公開草案
「組織体の回復力」トピック別要求事項

「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。

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。

詳細については、『組織体の回復力 トピック別要求事項ユーザーガイド』を参照のこと。

組織体の回復力

組織体の回復力とは、ISO 22316:2017、「セキュリティと回復力-組織体の回復力-ISO（国際標準化機構）によって発行された原則と属性」において、「変化する環境の中で組織体が吸収し、適応する能力」と定義されている。組織体の回復力は広範なテーマであり、戦略的、業務的、技術的、人的、社会的及び財務的な重要要素を包含している。組織体の回復力は、中核となる製品や業務を提供し、ステークホルダーの信頼を維持し、又は戦略的な目標を遂行する組織体の能力を著しく阻害、又は損なわせる可能性のあるリスクに対処するものである。これらのリスクは、突発的な事象（自然災害、サイバー攻撃及び地政学的な紛争など）、環境的な圧力の長期化（資源不足や公衆衛生上の危機など）、又は外部環境の変化（技術的混乱、規制変更、評判の低下など）から生じる可能性がある。また、これらのリスクは徐々に変化したり、長期的には組織体の安定性や適応力を損なうような圧力の構築を遅らせたりすることもある。このようなリスクの増加は、日常的に見落とされることがある。回復力のある組織体は、成功を収めるために、突発的なリスクと緩やかで目立たないリスクの両方を予測し、適応する。

回復力への脅威を高める固有のリスク要因には、業務の複雑性の高さ、グローバル化されたサプライチェーン、集中化されたインフラ又はデータシステム、労働力不足、不安定な市場条件、重要な第三者又は地理的な場所への依存度の高さなどが含まれる。高い信頼性のある分野における組織体や、厳格な規制による監督下で活動する組織体は、社会的影響やコンプライアンス義務により、本質的に高いリスクに直面している可能性がある。

内部監査人は、一般に、事業継続と災害復旧に関する情報技術（IT）プロセスとコントロールを評価する。事業継続計画は、災害発生時に組織体が通常の業務機能を回復するために講じる手順を詳細に定めたものである。災害復旧計画は、中断時に組織体が IT システムと重要なデータをどのように保護するかを記述したものである。しかし、組織体の回復力にはこれらに加えて、戦略的計画立案、全社的リスクマネジメント、有効なリーダーシップと文化、そして組織体全体のコントロール・プロセスも必要である。組織体の回復力に対する強力なコントロール・プロセスは、組織体が継続的に変化を予測、準備、対応、適応することを可能にするだけでなく、存続、発展することを可能にする。

組織体の回復力のガバナンス、リスク・マネジメント及びコントロールの各プロセスの評価

このトピック別要求事項は、組織体の回復力のガバナンス、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、組織体の回復力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、組織体の回復力に関するガバナンスの以下の側面を評価しなければならない。

A. 取締役会によって、組織体の回復力の戦略が正式に策定、文書化され、組織体の使命とビジョンに沿って、これらを支援する目標が含まれている。この戦略には、危機、混乱、緊急事態の中で業務を継続し、その後の回復や適応に必要な業務面、技術面、財務面の要素が含まれている。この戦略は、組織体のリスク・マネジメントに対する全体的なアプローチと整合しており、定期的に検証、更新される。

B. 組織体の回復力の戦略と目標の達成状況に関する最新情報は、定期的に取締役会に報告、審議される。これによって、回復力が戦略的な監督、長期計画プロセス及び組織文化に組み込まれることが確実になる。これには、重要な事業活動を支援するために必要な資源及び予算上の考慮すべき事項も含まれる。

C. 組織体の回復力に関連する重要な業務プロセス、技術プロセス、及び財務プロセスが識別されている。重要プロセスに関する方針と手続が確立されており、統制環境を強化するため定期的に見直され、必要に応じて更新されている。

D. インシデント時の指揮体制が確立され、これには意思決定の階層、コミュニケーションと上申手続、及びリーダーシップと業務上の役割と責任が含まれる。この体制は、組織体の回復力の目標設定を監督し、支援するために活用される。

E. 回復力のプロセスにおいて重要な役割を担う個人の能力を定期的に再評価するプロセスが確立されている。後継者計画が存在し、主要な役職と後任候補者を識別している。

F. 組織体の回復力の目標達成に影響を及ぼす可能性のある既存の脆弱性や新たな脅威を識別、分析、対応するために、関連する内外のステークホルダーを巻き込むプロセスが確立されている。ステークホルダーには、最高経営者、業務部門、リスク・マネジメント部門、IT 部門、サプライチェーン／調達部門、施設管理部門、人事部門、財務部門、法務部門、コンプライアンス部門、広報部門、重要ベンダー、顧客、規制当局などが含まれる場合がある。

リスク・マネジメント

要求事項：

内部監査人は、組織体の回復力に関するリスク・マネジメントの以下の側面を評価しなければならない。

A. 組織体のリスク評価およびリスク・マネジメントプロセスには、業務運営を妨げる可能性のある脅威を識別し、分析し、軽減し、モニタリングすることが含まれる。組織体の回復力のためのリスク・マネジメント戦略は、組織全体に周知され、定期的に見直されている。

B. 組織体の回復力に関連するリスクは、組織体全体で定期的に評価および管理されている。リスク評価と管理には、業務、全社的リスクマネジメント、IT、サプライチェーン／調達、施設、人事、財

務、法務、コンプライアンス、規制対応、広報、重要ベンダー、評判、新たなリスクなどの領域が含まれる場合がある。

C. 組織体の回復力のリスク・マネジメントに関する説明責任と管理責任が確立されている。組織体の回復力リスクの管理状況（リスク軽減に必要な資源や新たな組織体の回復力の脅威の識別を含む）を定期的にモニタリングし、報告する個人又はチームが識別されている。

D. 組織体の回復力リスク（新たに発生したリスク又は識別されたリスク）のレベルをモニタリングし、組織体が定めたリスク・マネジメントのガイドライン及びリスク許容度、又は適用される法的・規制上の要件に基づき「許容できない」と定義されるレベルに達したリスクを迅速に上申する手続が確立されている。組織体の回復力がもたらす財務的及び非財務的影響が考慮されている。

E. 経営管理者が、危機、混乱、緊急事態の発生に対応し、復旧するためのプロセスを導入し、定期的にテストしている。インシデント対応及び復旧プロセスには、検知、抑制、復旧、及び事後分析が含まれている。インシデント対応アプローチには、想定される様々な混乱を引き起こす事象に対するシナリオ分析と定期的なストレステストが含まれている。これらの演習の結果は取締役会及び最高経営者によってレビューされ、改善措置は追跡され、定期的に報告される。改善のための提言は実行可能であり、明確な責任者と期限が設定されている。

コントロール

要求事項：

内部監査人は、組織体の回復力に関連するコントロールの以下の側面を評価しなければならない。

A. 重要な第三者プロバイダ（サプライヤーとベンダー）と重要な業務を継続するために最低限必要な在庫水準を識別するプロセスが確立されている。このプロセスには、代替サプライヤーのリストを維持することが含まれる。

B. 業務に不可欠なデータが識別され、分類されている。データ分類には、データがどこに存在するか、誰がアクセスを必要とするか、どのようにアクセスされるか、緊急時にバックアップされ、回復可能かどうかを識別することが含まれている。

C. 情報セキュリティリスク（サイバー関連リスクを含む）を軽減し、危機、混乱、緊急事態においても機密データが保護されるよう、重要な IT コントロールと継続的なモニタリング体制が確立されている。コントロールと継続的なモニタリングには、リアルタイムの脅威インテリジェンスと、許可されたユーザーのみへのアクセス制限が含まれている。

D. 重要な IT 資産が台帳に記録されている。これには、危機、混乱、緊急事態における業務部門を支援するために必要なハードウェア、ソフトウェア、及び業務が含まれている。

E. 事業継続と災害復旧計画が策定されている。計画には、割り当てられた要員と復旧チームに対する明確な役割が含まれている。計画は定期的にテストされ（例：「卓上演習」）、テスト結果（改善機会を含む）は取締役会と最高経営者に報告されている。

F. 危機、混乱、緊急事態時に作業環境を変更するプロセスが確立されている。変更には、在宅勤務や仮設オフィスの設置など、代替的な職場の利用が、適時かつ効率的な方法で含まれる場合がある。

G. 組織体の回復力に関連する新たな脅威や脆弱性を継続的にモニタリングし、報告するとともに、組織体の回復力の業務を改善する機会を識別し、優先順位付けし、導入するためのプロセスが確立されている。このプロセスには、内部通報システム（ホットライン）やリスク情報の収集システムが含まれる場合がある。

H. 組織体の回復力に関する教育訓練プロセスを確立し、危機、混乱、緊急事態発生時に従うべき方針と手続及び取るべき行動について、関係者が認識していることを確実に確保している。このプロセスには、混乱を招くシナリオをシミュレートする演習が含まれる。

I. 危機、混乱、緊急事態発生時に必要な人的、技術的及び財源が予算化され、利用可能となるよう、プロセスが確立されている。このプロセスには事前に承認された資金が含まれる場合がある。

J. 組織体の回復力を支えるために必要な財源が、定期的に分析され、取締役会に報告されている。分析には、流動性、保険適用範囲、及び緊急時の資金調達手配の取り決めが含まれている。

K. 危機、混乱、緊急事態が発生した後にそれらを振り返り、事後レビューの教訓学習プロセスを通じて分析し、教訓を将来の組織体の回復力計画に統合するためのプロセスが確立されている。

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 5 千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。

著作権

2025 年 9 月