サイバーセキュリティ

Topical Requirement

トピック別要求事項

The Institute of
Internal Auditors

サイバーセキュリティ：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」は必須事項として位置付けられており、「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。

「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。

この「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含まれていないが、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。

詳細については、『サイバーセキュリティ　トピック別要求事項ユーザーガイド』を参照のこと。

サイバーセキュリティ

米国国立標準技術研究所（NIST）は、サイバーセキュリティを単に「サイバー攻撃からサイバースペースの使用を保護又は防御する能力」と定義している。サイバーセキュリティは、包括的な情報セキュリティの一部であり、NIST は「機密性、完全性及び可用性を提供するために、不正アクセス、使用、開示、中断、改変あるいは改ざん、又は破壊から情報と情報システムを保護すること」と定義している。

サイバーセキュリティは、全体的な統制環境を強化し、組織体の情報資産を不正アクセス、混乱、改ざん又は破壊から保護することで、リスクを低減する。コンピュータ、ネットワーク、プログラム、データ、及び機密情報は、ほとんどの組織体にとって重要な構成要素であるため、サイバー攻撃は、多くの場合、重大な直接的・間接的影響をもたらす可能性がある。

サイバーセキュリティのガバナンス、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、サイバーセキュリティのガバナンス、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、組織体におけるサイバーセキュリティ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：サイバーセキュリティのガバナンスの評価

要求事項：

内部監査人は、組織体のサイバーセキュリティのガバナンスに関連して、以下を評価しなければならない。

A. 正式なサイバーセキュリティ戦略と目標が設定され、定期的に更新されている。サイバーセキュリティ戦略をサポートするための資源や予算の検討も含め、サイバーセキュリティ目標の達成に関する最新情報が定期的に伝達され、取締役会によってレビューされている。
B. サイバーセキュリティに関する方針と手続は、統制環境を強化するために策定され、定期的に更新されている。
C. サイバーセキュリティの目標をサポートする役割と責任が確立され、その役割を果たす個人の知識、スキル及び能力を定期的に評価するプロセスが存在する。
D. サイバーセキュリティ環境における既存の脆弱性や新たな脅威について議論し、対処するために、ステークホルダーが関与している。ステークホルダーには、最高経営者、業務部門、リスク管理部門、人事部門、法務部門、コンプライアンス部門、ベンダーなどが含まれる。

リスク・マネジメント：サイバーセキュリティのリスク・マネジメントの評価

要求事項：

内部監査人は、組織体のサイバーセキュリティのリスク・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. 組織体のリスク評価とリスク・マネジメントのプロセスには、サイバーセキュリティ上の脅威と、それが戦略目標の達成に及ぼす影響の識別、分析、低減及びモニタリングが含まれる。
B. サイバーセキュリティのリスク・マネジメントは組織体全体で実施する。情報技術、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、サプライチェー

ン、経理及び財務などの分野を含めてもよい。

C. サイバーセキュリティのリスク・マネジメントに関する遂行責任と説明責任の所在が明確に定められている。リスクを低減し、新たなサイバーセキュリティの脅威を識別するために必要な資源を含め、サイバーセキュリティのリスクがどのように管理されているかを定期的にモニタリングし、報告する個人又はチームが特定されている。

D. 組織体において策定されたリスク・マネジメント・ガイドライン又は適用される法規制の要求事項に従って、許容できないレベルに達したサイバーセキュリティのリスク（顕在化したリスク又は過去に識別されたリスク）を迅速に上申するプロセスを確立している。サイバーセキュリティのリスクの財務的及び非財務的な影響を考慮すべきである。

E. 経営管理者と従業員にサイバーセキュリティのリスクの認識を伝え、定期的に経営管理者が、問題、ギャップ、不備及びコントロールの機能不全を確認し、適時に報告し、是正するためのプロセスが確立されている。

F. 組織体は、サイバーセキュリティ・インシデントの検知、抑制、復旧、及び事後分析を含む、インシデント対応・復旧プロセスを導入している。インシデント対応・復旧プロセスは定期的にテストされている。

コントロール：サイバーセキュリティのコントロール・プロセスの評価

要求事項：

内部監査人は、組織体のサイバーセキュリティのコントロール・プロセスに関連して、以下を評価しなければならない。

A. 組織体のシステムとデータの機密性、完全性、可用性を保護するために、内部統制とベンダーに基づくコントロールの両方を確実に実施するためのプロセスが確立されていること。組織体のサイバーセキュリティのリスクへの対応目標の達成と問題の迅速な解決を促進する方法でコントロールが機能しているかどうかを判断するために、定期的に評価が実施されている。

B. サイバーセキュリティのリスクを低減するコントロールに関連する技術的能力を開発・維持するための教育訓練を含む、人材管理プロセスが確立されている。このプロセスは定期的に見直されている。

C. 新たなサイバーセキュリティの脅威と脆弱性を継続的にモニタリング・報告し、サイバーセキュリティのリスクを低減するコントロールを改善する機会を識別、優先順位付け、実施するプロセスが確立されている。

D. サイバーセキュリティは、ハードウェア、ソフトウェア、ベンダー・サービスを含むすべての IT 資産のライフサイクル管理（導入、使用、メンテナンス及び廃棄）に含まれている。

E. 構成、エンドユーザーデバイスの管理、暗号化、パッチ適用、ユーザーアクセス管理、可用性とパフォーマンスのモニタリングなど、サイバーセキュリティを強化するためのプロセスが確立されている。ソフトウェア開発（DevSecOps）にサイバーセキュリティへの考慮が含まれている。

F. ネットワーク・アクセス・コントロールとセグメンテーション、ファイアウォールの使用と設置、外部ネットワークとの接続制限、仮想プライベートネットワーク（VPN）／ゼロトラストネットワークアクセス（ZTNA）、モノのインターネット（IoT）ネットワーク制御、及び侵入検知／防止システム（IDS と IPS）など、ネットワーク関連のコントロールが確立されている。

G. 電子メール、インターネットブラウザ、ビデオ会議、メッセージング、ソーシャルメディア、クラウド、及びファイル共有プロトコルなどのサービスに対して、エンドポイント・コミュニケーションのセキュリティ・コントロールが確立されている。

2025 年 2 月

The Institute of Internal Auditors

Global Headquarters
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1^407-937-1101