERMの支援を受け、リスク選好とリスク許容度の範囲内でリスク対応策を決定する。内部監査人は、こうした意思決定には関与しない。しかし、内部監査部門長がリスク・マネジメント部門を監督している場合、内部監査部門によるリスク・マネジメント活動に対する事後の評価が、内部監査部門長が両部門を統括することによって、直接的又は間接的に、影響を受ける可能性があるという懸念が生じ得る。

• モニタリング :

リスク・マネジメント部門は、主要なリスク指標やリスク低減策をモニタリングする。内部監査部門は、そのモニタリング・プロセスが有効であるかを評価する。実行は別々に行われているものの、ステークホルダーからは、内部監査人が同じ報告体制の下で監督されているプロセスの有効性について、十分に異議申し立てができるのかという疑問が投げかけられる可能性がある。

• 報告 :

リスク・マネジメント部門は、最高経営者と取締役会向けに全社的リスク報告書を作成する。内部監査部門は、独自のアシュアランス報告を行う。リスク報告書の草案作成に直接関与していなくても、指示・報告経路が共通であることから、リスク報告とアシュアランスとの距離が近いという印象を与える可能性がある。

このシナリオでは、実行とアシュアランスの間の技術的及び形式的な分離は維持されているかもしれない。しかし、客観性の侵害の疑いが生じる可能性があるため、内部監査人と内部監査部門長の客観性に対するステークホルダーの信頼を維持するためには、こうしたデリケートな点を認識して理解しておく必要がある。

このようなシナリオで内部監査部門の独立性と客観性を維持するには、組織構造の明確さが不可欠である。このシナリオは、透明性と構造的な防御措置が整備されていれば効果的に機能する。ERM 活動の監督は、リスク・マネジメントやコンプライアンスに関する意思決定の主導権を握ることと同義ではなく、アシュアランス業務は、その実施と報告において独立性が維持され得る。

優れた取り組み：統合的アシュアランス

一部の組織体では、連携と依拠が、一般に「統合的アシュアランス」と呼ばれる、より体系的で意図的なモデルへと発展している。統合的アシュアランスという概念は、ガバナンス、リスク・マネジメント、コンプライアンス及びコントロールの有効性について一貫した見解を提供するために、組織体全体でアシュアランス業務とアドバイザリー業務を調整し、関連付け、伝達する、体系化されたアプローチとして理解できる。

統合的アシュアランスは、リスク環境がますます複雑化して相互に関連し合う中で、組織体にとって有益となり得る成熟した連携と依拠の形態である。その設計と実施においては、組織体の状況を反映し、リスクプロファイルやガバナンスへの期待事項を考慮すべきである。

経営管理者によるモニタリング活動、第2ラインの役割、内部監査部門、そして場合によっては外部のアシュアランス・プロバイダを含むアシュアランス・プロバイダは、互いに縦割り状態で活動するのではなく、手法を統一し、リスク情報を共有し、計画サイクルを調整することができる。これにより、対象範囲の透明性が高まり、業務の重複が減少し、アシュアランスが十分である部分と不足している可能性のある部分がより明確に把握できるようになる。



実際には、統合的アシュアランスには、体系的なアシュアランス・マップの作成、共通のリスク分類体系の策定、報告様式の統一、あるいはアシュアランス・プロバイダ間の計画策定に関する協議の調整などが含まれる場合がある。内部監査部門長と内部監査人は、組織体全体を見渡す視点を持ち、取締役会への直接の指示・報告経路を有していることから、こうした体制において各役割の促進や連携を主導するのに最もふさわしい立場にある。しかし、こうした取り組みは、第2ラインの業務に対する主導権を握ることなく、明確性と一貫性の促進に焦点を当てたまま進めることも可能である。一貫性が確保されていても、内部監査部門長は、第1ラインや第2ラインからの情報が不正確、不完全又は信頼性に欠ける場合は、引き続きその点に異議申し立てや指摘を行わなければならない。

統合的アシュアランスは、重大なリスク全般にわたるアシュアランス状況について、取締役会と最高経営者に、より包括的かつ統合的な視点を提供することで、ガバナンス、リスク・マネジメント及びコンプライアンスを強化できる。これにより、効率性が向上し、リスクに関する用語や報告の一貫性が改善され、より情報に基づいた監督や戦略的議論が促進される可能性がある。統合的アシュアランスが導入された場合でも、最高経営者はリスク・マネジメントとコンプライアンスについて取締役会に対して説明責任を負い続け、内部監査部門の独立性と客観性は維持されなければならない。

用語一覧

定義は、主に IIA の『グローバル内部監査基準』の用語一覧を参考にしたものである。

advice 〈助言〉 – アシュアランスを行わず、また経営管理者としての責任を負わず、組織体のステークホルダーに提供する情報。

assurance 〈アシュアランス〉 – 組織体のガバナンス、リスク・マネジメント、コンプライアンス及びコントロールのプロセスについて、ステークホルダーの信頼度を高めることを目的とした表明。

assurance map 〈アシュアランス・マップ〉 – 様々なアシュアランス・プロバイダによる組織体の包括的なリスク対象範囲を識別する概要文書。これにより、アシュアランス対象範囲のギャップや重複の特定に役立つ。

board 〈取締役会〉 – ガバナンスを担う最上位の機関。例えば次のものがある。

- 取締役会 (board of directors)
- 理事会又は評議員会 (board of governors or trustees)
- 公選議員又は政治任用官のグループ (group of elected officials or political appointees)
- 相応なガバナンス機能の権限を有する他の機関

複数のガバナンス機関が存在する組織体では、「取締役会 (board)」は、内部監査部門に適切な権限、役割及び責任を付与する権限を認められた 1 つ又は複数の機関を指す。

上記のいずれもが存在しない場合、「取締役会 (board)」は、組織体の最高レベルのガバナンス機関¹として機能するグループ又は人物を指すものと読むべきである。取締役会は、監査委員会などの委員会に、一定の責任を委任することができる。

chief audit executive 〈内部監査部門長〉 – 組織体における内部監査部門の責任者を指す用語。具体的な役職名や職責は、組織体によって様々なことがある。

compliance 〈コンプライアンス〉 – 法令、規則、契約、方針、手続及びその他の要件を遵守すること。

control 〈コントロール〉 – 経営管理者、取締役会及びその他の者が、リスクを管理し、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。

governance 〈ガバナンス〉 – 取締役会が、組織体の目標達成に向けて、組織体の活動について、情報を提供し、指揮し、管理し、及びモニタリングするために、プロセスと組織構造を併用して実施すること。

¹ 訳注：2026年7月8日に公開された原文では、「highest-level board」と記載されているが、IIAに確認の上、『グローバル内部監査基準』の用語集に合わせて、「highest-level governing body (最高レベルのガバナンス機関)」と訳した。

risk appetite 〈リスク選好〉 - 組織体が戦略や目標を追い求めて積極的に受容する、リスクの種類と量。取締役会は、組織体のリスク選好を設定する。

risk management 〈リスク・マネジメント〉 - 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又は状況を、識別、評価、管理、コントロールするプロセス。

risk tolerance 〈リスク許容度〉 - 目標の達成に当たり、パフォーマンスの変動が許容される範囲。

stakeholder 〈ステークホルダー〉 - 組織体の活動や成果に直接的又は間接的な利害関係を持つ関係者。ステークホルダーには、取締役会、経営管理者、従業員、顧客、ベンダー、株主、規制当局、金融機関、外部監査人、一般市民などが含まれることがある。

内部監査人協会（IIA）について

IIA は国際的な専門職団体であり、世界中で 26 万 5 千名以上の会員を擁し、22 万名以上に公認内部監査人[®]（CIA[®]）資格の認定をしている。1941 年に設立された IIA は、内部監査の分野において、基準、資格認定、教育、調査、そして専門的なガイダンスの指導者として世界的に認知されている。詳細は theiia.org を参照されたい。

意見書について

「意見書」は、ガバナンス、リスク・マネジメント、コンプライアンス及びコントロールに影響を与える重要な課題について、IIA の公式な立場とビジョンを示すものである。これらは、内部監査の文脈において当該事項をどのように解釈又は適用すべきかを説明するものであり、規制当局、基準設定機関、取締役会及び経営幹部に影響を与えるために活用される。

本文書は原則ベースであり、組織構造を規定するものではない。組織体の状況、複雑性及びガバナンス上のニーズを考慮し、専門職としての判断に基づいて適用すべきである。「意見書」は、主に内部監査人ではなく経営幹部を対象としているため、IIA の「専門職的实施の国際フレームワーク（IPPF）」の一部ではない。

免責事項

IIA は、情報提供及び教育目的で本文書を発行する。本文書は、個別具体的な状況に対する確答を提供することを目的とするものではなく、あくまで指針として利用されることを意図している。IIA は、特定の状況に直接関連する独立した専門家の助言を求めることを推奨する。IIA は、本文書のみに依拠する者に対して一切の責任を負わない。

著作権

© 2026 The Institute of Internal Auditors, Inc. 無断転載を禁ずる。転載の許諾については Copyright@theiia.org まで連絡されたい。



®

The Institute of
Internal Auditors

1035 Greenwood Blvd., Ste. 401
Lake Mary, FL 32746 USA
theiia.org