

第三者

Topical Requirement

トピック別要求事項



第三者 トピック別要求事項

「専門職的实施の国際フレームワーク® (International Professional Practices Framework®)」は、「グローバル内部監査基準™ (Global Internal Audit Standards™)」、「トピック別要求事項」及び「グローバル・ガイダンス」により構成されている。トピック別要求事項は、「グローバル内部監査基準」と共に使用され、これらは、必須事項に関する権威ある基礎を提供する。

トピック別要求事項は、特定のリスクトピックを監査するための最低基準を設定することにより、内部監査人に明確な期待を与えるものである。組織体のリスクプロファイルにより、内部監査人は、トピックの追加的な側面を考慮しなければならない場合がある。

トピック別要求事項への適合により、内部監査業務の実施の一貫性が高まり、内部監査業務と結果の品質と信頼性が向上する。最終的には、トピック別要求事項は、内部監査専門職の水準を高めることになる。

内部監査人は、「グローバル内部監査基準」に適合して、トピック別要求事項を適用しなければならない。トピック別要求事項への適合は、アシュアランス業務では必須事項であり、アドバイザリー業務では推奨事項である。

トピック別要求事項は、トピックが以下のいずれかに該当する場合に適用される。

1. 内部監査計画における個々の監査対象に、特定された課題が含まれる場合
2. 個々のアシュアランス業務の実施中に、特定された課題が識別された場合
3. 当初の内部監査計画にはないが、特定された課題が個々のアシュアランス業務の依頼対象となった場合

トピック別要求事項の各要求事項について適用可能性の評価を行った証拠は、文書化し、保管しなければならない。すべての個別の要求事項がすべての個々の業務に適用されるとは限らない。要求事項を除外する場合は、その根拠を文書化し、保管しなければならない。トピック別要求事項への適合は必須事項であり、品質評価の際に評価される。

第三者

「第三者」とは、組織体（「主体となる組織体」）が製品やサービスを得るためにビジネス上の関係を構築する外部の個人、グループ、又は事業体のことである。当該関係は、契約、合意、又はその他の手段を通じて正式に構築される場合がある。このトピック別要求事項では、「第三者」という用語は、ベンダー、サプライヤー、請負業者、下請業者、外部委託サービス・プロバイダ、その他の機関、及びコンサルタントを指す。この用語には、第三者とその下請業者との契約、すなわち「川下」の下請業者と呼ばれる契約を含む。

このトピック別要求事項は、内部監査部門が、第三者又は下請関係に対するアシュアランス業務を実施する場合に適用される。特に、主体となる組織体と第三者との契約又は合意に基づき認められた、第四次以降の「川下」の下請関係に対するアシュアランス業務を実施する場合に適用される。内部監査人は、後述のリスク・マネジメントの章で説明する通り、リスクに基づき第三者及びそれ以降の「川下」の下請業者を優先付けるべきである。内部監査



人は、リスク評価の結果によって示されたすべての要求事項を適用しなければならず、適用から除外する場合には、その根拠を文書化しなければならない。

このトピック別要求事項は、規制当局、代理人、受託者／取締役会メンバー、又は従業員などの内部関係者、主体となる組織体との間接的な外部関係、利害、又は関与に対処することを意図していない。

「第三者」という用語の定義や用法は、業界やその他の文脈によって異なる場合がある。内部監査人には柔軟性が認められており、主体となる組織体が定義する「第三者」の概念に即してこのトピック別要求事項を適用する際には、専門職的判断に依拠すべきである。

主体となる組織体（第三者契約を締結する組織体）は、第三者を活用して一つ又は複数の目標の達成に役立てることができるが、その目標の達成に伴うリスクに対する説明責任は依然として保持する。「第三者」との協働は、このトピック別要求事項に記載されているように、適切なガバナンス、リスク・マネジメント、及びコントロールの各プロセスを通じて識別、評価、及び管理されなければならないリスクをもたらし。「第三者」が契約通りに業務を遂行できなかつたり、非倫理的な行為に加担したり、業務に支障をきたしたりした場合、主体となる組織体はその影響を受ける可能性がある。「第三者」に関するカテゴリー及びリスクの事例が含まれる。

- 戦略的リスク：主体となる組織体の使命又は上位目標の達成能力、又は合併・買収の影響を管理する能力に関するもの。
- 風評リスク：環境破壊、又は主体となる組織体と顧客、取引先、ステークホルダーとの信頼関係を損なうことに関するもの。
- 倫理的リスク：誠実性の欠如、利益相反、不正なリベート、汚職などに関するもの。
- 業務運営リスク：物理的及び情報セキュリティ、内部者リスク、サービスの中断、目標未達成などに関するもの。
- 財務的リスク：第三者の支払不能（倒産）及び不正に関するもの。
- コンプライアンスリスク：適用される地域、国、及び国際的な規制要件に関するもの。
- サイバーセキュリティやその他のデータ保護リスク：機密データの侵害や漏えいなどに関するもの。
- 情報テクノロジー・リスク：重大な業務運営を支えるための業務の欠如などに関するもの。
- 法的リスク：利益相反、紛争及び契約違反による訴訟などに関するもの。
- サステナビリティ・リスク：環境、社会及びガバナンスに関するもの。例として、組織体が自然環境に与える影響に関連するリスクや、組織体と地域社会との関わりについてのリスクが含まれる。
- 地政学的リスク：貿易摩擦・制裁、政情不安などに関するもの。

「第三者」のライフサイクルは、選定、契約、オンボーディング、モニタリング、及びオフボーディングで構成される。内部監査人は、ガバナンス、リスク・マネジメント及びコントロールの各プロセスに係る要求事項を評価する際に、これらの段階を考慮しなければならない。



「第三者」のガバナンス、リスク・マネジメント、コントロールの各プロセスの評価

このトピック要件は、「第三者」のガバナンス、リスク・マネジメント及びコントロールの各プロセスの設計と導入を評価するための一貫した包括的なアプローチを提供する。この要求事項は、「第三者」を評価するための最低基準を示すものである。

ガバナンス

要求事項：

内部監査人は、取締役会の監督を含め、「第三者」に対する主たる組織体のガバナンスについて、以下の側面を評価しなければならない。

- A. 「第三者」と契約するかどうかを決定するために、正式なアプローチを設定し、導入し、定期的に見直す。このアプローチには、製品又はサービスを提供することによって、目標を達成するために利用可能な資源を定義し、評価するための適切な基準が含まれている。
- B. 「第三者」のライフサイクル全体を通じて、「第三者」との関係及びリスクを定義、評価、管理するための方針と手続が確立されている。方針と手続は適用される規制要件に沿ったものであり、統制環境を強化するために定期的に見直され、更新されている。
- C. 組織体の「第三者」マネジメントの役割と責任が定義され、誰が「第三者」の選定、指揮、管理を行うか、「第三者」とのコミュニケーション、モニタリングを行うか、また「第三者」の活動について誰に報告しなければならないかが詳述されなければならない。「第三者」の役割と責任を割り当てられた個人が、適切な能力を有していることを確実にするためのプロセスが存在する。
- D. 関連するステークホルダーとのコミュニケーション手続が定義され、優先順位付けされた「第三者」のパフォーマンス、リスク、及びコンプライアンス（特に、法規制の違反）に関する適時な状況報告が含まれる。第三者への対応は、リスクに基づいて優先付けされる。関係するステークホルダーには、取締役会、最高経営者、調達部門、業務部門、リスク・マネジメント部門、コンプライアンス部門、法務部門、情報技術部門、情報セキュリティ部門、人事部門などが含まれる。

リスク・マネジメント

要求事項：

内部監査人は、組織体の「第三者」のリスク・マネジメントに関連して、以下を評価しなければならない。

- A. 「第三者」のリスク・マネジメントプロセス及び業務は、標準化され、包括的であり、明確な役割と責任を含み、組織体に関連する主要なリスク（戦略、風評、倫理、業務、財務、コンプライアンス、サイバーセキュリティ、情報技術、法務、持続可能性、地政学など）に十分に対応している。プロセスの遵守はモニタリングされ、何らかの逸脱があれば改善措置が実施される。



- B. ライフサイクルを通じて「第三者」に関連するリスクは、定期的に識別・評価される。リスク評価は、「第三者」及びそれ以降の川下の下請業者を含め順位付けし、優先順位付けするために用いられる。また、リスクへの対応も、順位付けされ、優先順位付けされるために用いられる。リスク評価は定期的に見直され、更新される。
- C. リスクへの対応は適切かつ正確で、順位付けに見合ったものである。リスクへの対応は、実施、レビュー、承認、モニタリング、評価、必要に応じて調整される。
- D. 「第三者」から発生した問題を管理し、必要に応じて上申するためのプロセスが整備されており、結果に対する説明責任を確保し、契約やその他の合意事項を達成する可能性を高めている。上申された懸念事項に「第三者」が対応しない場合、経営陣が当該事業関係の継続に伴うリスクを評価し、必要に応じて、さらなる対応、是正措置又は契約解除を行うためのプロセスが整備されている。

コントロール

要求事項：

内部監査人は、リスクに基づいて優先順位付けされた「第三者」の以下のコントロールを評価しなければならない。その評価には、組織体の第三者について、継続的に評価・モニタリングを行うマネジメントのプロセスを含まなければならない。

- A. 「第三者」の発掘・選定のための強固なデュー・ディリジェンス・プロセスが整備されており、第三者との関係の必要性と性質を説明し正当化する、文書化され、承認されたビジネスケース又はその他の関連文書が存在する。
- B. 契約と承認は、組織体の「第三者」リスク・マネジメント方針と手続に従って行われ、組織体の適切な部署との協働を含む。
- C. 最終的な契約書又は合意書は、法務及びコンプライアンスを含むすべての関係者によってレビューされ、承認され、両当事者の権限を有する個人によって署名され、安全に保管される。契約マネージャー又は管理者には、個々の契約の責任が割り当てられる。
- D. 一元化された契約管理システムなどにおいて、すべての「第三者」との関係を正確、完全、かつ最新に維持する。
- E. 「第三者」が契約又は合意の条件を満たすために、文書化されたオンボーディング・プロセスを確立し、それに従う。
- F. 「第三者」が、ライフサイクルを通じて契約又は合意の条件に従って業務を遂行しているかどうか、契約上の義務を果たしているかどうかを評価するために、継続的なモニタリング・プロセスが存在する。そのプロセスには、提供された情報の信頼性を検証し、定期的に、また契約が変更されるたびにパフォーマンスを再評価することが含まれる。
- G. 「第三者」が期待に沿わなかったり、リスクが増大したり、予期せぬ事態を引き起こしたりした場合に、改善措置を開始するための手続が定められている。この手続には、重大性に基づくインシデントの上申、インシデント発生後のレビューの実施、インシデントの根本原因の分析などが含まれる。
- H. 契約の期限や更新日はモニタリングされ、必要に応じて更新手続きが取られる。



- I. 契約で定められた時期的要件や期待事項が適切に対処されることを確実にするために、公式のオフボーディング計画が導入され、それに従う。そのプロセスには以下のような項目を含む。
- 「第三者」との契約を解除する。
 - 必要に応じて「第三者」を入れ替える。
 - 機密データの保管責任を再設定し、「第三者」が管理していた機密データは、主体となる組織体へ返却又は破棄する。
 - 「第三者」による主体となる組織体のシステム、ツール、及び施設へのアクセス権を削除する。

内部監査人協会（The Institute of Internal Auditors（IIA））について

IIA は、全世界で 265,000 人以上の会員を擁し、200,000 人以上の公認内部監査人®（CIA®）資格を認定している国際的専門職団体である。1941 年に設立され、国際基準、認定資格、教育、研究、技術指導における内部監査専門職のリーダーとして世界中で認知されている。詳しくは、www.theiia.org を参照。

著作権

© 2025 The Institute of Internal Auditors, Inc. 無断転載を禁じる。転載の許諾については、copyright@theiia.org にお問い合わせください。

2025 年 9 月



The Institute of
Internal Auditors

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401 Lake
Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101

