「第三者」トピック別要求事項

Public Consultation Draft

The Institute of Internal Auditors

「専門職的実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準拠して、「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。

A. 内部監査計画における個々のアシュアランス業務の対象となった

B. 個々のアシュアランス業務の実施中に識別された

C. 当初の内部監査計画にはないが、個々のアシュアランス業務の依頼対象となった

「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、組織体がビジネス上の関係を持つ外部の個人、グループ、又は事業体のことである。「第三者」との関係は、契約、合意、又は組織体に製品やサービスを提供するためのその他の手段を通じて正式に構築される。「第三者」という用語の使用は、業界やその他の文脈によって異なる場合がある。このトピック別要求事項では、「第三者」という用語を、ベンダー又はサプライヤー、請負業者または下請業者、外部委託サービスプロバイダー、その他の機関、及びコンサルタントを指し、しばしば「川下」下請業者として知られる、第三者とその下請業者との間の契約を含む。

このトピック別要求事項は、従業員、財務面でのパートナー、規制当局、代理人、又は受託者など、主体となる組織体との間接的な関係、利害、又は関与に対処することを意図していない。

主体となる組織体は、1つ又は複数の事業目標の達成を支援するために「第三者」を雇うことができるが、その組織体は、それらの目標の達成に関連するリスクに対する説明責任を保持する。組織体と「第三者」との契約又は合意により、「第三者」が第四又はそれ以上の「川下」の関係者への下請けが認められている場合、このトピック別要件は、それらの下請け関係のガバナンスとモニタリングに関するアシュアランスを提供する場合にも適用される。このような場合、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件を適用しなければならない。要求事項を除外する場合は、その根拠を文書化しなければならない。

「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す。「第三者」が契約通りに業務を遂行できなかったり、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。カテゴリー 及びリスクの事例「第三者」に関するリスクが含まれる。

- サービスの中断や事業目標の未達成などの業務運営上のリスク。
- 機密データの漏洩などのサイバーセキュリティリスク。
- 「第三者」の倒産などの財務的リスク。
- 適用される地域、国、及び国際的な規制要件のコンプライアンスリスク。
- 利益相反、紛争及び契約違反による訴訟などの法的リスク。
- 環境又は主体となる組織体の顧客、ステークホルダーに与えたに与えた損害などの風評被害。

「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、コントロールの各プロセスの要件を評価する際に、これらのフェーズを考慮すべきである。

「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、組織体における 「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「第三者」のガバナンスの評価

要求事項

内部監査人は、取締役会の監督を含め、「第三者」に対する組織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. 製品又はサービスを提供することによって事業目的を達成するのを支援するために「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、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、手順及びプロセスが確立されている。方針と手続き及びプロセスは適用さ

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. 組織体内の「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る。「第三者」の役割と責任を割り当てられた個人が、適切な知識、スキル及び能力を有していることを確認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の状況報告が含ま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、業務部門、リスク・マネジメント部門、人事部門、情報セキュリティ部門、法務部門、コンプライアンス部門、調達部門などが含まれる。

リスク・マネジメント「第三者」のリスク・マネジメントの評価

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は、標準化され、包括的であり、明確な役割と責任を含み、主要なリスク（財務、業務、戦略、サイバーセキュリティ、コンプライアンス、評判、倫理、持続可能性、地政学、法務など）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」に関連するリスクを識別し、評価する。リスク評価は、「第三者」を分類し、順位付けし、リスクへの対応に優先順位付けするために用いられる。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、契約解除を含む是正のためのプロセスが整備されている。

コントロール：「第三者」のコントロール・プロセスの評価

要求事項

内部監査人は、組織体の「第三者」のコントロール・プロセスに関連して、継続的な評価とモニタリングのための経営管理者のプロセスを含め、優先順位の高い「第三者」について、以下を評価しなければならない。

A. 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には、「第三者」との関係の必要性と性質が記載され、正当化されている。

B. 「第三者」の調達と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いる。このプロセスには、サイバーセキュリティ手続の見直し、財務状況のチェック、銀行の詳細情報の確認など、重要な側面に関する基準が含まれている。

C. 契約と承認は、組織の「第三者」リスク・マネジメント方針、手順及びプロセスに従って行われ、組織体内の適切な部署との協働を含む。

D. 最終的な契約書又は合意書は、該当する場合に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。すべての契約の責任は、契約マネージャー又は管理者に割り当てられる。

E. 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。

F. 「第三者」が契約又は合意の条件を満たすことができるように、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。

G. 優先順位付けされた「第三者」が、ライフサイクルを通じて契約条件に従って業務を遂行し、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。

H. 「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順が定められている。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。

I. 契約更新日は監視され、必要に応じて更新手続が取られる。

J. 優先順位の高い「第三者」については、公式のオフボーディング計画を導入し、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。

内部監査人協会について

内部監査人協会（The Institute of Internal Auditors: IIA）は、全世界で 26 万人以上の会員を擁し、20 万人以上の公認内部監査人（Certified Internal Auditor: CIA©）資格を認定している国際的専門家団体である。1941 年に設立され、国際認定資格、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。

免責事項

IIA は、情報提供及び教育を目的として本文書を発行する。本文書は、特定の個別状況に対する明確な回答を提供することを意図したものではなく、あくまでガイドとして利用す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、本文書に全面的に依拠する者に対し、いかなる責任も負わない。

著作権

