第三者

Topical Requirement

トピック別要求事項
ユーザーガイド

The Institute of
Internal Auditors

目次

トピック別要求事項の概要

トピック別要求事項は、「グローバル内部監査基準™（Global Internal Audit Standards™）」及び「グローバル・ガイダンス」と共に、「専門職的実施の国際フレームワーク（International Professional Practices Framework®）」の不可欠な構成要素である。内部監査人協会は、トピック別要求事項を「グローバル内部監査基準」と共に使用されなければならず、これらは、必須事項に関する権威ある基礎を提供する。より詳細な情報は、本ガイド内の基準の記述を参照のこと。

トピック別要求事項は、内部監査人が広く知られたリスク領域を扱う際に、高い監査品質と一貫性を促進することを目的として公式化したものである。トピック別要求事項は、各トピックの要求事項の対象に関連する個々のアシュアランス業務を実施するための基礎を確立し、関連する評価規準を提供する（基準 13.4「評価規準」）。トピック別要求事項への適合は、個々のアシュアランス業務では必須であり、アドバイザリー業務では評価が推奨される。トピック別要求事項は、個々のアシュアランス業務を実施する際に考慮すべきすべての潜在的な側面をカバーすることを意図しているのではなく、むしろ、トピックに関する一貫性のある信頼性の高い評価を可能にするための最低限の要求事項を提供することを意図している。

トピック別要求事項は、IIA の「３ラインモデル」及び「グローバル内部監査基準」と密接に関連している。ガバナンス、リスク・マネジメント及びコントロール・プロセスは、基準 9.1「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理解」と整合するトピック別要求事項の主要な構成要素である。「３ラインモデル」を参照すると、ガバナンスは取締役会／統治機関に、リスク・マネジメントは第２ラインに、コントロール又はコントロール・プロセスは第１ラインに関連している。経営管理者は第 1 ラインと第 2 ラインの両方に含まれるが、内部監査機能は、独立にして客観的なアシュアランス提供者として第 3 ラインに位置付けられ、取締役会／統治機関に報告する（原則 8「取締役会による監督」）。

適用可能性、リスク及び専門職としての判断

内部監査部門が、トピック別要求事項が存在する対象に関する個々のアシュアランス業務を実施する場合、又は他のアシュアランス業務の中にトピック別要求事項の側面が特定される場合には、トピック別要求事項に従わなければならない。

基準に記載されているように、リスク評価は、内部監査部門長の監査計画を策定する際の重要な要素である。内部監査の計画に含まれる個々のアシュアランス業務を決定するには、少なくとも年 1 回、組織体の戦略、目的及びリスクを評価する必要がある（基準 9.4「内部監査の計画」）。個々のアシュアランス業務を計画する際、内部監査人は、その業務に関連するリスクを評価しなければならない（基準 13.2「個々の内部監査業務におけるリスク評価」）。

リスクベースの内部監査の計画策定プロセスにおいて、各トピックの要求事項の対象が特定され、監査計画に含まれている場合には、該当する業務において、各トピックの要求事項に概説されている要求事項を用いて評価しなければならない。また、内部監査人が業務を実施し（監査計画に含まれているかいないかにかかわらず）、各トピックの要求事項の要素が

特定された場合、各トピックの要求事項は、業務の一環として適用可能性を評価しなければならない。最後に、当初は計画に含まれていなかったが、そのトピックを含む業務を依頼された場合、トピック別要求事項の適用可能性を評価しなければならない。

専門職としての判断は、トピック別要求事項の適用において重要な役割を果たしている。リスク評価は、内部監査の計画にどのような業務を含めるかについて、内部監査部門長の決定を後押しする（基準 9.4「内部監査の計画」）。さらに、内部監査人は、専門職としての判断を用いて、各業務でどのような側面をカバーするかを決定する（基準 13.3「個々の内部監査業務の目標及び範囲」、基準 13.4「評価規準」、基準 13.6「監査プログラム」）。

トピック別要求事項の各トピックの要求事項は適用可能性について評価されたという証拠を、要求事項の除外を説明する根拠を含めて、保持しなければならない。トピック別要求事項への適合は、基準 14.6「個々の内部監査業務の文書化」に記載されているように、監査人の専門職としての判断を用いて文書化されなければならない。

トピック別要求事項は、考慮すべきコントロール・プロセスの最低基準を設定しているが、当該リスクを非常に高いと評価する組織体は、さらに追加的な側面を評価しなければならない場合もある。

内部監査部門長は、内部監査部門がトピック別要求事項に関する個々の内部監査業務を実施するために必要な知識を有していないと判断した場合には、監査資源の不足の影響及び対応方法について、取締役会及び最高経営者に適時に報告しなければならない。内部監査部門長は、監査資源をどのように獲得するかに関わらず、内部監査部門がトピック別要求事項の適合性を確保するための最終的な責任を保持する（基準 3.1 専門的能力、基準 7.2 内部監査部門長の適格性、基準 8.2 監査資源、基準 10.2 人的資源の管理）。

パフォーマンス、ドキュメンテーション及びレポーティング

また、内部監査人は、トピック別要求事項を適用する場合、基準に準拠し、「ドメイン Ⅴ：内部監査業務の実施」に従って業務を実施しなければならない。ドメイン Ⅴ の基準では、監査計画の立案（13 原則「個々の内部監査業務の計画の効果的な策定」）、監査業務の実施（14 原則「個々の内部監査業務の実施」）、監査結果の伝達（15 原則「個々の内部監査業務の結論のコミュニケーション及び改善措置の計画のモニタリング」）について規定している。

トピック別要求事項は、内部監査業務の一貫性と高品質の確保を支援することを目的としている。各国の法令や規制、監督当局からの期待、及び専門職に認識されているフレームワークは、追加的又はより範囲が特定された要件を課すかもしれない。内部監査人は、組織体が活動する業界や法域に関連する法令や規制を理解し、それらを遵守しなければならない。また、基準 1.3 適法かつ倫理的な行動に従って、必要に応じて開示を行わなければならない。内部監査人は、これらの追加的な要件を既に監査プログラムやテスト手続きに統合しているかもしれないが、適切性な範囲を確保するために、トピック別要求事項と照合すべきである。

トピック別要求事項は、監査人の専門職としての判断に基づき、内部監査の計画又は個々の内部監査業務の監査調書に文書化することができる。１つ又は複数の個々の内部監査業務が、要求事項をカバーしている場合がある。また、すべての要求事項が該当するとは限らない。適

用除外を説明する論理的根拠を含め、トピック別要求事項は適用可能性について評価されたという証拠を保持しなければならない。

品質のアシュアランス

基準は、内部監査部門長に対し、内部監査部門のあらゆる側面をカバーする品質のアシュアランスと改善のプログラムを策定、実施、維持することを求めている（基準 8.3「品質」）。その結果は、取締役会及び最高経営者に報告されなければならない。伝達事項には、内部監査機能の基準への適合状況とパフォーマンス目標の達成状況について含めなければならない。

トピック別要求事項への適合性は、品質評価において評価される。

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、組織体に製品、サービス、労働力、製造、又はデータの保存、処理、保守などの情報技術ソリューションを提供するための契約、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。

> 注記
>
> トピック別要求事項は、グローバル内部監査基準で定義されている一般的な内部監査用語を使用している。読者は基準の用語一覧の用語と定義を参照すべきである。

「第三者」という用語は、業界やその他の文脈に基づいて異なって使用される場合がある。各内部監査部門は、主体となる組織体（第三者契約を締結する組織体）が第三者をどのように定義するかに従って、トピック別要求事項の適用において判断を用いる柔軟性を有する。第三者トピック別要求事項とユーザーガイドでは、「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。「第三者」という用語は、第三者とその下請業者との間の取り決めを含むすべてのそのような取り決めを包含し、しばしば「川下」の下請業者、又は「第四者」、「第五者」、又は「第 N 者」として知られている。

このトピック別要求事項は、規制当局、代理人、ブローカー、投資家、受託者／取締役会メンバー、公共サービス、及び一般公衆のメンバーなどの主体となる組織体との間接的な外部関係、利害、又は関与、又は従業員やグループ内サービス・プロバイダなどの内部関係者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、専門職としての判断に依拠すべきである。

組織体の第三者との取引関係を管理するプロセスの有効性は、組織体全体、又は一つ以上の個別の契約、合意、又は関係のレベルで評価できる。内部監査人は、組織体の第三者方針、手続、プロセス、フレームワーク、及びライフサイクルの理解を深めるためにトップダウン・アプローチを採用すべきである。内部監査人は、個々の業界、組織体、及び業務トピックに基づく第三者リスクのニュアンスを理解するために判断を用いるべきである。基準 5.1 情報の利用と整合して、内部監査人は、アクセスする可能性のある第三者情報に関連する方針及び手続を認識し、遵守すべきである。

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。

第三者トピック別要求事項とユーザーガイドは、組織体とその第三者との関係の段階、すなわちライフサイクル段階として知られる選定、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に言及している。これらの段階は、一部の業界が独自のライフサイクルのバージョンを持っているにもかかわらず、第三者トピック別要求事項とユーザーガイドの目的で使用される。段階は以下のとおりである：

- 選定：第三者の必要性を判断するプロセス、その使用計画、及び選定のためのデュー・ディリジェンスを含む。さらに、選定には潜在的及び契約済みの第三者のリスク評価を含むべきである。
- 契約：第三者との法的合意の起草、交渉、承認、及び実施のためのデュー・ディリジェンス・プロセスを含む。
- オンボーディング：関係を開始するために契約が署名されたときに始まり、第三者が契約又は合意の条件を満たすための基盤を確立する。
- モニタリング：契約が確立され承認された後の第三者の「稼働中」管理及び継続的なモニタリングのプロセスを含む。アプローチは通常、体系的かつリスク・ベースであり、継続的改善を考慮すべきである。モニタリングには、必要に応じて継続的な第三者契約又は合意の更新が含まれる。
- オフボーディング：契約及び合意を終了するプロセス、リスクに基づいて優先順位付けされた第三者の出口戦略の維持、及び必要に応じて関係を終了することを含む。プロセスは通常、リスク・ベースのアプローチを使用し、正式な出口計画を含む場合がある。

主体となる組織体は、第三者を活用して一つ以上の目標を達成するのを助ける場合でも、そ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。第三者との関与は、組織体のプロセス実行のコストの一部を削減する可能性がある。しかし、主体となる組織体が第三者のコントロール・プロセスに対する可視性と権限が少ないため、業務運営リスクをもたらす可能性がある。第三者が契約どおりに業務を遂行できない場合、非倫理的な行為に関与した場合、又は事業を中断した場合、主体となる組織体は影響を受ける可能性がある。

主体となる組織体は、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・プロセスを通じてリスクを識別、評価、及び管理しなければならない。「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：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。

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。

第三者トピック別要求事項における要求事項は、基準 9.1 ガバナンス、リスク・マネジメント、及びコントロール・プロセスの理解に従って、3 つのセクションに分かれている：

- ガバナンス - 組織体の目標、方針、及び手続をサポートするために第三者を活用するための明確に定義された基準となる目標と戦略。
- リスク・マネジメント - 事象を迅速にエスカレートするプロセスを含む、第三者を活用するリスクを識別、分析、管理、及びモニタリングするプロセス。
- コントロール - 第三者を活用する際のリスクを軽減するために、経営管理者によって確立され、定期的に評価されるコントロール・プロセス。

トピック別要求事項と本ガイドに加えて、内部監査人は、IPPF グローバル・ガイダンスや業界固有のリソースなど、第三者に関する追加の専門的ガイダンスを参照したい場合がある。

考慮すべき事項

以下の考慮すべき事項は、内部監査人が第三者トピック別要求事項における要求事項を実施する際に役立つ可能性がある。以下の各セクションのアルファベット記号で示された記述は、トピック別要求事項の対応する要求事項を再掲又は言い換えたものである。これらの必須ではない考慮すべき事項は、要求事項を評価する方法の例を提供するための例示である。内部監査人は、評価に何を含めるかを決定する際に、専門職としての判断を適用すべきである。

ガバナンスに関し、考慮すべき事項

取締役会の監督を含むガバナンス・プロセスが第三者の目標にどのように適用されるかを評価するために、内部監査人は以下の証拠をレビューすることが考えられる：

A. 第三者を活用するかどうかを決定するための正式化され文書化されたリスクベースのアプローチ又は戦略。このアプローチは定期的にレビューされ、以下を含む：
   - 組織体による使用が承認された、アプローチを実施するための明確に定義され標準化されたプロセス。
   - 第三者との契約を正当化し、戦略的整合性と資源効率を確保するためのコスト便益分析に基づく予算化された資源。
   - 第三者との問題に対処するものを含む、リスクとコントロールの経営管理者による評価。
   - 第三者のパフォーマンスを契約、管理、及びモニタリングするための適切な資源。
   - アプローチ又は戦略へのステークホルダーのフィードバックの統合。

B. ライフサイクル全体を通じて第三者との取引関係を定義、評価、及び管理するために使用される方針、手続、及びその他の関連文書。方針と手続には以下が含まれる場合がある：
   - 主要なガバナンス、リスク・マネジメント、及びコントロール・プロセスを促進するための標準化されたツールとテンプレート。
   - 方針と手続を定期的に評価し、その妥当性を判断し、必要に応じて更新するプロセス。
   - 第三者の選定、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のための確立された規準。
   - 方針及び手続との整合性のための適用される規制要件の識別と定期的なレビュー。
   - 第三者の管理に関する先進的な実務を識別し比較するために実施されるベンチマーク演習。

C. 第三者を活用する目的の達成を支援する定義された役割と責任。さらなる証拠には以下が含まれる場合がある：

- 第三者の価値観、倫理、及び企業の社会的責任が主体となる組織体の原則と整合しているかどうかを評価するプロセス。
- プロセスには、潜在的な利益相反又は非倫理的な行為に迅速に対処する方法を含むべきである。
- 第三者の管理の役割を担う人員の定期的な研修及びその能力の定期的な評価。
- 第三者に関する組織全体の認識を生み出すために研修が実施されたかどうかを評価するプロセス。
- 役割と責任が 3 ラインモデルと整合している。

D. 第三者ライフサイクル全体を通じて関連するステークホルダーとの適時のコミュニケーションと関与（例えば、取締役会、最高経営者、調達、運用、リスク・マネジメント、コンプライアンス、法務、情報技術、情報セキュリティ、人事、その他）、これには以下が含まれる：

- 会議の議事録、報告書、又は電子メールにおける第三者リスクと既知の潜在的脆弱性に関する情報。
- 第三者の管理に関する情報交換と協力の促進（例えば、定期的な部門横断会議を通じて）。

リスク・マネジメントに関し、考慮すべき事項

リスク・マネジメント・プロセスが第三者を活用する目的にどのように適用されるかを評価するために、内部監査人は以下の証拠をレビューすることが考えられる：

A. 第三者業務のユーザーのための、標準化され、包括的なリスク・マネジメント・プロセスには、定義された役割と責任が含まれており、組織体に関連する主要なリスクに十分に対処している：

- 第三者リスクを評価し管理するプロセスには、以下のように主要なリスクがどのように扱われるかが含まれる：
  - 最初の識別と報告。
  - 組織目標の達成能力への影響を評価するための分析。
  - リスクを許容可能な水準まで低減するための改善措置を含む軽減策。
  - 早期警告の検知と対応、及び脅威が完全に解決されるまでの継続的な報告計画を含むモニタリング。

- 組織体の長期的な目標又は戦略を損なうことを防ぐために、プロセスの遵守及び逸脱に対する改善措置の実施のモニタリングが行われる。
- リスク・マネジメント委員会又はその他のグループが第三者の直接的な監督と取締役会への意見を提供する。委員会は定義された目的を持ち、定期的に開催される。証拠には会議の議事録が含まれる場合がある。

B. ライフサイクル全体を通じて第三者に関連するリスクが定期的に識別され、評価される。リスク評価は第三者をランク付けし、優先順位付けする。リスクへの対応もランク付けされ、優先順位付けされる。

- 主体となる組織体は、第三者リスク評価を策定する際に、その規模、成熟度、及び関与する第三者の数などの要因を考慮する。
- リスク評価は文書化され、固有リスクと残余リスクを識別する。
- 組織体はリスク評価をレビューし更新するためのデュー・ディリジェンス・プロセスに従う。
- リスクに応じて第三者をランク付けし、優先順位付けするための規準が確立される。そのような規準の例には以下が含まれる：

    - 提供される業務が組織体の運営に不可欠である。
    - 契約の財務的影響が大きい。
    - 新規の取引関係である、契約が急いで締結された又は契約期間が長期に渡る。
    - 複数の外部関係者が関与している。
    - 第三者が業務の一部又はすべてを下請けに出すことを計画している。

- 組織体は、広く受け入れられているリスク評価の実務に従う。その実務には、リスク評価が可能な限り早い段階、典型的には選定段階での提案分析時、かつオンボーディング前に実施されることを含む。
- ベンダーは、固有リスクに基づいてリスク順位と優先順位を決定するためのアンケートに記入する。組織体は、アンケートが関係者に記入され、正確性であるようにレビューされることを確実にする。
- 組織体は、情報技術、調達、全社的リスクマネジメント、人事、法務、コンプライアンス、業務運営、会計、及び財務などの機能分野から第三者リスク管理に関する定期的な意見を聴取する。

C. 軽減、受容、回避、及び移転などのリスクへの対応が識別され、リスク順位に見合ったものになっている。

- リスクへの対応は文書化され、第三者の統制環境の考慮を含む。
- 主体となる組織体のリスク許容度を超えるリスクへの対応が適切性についてレビューされるという文書、特にリスクが受容される場合。リスクへの対応には第三者との潜在的な利益相反に対処するものが含まれる。

D. 脅威又はリスクのレベルがどのように評価され、割り当てられ、優先順位付けされるかを含む、第三者リスクを管理し上申するプロセス。レビューには以下の識別が含まれる場合がある：

- 組織体のリスクレベル（高、中、低など）の定義と説明、及び各リスクカテゴリーの上申手続。
- 識別されたリスクによって優先順位付けされた第三者のリスト及びリスク事象の軽減状況。
- 適用される法律、規制、及びコンプライアンス要件。
- 財務的及び非財務的（例えば、風評）の両方のリスクの影響。
- 取締役会（又はその他の適切な機関）へのリスクプロファイルの定期的な報告を含む、経営管理者と従業員への第三者リスクを伝達するプロセス。コミュニケーションには、優先順位付けされた第三者で指摘された問題の是正に関する更新を含むべきである。

- 主体となる組織体のリスク選好度とリスク許容度の水準が変化したときに順位と優先順位付けを再評価するプロセス。

コントロールに関し、考慮すべき事項

コントロール・プロセスが第三者との取引関係にどのように適用されるかを評価するために、内部監査人は以下の証拠をレビューすることが考えられる：

A. 第三者の調達及び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、第三者との取引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。
   - ビジネスケースには以下も含まれる場合がある：
     - 第三者が期待を満たす能力へのリスク及び組織体への潜在的影響に対処する。
     - 詳細なコスト便益分析を含む。
   - 競争入札、提案依頼、及び単独調達などの確立された調達プロセスが遵守されている。プロセスには以下が含まれる：
     - サイバーセキュリティ・プロトコルのレビュー、銀行口座情報の照合、財務状況の背景調査、及び第三者の組織構造、犯罪及び法的記録、運転記録、政治活動、及び犯罪活動との関係の調査などの重要な側面の規準。
     - 過去のパフォーマンス、参照、風評、及び契約コストの評価を含む明確に定義された選定規準。
     - 提案をレビューするための部門横断チームの結成など、ベンダーの適切な選定を確保するためのデュー・ディリジェンス。バイアスのリスクを軽減するために、レビューチームのコントロールには、チーム作成の手続と潜在的な利益相反の開示要件が含まれる。
     - 第三者の統制環境を評価するデュー・ディリジェンス。例えば、現地訪問の実施又は第三者の以下のレビュー：
       - システム及び組織管理（SOC）報告書。
       - 財務的安定性。
       - 定款又は適正証明書。
       - 主要な経営管理者とステークホルダーの意思決定における透明性。
       - 組織構造。
       - 運用の安定性。
       - サイバーセキュリティ・プロトコル。
       - 関連する法律、規制、及び基準へのコンプライアンス。
       - 倫理。
       - 主体となる組織体との歴史。
       - 風評。
     - 潜在的なベンダー又は請負業者が関連するデュー・ディリジェンス・プロセスが実施され、結果が分析された後にのみライフサイクルの契約段階に進むという証拠。
B. 契約方針と手続が確立され、それに従う。
   - 契約は曖昧でない条件で書かれている。

- 主要なリスクは契約のドラフト段階で考慮され、関連条項が含まれる。解決を必要とする問題は、この段階で第三者とコミュニケーションがとられる。
- 契約の不可欠な要素は、組織体の契約方針と手続及び第三者の優先順位に基づいて決定される。要素には以下が含まれる場合がある：

  - 守秘義務（プライバシー）契約。
  - 解約条項とデータアクセスのための定義されたパラメータ。
  - すべてのデータへのアクセスと共有、及び指定された期間内の事象又は違反の報告を含むサイバーセキュリティ要件。
  - 主体となる組織体のデータに影響を与える違反の通知要件。
  - 完全な法的名称、住所、物理的な場所、及びウェブサイトを含む第三者の識別を検証するための標準化されたプロセス。標準的な実務は、識別プロセス中にチェックリストを使用し、情報の正確性をレビューすることである。
  - 期待される結果と各当事者の権利、義務、違約金、報酬、及び責任を指定する明確に定義されたサービス・レベル契約（労働コストの支払い責任を含む（川下の下請業者を含む））。
  - 川下の下請業者を含む監査権条項、又は評判の良い独立したアシュアランス・プロバイダが当事者を監査したという証拠の要件。監査権条項がなければ、内部監査部門のアシュアランスを取得又は提供する能力が制限される可能性がある。

- 主体となる組織体は、独立監査人のコントロール評価報告書にアクセスできる。例えば、国際保証業務基準（ISAE）又は SOC 報告書などの財務、コンプライアンス、及びデータセキュリティに関するもの。
  - 第三者の外部アシュアランス・プロバイダの業務に依存する場合、信頼性を確保するために文書がレビューされる。
  - SOC 報告書は、不適切なリスク及び変更管理プロセスを識別するために使用される。

- 方針と手続は、特定の組織体又は契約の種類に不可欠な構成要素に対処する：
  - 環境及び持続可能性条項。
  - 内部通報プロトコル。
  - パフォーマンス測定評価の要件。
  - 第三者のためのテスト済み事業継続計画。
  - 業務提供における AI（人工知能）の使用。
  - 川下の下請業務の明確な識別、開示、条件、及び範囲。
  - 契約期間中の範囲、条件、又は運用要件（技術又は規制の更新などの変更）への変更を処理する方法を概説する変更管理プロセス。
  - 請求できる変更注文の数又は金額の制限。

- 方針と手続は、支払いが行われる前又は留保金が支払われる前に最終製品の正式な受け入れを要求する。
- 第三者は、倫理方針又は行動規範を共有する又は主体となる組織体のものに従うことが要求される。

- 第三者が契約を提供する場合、主体となる組織体は法的レビューを実施し、主要なリスクが理解され、適切なリスク軽減戦略によってサポートされている。

C. 最終契約又は合意は、法務及びコンプライアンスを含む適切なステークホルダーによってレビューされ承認され、安全に保管され、責任のために契約マネージャー又は管理者に割り当てられる。

- 外部委託関係と第三者の義務を示す契約又はその他の公式文書、及び必要な法務及びコンプライアンスレビューの証拠。

D. 一元的に管理された契約管理システムなどで、すべての第三者との取引関係について、正確かつ完全で現行のリストが維持されている。

- リスト又はシステムに新しい第三者契約又は合意を追加するプロセス。
- 潜在的な第三者をベンダーシステムに入力し、契約が承認されない場合は削除するプロセス。
- リスト又はシステムから第三者契約又は合意を削除するプロセス。
- 将来の参照のために、特定の請負業者又はベンダーとの問題を文書化する追跡システム。
- 第三者の母集団が正確で完全かどうかを判断するレビュープロセス。

E. 第三者が契約又は合意の条件を満たすことを可能にするために、文書化されたオンボーディング・プロセスが確立され、それに従う。レビューには以下の検証が含まれる場合がある：

- 標準化されたオンボーディング手続により、必要なすべての文書、研修、及びコンプライアンス・レビューが完了することを確保する。
- 第三者のシステムとプロセスが、主体となる組織体の技術と円滑に統合できる。
- 共有システムが互換性があり安全である。証拠には、SOC 報告の一部として補完的なユーザー・エンティティ・コントロールが含まれる場合がある。
- 主体となる組織体は、緊急時に業務が継続することを確実にする第三者の事業継続計画を評価する。潜在的な事業の中断に対処するための緊急時対応計画が含まれる。

F. 重要業績評価指標の評価を含む、契約又は合意の目標に対するベンダー・パフォーマンスの継続的なモニタリングのプロセス。

- モニタリング・プロセスは第三者リスク評価に情報を提供し、識別されたコントロールの弱点は必要に応じてレビュー、エスカレート、及び対処される。
- リアルタイムでモニタリングを管理するために確立されたプロセス、技術、及びツールの報告書又は観察。
- プロジェクトの適時性、マイルストーン、及びコミュニケーション要件の達成など、契約又は合意条件に従って支払いが行われることを確実にするプロセス。支払いは、オンボーディング段階を完了し、ベンダー支払いシステムに入力された承認済み請負業者にのみ行われる。成果物が契約で指定されている場合、最終支払いは成果物が検証された後にのみ行われる。
- 価値を確保し投資収益率を決定するために第三者契約に関連するコストを管理するモニタリング。コスト便益分析の結果は契約を再交渉するために使用される。

- 契約又は合意書におけるサービス・レベル契約の不履行に対する違約金を査定するプロセス。違約金は、発生時に計算され請求される。
- 優先順位付けされた第三者のリスク・ベースの順位は、定期的、合意に変更があるとき、及び契約が期限切れ又は自動更新に近いときに再評価される。
- コントロールと運用の完全性を検証するための、現地訪問又は四半期ビジネス・レビューなど、優先順位付けされた第三者のレビュー。
- 追加の継続的なモニタリングの証拠には以下が含まれる場合がある：

    - 第三者の財務的安定性の分析。
    - 第三者に対する苦情の評価。
    - 経営管理者による、第三者から提供される独立監査人報告書のレビュー（国際保証業務基準（ISAE）、証明業務基準書（SSAE）、財務、監査、コンプライアンス、及びデータセキュリティに関する報告書など）、並びに ISO 認証。
    - 識別された重要な問題を含む、第三者によって実施された事業回復力テストの経営管理者のレビュー。
    - 下請業者又は川下の業者の活用に関する条件と制限。
    - 第三者の倫理的価値、文化、及び行動の評価。
    - メディアからの問い合わせへの対応。
    - AI（人工知能）などの先進技術の使用を含む、主体となる組織体のデータと情報の保存と転送を保護するためのプライバシーとサイバーセキュリティ・プロトコルの評価。
    - 組織体が、第三者のパフォーマンスの継続的な改善と契約又は合意の目標達成に向けた機会を識別。
    - 職務分離のレビュー。

G. 第三者が契約又は合意の要件を満たさない場合、又は第三者の行動が主体となる組織体へのリスクを増大させる場合に、識別された事象に対して是正措置を開始するプロトコル。

- 事象の重大度と第三者の優先度に基づいて事象を上申するプロトコル。
- 根本原因分析を含む事象発生後のレビュー。

H. 契約及び合意の期限到来又は自動更新が近づいていることを警告するプロセス。自動更新プロセスには以下のレビューが含まれる：

- 第三者のパフォーマンス。
- 契約又は合意条件及び追加条項。
- リスク要因。

I. 川下の下請業者を含み、時期的要件や期待事項を含む契約要件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実施され、それに従う。

- セキュリティ対策が効果的であることを確実にするためのチェックリスト又は主要なステークホルダーとのインタビュー。
- 第三者の保管下にある組織体の情報又はデータは、返却又は破棄されている。
- 組織体のデータ、システム、又は施設への第三者のアクセスが取り消されている。

- デバイス、ソフトウェア・ライセンス、知的財産、及び文書などの主体となる組織体の資産が返却されている。
- 正当な理由により第三者との契約を解除する場合、その背景事情又はリスクが識別され、最高経営者又は取締役会に上申される。
- 優先度の高い第三者との契約が終了する場合、契約完了又は不要となった場合を除き、同一のリスク評価基準に基づいて代替業者を確保する。

付録 A.実務上の適用事例

以下の例は、第三者のトピック別要求事項が適用されるシナリオを説明するものである。

例 1：内部監査の計画に含まれる内部監査業務において、現在第三者によって提供されている業務又は成果物が含まれる。

内部監査部門がリスクベースの計画プロセスを完了し、契約又は合意の下で第三者によって現在提供されている業務又は成果物の内部監査計画に一つ以上の業務を含める場合、トピック別要求事項は必須である。

トピック別要求事項のすべての要求事項がすべての業務に適用されるとは限らない。内部監査人が専門職としての判断を適用し、第三者トピック別要求事項の一つ以上の要求事項が適用されないため業務から除外すべきと判断する場合、内部監査人はそれらの要求事項を除外する根拠を文書化し保持しなければならない。例えば、特定の要求事項を除外する根拠は、内部監査部門が組織体のミッションかつ重大な業務に対する第三者への依存が低い、又は財務的影響が低い確立された取引関係であると判断した可能性がある。

例 2：第三者又は契約管理以外のトピックに関するアシュアランス業務中に第三者リスクが識別される。

内部監査人は、当初第三者又は契約管理に関連すると判断されなかったプロセスを評価しながら、重要な第三者リスクを識別する場合がある。例えば、データストレージを評価する業務を計画する際、内部監査人はクラウドサービスが第三者を通じてホストされていることを知る。業務提供者である第三者の経営管理者とのインタビュー中に、内部監査人は第三者に関連するサイバーセキュリティリスクを識別する。

関連するリスクが識別されたら、内部監査人は第三者とサイバーセキュリティの両方のトピック別要求事項をレビューし、どの要求事項が適用可能かを判断しなければならない。監査人は、監査業務の範囲から第三者のガバナンス・プロセス又は第三者のリスク・マネジメント・プロセスを除外し、監査対象となっている業務に対する第三者のコントロールに焦点を当てる可能性がある。この同じ専門職としての判断は、サイバーセキュリティのトピック別要求事項の適用にも適用される。監査人は、第三者又はサイバーセキュリティのトピック別要求事項の要求事項を除外する根拠を監査調書に文書化し、文書を保持しなければならない。

例 3：当初、内部監査の計画に含まれていなかった第三者に関する業務の要請を受けた。

組織体内において、優先度の高い第三者に関する問題が生じ、内部監査部門からの緊急の対応を要する。問題はコントロールの失敗に関係していた。内部監査部門長は、ニーズに対応するために内部監査部門の監査計画と監査資源を再び優先順位付けすることについて取締役会とコミュニケーションをとるべきである。

監査人は、影響を受けた管理者と協働して、状況を評価し将来の発生を防ぐための推奨事項を作成する監査目標を策定すべきである。内部監査部門長は、業務の範囲を決定し、どの要求事項が適用されるかを決定し、それに応じて除外を文書化するためにトピック別要求事項をレビューすべきである。

付録 B.任意の文書化ツール

内部監査人は、リスク評価に基づき、各要件の適用可能性を判断するにあたって専門的判断を働かせ、特定の要件を除外する場合には、その旨を適切に文書化することが求められる。トピック別要求事項は、監査人の専門職としての判断に基づき、内部監査の計画又は個々の内部監査業務の監査調書で文書化することができる。1 つ以上の個々の内部監査業務が要求事項をカバーする場合がある。また、すべての要求事項が適用されるわけではない。以下の印刷可能フォームは、「第三者」トピック別要求事項への適合性を文書化する一つの選択肢を提供するが、その使用は必須ではない。

第三者ガバナンス

要求事項	実施した範囲又は除外の理由	参照資料
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。		

要求事項	実施した範囲又は除外の理由	参照資料
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。		

第三者リスク・マネジメント

要求事項	実施した範囲又は除外の理由	参照資料
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. ライフサイクル全体を通じて第三者に関連するリスクが定期的に識別され、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。		

要求事項	実施した範囲又は除外の理由	参照資料
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。		

第三者コントロール

要求事項	実施した範囲又は除外の理由	参照資料
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。		

要求事項	実施した範囲又は除外の理由	参照資料
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。

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、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、あくまでも指針として使用していただくものである。IIA は、特定の状況に直接関係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、本稿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

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