内部監査人協会（ＩＩＡ）情報

グローバルな視点と洞察

2018年：ＣＡＥが直面するトップリスク

内部監査人協会（ＩＩＡ）
訳者：堺　　咲　子
内部監査財団（Internal Audit Foundation）　評議員
インフィニティコンサルティング　代表
ＣＩＡ，ＣＣＳＡ，ＣＦＳＡ，ＣＲＭＡ，ＣＰＡ（ＵＳＡ）

目　次

はじめに

2018年という新しい年には、新しい法律、規則、意見、アイデア、テクノロジー、およびリスクがあらわれる。今日の事業環境は過去のものとは大きく異なり、より複雑でより結びついている。組織は新たなリスクや未知のリスクに直面するが、新たな機会や手つかずの機会にも直面する。この１年の機会と潜在的な課題やリスクの数（予期されているものも、2018年に特有のものもある）を考えると、監査計画を、破壊的なものも含めた様々な事象の発生に従って変化するフレームワーク、と捉えるべきだろう。

内部監査は、組織全体の観点からリスク・マネジメント、コントロール、およびガバナンスの各プロセスの有効性を評価し改善するために、体系的で規律ある手法で組織の目標達成を支援する。監督機関と監査委員会は、手強い競争相手、進歩するテクノロジー、市場動向の変化、および規則の制定によってもたらされる脅威に対処するために、リスク・マネジメントの取り組みが適切であるというアシュアランスを求めており、また必要としている（Internal Audit Future Trends: Emerging Trends and High-impact Areas of Focus[1]参照）。

内部監査に対しては、全産業へより多くの付加価値と戦略的支援を提供するというニーズがあるため、監査人は自身の業務を重要なすべてのリスク、特に戦略リスクと業務リスクに整合させる必要がある。内部監査は、ダイナミックなリスク環境に対応し適応しなければならない。

リスクは変化するので、十分に練られた監査計画であっても柔軟性を持つべきであり、組織のあらゆる階層で浮上する新たなリスクに合わせて変更すべきである。本稿では、ＩＩＡの国別代表機関が明らかにした、内部監査部門長（ＣＡＥ）が直面する（内部監査または組織に対する）上位５つのリスクを説明する。これらは、人材管理、データアナリティクス、サイバー、規制、および破壊的変化への対応である。

人材管理

人材管理は、ＣＡＥと内部監査専門家にとって常に最大の関心事である。過去数年間ＣＡＥは、新たな役割を果たすスキルや、新規や既存のリスクの対処に必要なスキルを持つ採用候補者を見つけるのに苦労してきた。内部監査の進化するニーズを満たすスキルを備えた候補者は、明らかに限られている。加えて、職場環境をミレニアル世代労働者特有の特徴である、支援や感謝に対するより大きな期待や異なる期待、明確に思い描く職場環境、および柔軟な勤務スケジュールを好むこと、などに合わせるという課題もある（4 Strategies for Bridging the Internal Audit Talent Gap[2]参照）。

2015年に内部監査人協会（ＩＩＡ）が行った国際調査では、回答者の40％以上が**人材を惹きつけ維持すること**を重要または極めて重要であると回答し、また、回答者の半数以上が限られた熟練監査人の中に**知識ギャップ**があると考えていた。さらに、2017年にＩＩＡのオーディット・エグゼクティブ・センター©（ＡＥＣ©）が行った調査では、200名近くのＣＡＥの大多数（79％）が、内部監査専門職にとって最も重要または非常に重要なリスクとして人材管理を挙げた。ＫＰＭＧ社[3]

[1] 訳注：https://www2.deloitte.com/us/en/pages/risk/articles/internal-audit-future-trends.html
[2] 訳注：https://blog.shrm.org/blog/4-strategies-for-bridging-the-internal-audit-talent-gap
[3] 訳注：https://assets.kpmg.com/content/dam/kpmg/ch/pdf/brq-talent-en.pdf

によると、取締役会は人材（またはその欠如）を**全社的リスク**と考えている。組織がグローバル化するにつれて組織を支える従業員は変化し続けるので、人材管理は非常に重要である。グローバルな人材不足の潜在的な影響と意味合いには、将来のリーダーの優良な供給ルートがないためにリーダーシップスキルを維持できないことや、採用候補者に重要な役割を担う能力がないために事業戦略の成果が危うくなることなどがある。組織は、新しい世代を指導したり優秀な人材や特殊能力を持つ人材を維持したりする能力がないことが、知的資本と競争優位を失う原因になっていることに気づいている。さらに、そして絶えず、ベテランの引退がスキル不足を引き起こしている（Boardroom Questions: Talent Management...or Talent Risk?[4]参照）。

さらに追い打ちをかけるように、新たなリスク（例えばデータアナリティクス、第三者の管理、サイバーセキュリティ、持続可能性、政治などの不確実性）のために、組織は内部監査人へより多くを期待している。内部監査の焦点が伝統的な財務やコンプライアンスに基づいた業務や関心に限定される時代は終わった。

人事は内部監査の業務ではないが、内部監査は経営陣がこれらのリスクに**どれだけうまく**対応しているかを評価すべきである。今日の組織は、内部監査人が監査に対して統合的なリスク監視や価値創造も含めたより全面的なアプローチを採ることを求めており、また期待している。このため、内部監査の最高の人材、スキル、および知力を探す競争は激化している。

適切なスキルがなければ、内部監査はテクノロジー、地政学、経済、進化する企業報告、文化、および国内や国際的な規制などの、特定のリスクや従来とは異なるリスクを、見落としやすくなったり徹底的に監査しなくなったりする。ヒューマンリソースマネジメント協会[5]によると、従来の財務、業務、およびＩＴ全般のスキルセットを超えて進化する能力と、大局を見据える能力は、内部監査にとって非常に重要である。

組織のリスクプロファイルをより包括的に理解した上で、慎重に能力を伸ばして業務を引き受けることは、内部監査部門にとって組織に役立つためのより良い準備となる。その準備の一部は、特定分野の専門知識や業界固有の知識と合わせて、高度な批判的思考能力と鋭いビジネス感覚を持つ人々を呼び寄せることである。従来にはない新たなリスクは監査対象領域に影響するため、内部監査は自身のスキルの幅と深さを拡充しなければならない。

ＣＡＥにとって不可欠なのは、監査人が自身の経験やスキルを広げるように導き、また、監査計画を評価し実施する際にリスクの「新常態」を考慮することである。間違いなく従来の監査研修には関連性があり、これからも関連性があるだろうが、継続的な教育とエクスポージャー、適応能力、優れたソフトスキル、およびプロセスと業務の知識は、新たなビジネスの世界の舵取りに不可欠である。

すべての人材を管理する能力は内部監査の成功にとって必須であり、一時的な人員不足を埋めること以上に長期にわたるメリットをもたらすことができる。ＣＡＥと経営幹部は人材管理の取り組みを最適化するために、人材の再編成と強化を目的とした綿密で充実したアプローチを考案すべきである。効果的であり、さらに、新たなリスクに直面する中でも可能な限り最高の内部監査部門を構築し、展開し、維持するために、ＣＡＥは、既存の

[4] 訳注：同上。
[5] 訳注：https://blog.shrm.org/blog/4-strategies-for-bridging-the-internal-audit-talent-gap

スタッフに必要なもの、追加するスタッフに必要なもの、さらに重要なのは、スタッフが成長し成功するために彼らのリーダーから学ぶ必要のあるもの、を判断するための戦略を策定しなければならない。

堅実な人材管理戦略は、アプローチの組み合わせによって決まる。ＣＡＥは人材不足から逃れることは出来**ない**。データサイエンス、革新的思考、分析的思考、批判的思考、コミュニケーションなどの、明日のリスクに対処するために必要なスキルを備えた採用候補者が不足している。効果的な戦略には、必要なスキルと特徴を理解することや、優秀な人材を獲得し、育成し、維持するための継続的努力などがある。

目標

- ■内部監査の集団として求められる能力は、内部監査の範囲を左右するリスクによって決定される。
- ■ＣＡＥ、監査委員会、および経営幹部は、組織目標を支援するために必要なスキルと内部監査スタッフの総費用をしっかりと理解している。
- ■内部監査は、一貫性のある業績管理プロセスを実施している。
- ■内部監査のリーダーは、新しい世代の者や初めて内部監査の職に就く者を指導し惹きつける能力を持っている。
- ■すべての内部監査スタッフ用の正式なキャリアプランが整備されている。
- ■内部監査は、新入社員研修プログラムを策定しており、組織文化、リスク選好、および戦略的方向性について全員に継続的に教育している。

目標に向けた行動

- ■リスク評価と監査計画をレビューして、計画実施に必要なスキルを特定する。現在のスキルと必要なスキルのギャップ分析を行い、ギャップを埋める戦略を立てる。
- ■具体的な職務能力、組織の戦略計画に沿った実行可能な目標、およびデータアナリストのような専門職の給与体系を含めるように、人事考課を設計または再設計する。
- ■既存のスタッフを指導してスキルを向上させることにより、混乱を最小に抑えて、既存の企業知識を新たに必要なスキルと統合する。
- ■新しいスキルを市場で常に獲得する。財務や経理の学位だけでなく、様々な経歴を持つ採用候補者を探す。複雑で特殊なリスクの対処に必要なスキルを迅速に獲得するためのリソースとして、第三者のサービスプロバイダーを検討する。
- ■効果的な新人研修や知識移転プログラムを考案する。

「もしも内部監査が将来に備えようとするならば、上位５つのリスクの１つである人材管理において内部監査が取り組むべき課題は俊敏さである。新たなリスクを認識して対処し、リスクを継続的に評価し、それに応じて監査範囲を調整するためには、十分に俊敏でなければならない。また、能力のギャップを認識して迅速に埋めるためにも、十分に俊敏でなければならない。ダイナミックな人材管理戦略がある内部監査部門は、将来成功するだろう。」

ＩＩＡ国際本部　事務総長兼ＣＥＯ
リチャード・チャンバース

関連するガイダンス

ＩＩＡ基準1210：熟達した専門的能力

内部監査人は、自らの職責を果たすために必要な「知識、技能およびその他の能力」を備えていなければならない。内部監査部門は、部門の責任を果たすために必要な「知識、技能およびその他の能力」

を、部門総体として備えているか、または備えるようにしなければならない。

ＩＩＡ基準1230：継続的な専門的能力の開発

内部監査人は、継続的な専門的能力の開発を通じて、「知識、技能およびその他の能力」を高めなければならない。

データアナリティクス

データアナリティクスとは、データを収集して分析し、結果を利用してより良い意思決定を行うプロセスである（訳者私訳。2017年、内部監査財団出版、「*Internal Auditing*」第４版、11-12頁）。組織は業務から大量のデータを生成しているが、これが内部監査に２つの重要な課題を与えている。１つ目は、取締役会や経営陣がデータの収集、管理、保護、および活用の方法を理解するために、どのような支援をするかである。２つ目は、既存の監査プロセスに分析ツールを適用し、定型的な監査を自動化して新たなリスク領域に注力する際に、増え続けるデータを内部監査の観点からどのように活用するかである（Risk in Focus: Hot Topics for Internal Audit 2018[6]参照）。

基本的にデータアナリティクスは、データの量を分割し、小さな塊の形で再編し、データから意味と理解を取り出す機会を提供する。内部監査はその情報を使って、リスクの**総量**と潜在的な相関関係を分析し、洞察と展望を提供し、ステークホルダーが懸念し関心を持つ問題について報告することができる。データアナリティクスとそれに関連するリスクを管理するのは骨が折れる。そのデータから意味のある洞察を導き出して知識を行動に移すのは、口で言うほど簡単でないこともある。データアナリティクスを効果的なものにするには、適切な人材、フォーマット、プロセス、およびテクノロジーを整備する必要がある。

かつてないほど多くのデータを即座に意のままに使えることから、経営陣と取締役会は大量のデータが組織をデータ関連の財務・非財務リスクに曝すことを認識しなければならない。どのようなアナリティクスの取り組みにおいても対処しなければならないリスク領域には、次のようなものがある（Understanding and Managing the Risks of Analytics[7]参照）。

- **データと情報の品質リスク**ー意思決定者が必要とするデータは、複雑なデータについての理解を伝達し促進するようなデータである。すべてのデータと情報について明確な定義と品質基準がなければならない。
- **データと情報のコンプライアンスリスク**ー（通常は、州、連邦、または国際に関連する）権限ある機関や認定機関の要件を遵守しないと、罰金、追加作業、または個人的賠償責任などの好ましくない結果を招く恐れがある。
- **データと情報のガバナンスリスク**ーデータと情報は、プライバシー、セキュリティ、品質、および監査可能性を確保するために、適切なレベルでリスク・マネジメントの原則とプロセスを利用して慎重に管理しなければならない。
- **不適切または早計なアナリティクス利用のリスク**ーアナリティクスは、次のような場合には役に立たない。データを収集、処理、解釈する時間がない場合、その意思決定に関連する履歴や先例がない場合や過去のデ

[6] 訳注：https//www.iia.org.uk/media/1689344/risk-in-focus.pdf
[7] 訳注：https://er.educause.edu/articles/2012/7/understanding-and-managing-the-risks-of-analytics

ータが誤解を招くような場合、重要な変数を測定できないか不確実性が高い場合。

■**文化的抵抗の影響によるリスク**ーデータ指向ではない組織文化にアナリティクスの取り組みを強要することは、リーダーに大きなリスクをもたらす恐れがある。アナリティクスの取り組みには、組織の意思決定システムの評価と組織文化がどの程度データ指向かの評価を含めるべきである。

■**データに関する倫理的リスク**ーデータアナリティクスの取り組みは、組織のコアバリュー、意思決定、および行動に沿ったものとすべきである。倫理的なデータの収集と使用を確実にするためのコントロールを整備すべきである。

内部監査は、組織がビッグデータプロジェクトで直面する恐れのある危険性、特にスタッフのスキル不足という状況には常に注意しなければならない。データアナリティクスの需要はますます高まっているので、既にそうなっていないとしてもすぐに**あらゆる**組織にとって不可欠な要素になるだろう。組織が競争力を維持して後れを取らないようにするためには、ビッグデータプロジェクトに参加することが重要だが、その際に考慮すべきリスクには次のようなものがある。

■データセキュリティ。

■データプライバシー。

■費用。

■信頼できない、無効な、不十分な、または無関係なデータ。

■信頼できない、無効な、不十分な、または無関係なアナリティクス・プロセス。

テクノロジーは私たちが住む世界を電光のような速さで変えるので、適切に準備していなければ苛立つことになると言わざるを得ない。テクノロジーは大量のデータを生成するが、内部監査はそれを利用してリスクをより徹底的に評価し、監査業務を改善し、提供するアシュアランスのレベルを高めることが可能である。

最近実施された**ケーススタディ**[8]の結果によると、内部監査にとってのデータアナリティクスの主な利点には、効率の向上、効果の増大、アシュアランスの改善、戦略リスクの一層の重視、監査範囲の拡大、および長期にわたる時間と経費の大幅な削減などがある。ただし、これらのメリットを実感するためには、内部監査はデータアナリティクス・プログラムが内部監査の包括的目標と望ましい活動にどの程度効果があるかを評価しなければならない。

データアナリティクスは、データに深く埋もれた洞察を提示するとともに、より効率的かつ効果的なテストを可能にするので、内部監査にとって不可欠のツールセットである。だが多くの内部監査チームは、より高度なデータアナリティクスのテクノロジーを取り入れておらず、未だに表計算ベースのツールやアプリケーションに頼っている。そこで、監査委員会の支援が不可欠である。内部監査は、監査委員会がデータアナリティクスの重要性を理解しているかを確認すべきである（Data Analytics: Is it Time to Take the First Step?[9]参照）。

データアナリティクス・プログラムを構築または改善するには、ＣＡＥは望ましい成果についてステークホルダーと討議して、アナリティクスの目標を定め、必要な**能力**とテクノロジーを判断すべきである。

効率的なデータアナリティクス・プログラムの構築に対する主な障壁の１つであり、内部監査にとって常にリスクとなるのが、ビッグデータを処理するスタッフのスキル不足で

[8] 訳注：https//www.iia.org.uk/media/1689102/0906-iia-data-analytics-5-4-17-v4.pdf

[9] 訳注：同上。

ある。この専門分野が不足しているために、内部監査のアナリティクス・プログラムは最適でない場合があるが、問題なのは必ずしもプログラムそのものではなく、むしろその可能性が最大限に活用されていないことである。あらゆる新事業の取り組みと同様に、ビッグデータプロジェクトにはリスクの要素がある。ビッグデータを管理する人材が欠けていると、リスクの要素が一層増える。

目標

- 内部監査は、データアナリティクスとテクノロジー、および高度なテクノロジーが内部監査の有効性と効率性を向上させる方法について深く理解する。
- 内部監査は、データアナリティクスの利用拡大に伴う新たなリスクに対する経営陣の対応状況を評価する。
- 内部監査は、組織の全面的な利益のために、データアナリティクス・プログラムの高度な能力を活用する（例えば、リスクの高いスキームや行動の検証と監視、組織に固有のリスク評価プロセスの正確性評価など）。
- 内部監査は、異常値や不正リスクのパターンを早期に特定するテクノロジーを活用して、重要な発見を伝える。
- 内部監査は、テクノロジーを活用して、より少ない労働時間と人件費で組織全体のリスクカバレッジを向上させる。

「First Steps in Building a Data Analytics Program for Your Internal Audit Team[10]」を部分的に編集。

目標に向けた行動

- データアナリティクス・プログラムに対する基本的ニーズと具体的ニーズがどのようなものかを決定することにより、アナリティクスのどのような成果が内部監査の目標に最も役立つかを判断する。
- イノベーションと機会の観点から、アナリティクス・プログラムが組織と内部監査に提供できるメリットを理解する。プログラムを最適に導入してメリットを実現するために必要なスキルを特定する。
- データアナリティクスを重要な業務構成要素として捉える。さらに、組織のコンプライアンスとコントロールのフレームワーク全体を管理するために、可能な限り最も持続可能で質の高いアプローチとなるように監査業務をカスタマイズする。
- プログラムの中の個々のルール、データポイント、コード、前提条件について経営陣と検討して、詐欺や不正のパターンを正確に検出する。

関連するガイダンス

ＩＩＡ基準1220：専門職としての正当な注意

内部監査人は、平均的にしてかつ十分な慎重さと能力を備える内部監査人に期待される注意を払い技能を適用しなければならない。専門職としての正当な注意とは、全く過失のないことを意味するものではない。

1220.A2－専門職としての正当な注意を払うに当たって、内部監査人は、テクノロジー・ベースの監査技法とその他のデータ分析技法の使用を検討しなければならない。

サイバー

組織に対する執拗で猛烈な情報侵害であろうと、果てしなく続くなりすまし犯罪であろ

[10] 訳注：https://www.cebglobal.com/blogs/internal-audit-first-steps-in-building-a-data-analytics-program/?business_line=risk-audit

うと、高度で資金力のあるサイバー犯罪者は手強い敵である。相互接続性は複雑かつリスクベースの世界を生み出し、サイバー犯罪者にとってはまさにうってつけの時代である。彼らが利用するテクノロジーは拡張し進化し続けているので、彼らに追い付くのは厄介である。

サイバー攻撃に対する防御計画に着手してその計画の効果を確認することは、24時間体制の仕事である。なぜならば、問題は攻撃が**発生するかどうか**ではなく、**いつ発生するか**だからである。サイバーリスクに対する認識とサイバーリスクに対する**準備**の間には大きな違いがある。誰もがリスクを**認識**しており、毎日その事実に直面している。だが準備には、試行された攻撃を完全に**阻止**したり、あるいは攻撃に**耐えて**無傷かわずかな損害で回復したりする能力が含まれる。侵害という災害に対する防御を少しでも享受するには、サイバー攻撃に抵抗し、反応し、攻撃から回復できる、つまり**サイバーレジリエント**になる必要がある。

サイバー問題（例えば、ハッキング、侵入、フィッシング詐欺、経済スパイなど）の懸念が高まるにつれて、ステークホルダーは組織のサイバーセキュリティ・リスクマネジメントプログラムに一層の可視性を求め、取締役会は内部監査がサイバーリスクとサイバープログラムを独立的、客観的、包括的にレビューすることを望む。したがって、内部監査も起こり得るリスクに精通して、サイバーレジリエンスにおける重要な役割を果たさなければならない。

残念ながら、サイバーセキュリティ・リスクは外部からの脅威によって起こるとは限らず、潜在的脅威は従業員や業務提携先の行動から起こる場合もある。したがって、サイバーレジリエンスで重要なのは、組織文化を適切かつ効果的に管理して、その**リスク**を評価することである。リスク文化は、組織全体のすべての意思決定、行動、およびリスクテイクの基盤なので、取締役会は文化を考える時に**リスク文化**も含めている。内部監査は、データ収集と非公式のレビューを行うことによって、標準的な業務監査や財務監査の中でリスク文化を監査することが可能である。

内部監査は、組織文化が必要条件、プロセス、および能力というレベルに影響を及ぼす場合であっても、率先してすべての分野のサイバーセキュリティ・コントロールの有効性に関する経営陣の知識を深めることができる。文化は組織内の生産性、価値観、態度、慣行を推進し、また、様々な要因によって形成され維持されるので、内部監査は組織の他の分野を評価するのと同じ方法でリスク文化を評価することができる（Internal Audit Future Trends[11]を参照）。内部監査は、文化の評価方法を理解し、経営者にその重要性を伝えることによって、価値を最大化することができる。

文化を含むサイバー関連のリスクを克服するためには、経営陣が予防策を講じ、研修と啓発プログラムとともに予防策を実施した上で、それらが継続的に行動で示されるようにすることが重要である。したがって、従業員、納入業者、提携先、および請負業者などを訓練して、サイバーセキュリティの対策と手順に関して期待することを正確に理解させなければならない。

内部監査のリスク評価戦略は、サイバーセキュリティに特有の全リスクについて策定すべきであり、また、方針とインターナルコントロールの遵守を確認すべきである。内部監査は、サイバー問題が及ぶ可能性があるすべての分野で、組織とステークホルダーのニーズを満たす集中的な監査手法を考案する必要

[11] 訳注：https://www2.deloitte.com/us/en/pages/risk/articles/internal-audit-future-trends.html

がある。効果を得るためには最低でも、統制活動、統制環境、リスク評価、コミュニケーション、およびモニタリング、ならびにサイバーセキュリティ対策評価のフレームワークを導入することが求められる（Risk in Focus: Hot Topics for Internal Audit 2018[12]参照）。

第３のディフェンスラインである内部監査はサイバーセキュリティ戦略と方針を策定する際に経営陣や取締役会と協力して、組織がサイバーセキュリティのリスクを特定し低減する能力を向上させ、監査委員会や取締役会との関係を活用して彼らが関与し続けていることを確認し、さらに、サイバーセキュリティ・リスクが監査計画に**正式に**統合されていて、計画実施に必要なスキルが（社内またはコソーシングで）備わっているかを確認すべきである。新たなテクノロジーや傾向は、組織のサイバーセキュリティ・リスクプロファイルに影響するので、内部監査も新たなテクノロジーの状況を常に把握して、組織の脆弱性レベルや望ましいサイバーセキュリティ計画に対するリスク活動を評価すべきである。

「サイバーリスクの監視役割を効果的に果たすために、取締役が技術者である必要はない。しかし、各取締役はサイバー監視の実効性を向上させる機会を活かすことができる。」

全米取締役協会（ＮＡＣＤ）
ＮＡＣＤハンドブック「サイバーリスクの監視」2017年

出典：The Value of Visibility: Cybersecurity risk management examination[13]

目標

■組織には、サイバーに対してレジリエントな文化がある。

■内部監査は、サイバーセキュリティの調査と準備に欠かせない重要な要素[14]に貢献する。

○防御と検出：内部監査は、組織の脆弱性を特定するための包括的アプローチを提供し、データアナリティクスを内部監査の責任領域に組み込むことにより、異常が起きていることを警告する。

○事業継続：現在行っている業務に影響を与え得るリスクシナリオ（サイバー攻撃、自然災害、事業継承を含む）に対処して克服するための計画を経営陣が立てる際に、内部監査は経営陣に助言して協働する。

○危機管理とコミュニケーション：内部監査は、有効性と適時性に関するアシュアランスチェックを提供し、実施された計画の分析と批評をすることにより、危機管理計画とコミュニケーションの準備を支援する。

○継続的改善：内部監査は、洞察を提供し、サイバー攻撃に対するより良い準備のために戦略と手順を改善することにより、価値を付加する。

目標に向けた行動

■サイバーレジリエンスに関する組織文化を評価する。

■セキュリティモデルとサイバーセキュリティ・プロセスのリスク評価を実施して、改善を勧告する。

■ＩＴ部門や請負業者とデータの侵入テストを実施して、確立されたプロトコルに準拠する能力が請負業者にあるかを評価する。

■サイバーレジリエンスのギャップ分析を実

[12] 訳注：https//www.iia.org.uk/media/1689344/risk-in-focus.pdf
[13] 訳注：https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cybersecurity-risk-management-examination.pdf
[14] 訳注：http://info.knowledgeleader.com/what-is-internal-audits-role-in-cyber-security

施し、改善を勧告し、是正措置についてフォローアップする。
- ■サイバーセキュリティの監視と対応を最重要課題として強調して、文化に影響を与える。
- ■事業継続計画が定期的にテストされ、是正措置が取られていることを確認する。
- ■強力なサイバー文化とリスク文化を組織全体に導入して奨励し、長期にわたってサイバーセキュリティの対策と手順に影響を与える。

規制

世界中の組織は、消費者や公益をある程度守るために設計された新しい規制要件や変更された規制要件に直面している。最も注目される規制は、財務上のリスクとコントロールおよびデータのプライバシーとセキュリティに重点を置いており、あらゆる業種の組織に影響を与えている。

関連するガイダンス

ＩＩＡ基準2130：コントロール

内部監査部門は、コントロール手段の有効性と効率性を評価し、継続的な改善を進めることにより、組織体が有効なコントロール手段を維持することに役立たなければならない。

2130.A1－内部監査部門は、以下の各事項に関わる組織体のガバナンス、業務および情報システムにおけるリスクに対応したコントロール手段の妥当性と有効性について評価しなければならない。

- ●組織体の戦略目標の達成状況
- ●財務および業務に関する情報の、信頼性とインテグリティ
- ●業務とプログラムの有効性と効率性
- ●資産の保全
- ●法令、方針、定められた手続および契約の遵守

仮想通貨

ＣＮＢＣ社[15]によると、最近のデジタルコインの急激な売却に伴い、仮想通貨の価値は１兆ドルを超える可能性がある。ビットコイン[16]の価値は不安定で、2018年初頭には６千ドルから１万ドルの間で変動した。仮想通貨交換業者ゲートコイン社のアジア太平洋地域事業開発責任者トーマス・グリュックスマン氏は、「仮想通貨交換業者に対する監督機関の認識の高まり、機関投資家の参入、およびテクノロジーの大きな進歩は市場の回復に寄与して、今年は仮想通貨価格を全面的な高値に押し上げるだろう。（2018年）12月までにビットコインが５万ドルまで上がらないはずはない」と述べた。

世界中の大手金融機関がブロックチェーン技術や仮想通貨取引に関与しているので、金融機関は従業員が個人口座でデジタルコインを取引する際に起こり得る利益相反への対処方法を見つけ出す必要がある。デジタルコインの価格高騰は、投資家や銀行の関心を煽るだけでなく、コンプライアンス部門もかなり注意を払っている。仮想通貨に関与する（または投資したいと思う）従業員が不当な優位性のある立場で取引すると、利益相反が起こり得る。一般的には、従業員は利益相反の可能性のある証券取引をする前に許可を得なければならない。しかし、仮想通貨取引は断片化された交換業者のネットワークを介して（時には匿名で）行われ追跡が複雑なので、

[15] 訳注：https://www.cnbc.com/2018/02/07/bitcoin-price-could-hit-50000-this-year-experts-say.html
[16] 訳注：https://www.cnbc.com/quotes/?symbol=BTC%3D

このような方針を課すのはかなり難しい。

さらに、国際的な監督機関から明確なルールが示されていないため、金融機関が独自にルールを設定することが難しい。また、仮想通貨を商品とみなす企業もあれば、有価証券かもしれないという企業もあるが、どちらかは規定していない。最近のビットコインや他のデジタル通貨の衝撃的な不安定さにより、国際的な監督機関は不安を募らせており、厳しい規制が導入される可能性がある。

グローバルなデータ保護規則

多くの政府がデータのプライバシー保護に関する規則を強化している。２つの例は、欧州連合（ＥＵ）と中国である。

４年間の準備と議論を経て、ＥＵデータ保護指令95/46/ECに代わるものとしてＥＵ一般データ保護規則（ＧＤＰＲ）が2016年４月にＥＵ議会で採択された。ＧＤＰＲは、年を追うごとにデータ侵害がより大きく、より煩わしく、費用がかかるようになっている2018年５月に発効する。データ侵害は、2015年から2016年にかけて40％増加したと報告されているが、2017年の侵害はこれを大幅に上回った（詳細は、次ページ「2017年のデータ侵害」を参照）。

多くの企業には古いデータ保護指令に沿ったプライバシー方針があるが、新しいＧＤＰＲには、ＥＵデータに対する新たな保護規則が多数含まれており、ＧＤＰＲ発効後にコンプライアンス違反があったデータ管理者と処理者には、制裁金や罰則が科されることになっている。簡単に言うと、欧州で事業を行う、またはＥＵ住民の個人データを扱う（現地の、または国際的な）あらゆる組織は、新規則を遵守しなければならない。

監督機関は、主な条項への最も重いコンプライアンス違反に対して、最高で当該企業の前事業年度の全世界年間売上高の４％または2,000万ユーロのいずれか高い方を制裁金として課す権限を持っている。制裁金については段階的なアプローチがある（例えば次のような場合には、最高で当該企業の前事業年度の全世界年間売上高の２％または1,000万ユーロのいずれか高い方の制裁金が課せられる。適切に記録を保持しなかった場合［第28条］、侵害について監督機関とデータ主体に通知しなかった場合、データ保護影響評価を実施しなかった場合）。これらの規則は管理者と処理者の両方に適用されることに注意することが重要であり、クラウドサーバはＧＤＰＲの適用を免れないだろう。最高の制裁金の対象となる例には、個人データの処理に関する基本原則を遵守しなかった場合、データ主体の権利を侵害した場合、適切なレベルのデータ保護を保証しない第三国または国際機関に個人データを転送した場合、などがある（ＥＵ ＧＤＰＲ[17]参照）。

「ＧＤＰＲとその影響が注目されている。監査委員会はアシュアランスの観点から、当初は内部監査にプログラム自体を評価することを求めるが、その後は継続的なコンプライアンスのために、適切なプロセスが適切に実施されていることを確認するための継続的な独自プログラムを策定することを求めるだろう。」

多国籍銀行グループ　ＣＡＥ

出典：Risk in Focus: Hot Topics For Internal Audit 2018[18]

[17] 訳注：https://www.eugdpr.org/

[18] 訳注：https://www.iia.nl/SiteFiles/Hot%20Topics%202018%2011_9_2017_digital%20version.pdf

2017年のデータ侵害		
月	組織	違反または侵害
１月８日	E-Sports Entertainment Association (ESEA)	1,503,707件のレコードがデータベースに追加され、個人情報等が漏洩。
２月２日	Xbox 360 ISO and PSP ISO	120万のXbox 360 ISOと130万のPSP ISOのアカウントが影響を受け、個人情報が盗難。
３月15日	Dun & Bradstreet	ウェブ上で共有される米国国防総省や米国郵便公社を含む企業の3,300万人を超える連絡先と個人情報が漏洩。
４月６日	FAFSA: IRS Data Retrieval Tool	最大10万人の納税者や学生の個人情報が盗難の可能性。
５月10日	Bronx Lebanon Hospital Center	2014年から2017年の間に少なくとも7,000人の患者の、中毒、精神・健康診断、ＨＩＶの状態、および暴行報告を含む極めて個人的な情報が漏洩した可能性。
６月20日	Deep Root Analytics	共和党全国委員会が雇った同社がパスワード保護のないクラウドサーバ上に個人情報を保管して２週間以上公開し、約１億9,800万人の米国市民に影響。
７月13日	Verizon	顧客が同社に電話連絡した時に生成されるログファイルがセキュリティ対策されていないサーバで保持されていたため、1,400万人の加入者情報が露出。
８月30日	Online Spambot	セキュリティ対策されていないサーバから７億1,100万件の電子メールアドレスとパスワードが盗難。
９月７日	Equifax	ウェブサイトソフトウェアの弱点を突いたハッキングで１億4,300万人の顧客が影響を受けた可能性。社会保障番号やクレジットカード番号などの個人情報が露出。
10月12日	Hyatt Hotels	11か国41施設で使用（スワイプ）されたデビットカードとクレジットカードの支払い情報（クレジットカード番号、内部認証コード、カード所有者の氏名等を含む）への不正アクセス。
11月21日	Uber	氏名、電子メールアドレス、電話番号など、5,700万人の運転者と顧客の個人情報が露出。
12月10日	TIO Networks (PayPal)	銀行口座情報、支払いカード情報、パスワード、ユーザ名、社会保障番号など、160万件超の顧客ＩＤが漏洩。

「2017 Data Breaches – The Worst So Far[19]」から編集。

関連するガイダンス

ＩＩＡ基準2130：リスク・マネジメント

内部監査部門は、リスク・マネジメント・プロセスの有効性を評価し、リスク・マネジメント・プロセスの改善に貢献しなければならない。

2120.A1－内部監査部門は、以下の各事項に関わる組織体のガバナンス、業務および情報システムに関するリスク・エクスポージャー（リスクに曝されている度合い）を評価しなければならない。

- 組織体の戦略目標の達成状況
- 財務および業務に関する情報の、

[19] 訳注：https://www.identityforce.com/blog/2017-data-breaches

信頼性とインテグリティ
- 業務とプログラムの有効性と効率性
- 資産の保全
- 法令、方針、定められた手続および契約の遵守

「同意」の定義と要件でさえかなり限定されている。以前は、データ管理者が状況によっては暗黙の了解や「オプトアウト[20]」という同意を利用することが許されていた。だが2018年５月25日以降はＧＤＰＲが同意の要件を強化したので、企業は同意の対象となるデータ処理の目的が記載された、容易にアクセスできる形式の同意書を提出しなければならないため、法律用語だらけの長くて判読不能な約款をもはや使用することができなくなる。同意は、他の案件と明らかに区別でき、明確で平易な文言で示さなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。さらに、一旦同意が撤回されると、データ主体は、個人データを削除させ処理できなくさせる権利を有する（The Top 10 Operational Impacts of the EU's General Data Protection Regulation[21]参照）。

ＧＤＰＲは、ドイツのサイバーセキュリティの取り組みに大きな影響を与えるだろう。2017年５月、ドイツ議会は連邦データ保護法の改訂版を採択し、2018年５月25日にＥＵ ＧＤＰＲとともに発効する。最高30万ユーロの罰金を課す強力な国家データ保護法で知られるドイツは、厳しいサイバーセキュリティ基準に移行しており、重要インフラのサービスプロバイダーや事業者に対して、ユーザを保護しサイバー情報を守る責任を課している。新法には85の条項があり、そのうちいくつかはＥＵ ＧＤＰＲと相互参照している。重要インフラ事業者は、これらの保護措置を規定する法律が発効してから２年以内に、**最高水準の技術**で適切な組織的および技術的保護措置を実施しなければならない。加えて、重要インフラ事業者は、セキュリティ要件を満たしていることを定期的に証明し、運営する重要インフラの機能障害または障害をもたらす可能性があるＩＴシステム、コンポーネント、およびプロセスの可用性、完全性、真正性、機密性に対する重大な障害がある場合は、直ちに**連邦情報セキュリティ局**（ＢＳＩ）に通知しなければならない（What You Need to Know About Germany's Cybersecurity Law[22]参照）。

中国には既に情報セキュリティに関する厳格な法令や規則があるが、サイバーセキュリティとデータ保護のギャップを埋める広範な法律が導入され（2017年６月施行）、これにはＥＵ ＧＤＰＲの条項を取り入れている。中国サイバーセキュリティ法（ＣＳＬ）は、多くの点でＧＤＰＲと一致している（Risk in Focus: Hot Topics For Internal Audit 2018[23]参照）。ＣＳＬは改正されて、個人情報と個人のプライバシー保護をより重視しており、個人情報の収集と使用を標準化している。例えば、以前は外国企業が中国国外に情報を移転できたが、現在は同法により、機密データは国内に保管しなければならず、同法に違反すると事業活動の停止などの厳しい罰則が課せられる。罰金は100万人民元に達する可能性がある（詳細は、次ページの「ＣＳＬの改正」参照）。

[20] 訳注：企業などが個人情報を収集・利用することができるということを事前に決め、本人に知らせておいた上で、後に本人に利用を制限できる機会を与えることを意味する。
[21] 訳注：https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/
[22] 訳注：https://natlawreview.com/article/what-you-need-to-know-about-germany-s-cybersecurity-law
[23] 訳注：https://www.iia.nl/SiteFiles/Hot%20Topics%202018%2011_9_2017_digital%20version.pdf

ＣＳＬの改正		
条項	**最終版**	**重要な改正点**
31	サイバーセキュリティ保護に関しては、**公共通信・情報サービス、エネルギー、金融、交通、水道、公共サービス、電子政府**の重要情報インフラの保護、ならびに、破壊、機能喪失、またはデータ漏洩の場合に国家安全保障、国家経済、および公益に深刻な打撃を与える恐れのある他の重要情報インフラの保護を国家は重視する。	この条文は、重要情報インフラの保護が優先される業界とセクターを明確にしている。
43	個人は、ネットワーク運営者に対し、収集または保管された個人情報の誤りの訂正を求める権利を有する。**ネットワーク運営者は、誤りを削除または訂正する措置を講じなければならない。**	この条文は、市民に対して個人情報を保護するためのより大きな権利を与え、ネットワーク運営者に対して誤りを適時に訂正する義務を課している。
46	個人または組織は、**ネットワークの使用に責任があり、**詐欺的な目的やその他の違法行為のためにウェブサイトやコミュニケーショングループを開設してはならない。	この条文は、個人や組織がネットワークの使用に対して責任を負うことを強調している。
76（5）	「個人情報」とは、電子的またはその他の方法で記録された、自然人の身元を単独で、または**自然人の名前**、生年月日、識別番号、個人の生体情報、住所、および電話番号のような情報との組合わせで特定できるあらゆる種類の情報を指す。	この条項は、個人情報保護の範囲を「市民」から「自然人」に拡大している。
63	第27条に違反し、サイバーセキュリティを危うくする活動に関与した者は、事件の重大性に応じて５日から15日間の拘禁、また、**10万から100万人民元**の罰金が科されることがある。	サイバーセキュリティ法違反に対する最高の罰金は100万人民元に増加した。

出典：Overview of China's Cybersecurity Law[24]

しかし、ＣＳＬに対する反対がないわけではない。2017年５月にニューヨーク・タイムズ紙が報じたように、「欧州、アメリカ、およびアジアの財界は連携して、法律の施行を延期するよう中国に要請し、中国の欧州連合（ＥＵ）商工会議所は、企業が「かなりの遵守義務」を守る準備をするための時間を求めた」。

ＥＵ、中国、あるいはデータのプライバシーに関する規則が増えている他の多くの国々で事業を行っている組織でさえも、規則の影響を感じている。取締役会は、組織内のガバナンス・フレームワークの強化を強く求めており、また取締役会は、監督当局、投資家、およびプロセス全体の有効性について取締役会に責任を負わせる他のステークホルダーから圧力をかけられている（Of Corporate Governance, Risk Management, and Internal Audit[25] 参照）。新しい規則は、リスク・マネジメント、コントロールおよびガバナンスの各プロセスを複雑にすることで、コストを増大させ組織に圧力をかけている。

取締役会に対する圧力が高まるにつれて、内部監査にも圧力がかかる。組織は、大きな期待を込めて内部監査を頼りにしている。組織は、変化し続ける規制に対応すると同時に破壊的な力を機会に変える際に、内部監査の

[24] 訳注：https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

[25] 訳注：https://www2.deloitte.com/mt/en/pages/risk/articles/mt-risk-article-of-corporate-governance-risk-management-and-internal-audit.html

助言とアシュアランスの必要性を認めている（KPMG Internal Audit: Top 10 Key Risks in 2016[26]参照）。

破壊的な力に対して生き残るための鍵は、ガバナンス、リスク・マネジメント、コンプライアンス、および業績のバランスの達成である。これらの課題を乗り切ると、事業価値を保全し強化し、業務効率を向上することができる。

目標

- ■プロジェクトや戦略を評価する際のリスク選好を明確化する。
- ■現在の国内および国際規則に関する組織全体の認識を向上する。
- ■現在の国内および国際規則へのコンプライアンス対策を確立する。
- ■内部および外部のアシュアランス提供者と連携する。

目標に向けた行動

- ■国際的なコンプライアンスのフレームワークとアシュアランスの基準を理解する。
- ■既存の監督機関とその要件に関する一覧表を作成する。
- ■新しく買収した組織の統合を含め、グローバルなコンプライアンス活動の管理に対する組織の取り組み方を評価する。
- ■顕著なコンプライアンス違反事例に対する組織の対応を評価する。
- ■コンプライアンス研修プログラムをレビューして、各自の役割の妥当性を評価する。
- ■適切な対象範囲を確保しつつ重複を最小限に抑えるために、内部および外部のアシュアランス提供者と連携する。
- ■コンプライアンスの文化を奨励するために、組織の利益と優先事項に合わせたコミュニケーションを作り出す。
- ■法令・規則のコンプライアンスに関する組織の責任の割り当てを評価する。

関連するガイダンス

ＩＩＡ基準2210：内部監査（アシュアランスおよびコンサルティング）の個々の業務における目標

内部監査（アシュアランスおよびコンサルティング）の個々の業務ごとに、目標が設定されなければならない。

2210.A3ーガバナンス、リスク・マネジメントおよびコントロール手段を評価するためには、妥当な規準が必要となる。内部監査人は、経営管理者および取締役会、またはそのいずれかが、目標やゴールが達成されたかどうかを見極めるための規準としてどの程度まで妥当なものを設定しているかを確認しなければならない。妥当であるときには、内部監査人は、評価に当たり当該規準を使用しなければならない。妥当でないときには、内部監査人は、経営管理者および取締役会、またはそのいずれかと協議して適切な評価規準を識別しなければならない。

ＩＩＡ基準2050：連携と依拠

内部監査部門長は、適切な内部監査の業務範囲を確保し、業務の重複を最小限にするために、内部監査部門以外のアシュアランス業務やコンサルティング業務を提供する組織体内部および外部の者と、情報を共有し、活動について連携し、これらの者の仕事に依拠することを検討すべきである。

[26] 訳注：https://home.kpmg.com/content/dam/kpmg/id/pdf/2016/10/id-kpmg-internal-audit-top10-risks-2016.pdf

破壊的変化への対応

新しい一日には、新しい何かが起こる。今日のテクノロジーは絶えず変化しており、それはより速く、より強く、より大きく（そしてより小さく）なり、より遠くに届き、また、より集中する。それは、かつてないほどである。内部監査人は毎日、洞察と展望をステークホルダーに提供する新たな機会に直面しているが、批判的思考や創造性のようなイノベーションに関連するスキルを磨いていない可能性がある。そしてイノベーションがなければ、予期せぬことに対処できず、自己満足に陥りやすくなる。内部監査人が俊敏かつ積極的になり、また、イノベーションに歩調を合わせて素早く方向転換するためには、テクノロジーを活用するように業務のやり方を変えなければならない。

新たなテクノロジーのようなイノベーションは、内部監査が監査業務を行う素晴らしい機会をもたらすが、多くの場合、内部監査の懸念を増大させる新たなリスク、脅威、および**破壊的変化**が伴う。例えば、（伝統的に）リスクにのみ焦点を当てる代わりに、今や内部監査人は、破壊的変化の予兆を素早く**見極めて**早急な対応や追加の対応が必要なものを判断できるようになる必要がある。

組織がイノベーションすべき主な理由の１つは競争から一線を画すことであり、内部監査はその先頭に立つことができる。2018年の北米内部監査の動向調査によれば、イノベーションは内部監査に２つの選択肢を提示する。それは、組織内でますます重要な役割を果たす能力を思い描くか、過去の慣例を前提にしてそれを将来に持ち込むか、のどちらかである。後者を選べば将来の失敗はほぼ確実なので、内部監査は創造的な（あるいは、もっと言えば過激な）考え方を進んで取り入れて、関連するリスクの効果的な管理に焦点を当てることに備え、また、意欲を持たなければならない。

それには課題がある。経営者は違ったやり方に違和感を持つ可能性があり、事業環境のせいで予算が制約される可能性があり、また、必要なスキルを持つ採用候補者が少ない可能性がある。しかし、うれしいことに内部監査は孤独ではない。内部監査は、イノベーションのプロセスを管理するための具体的な手法を既に編み出した他の事業部門、組織、または内部監査部門から学ぶことができる。

イノベーションを正しい方法で活用すると、次のような理由から、内部監査や組織全体にとって極めて有益である。

- ■費用が削減される。
- ■価値が増大する。
- ■成長と業績の向上が実現する。
- ■製品がより早く開発され、サービスがより早く開始される。
- ■顧客経験と顧客満足が向上する。
- ■組織の柔軟性と俊敏さが高まる。
- ■ステークホルダーの満足度が高まる。

イノベーションは、より良くより効率的な監査につながるだけでなく俊敏さを直接後押しして、破壊的変化の際により迅速で、より賢明で、より集中的な対応を可能にする（2018年北米内部監査の動向調査：The Internal Audit Transformation Imperative[27]参照）。ＩＩＡ北米理事会会長シャノン・アーバン氏は、内部監査の成長に不可欠である、また、変化し続けるステークホルダーのニーズを満たす上で必要である、という両方の理由から、内部監査におけるイノベーションを奨励している。それは多少の違和感と苛立ちを伴うかもしれないが、継続的なものであり、コミットメントと勇気が求められる。イノベーションには大きなやりがいもある。内部監

[27] 訳注：https://www.theiia.org/centers/aec/Pages/2018-Pulse-of-Internal-Audit.aspx

査がステークホルダーを理解し、将来的に彼らに十分役立ちたいと思うならば、イノベーションに取り組むことが唯一の選択肢である（The Innovative Internal Auditor[28]参照）。

「内部監査が組織の成功に不可欠な役割を果たしていると、私は固く信じている。しかし、役割を果たすには、内部監査におけるイノベーションへのコミットメントを新たにする必要があるとも信じている。組織の発展に追いつきその先を行くためには、イノベーションは内部監査の職務の核でなければならない。」

2017－2018年　ＩＩＡ北米理事会会長
シャノン・アーバン

目標

- ■内部監査は、事業環境の変化を認識する。
- ■内部監査は、イノベーションの文化を育み、能力と業績の強化を目指す。
- ■内部監査は、イノベーションによって、ベストプラクティスと改善を目指す。
- ■内部監査は、イノベーションによって、より高い効率性を求めて努力する。

目標に向けた行動

- ■新しいアイデアを考案して導入し、イノベーションを内部監査実務の中核的基盤にする。
- ■リーダーシップの役割を引き受け、事業の破壊的変化を予測し、環境の変化を監視し、幅広い対応策を提供する。
- ■人間関係を構築して投資する。事業部門とのつながりを保ち、起こっているイノベーションを把握する。
- ■一層の注意が必要な破壊的変化がどれであるかを判断することにより、進化するリスクの状況を明らかにする。
- ■破壊的な出来事に関連するエマージングリスクについての洞察と視点を提供する。
- ■新たなリスクやエマージングリスクに迅速かつ断固として対応するために、適切な能力のある採用候補者を見つけて惹きつける。
- ■リスク・マネジメントおよびコンプライアンス部門と協力する。

最後に

本稿で取り上げたリスクは、最も懸念するリスクとしてＩＩＡの国別代表機関が明らかにしたものだが、組織や内部監査に対するすべてのリスクを表すものではない。これらの分野に加えて、ＩＩＡの国別代表機関は、監査委員会、予算、ディフェンスライン、および戦略に内在するリスクも明らかにしたが、これらはすべて、認識され検討される必要がある組織的ガバナンスの重要な分野である。リスクは、組織のミッションと戦略目標の達成を阻害し、組織の全体的な価値を脅かすことにつながる。したがって、リスク・マネジメント、コントロール、およびガバナンスの各プロセスを支援する信頼されるアドバイザーとしての内部監査の責任は、すべてのリスクの機会を考慮し、適切な勧告を行うことを求めている。

世界中の組織は、内部監査とその評価を頼りにしている。内部監査は、関連性を維持し信頼されるアドバイザーとして認識されるために、組織の目標だけでなく自らの目標達成のためにリスクを検討する義務がある。このため内部監査は、成果を重視し、組織全体の利益のために能力の向上に努めなければならない。そのためには、批判的に考える、独立性と客観性を保つ、俊敏さを維持する、（現実または仮想の）リスクに対する**リーダーシッ**

[28] 訳注：https://iaonline.theiia.org/2017/Pages/The-Innovative-Internal-Auditor.aspx

プを重視する、必要に応じてコンサルタントとして機能することによって「時代」を乗り切る、必要に応じてアシュアランスを提供する、すべてのシステム、プロセス、規制、および業務の相関関係を理解するなどを含めた、課題や障害を乗り越える能力が必要である。

ＩＩＡの国別代表機関

ＩＩＡの国別代表機関は、ＩＩＡに欠かせない要素である。ＩＩＡは170を超える国や地域のＩＩＡ代表機関と協力して、内部監査専門職の進歩と全世界で19万人を超える会員へのサービス提供のために使命を果たしている。ＩＩＡ国別代表機関は、ＩＩＡの専属代表機関として、各地の内部監査コミュニティで倫理と専門職的実施の高い基準を推進し、内部監査専門職の意見をまとめて伝えている。

既刊号

既刊の『グローバルな視点と洞察』は、 www.theiia.org/gpi をご覧ください。

読者のご意見等

ご質問やご意見は、globalperspectives@theiia.org.にお寄せください。

ＩＩＡについて

内部監査人協会（ＩＩＡ）は、内部監査専門職の提唱者として、教育者として、さらに基準、ガイダンス、公認資格の提供者として、最も広く認められている。1941年に創立されたＩＩＡには、現在170を超える国と地域に19万人を超える会員がいる。ＩＩＡ国際本部の所在地はアメリカ合衆国フロリダ州のレークマリーである。詳細な情報は、www.globaliia.org を参照のこと。

免責

「グローバルな視点と洞察」で表明した意見は、必ずしも個々の寄稿者または寄稿者の雇用主のものではない。

著作権