International Professional Practices Framework

Supplemental Guidance

Practice Guide

FINANCIAL SERVICES

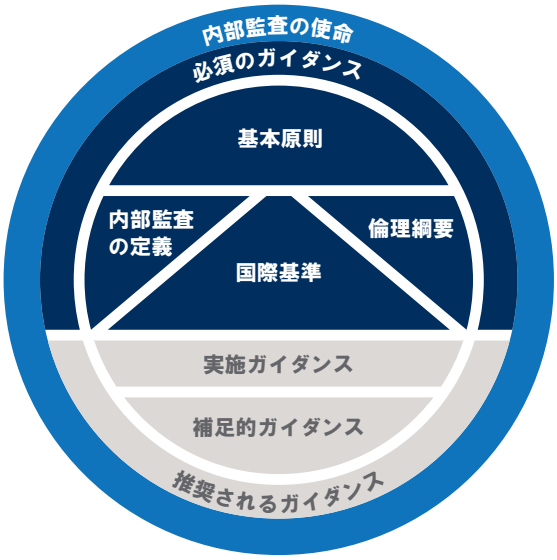
コンダクト・リスクの監査

The Institute of Internal Auditors | Global

ＩＰＰＦについて

「専門職的実施の国際フレームワーク（ＩＰＰＦ）」は、内部監査人協会 (The Institute of Internal Auditors（ＩＩＡ）) が公表している正式なガイダンスを体系化した「考え方（概念）のフレームワーク」です。ＩＩＡは、信頼できる、国際的な、ガイダンスの設定機関であり、世界中の内部監査の専門職に対し、正式なガイダンスを提供しています。

IPPF International Professional Practices Framework



「必須のガイダンス」の諸原則類に適合することは、内部監査の専門職的実施に必要不可欠です。「必須のガイダンス」は、関係者の皆さまからのご意見を反映すべく公開草案の手続を経て設定されたものです。「必須のガイダンス」の構成要素は、次の４つです。

- 「内部監査の専門職的実施の基本原則」
- 「内部監査の定義」
- 「倫理綱要」
- 「内部監査の専門職的実施の国際基準（「基準」）」

「推奨されるガイダンス」は、IIA の正式な承認プロセスを通じて設定されており、「内部監査の専門職的実施の基本原則」「内部監査の定義」「倫理綱要」「内部監査の専門職的実施の国際基準」を効果的に実施するための実務内容を示しています。

補足的ガイダンスについて

「補足的ガイダンス」は、ＩＩＡの「専門職的実施の国際フレームワーク（ＩＰＰＦ）」の構成要素であり、必須ではないが、内部監査実務を行うための追加的な推奨されるガイダンスを提供する。「補足的ガイダンス」は、「基準」を支援するが、「基準」に適合する目的に対して直接的な関連は意図されていない。代わりに、ある特定の領域やある部門特有の課題へ対応することを意図されており、詳細なプロセスと手順を含む。ガイダンスはＩＩＡの正式なレビューおよび承認プロセスを通じて設定されている。

プラクティス・ガイド

プラクティス・ガイドは、内部監査実務を行うための詳細なガイダンスを提供する。それらにはツールと手法、プログラム、段階的アプローチ、成果物等の例などを含んでいる。プラクティスガイドは内部監査人を支援することを意図しており、また以下の分野を支援することにも有効である。

- 「プラクティス・ガイド（金融サービス）」
- 「プラクティス・ガイド（パブリック・セクター）」
- 「IT 監査の国際的ガイド（ＧＴＡＧ）」

ＩＩＡが提供するその他のガイダンスについては、ＩＩＡのホームページ（https://global.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx）を参照。

目　次

エグゼクティブ・サマリー

組織体のカルチャー、そしてコンダクトに対してどのように組織体自身を適合させるかは、ビジネスがどのように行われるのかを左右する。また、これは組織体の目標達成を支援する統制環境の有効性の基礎となる。

貧弱なカルチャーおよび有効でない従業員のコンダクト管理は、多くの経営破綻に影響し、多くの深刻な課題の根本原因として識別されてきた。これに対応し、統制環境の監督に責任のある取締役会（訳者注：原典では「board」を使用しているが、金融サービスにおいては、board を取締役会と呼ばないこともある。しかし、本翻訳においては、取締役会で統一した。）および規制当局を含む主要な金融サービスの利害関係者は、組織体のカルチャーの適切性およびコンダクト・リスク・マネジメントの有効性に高い優先度をもって焦点を当てている。

内部監査の中核的役割の一つは、内部統制環境の妥当性および有効性を評価することである。このガイダンスの目的は、内部監査人が、コンダクト・リスクの管理を理解し評価することに役立つことにある。

はじめに

コンダクトの課題を、組織体のカルチャーと分けて考えることは困難である。むしろ、カルチャー全体としては独特な部分である。

規制当局およびその他の主要な利害関係者は、組織体が有効な統制環境に存在するべき強固な倫理観に基づき業務を運営することを期待している。特定の業界や地域で活動する監査チームには、組織カルチャーの妥当性とコンダクト（このガイド全体では、「コンダクト」を“動詞”ではなく“名詞”として使用する）・リスク・マネジメント活動の有効性を評価し、定期的に報告することが求められている。具体的に、一部の金融サービスの規制当局は、これらの期待事項を基準およびその他のガイダンスとして正式化している。

注：文中にある太字の用語の定義は「付録 B 用語一覧」にある。

資料

組織体のカルチャーに関するより詳細な情報およびカルチャーやコンダクト・リスクを個々の監査業務に含めるアプローチに関しては、ＩＩＡプラクティス・ガイド「Auditing Culture（カルチャーの監査）」を参照のこと。

内部監査人は、組織体のコンダクト・リスク・マネジメントの評価と報告を通じて、価値を付加することができる。**内部監査部門**は、利害関係者の期待事項に沿った強力な内部統制（コンダクト・リスクを含む）リスク・マネジメント・フレームワークを推進することができ、取締役会や監査委員会そして最高経営者における監督の役割を支援する。このガイダンスをレビューすれば、内部監査人は、次の事項が可能となるはずである。

- 組織体の統制環境におけるコンダクト・リスクの重大性を理解すること
- コンダクト・リスクの主要な構成要素を理解すること

- コンダクト・リスクに関する、規制当局を含む主要な利害関係者の懸念事項と期待事項を理解すること
- 組織体のカルチャーおよびコンダクト・リスク管理の評価と報告における内部監査の役割を理解すること
- 組織体のカルチャーおよびコンダクト・リスク管理の評価と報告に関するアプローチを理解すること

ビジネスの重大性：リスクと機会

職場での個人のコンダクトは、他の場所と異なる場合がある。多くの場合、強い倫理的カルチャーまたは管理責任の存在に欠ける組織体は、不正行為または少なくとも他の人の良からぬ行為を見て見ぬふりをすることを許しているのと同じである。ハーバードビジネスレビューの記事は、２つの調査機関が実施した研究に言及している。

> 調査回答者の３分の１は、自社が従業員に不正行為の責任を一貫して負わせていないと信じている。従業員が、処罰されない、または処罰が不公平に行われているとの印象を受けている場合、従業員は、これを、悪い行動を報告しないことの正当化（何が悪いの？）として、また、従業員自身の対応に注意を払わない理由の両方に使うかもしれない[1]。

さらにいえば、この記事は、「従業員の 28%が、会社の行動と表明した価値観が一致していると強く同意する」という最初の研究の指摘を引用した。これは、個人の行動に関して組織体に対するリスクと見なされる可能性のある相当数の従業員が残っているということでもある。

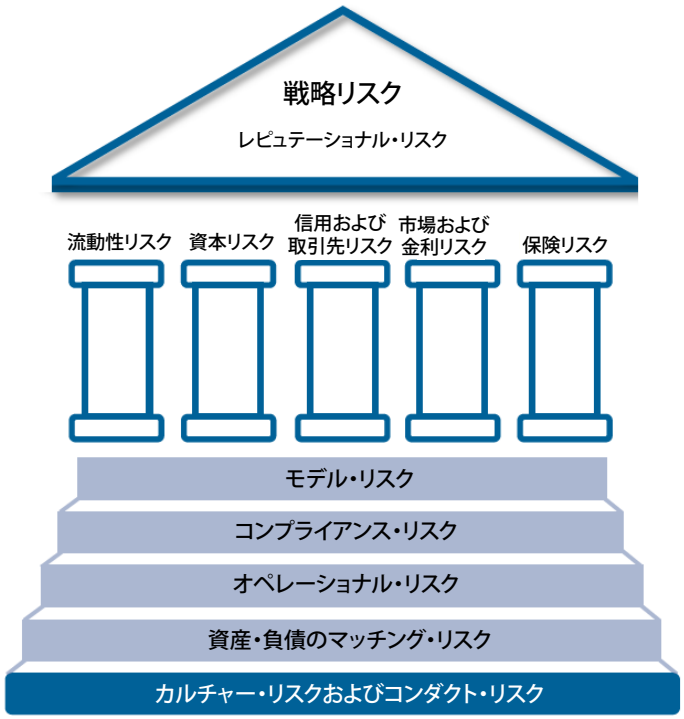
これらの値と言外の意味は、リスクと機会の両方を示唆する。監査、従業員調査、その他の重大なリスクを縮減する可能性のある行動傾向を測定するためのツールによって裏付けられた強力な倫理的カルチャーを誇る一方で、無関心なカルチャーは、組織体がコンダクト・リスクを含む複数のリスクを受け入れなければならない余地がある。

共通の言語で話す

組織体が直面しているリスクを理解するには、従業員はリスク・マネジメント、コンプライアンスおよび内部監査に関連する用語を理解しなければならない。組織全体で、リスク情報を伝達する１つのツールは、リスク・フレームワークである。内部監査人協会（ＩＩＡ）の金融サービスガイダンス委員会は、金融サービス組織に専用の包括的なリスク・フレームワークを策定した。図表１のリスク・フレームワークは、金融サービス業界にグローバルに当てはまるリスクの主要な領域を考慮しており、カルチャーやコンダクトを基盤である土台として明確に特徴付けている。

1. サラ・クレイトン、「企業文化をリスクにさらす６つの兆候」、*Harvard Business Review*、2019 年 12 月 5 日。
https://hbr.org/2019/12/6-signs-your-corporate-culture-is-a-liability.

図表１：内部監査人協会（ＩＩＡ）の金融サービスにおけるリスク・フレームワーク



出典：内部監査人協会（ＩＩＡ）

ＩＩＡの金融サービスにおけるリスク・フレームワークは、英国勅許内部監査人協会が公表した規約「Conduct Risk（コンダクト・リスク）」の定義を利用している。上記の出版物で使用されている「コンダクト」の定義は、「金融サービス組織が、組織体、スタッフ、代理店およびアドバイザーによる、顧客および広範な金融サービス市場との関わり方に伴うリスクを表現するために使用されている。」[2]となっている。

金融サービスの規制当局と組織体は、コンダクト・リスクに数多くの定義を使用しているが、組織体のカルチャーが従業員のコンダクトを左右することにはおおむね合意する。

資料

ＩＩＡの金融サービスにおけるリスク・フレームワークの詳細については、ＩＩＡプラクティス・ガイド「Foundations of Internal Auditing in Financial Services Firms（金融サービス会社における内部監査の基礎）」を参照のこと。

ニューヨーク連邦準備銀行は、「不正行為リスク」が金融機関で目立つようになってきており、これがコントロールされるようになれば、幅広いリスクに耐え得るレジリエンスをもっと持つことができるのではないか

2. 英国勅許内部監査人協会「（コンダクト・リスク）」、2019 年 10 月 2 日、https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/conduct-risk/?downloadPdf=true.

と認識している。そこでは、従業員の不正行為リスクを、「違法、非倫理的、または表明された会社の信念、価値観、方針と手続に反する、行為またはビジネス慣行の可能性」と説明している[3]。この解釈は、顧客や利害関係者などの個人へ悪影響を及ぼす行為、または組織内の個人に害を及ぼす行為に適用される。

不正行為は、組織体のあらゆる階層で発生する可能性がある。これは、稀で、散発的であるが、蔓延する可能性もある。また、いつでも、ほぼすべての状況で起こり得る可能性がある。不正行為は様々な理由で発生し、時には不正行為とカルチャーとの関連性が明らかである。組織体はそのカルチャーの中に反抗的または破壊的な一派が存在する可能性がある。そこでは、不正行為がその事業活動に明確に現れないかもしれない。また別の組織体では、確固たるカルチャーを持っているように見えるかもしれないが、コンダクトが理想的とはいえない事例や集団があるかもしれない。残念な可能性や形態は無くならない。警戒が重要であり、それは内部監査が役立つことができる分野である。

カルチャーとコンダクトが同義ではないのと同様に、不正行為と評判上の損害には違いがある。従業員の行為が規則や規制を破り、または顧客もしくは同僚に害を与えれば、その情報はニュースやソーシャルメディアを介して公になり、不正行為は、評判上の損害の結果となることがある。すべてのコンダクト・リスクが評判上の損害をもたらすことに決まっているわけではないが、これらは組織体の目標達成の支障となる可能性がある。

英国保険市場におけるロイヤルティペナルティ

「『金融行為規制機構』は、『住宅保険および自動車保険』市場がすべての消費者に対してうまく機能しているわけではないことを発見した。多くの人々がいろいろと探し回る一方で、多くの忠実な顧客はよい取引をしているわけではない。我々は、これが約 600 万人の消費者に影響を与えると考えており、消費者がリスクに対し平均的な保険料を支払ったのであれば、12 億ポンドを節約できたであろう。」

出　典：“Citizens Advice supercomplaint to the CMA - update,” *Financial Conduct Authority, Jan. 9, 2020*, https://www.fca.org.uk/news/news-stories/citizens-advice-supercomplaint-cma-update

評判上の損害を引き起こしたカルチャー、レピュテーショナル・リスクまたは事象を評価することは、組織体のコンダクト・リスクのすべての評価要素である。しかし、内部監査人は、コンダクト・リスクの徹底した評価を提供するのに当たり、過去のカルチャー関連のリスク事象だけに依存すべきではない。コンダクト・リスクは、不正行為のシナリオ、インセンティブ、およびこのガイドのリスク評価セクションでレビューするその他のリスクを含め、遥かに多くの領域をカバーしている。

コンダクトの規制環境

規制における「コンダクト・リスク」とう用語が普及する一方で、「コンダクト」という用語は使用されることはなかったかもしれないが、規制当局は検査プログラムにおいてコンダクト・リスクを常に考慮してきた。グローバルな規制当局は、「コンダクト・リスク」のガイダンス、要件および期待事項についていえば、先頭を切っているように見える。

3. ステファニー・チャリー、ジェームズ・ヘネシー、レフ・メナンド、ケビン・スティロー、ジョゼフ・トレーシー、「*Misconduct Risk, Culture, and Supervision*（不正行為のリスク、カルチャーそして監督）」（ニューヨーク連邦準備銀行、2017 年）、p. 3。 https://www.newyorkfed.org/medialibrary/media/governance-and-culture-reform/2017-whitepaper.pdf.

金融サービス業界の安全性、健全性、およびレジリエンスのために、規制機関が不正行為を識別し、場合によっては防止する方法を模索していることは賢明である。金融サービス業界は、世界のほぼすべての人に何らかの形で影響を与えるため、商品販売および資金運用管理を行う企業にとって、コンダクト・リスクとそれに関連するコントロール手段が重要な焦点となることは適切である。

規制機関にとっての課題は、コンダクト・リスクを定義することである。現在、コンダクト・リスクは、「バーゼルIII基準」の第2の柱（Pillar 2）の資本追加においてオペレーショナル・リスクの構成要素として表されている。これは、金融サービス会社では測定が難しいハードリスクおよびソフトリスクの普遍的なカテゴリである[4]。

コンダクトは、規制要件の遵守として狭義に定義することも、顧客や従業員のライフサイクルのすべての段階に触れることとして広義に定義することもできる。国、文化、時間帯を越えて多数の国に関わる組織を管理するロジスティクスを考慮すると、課題は明白である。

疑問視される販売慣行

ウェルズ・ファーゴ社は、不当な販売目標を達成するために、顧客に無断で数百万の銀行口座を不正に作成したことに加えて、57万人もの消費者に不要な自動車保険に加入させたことを認めた。

さらに、これら顧客のうち約2万人が、結果として車を差し押さえられた可能性がある。ウェルズ・ファーゴ社は、補償のため8,000万ドル支払うことに同意した。

出典：エミリー・グレイザー、"Wells Fargo to Refund $80 Million to Auto - Loan Customers for Improper Insurance Practices," *Wall Street Journal*, July 28, 2017, https://www.wsj.com/articles/wells-fargo-to-refund-80-million-to-auto-loan-customers-for-improper-insurance-practices-1501252927.

世界中の規制機関には、カルチャーとコンダクトのリスクに関して様々な定義があり、そのうちのいくつかは、より大きな研究からの抜粋として図表2に示されている。各抜粋の全文は、「付録C．参考文献および追加で読むべき資料」に記載されている。

図表2：カルチャーおよびコンダクトに係る規制当局の定義の例

オーストラリア証券投資委員会（ASIC）
ASICの企業文化への取り組みの概要
カルチャーとは、共有される一連の価値観または前提である。それは組織体の考え方として説明可能である。これは新しい概念ではない。実際には、それは20年以上前に刑法に取り込まれ、組織の態度、方針、規則、行動指針、および実施を含むと定義されている。 より具体的には、リスクカルチャーは、組織体がどのようにリスクを識別、理解、議論、および行動するかを決定する姿勢の規範を表現している。
香港金融管理局（HKMA）
銀行のカルチャー改革
「カルチャー」は一般的に、銀行の株主、取締役会メンバーおよびスタッフが追求し維持する態度や行動を 支配する、一連の専門的および倫理的価値と見なすことができる。

4. バーゼル銀行監督委員会、*Overview of Pillar 2 supervisory review practices and approaches*, Basel, Switzerland: Bank for International Settlements、2019年6月。https://www.bis.org/bcbs/publ/d465.pdf.

図表２：カルチャーおよびコンダクトに係る規制当局の定義の例（続き）

シンガポール金融管理局（ＭＡＳ）

「カルチャーおよびコンダクト―当局の視点」

定義と表現の考え方は多いが、主に、私たちはそれを組織の行動を導く共有された価値観、態度、規範と見なす。カルチャーは、組織体の基本的な考え方を反映し、組織体とそのスタッフが、しばしば無意識のうちに、行動し、意思決定を行う方法に影響を与える。

英国

銀行基準審議会（Banking Standards Board）

カルチャーの説明と定義には多くのものがあり、最も頻繁に引用されるのは、「誰も見ていないときのやり方」である。これは、我々が反射的にカルチャーと結び付ける、容易に取り除けない、先天的なもの、の意味をうまく伝えているが、カルチャーを総括的に表現しているわけではない。かなり覚えにくくはなるが、より正確には、「権限を有する者が誰も見ていないときのやり方」を観察することからグループのカルチャーに関して多くのことを学ぶことができる、と言うことはできるだろう。もっとも、そのグループの多くの人がたまたま見ている場合の「やり方」からカルチャーを知ることができる、というのも正しいのかもしれない。

より厳密にいえば、カルチャーは、集団的な前提、価値、信念、およびどのように人がグループの中で行動するかを決定付ける期待と解釈することができる。

英国

金融行為規制機構（ＦＣＡ）

ＦＣＡの視点から「カルチャー」を理解するには、組織体を特徴付ける習慣的行動および考え方を定義することから始める。

米国

通貨監督庁（ＯＣＣ）：監督官のためのハンドブック、コーポレートガバナンスおよびリスクガバナンス

企業文化とは、組織内の振舞いを左右する規範と価値を示す。銀行にとって適切な企業文化とは、軽率なリスクテイク、非倫理的行為、または法規制もしくは利益や事業目標を追及する際の安全で良好な方針と手続の潜脱行為のいずれも奨励しないことである。適切な企業文化は従業員に責任を負わせる。これは取締役会から始まり、取締役会は、「経営トップの姿勢」を設定し、良好な企業文化とリスクカルチャーを育成・維持する経営者の役割を監督する責任がある。取締役会と最高経営者が確立した共有価値、期待事項そして目標は、良好な企業文化を促進する。

米国

通貨監督庁（ＯＣＣ）：Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches

リスクカルチャーに対する規制上の定義は存在しないが、これらのガイドラインの目的として、リスクカルチャーは、ガバナンス活動およびリスク判断を形成し、ガバナンス活動およびリスク判断に影響を及ぼす、銀行全体に存在する共有価値、態度、能力、および振舞いと見なすことができる。

さらに、規制当局のコンダクト・リスクに関するガイダンスの例は、次の図表３に示されている。

図表３：コンダクト・リスクに係る規制当局のプログラム

オーストラリア
オーストラリア健全性規制庁（ＡＰＲＡ）：Banking Executive Accountability Regime
https://www.apra.gov.au/banking-executive-accountability-regime
オーストラリア証券投資委員会（ＡＳＩＣ）：Close and Continuous Monitoring Program as part of the ASIC Corporate Plan 2019-23
https://download.asic.gov.au/media/5248811/corporate-plan-2019-23-published-28-august-2019.pdf
ヨーロッパ連合（ＥＵ）
欧州中央銀行（ＥＣＢ）：European Banking Authority is mandated by Article 74 of Directive 2013/36/EU
https://eba.europa.eu/sites/default/documents/files/documents/10180/1972987/eb859955-614a-4afb-bdcd-aaa664994889/Final%20Guidelines%20on%20Internal%20Governance%20(EBA-GL-2017-11).pdf
欧州保険・年金監督当局（EIOPA）：Framework for Assessing Conduct Risk Through the Product Lifecycle
https://www.eiopa.europa.eu/sites/default/files/publications/reports/2018.6644_en_03_mod-gp.pdf
香港
香港金融管理局（ＨＫＭＡ）：Bank Culture Reform/Manager-in-Charge regime
https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20181219e1.pdf
オランダ
オランダ銀行およびオランダ金融市場庁（ＡＦＭ）：Supervision of Behaviour and Culture
https://www.dnb.nl/en/binaries/Book%20Supervision%20of%20Behaviour%20and%20Culture_tcm47-380398.pdf
ノルウェー
ノルウェー財務省金融市場部：Revised Strategy for Combating Work-related Crime
https://www.regjeringen.no/contentassets/7f4788717a724ef79921004f211350b5/a-0049-e_revised-strategy-for-combating-work-related-crime.pdf
英国
イングランド銀行／健全性監督機構（ＰＲＡ）：シニアマネージャー・レジーム
https://www.bankofengland.co.uk/prudential-regulation/authorisations/senior-managers-regime-approvals
米国
連邦準備制度理事会：SR 12-17 / CA 12-14: Consolidated Supervision Framework for Large Financial Institutions
https://www.federalreserve.gov/supervisionreg/srletters/sr1217.htm
ニューヨーク州金融サービス局：Regulation 60: Market Conduct Profile
https://www.dfs.ny.gov/docs/insurance/reg60/mc_profile_2017.pdf

多くの業界で、企業はコンダクトの側面に適用される規制に従っている。例えば、米国の法律には、海外腐敗行為防止法、雇用機会均等法、障害のあるアメリカ人法などが含まれる。しかしながら、金融サービス会社向けには、英国の健全性監督機構（ＰＲＡ）に、銀行向けの「シニアマネージャー・レジーム」（ＳＭＲ：Senior Managers Regime）と呼ばれる、包括的かつ信頼できる、カルチャーおよびコンダクト・リスク・マネジメントのプログラムがある。このプログラムでは、指定された最高経営者が、会社がリスクカルチャーを採用することを直接監督し、会社がさらなる金融犯罪に慣れてしまうことを防止する対策を導入することを確実にすることを要求している。会社の統治機関のすべてのメンバーは、組織内の適切な担当者が監視する適切なトレーニングと専門能力の開発を受ける必要がある。

図表４は、英国のＰＲＡが、「シニアマネージャー・レジーム」（ＳＭＲ）の枠内にある非業務執行取締役（ＮＥＤ）の職務に対して、懲戒処分を検討する可能性があるかもしれないシナリオ例のいくつかを示す。

図表４：懲戒シナリオの例

結果責任を問われる可能性のあるＳＭＲの枠内にあるＮＥＤ

熟練者のレビューによって、企業のリスク委員会が取締役会に対して**リスク選好**の勧告をしていなかったこと、さらにリスクコントロール 3.1（2）に違反して経営幹部によるリスク戦略の実施を監督することを支援していなかったことが明らかになる。この状況では、ＰＲＡはリスク委員会の委員長に対し制裁を課す根拠があるかどうかを検討するかもしれない。

ＰＲＡは、取締役会の有効性のレビュー中に、報酬委員会が取締役会による検討と決定のために報酬制度に関する決定を準備できなかったことを発見した。この状況では、ＰＲＡは、報酬委員会の委員長に対して制裁を課す根拠があるかどうかを検討するかもしれない。

ＳＭＲの枠内にある企業の委員長とＮＥＤは、過度に支配的なＣＥＯに関しては深刻な懸念を抱く。これらの懸念事項は、取締役会によっても、またＰＲＡやＦＣＡの監督者との間でも、対応も、記録も、議論もされていない。

結果責任を問われる可能性のある最高経営者の職務

ある企業は、リスクリミットに繰り返し違反した主要なビジネス・ユニットにおける大きな損失の結果として、自己資本規制に違反する。リスクリミットは、リスク委員会および取締役会にて議論のうえ設定された。この状況では、ＰＲＡは最初に主要な事業領域の責任者や最高リスク管理責任者を含む、適切な経営幹部に制裁を課す根拠があるかどうかを検討するかもしれない。ただし、違反が取締役会やリスク委員会に報告された場合、ＰＲＡは、取締役会やリスク委員会がそれらについて議論し、何らかの勧告を行ったかどうかを調査するかもしれない。

新しいリスクの高い貸付戦略に対して取締役会の承認を得ようとする際、企業のある上級経営者は、そのような戦略のリスクを大幅に軽視する不完全で誤解を招くような経営情報を取締役会に提出する。ＣＥＯはまた、この課題に関するいかなる否定的または疑わしい助言を抑圧し、その結果、取締役会はこの戦略を承認する。その結果６か月後この企業に、ＰＲＡルールブックのリスクコントロール条項への大量の違反を発生させる。

企業の経営者は、アウトソーシング契約に基づく第三者によるサービスの提供の監視に失敗し、その結果、オペレーショナル・リスクがＰＲＡルールブックのアウトソーシング 2.1 の違反を発生させる。

出典：イングランド銀行、健全性監督機構、Strengthening individual accountability in banking, Supervisory Statement | SS28/15、2018 年７月。https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2018/ss2815update.pdf?la=en&hash=39EC46AE5FD217724BB307C420B80A4E09F42A24.

英国の金融行為規制機構（ＦＣＡ）は、金融サービス会社に対する規制当局の期待事項を次のように定義する「個人行動規範（別名：COCON 2.1）」も定めている。

1. 誠実に行動すること。
2. 十分なスキル、注意、かつ勤勉さをもって行動すること。
3. ＦＣＡ、ＰＲＡ、その他の規制当局に対して率直で協力的であること。
4. 顧客の利益を尊重し、公正な取り扱いをすること。
5. 市場行動の適切な基準を遵守すること[5]。

ＦＣＡは、ホールセール業務を行う銀行を調査する場合に、上記のルールに５つの質問を加える。

1. 会社として、ビジネスに固有のコンダクト・リスクを識別するために、どのような事前措置を講じているか？
2. フロント、ミドル、バックオフィス、コントロール、およびサポートの各部門で働く人々に、自分のビジネスのコンダクトを管理することに思いを巡らせ、責任を負うよう、どのように奨励するか？
3. 会社は、会社のために働く人々が自己のビジネスまたは部門のコンダクトを向上させるのを可能とするどのような（広義の）サポートを導入しているか？
4. 取締役会および執行委員会（ExCo）（または適切な最高経営者）は、どのように組織内のビジネスコンダクトの監督ができるようにしているか？そして、同様に重要なことであるが、取締役会または執行委員会は、自らが行った戦略的意思決定がコンダクトへ及ぼす影響をどのように考慮しているか？
5. 会社は、コンダクトを改善するための戦略を損なう可能性がある何か他の活動があるかどうかを評価したか[6]？

金融サービス会社は、もし会社が上記事項をまだ実施していない場合には、規制機関がこれらの質問をし、検査にこの種の規則を含めてくることを覚悟しなければならない。

コンダクト・リスク・マネジメントのフレームワーク

組織体のコンダクト・リスクを管理するには、カルチャーとコンダクト・リスクの定義、そしてこれらのリスクを管理する際の構成要素の両方に関して合意しなければならない。組織体は、どのようなコンダクトが適切であるかを定義することにコミットし、不正行為の結果を明確にしなければならない。

有効なコンダクト・リスク・マネジメントのフレームワークは、通常、図表５に示すように、少なくとも３つの構成要素からなる。

5. *FCA Handbook*, COCON, COCON 2（London: Financial Conduct Authority, last updated March 7, 2016）. https://www.handbook.fca.org.uk/handbook/COCON/2/?view=chapter.
6. *Progress and Challenges: 5 Conduct Questions*（London: Financial Conduct Authority, 2019）. https://www.fca.org.uk/publication/market-studies/5-conduct-questions-industry-feedback-2018-19.pdf.

図表５：コンダクト・リスク・マネジメントのフレームワークの構成要素

出典：ステイシー・シャーベル、"Maximizing Organizational Value: Auditing Conduct & Culture," presentation delivered at The IIA's 2019 Fi nancial Services Exchange, Washington, D.C., September 16, 2019.

定義された期待事項

すべての従業員が意識し、組織体の期待事項に沿ったビジネス・プロセスを意識し、実行できることを確実にするため、組織体には、カルチャーおよびコンダクト・リスクの明確な定義が要求されている。前述のように、ニューヨーク連邦準備銀行は、コンダクト・リスクを、「違法、非倫理的、または表明された会社の信念、価値、方針と手続に反する行為であるビジネス慣行の可能性」と定義した[7]。

この定義は、組織体が、コンダクトはビジネスとの関係で何を意味するのかを判断する出発点となるかもしれない。従業員のコンダクトに対する組織体の期待事項の説明を含む他の文書には以下が含まれることがある。

- バリュー・ステートメント
- 行動規範
- 倫理方針および研修資料
- リスク選好の表明またはフレームワーク
- 報酬慣行
- 職務分離の要求事項

7. ステファニー・チャリー、ジェームズ・ヘネシー、レフ・メナンド、ケビン・スティロー、ジョゼフ・トレーシー、「*Misconduct Risk, Culture, and Supervision*（不正行為のリスク、カルチャーそして監督）」（ニューヨーク連邦準備銀行、2017 年）、https://www.newyorkfed.org/medialibrary/media/governance-and-culture-reform/2017-whitepaper.pdf.

測定および報告

金融サービス業界には、どのように経営者がコンダクト・リスクのレベルを監視しているか、もしくはしていないか、を判断する際に有用な多くの主要業績評価指標（ＫＰＩ）がある。そのＫＰＩには次のような項目を含む。

- ｅ - トレーニングの完了率
- 苦情
- 経営者による無効化
- 不正の発生と関連する損失
- コンダクトに関連する違反から生じる負 の報酬変更
- 従業員調査の結果
- 顧客満足度調査の結果
- 統制環境調査の結果

これらのＫＰＩやその他の組織的に関連性 のあるその他のＫＰＩを長期にレビューすることによって、どのようにコンダクト・リスクのエクスポージャーが時間の経過とともに変化していくか、およびどのタイプの活動がエクスポージャーのレベルに影響するのかに関して、洞察を得ることができる。

不正行為の結果

尋ねるべき最も重要な質問は、経営者が経営者自身の行動とその管理下にある人々の行動の両方に対して、その結果に責任を負って いるかどうか、またどのように責任を負っているか、かもしれない。コンダクト違反やコンダクトの問題があったとしても、それでどのような結果が待ち受けているのかを予測できない場合には、従業員が自身の行動を組織体の行動規則に合わせるインセンティブは低くなる。従業員はルールに従わないことが容認されると考えているかもしれないので、違反と結果の関係が不明確であると、組織体のカルチャーに影響を与える可能性もある。

内部監査の役割

組織の要件とコンダクトの期待事項は、通常、一連の正式な文書と関連する研修（行動規範、価値観、倫理方針、調査委員会と関連する指示書、およびその他のガイダンスを含む）によって示される。多くの金融サービス組織は、行動規範を定期的にレビュー、更新、公表している。

内部監査部門は、組織体が価値観、期待事項、および従業員がそういった規準に対してどのくらいよく活動しているかを測定する機能を記述した、コンダクト・リスク・マネジメントのフレームワークを有しているかどうか判断すべきである。内部監査人はまた、コンダクトの要求と期待事項に対する従業員の理解レベルを確認するため、組織全体に質問すべきである。内部監査人は、従業員がコンプライアンス違反による潜在的な影響を認識しているかどうかを見極めるべきである。

従業員は、ビジネス上の意思決定を行う際に、自分自身に対して次のような質問をするか？　もしそうであれば、コンダクト・リスク・マネジメントのフレームワークは、従業員がそれらの質問に効果的に回答する際の手助けとなるか？

自分がお客さまだった場合はどうなるか？

- お客さまを公正、率直、正直に扱う。
- お客さまのニーズに合い、明確に説明され、かつ真の価値を提供する商品やサービスを、提供、推進する。
- お客さまを自分たちが行うことの中心に置く。

自分でビジネスを行っている場合はどうなるか？

- 株主の目で見る。
- 長期的で持続可能な価値を提供するビジネスを推進する。
- 新しい機会を自分のものとし、リスクの責任を取る。
- 自分のお金がリスクに晒されているのであれば、どうするかを自問する。

仲間とどのように協働するか？

- 自分自身のチームや世界中の両方の仲間と協働する。

家族や友人に何を伝えるか？

- コミュニティへの義務。
- 自分たちが何をしているのかを友人や家族に伝えることを誇りに思うべきである。

出典：Paraphrased from Prudential, PLC Code of Business Conduct, December 2019, https://www.prudentialplc.com/investors/governance-and-policies/code-of-business-conduct.

コンダクト・リスク・マネジメントのフレームワークが存在し、このフレームワークを従業員がおおむね認識している場合に、内部監査人は、このフレームワークの要求事項に沿ってビジネス活動が行われることを支援するために導入されているコントロール手段の設計と有効性を評価すべきである。このフレームワークには、方針、手続、経営情報、ガバナンス、違反管理、第２ラインによる監視、および要求事項との整合を支援するその他の活動が含まれる。

組織体のコンダクト・リスク・マネジメントは導入されているものの正確に伝達されていない場合には、「恐怖の環境」を助長するかもしれない。例えば、管理者は、ある従業員がインシデントを組織の倫理ホットラインに報告したと疑っている。インシデントは秘密にされ、内部告発者は識別されないが、経営者は（何らかの理由、すなわち個人的な反感、情報の入手、報告された活動に関する以前の議論などから）「この従業員」が犯人（この場合、内部告発者）であると決めてかかる。その結果、経営者はその従業員を、苦情に関連した、人や、情報、その他の知識と関わらない、責任の少ないポストに異動させる。

従業員がインシデントを報告したかどうかにかかわらず、従業員たちへのメッセージは明確である。すなわち、内部告発者または倫理ホットラインに問題を報告する者は、報復、懲罰、またはある種の処罰の対象となるということである。経営者は、それが特定の個　人であったことを知らずに疑う場合にもまだ、その人にマイナスの影響を与える可能性がある。内部監査人は、コンダクト・リスク・マネジメント活動が組織体のカルチャーに悪影響を与えるかどうかを認識すべきである。

内部監査の個々の業務の計画策定および実施

このガイドは、次の３つの事項についてのアプローチを検討する。⑴全体的なコンダクト・リスク・マネジメントのフレームワークに関連する一連の主要なプロセスとコントロール手段の選択、⑵個々の業務の計画策定、⑶選択した領域での目標を定めたテスティングの実施。テスティングは、内部監査人が従業員に対しコンダクト・リスクへの対処方法の評価に焦点を当てたインタビューをすることで補足される場合がある。具体的な詳細事項に関しては、基準 2300（内部監査（アシュアランスおよびコンサルティング）の個々の業務の実施）を参照のこと。

情報収集

内部監査人は、従業員のコンダクトに関連する経営者の期待事項を識別しなければならない。このガイドの「コンダクト・リスク・マネジメントのフレームワーク」セクションでは、コンダクト・リスクを監査するための個々の業務のプログラムを構築する際に収集し考慮すべき情報の種類の概要を提供している。

従業員のコンダクトへの組織体の期待事項に関する情報源は、下記の文書にあり、従業員の職務を実行する際の実際のコンダクトのテスト結果と比較することができる。

- バリュー・ステートメント
- 行動規範
- 倫理方針および研修資料
- リスク選好の表明またはフレームワーク
- 従業員カルチャー調査の結果（報告されたスコアと、質問への個々の回答および従業員の書いた自由記述コメントとの照 合）

資料

個々の業務

内部監査の個々の業務の計画策定および範囲設定に関する詳細な説明は、ＩＩＡのプラクティス・ガイド「個々の監査業務の計画策定：目標と範囲の設定（Engagement Planning: Establishing Objectives and Scope）」を参照のこと。

リスク評価

リスク評価を実行する方法の詳細に関しては、ＩＩＡのプラクティス・ガイド「個々の業務の計画策定：不正リスクの評 価（Engagement Planning : Assessing Fraud Risks）」を参照のこと。

このガイドには、リスク評価のどのようなトピックにも適用できる「ハウツー」が含まれている。

サードパーティ

カルチャーおよびコンダクト・リスクに関連する監査を計画する際に、内部監査人は、組織体による第三者との関係がもたらすリスクを考慮すべきである。

詳しい情報は、ＩＩＡのプラクティス・ガイド「サードパーティに関するリスク・マネジメントの監査（Auditing Third-party Risk Management）」を参照のこと。

リスク評価

コンダクト・リスクは様々な方法で定義されているが、通常、コンダクト・リスクとして扱われるものには、次のものが含まれる。

- 顧客への不当な扱い
- 顧客に誤解を生じさせること
- 規則および規制への違反
- 不正
- 従業員への不法行為
- 組織体が宣誓したリスク選好と一致しない方法でのビジネス推進
- 自然な市場環境を歪める戦略または措置の実施

一般的な意味では、コンダクト・リスクは、顧客、従業員、またはその他の利害関係者に害を及ぼす可能性を有するあらゆる行為によって生み出される。

コンダクト・リスクの評価は、うまくいけば、過去に起こったことに留まらず、将来起こるかもしれないことを考慮すべきである。組織体が提供する製品やサービスに関連する固有リスクを考慮することは不可欠である（例えば、リテールバンキングのリスクは、商業リスクと異なり、ユニバーサル保険のリスクとも異なる。）。さらに言えば、不正行為が発生する可能性のあるシナリオと不正行為発生のリスクを縮減するために導入されているコントロール手段を考慮することは、リスクとコンダクトに関連するコントロール手段との相互関係を特定するための効果的な方法であるかもしれない。

より洗練されたプログラムにおいては、金融サービスの組織体は、個々のインシデントだけでなく、長期的に不正行為との相関関係と傾向を調べて、コンダクト・リスクのエクスポージャーを評価している。それには、次のような事項が含まれる。

誰かが経費精算書を却下された、要求される欠勤規則に従わない、行動規範の研修を受けない場合などに、これらの行動をもっと詳細に調べるプロセスが存在しているか？／電話の通話記録、取引のモニタリング、統制の無視などに関わるインシデントは、パフォーマンスレビューとインセンティブプログラムで考慮されているか？／これらの課題は人と切り離されたものか？／複数の人が不正行為に関与している場合、この者たちには共通の管理者、部門、またはビジネスラインがあるのか？／誰が、いつ、何を、知っていたのか？／彼らは、それを適時に、または少しでも報告したのか？

組織体にこれらのリスクファクターならびに対応する相関関係および傾向が存在する場合に、内部監査人は、これらを識別し、基準 2060（最高経営者および取締役会への報告）に従って、最高経営者および取締役会に適切に報告しなければならない責任がある。加えて、ＩＩＡの「倫理綱要」の誠実性の原則および「倫理行動規範」「誠実性 1.2」では、「（内部監査人は、）法令を遵守し、法令で要求される、および専門職として期待される開示を行うこと。」としている。監査の発見事項とその後の調査次第では、当局に報告する必要があるかもしれない。

監査の最終的な範囲と目標には、事前に実施したリスク評価をどのように焦点を当て、実施したのかの情報を含むべきである。

内部監査の個々の業務の計画策定

基準 2201（計画の策定における考慮事項）、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）、基準 2220（内部監査（アシュアランスおよびコンサルティング）の個々の業務の範囲）、の各基準を満たすため、内部監査部門長（ＣＡＥ）は、個々の業務の計画を策定する際に、利用可能である過去に実施した監査の情報およびコンダクト関連の主要なプロセスとコントロール手段の情報を利用するかもしれない。個々の業務の計画は、様々な方法で構築できる。このガイドは、次の３つの事項についてのアプローチを検討する。⑴全体的なコンダクト・リスク・マネジメントのフレームワークに関連する一連の主要なプロセスとコントロール手段の選択、⑵個々の業務の計画策定、⑶選択した領域での目標を定めたテスティングの実施。このテスティングは、内部監査人が、抽出した従業員に対しコンダクト・リスクへの対処方法の評価に焦点を当てたインタビューをすることで補足される場合がある。

内部監査の個々の業務における目標は、組織体のコンダクト・リスクの定義と結び付け るべきである。前述のとおり、この定義は狭い場合もあれば、広い場合もあり得る。コンダクト･リスクの定義を理解したら、テストは、組織体の活動がこの定義に沿うことを支援するプロセスおよびコントロール手段の評価に焦点を当てるべきである。

コンダクト・リスク・マネジメントのフレームワークおよびこれに適合するよう導入されているプロセスおよびコントロール手段に焦点を当てた個々の業務の範囲設定を行う際に（基準 2220（内部監査（アシュアランスおよびコンサルティング）の個々の業務の範囲））、有用な最初のステップは、関連する領域のどこで監査（または他の活動）のアシュアランスをカバーしているかのマッピングをすることである。

資料

カルチャーとコンダクト・リスクを内部監査部門が実施する監査に統合する方法としては、ＩＩＡプラクティス・ガイド「Auditing Culture.（カルチャーの監査）」を参照のこと。

アシュアランス・マップの構築に関するより詳しい情報は、ＩＩＡのプラクティス・ガイド「連携と依拠：アシュアラ ンス・マップの作成（Coordination and Reliance：Developing an Assurance Map）」を参照のこと。

資源配分

コンダクト関連のリスク監査業務に割り当てられた監査人には、特定のスキルセットが必要である。基準 2230（内部監査（アシュアランスおよびコンサルティング）の個々の業務への資源配分）に適合し、内部監査部門が、コンダクト関連のリスクのマネジメントに対する重要な情報および洞察を提供するための適切なスキルを有していることを確実なものにするため、**内部監査部門長**は、内部監査チームメンバーのスキルを定期的に評価すべきである。

資源配分を決定する際の重要な要素は、コンダクトまたはカルチャーのリスク要因を評価する監査業務に新しい監査人を配置することである。内部監査部門の離職率が高い場合、新しい監査人はこの問題に関する説明を受けることを要求するかもしれない。したがって、この問題について新しい監査人に概要を説明し、早期に個々の監査業務に対する計画の策定に参加させることは有用かもしれない。例えば、機密性の高い行為に関連する問題について経営者と話し合う場合は特に、経験豊富な監査チームメンバーによるインタビューに新しい

監査人を参加させる。これは、新しい監査人が組織の専門用語や慣用句に慣れるのを助け、そのような議論のニュアンスを観察するためのトレーニングツールになる場合がある。これは、従業員の母国語による言語の壁などのように、独特の状況に遭遇する可能性がある監査人にとって適切な戦術である。

正しい質問が誤った方法で行われる場合には生産的なインタビューが妨げられることから、対象を絞った質問を含んだアジェンダを作ることが重要になる。ＣＡＥは、特にコンダクトの問題に関する知識と理解を向上させるために、新しい監査人をブレーンストーミングセッションやリスク評価などに含めることを検討すべきである。これは、特有で広範な文化的な慣習を持つかもしれないグローバルな拠点を有する組織体の分野でインタビューを実施する監査人にとって極めて重要であるかもしれない。

アシュアランス業務の目標

- 事前に実施したリスク評価にて重要であると評価された領域またはプロセスの事業目標にリスクを反映する（基準 2210.A1）。
- 重大な誤謬、不正、コンプライアンス違反およびその他のエクスポージャー（リスクに曝されている度合い）の可能性を考慮する（基準 2210.A2）。
- 適切な評価規準の識別（基準 2210.A3）。

コンダクトに関する内部監査の業務が、他のアシュアランス提供者によって実施される場合、ＣＡＥはその業務が客観的かつ完全であることも確認すべきである。基準 2050（連携と依拠）に記載されているように、ＣＡＥは、その提供者の行う業務の範囲、目標および結果を明確に理解するとともに、その提供者の専門的能力、**客観性**、および専門職としての正当な注意を慎重に考慮すべきである。内部監査部門が到達した結論と意見に対する適切なサポートが存在することを確実にする責任は、ＣＡＥにある。

内部監査の個々の業務の実施

計画の策定段階において、内部監査人は、情報を監査調書に文書化する。この情報は、基準 2240（内部監査（アシュアランスおよびコンサルティング）の個々の業務の作業プログラム）で要求されているように、個々の業務における目標を達成するために確立しなければならない作業プログラムの一部になる。

個々の業務における目標と範囲を確立するプロセスを通じて次の調書のいくつかまたはすべてが作成される。監査で使用する場合は、基準 2330（情報の文書化）に従って文書化しなければならない。

- プロセスマップ
- インタビュー概要
- 事前のリスク評価（例えば、リスクコントロールマトリクスおよびヒートマップ）
- どのリスクを監査業務に含めるかの判断 に対する根拠
- レビュー対象の領域またはプロセスを評価するために使用される規準（基準 2210.A3 に従って、アシュアランス業務に必要とされるもの）
- 以前どの範囲のアシュアランスを得られたのかのマッピング

コンダクト関連のリスクの監査中に表明された見解の一部が機密に関わることを考慮すると、監査調書は、内部監査部門の中でも「知る必要がある」者のみがアクセスできるようにするために、安全対策（例えば、インタビュー対象者を匿名化し、表明者を特定できる手掛かりへのアクセスを制限する）が必要かもしれない。これは、「倫理綱要」の「秘密の保持」の原則に関連する。

ＣＡＥが、コンダクト・リスク・マネジメントのフレームワークへの準拠に関連する主要なプロセスおよびコントロール手段一式を選択し、組織全体のこれらのプロセスをテストする個々の監査業務の計画を策定することで、個々の監査業務へアプローチすることを選択する場合には、組織体内で使用されているコンダクト・リスク・マネジメントのフレームワークの様々な構成要素をテストするために個々の監査業務を構築することが役に立つ。この説明の目的のため、図表５に示すフレームワークの構成要素は次のとおり。

- 定義された期待事項
- 測定および報告
- 不正行為の結果

定義された期待事項

最初に組織体の従業員への期待事項を定義した文書の存在を確認することが好ましいかもしれないが、内部監査人は、従業員におけるその文書の有効性を確認すべきである。この情報を得るための技法は次のとおりである。

- インタビューまたは調査を通じて、コンダクトに関する「経営者の姿勢」に対する従業員の認識を調査する。報告されたスコアと質問への個々の回答および従業員の書いた自由記述コメントとの照合を含む、従業員カルチャー調査結果の分析は、経営幹部が「伝達している」と考えているものと、従業員が実際に「聞いたり理解している」ものとのズレを識別する便利な方法となるかもしれない。
- バリュー・ステートメントをどのように構成し、伝達しているか調査する。バリュー・ステートメントは、シンプルで明確か？　従業員は、オフィスに掲示されているバリュー・ステートメントを実際に見ているか？　ウェブサイトにバリュー・ステートメントは掲載されているか？　経営幹部は、書面および口頭でバリュー・ステートメントを補強しているか？
  - シンプルで明確なバリュー・ステートメントの例は、ウーバー社の「文化的規範」文書：「正しいことをする。ただそれだけです。」にある。
- 組織体の行動規範が定期的に更新されているか確認する。もしそうなら、従業員は更新後の行動規範を受け入れることを示す必要があるか？　行動規範は、従業員が規範への違反を認識することの教育

コンダクト・リスクに関するリスク選好およびリスク許容度

組織体の不正行為への許容度とは何か？

従業員が大きな収入を稼ぎ、すべての良い顧客を抱えている場合、彼らが何か悪いことをした場合に組織体が目をそらしがちな性質は何か？

問題のモニタリングおよび報告のプロセスに、どの程度の変更または例外は起こる可能性があるか？

に関するシナリオを提供しているか？　違反の結果何が生じるかが行動規範に記載されているか？

- 組織体の倫理方針とそれに関連する研修資料を調査する。前述のように、従業員は組織体の倫理プログラムに関する研修を完了するよう要請されているか？　もしそうなら、従業員がこの研修を完了させたことはどのように文書化されているか？　この倫理プログラムに対する従業員の理解度最終テストにおける合格点を要求していない場合、組織体は、どのように従業員の理解度レベルを示すことができるか？
- コンダクト・リスクの管理における、組織体のリスクアペタイト・ステートメントとリスクアペタイト・フレームワークの有効性を評価する。金融サービスの組織体は、通常、様々な事業活動を管理するためのリスクアペタイト・ステートメントまたはリスクアペタイト・フレームワークを保有している。しかしながら、内部監査人は、これらのリスクアペタイト・ステートメントまたはリスクアペタイト・フレームワークが、コンダクト・リスクのような非金融分野のリスクまでカバーしているかどうかを調査したいかもしれない。そうでない場合は、なぜしたくないのか？

測定および報告

組織体が、自身のコンダクト・リスク・マネジメントのフレームワークに関連する必要な文書をすべて保有している場合、内部監査人の次のステップは、組織体が従業員の実際の行動をどのようにモニタリングしているかを理解することである。これらが遵守されているかを判定する監査での考慮事項のいくつかの例は、次のものである。

- 測定可能なＫＰＩ（この文書の「コンダクト・リスク・マネジメントのフレームワーク」セクションで説明）の推移が追跡され、測定規準が期待値から逸脱している場合は上位への報告手続（エスカレーション・プロトコル）に従っていることを確認する。
- 関連プロセスの有効性に関して懲戒処分または報酬への影響に繋がるようなインシデントのサンプルを調査する。
- 報告すべきインシデントに関する経営者のコミュニケーション活動を調査する。
- 組織体の内部通報および苦情取扱い手続を監査する。
- 組織体が、報酬に影響する規制および社内のコンダクト関連の要求事項に従っていることを確認する。
- 利益相反または職務分離の違反が発生する可能性のある個々のプロセスが、こういったリスクを回避するために適切に構造化されモニタリングされていることを確認する。

監査での考慮事項

金融サービス会社において、コンダクト・リスクを考慮したいかなる個々の監査業務の計画にも、次の検証を含めるべきである。⑴報酬に関する方針と実務、⑵報酬に関する方針と実務の、従業員のコンダクトに関する経営者と取締役会の定義された期待事項に対する関係。

個人が従うべき規範を明確にした後、関連する方針と手続が徹底されていることを確認するため、内部監査人は、インシデントについて、発生から報告まで、また報酬やインセンティブの影響までテストすべきである。

図表６にこれらの要素を含む、コンダクト・リスクおよびコントロールのテストマトリクスの例を示す。

図表６：コンダクト・リスクとコントロールのテストマトリクスの例

コンダクト・リスク
個人向け融資における不適切な職務分離
コントロール手段
■ 個人向け融資の方針と手続文書には、職務分離が組み込まれている。 ■ 融資事務担当者は、自分自身への融資を承認できない。 ■ 方針から外れた融資は、取締役会が承認した権限委譲マトリクスに従って承認しなければならない。 ■ 融資申請書類のレビュー部門は、融資を承認する前に、融資申請書類が完全かつ正確であることを検証し なければならない。
考えられる作業手順
■ 個人向け融資の方針と手続をレビューし、職務分離の要求事項が、含まれており、明確であり、かつ規制と組織体の行動規範に沿っていることを確認する。 ■ 規制上の要求事項や行動規範の条項からの逸脱に注意する。 ■ 主要なプロセスをウォークスルーし、実務が方針と手続に矛盾していないかを評価する。 ■ （システムへの）ユーザーアクセスの定義文書を入手し、融資事務担当者が自分自身への融資を承認できないこと、承認しないことを確認する。 ■ 融資事務担当者またはその管理者が融資システム内の処理機能と承認機能の両方にアクセスできることが判明した場合は、統計的に重要な融資のサンプルを追跡し、アクセスが悪用されていないことを確認する。 ■ アクセスの濫用が識別された場合、または疑わしい場合は、正式な上位への報告プロセスに従う。 ■ 過去の濫用事例をレビューし、違反の程度に応じて適切な結果となることを確実にする。 ■ 濫用が識別されず、疑わしくもない場合は、適切な職務分離を確保するためにアクセスを変更することを推奨する。 ■ 方針から外れた融資のサンプルを選択し、その承認プロセスを追跡して、設定された基準に従って組織体の適切なレベルで承認されたことを確認する。 ■ サンプリングの結果、方針から外れた融資が適切に上位へ報告されていないことが示されれば、その理由を調査する（例：不適切なアクセス、ソフトウェアのコントロールの欠如、例外レポートのレビューをしていないこと）。 ■ 取締役会および経営会議／審査委員会の議事録をレビューし、方針から外れた融資に関する議論と下された決定を識別する。 ■ 例外レビューのプロセスをウォークスルーし、コントロールの弱点を識別する。 ■ 過去の不適切に承認された方針から外れた融資をレビューし、違反の程度に応じて適切な結果となることを確認する。 ■ 融資申請書類のサンプルを抽出し、融資申請書類のレビュー者の業務を再実施し、承認された申請書類が完全であることを確認する。 ■ 全体的なテスト結果、コントロール文書、およびウォークスルーをレビューし、不正行為の何らかのパターンが存在するかどうかを識別する。もしあれば、必要に応じて、監査範囲およびサンプリングを拡大する。

資料：内部監査人協会（ＩＩＡ）

不正行為の結果

不正行為に対する処分に関して、内部監査人は「処分が犯した行為に見合うか」調査すべきである。経営者は、「寛容すぎる」と「厳しすぎる」との間のバランスをとるべきである。犯罪行為であるか、規制により明確に禁止されているか、またはその両方に該当するため、一切許容しないこととしなければならない不正行為の事例として、例えば、顧客や取引先に嘘をつくことがある。

調査すべき情報を探す他の方法には、次のような関連質問をすることが含まれる。

- 抽出した従業員は、おそらく経営者の一員かもしれないが、倫理、コンダクト、ハラスメントなどのトピックに関する必要な研修を受けなくともよいとされているか？
- 従業員は、必要な研修を受けずに顧客を直接扱う仕事をすることが許可されているか？
- 従業員は、経費精算書を、期限どおりに、かつ拒絶されずに正確に完了させているか？
- 従業員が経費精算書に不適切な費用を請求している場合はどうなるか？
- 組織体は、利益相反につながる可能性のある従業員の副業への出資および投資に関して申告を求めているか？
- 従業員は、顧客が当該顧客への信用限度を超えることを選好みで許容しているか？
- 資産運用や資産売買取引に関与する従業員は、携帯電話を使用し通話を録音する必要のある電話セールスを行っているか？
- 個人または大きなグループと関連した傾向を識別するために、不正行為の事例を長期にわたり収集し、相関関係または傾向を捉えているか？
- モニタリングおよび調査システムは見るべきものをすべて捉え、その情報は適切に分析されているか？
- 規制に違反した場合、どのような影響があるか？
- 商品開発活動では「公平な接客」を考慮しているか？

監査中にこれらの状況のいずれかが識別された場合、内部監査人は、もし発生したのであれば、その状況からどのような結果となったのかを調べるべきである。組織体の価値観に違反することによる結果が、限定的、一貫しない、または全くない場合には、価値観は無効だと判断されることがある。

報告

基準 2400（結果の伝達）は、個々の業務の結果は伝達されなければならないという点で、自明である。基準 2410（伝達の規準）の解釈指針によれば、「個々の業務レベルにおける意見は、結果についての評定、結論またはその他の記述であってもよい。このような個々の業務は、特定のプロセス、リスクまたはビジネス・ユニットを取り巻くコントロール手段に関係している場合がある。このような意見を形成するには、個々の業務の結果とその重大性を考慮する必要がある。」としている。

コンダクト・リスクに焦点を当てた監査の結果の伝達

内部監査人は、取締役会とコンダクトに関する発見事項を議論するための会議を、年に一度開催するよう要望するかもしれない。

この会議は、非公式な議論であっても構わないが、ＣＡＥは取締役会と議論を行う前には、結果について経営者に事前説明すべきである。

コンダクトに関連する課題の報告は慎重な取扱いを必要とするかもしれないが、ＣＡＥには、最高経営者および取締役会に対して、明確、簡潔、かつ率直に伝達する責任がある。テストの結果に焦点を当て、事実に基づき、監査チームの結論を正確に伝達する報告が最も効果的である。

付録Ａ．関連するＩＩＡの「基準」およびガイダンス

このプラクティス・ガイドでは、次のＩＩＡ資料が参照されている。「内部監査の専門職的実施の国際基準」を適用するためのより詳しい情報は、ＩＩＡの「実施ガイド」（編集注：https://global.theiia.org/standards-guidance/recommended-guidance/Pages/Practice-Advisories.aspx、個別のガイド類を参照するにはＩＩＡ国際本部会員のＩＤ、パスワードが必要）を参照されたい。

「倫理綱要」
誠実性
秘密の保持
「基準」
基準 2050- 連携と依拠
基準 2060- 最高経営者および取締役会への報告
基準 2200- 内部監査（アシュアランスおよびコンサルティング）の個々の業務に対する計画の策定
基準 2201- 計画の策定における考慮事項
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
基準 2220- 内部監査（アシュアランスおよびコンサルティング）の個々の業務の範囲
基準 2230- 内部監査（アシュアランスおよびコンサルティング）の個々の業務への資源配分
基準 2240- 内部監査（アシュアランスおよびコンサルティング）の個々の業務の作業プログラム
基準 2300- 内部監査（アシュアランスおよびコンサルティング）の個々の業務の実施
基準 2330- 情報の文書化
基準 2400- 結果の伝達
基準 2410- 伝達の規準
関連するＩＩＡの資料
プラクティス・ガイド「Auditing Culture」2019 年
プラクティス・ガイド「Auditing Third-party Risk Management」2018 年 ＊編集注：邦訳は「サードパーティに関するリスク・マネジメントの監査」『月刊監査研究』2019 年９月号掲載
プラクティス・ガイド「Coordination and Reliance: Developing an Assurance Map」2018 年 ＊編集注：邦訳は「連携と依拠：アシュアランス・マップの作成」『月刊監査研究』2019 年２月号掲載
プラクティス・ガイド「Engagement Planning: Assessing Fraud Risks」2017 年 ＊編集注：邦訳は「個々の監査業務の計画策定：不正リスクの評価」『月刊監査研究』2018 年７月号掲載
プラクティス・ガイド「Engagement Planning: Establishing Objectives and Scope」2017 年 ＊編集注：邦訳は「個々の監査業務の計画策定 : 目標と範囲の設定」『月刊監査研究』2018 年３月号掲載
プラクティス・ガイド「Foundations of Internal Auditing in Financial Services Firms」2019 年

付録Ｂ．用語一覧

アスタリスク（*）を付した用語は、ＩＩＡの「専門職的実施の国際フレームワーク」2017 年版の「用語一覧」から引用した。

Chief Audit Executive * **＜内部監査部門長＞**－内部監査部門長とは、内部監査基本規程および「専門職的実施の国際フレームワーク」の必須の構成要素に従って、内部監査部門を有効に管理する職責を負う高い階層の地位にある者の職務を指す。内部監査部門長または内部監査部門長に直属する者は、適切な専門職資格や認定を持つ必要がある。内部監査部門長の具体的な肩書や職責は、組織体により様々である。

competency ＜専門的能力＞－内部監査人は、内部監査業務の実施に当たり必要な知識、技能および経験を用いる[8]。

confidentiality ＜秘密の保持＞－内部監査人は、入手する情報の価値およびその情報の所有権（ownership）を尊重し、法的なまたは専門職としての開示義務がない限り、適切な権限なしには情報を開示してはならない[8]。

Internal Audit Activity * **＜内部監査部門＞**－組織体に価値を付加し、組織体の運営を改善するために行われる、独立にして、客観的な、アシュアランス業務およびコンサルティング業務を提供する、部門、部、コンサルタントのチームまたはその他の専門家をいう。内部監査部門は、ガバナンス、リスク・マネジメントおよびコントロールの各プロセスの有効性の評価、改善を、内部監査の専門職として規律のある姿勢で体系的な手法をもって行うことによって、組織体の目標の達成に貢献する。

objectivity * **＜客観性＞**－内部監査人の公正不偏な精神的態度であり、客観性があることにより、内部監査人は、自己の業務（work）の成果を真に確信し、かつ品質を害さない方法で、個々の業務を遂行することができる。客観性は、内部監査人に対して、監査上の諸問題に関する判断を他人に委ねないことを求めている。

Risk appetite * **＜リスク選好＞**－組織体が積極的に受容するリスクのレベル。

8. *International Professional Practices Framework* (Altamonte Springs, FL: The IIA, 2017), 34.
https://bookstore.theiia.org/international-professional-practices-framework-ippf-2017-edition.（編集注：邦訳は、『専門職的実施の国際フレームワーク－ 2017 年版－』37 頁）

付録Ｃ．参考文献とさらなる学習のための文献

参考文献

Basel Committee on Banking Supervision, *Overview of Pillar 2 supervisory review practices and approaches*, Basel, Switzerland: Bank for International Settlements, July 2019. https://www.bis.org/bcbs/publ/d465.pdf.

Chaly, Stephanie, James Hennessy, Lev Menand, Kevin Stiroh, and Joseph Tracy. *Misconduct Risk, Culture, and Supervision*. New York: Federal Reserve Bank of New York, 2017. https://www.newyorkfed.org/medialibrary/media/governance-and-culture-reform/2017-whitepaper.pdf.

Chartered Institute of Internal Auditors. *Conduct risk*. October 2, 2019. https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/conduct-risk/?downloadPdf=true.

Clayton, Sarah."6 Signs Your Corporate Culture Is a Liability." *Harvard Business Review*, December 5, 2019. https://hbr.org/2019/12/6-signs-your-corporate-culture-is-a-liability.

Financial Conduct Authority. *FCA Handbook, COCON, COCON 2*. Last updated March 7, 2016. https://www.handbook.fca.org.uk/handbook/COCON/2/?view=chapter.

Financial Conduct Authority. *Progress and Challenges: 5 Conduct Questions*. May 2019. https://www.fca.org.uk/publication/market-studies/5-conduct-questions-industry-feedback-2018-19.pdf.

The IIA. *International Professional Practices Framework*. Altamonte Springs: Internal Audit Foundation, 2017. https://bookstore.theiia.org/international-professional-practices-framework-ippf-2017-edition.

さらなる学習のための文献

Australian Securities and Exchange Commission. Market Supervision Update Issue 57."Conduct Risk." Accessed April 17, 2020. https://asic.gov.au/about-asic/corporate-publications/newsletters/asic-market-supervision-update/asic-market-supervision-update-previous-issues/market-supervison-update-issue-57.

Chartered Institute of Internal Auditors. "Financial Services Code: Effective Internal Audit in the Financial Services Sector, Second Edition."September 2017. https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/financial-services-code/.

Chartered Institute of Internal Auditors."Conduct risk. "April 14, 2020. https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/conduct-risk/?downloadPdf=true.

Clayton, Jay. SEC. "Observations on Conduct at Financial Institutions and the SEC,"speech delivered in New York, June 18, 2018.
https://www.sec.gov/news/speech/speech-clayton-061818.

Department of the Treasury, Office of the Comptroller of the Currency（US）. "OCC Guidelines stablishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of 12 CFR Parts 30 and 170."September 11, 2014.
https://www.govinfo.gov/content/pkg/FR-2014-09-11/pdf/2014-21224.pdf.

European Banking Authority."Guidelines for Common Procedures and Methodologies for the Supervisory Review and Evaluation Process（SREP）and Supervisory Stress Testing. "Accessed April 17, 2020.
https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing.

European Systemic Risk Board. "Report on Misconduct Risk in the Banking Sector." June 2015.
https://www.esrb.europa.eu/pub/pdf/other/150625_report_misconduct_risk.en.pdf.

Financial Conduct Authority. "Progress and Challenges: 5 Conduct Questions." May 2019.
https://www.fca.org.uk/publication/market-studies/5-conduct-questions-industry-feedback-2018-19.pdf.

Financial Conduct Authority（UK）. "Transforming Culture in Financial Services"Discussion Paper. March 12, 2018.
https://www.fca.org.uk/publication/discussion/dp18-02.pdf.

Financial Stability Board. "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture." April 7, 2014.
https://www.fsb.org/2014/04/guidance-on-supervisory-interaction-with-financial-institutions-on-risk-culture-a-framework-for-assessing-risk-culture-2/.

Financial Stability Board. "Recommendations for Consistent National Reporting of Data on the Use of Compensation Tools to ddress Misconduct Risk." May 7, 2018.
https://www.fsb.org/2018/05/recommendations-for-consistent-national-reporting-of-data-on-the-use-of-compensation-tools-to-address-misconduct-risk/.

FINRA. "Targeted Examination Letter on Establishing, Communicating, and Implementing Cultural Values." February 2016.
https://www.finra.org/rules-guidance/guidance/targeted-exam-letter/establishing-communicating-and-implementing-cultural-values.

Glazer, Emily. "Wells Fargo to Refund $80 Million to Auto-Loan Customers for Improper Insurance Practices," Wall Street Journal, July 28, 2017.
https://www.wsj.com/articles/wells-fargo-to-refund-80-million-to-auto-loan-customers-for-improper-insurance-practices-1501252927.

Monetary Authority of Singapore. "Framework for Impact and Risk Assessment of Financial Institutions." September 2015.
https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/MAS%20Framework%20for%20Impact%20and%20Risk%20Assessment%20of%20Financial%20Institutions.pdf.

Ngiap, Lee Boon. Monetary Authority of Singapore. “Culture and Conduct ? A Regulatory Perspective,” speech presented to the 2017 Annual Luncheon of the Life Insurance Association of Singapore, March 6, 2017. https://www.mas.gov.sg/news/speeches/2017/culture-and-conduct.

Office of the Comptroller of the Currency（US）. Comptroller's Handbook: Corporate and Risk Governance, p 15. Version 2.0, July 2019. https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/index-corporate-and-risk-governance.html.

Price, John. Australian Securities and Investments Commission. “Outline of ASIC's Approach to Corporate Culture,” speech presented at the AICD Directors' Forum: Regulators' Insights on Risk Culture, Sydney, Australia, July 19, 2017. https://download.asic.gov.au/media/4393665/john-price-speech-aicd-regulator-insights-on-risk-culture-published-20-july-2017.pdf

Risk.net. “Asia-Pacific Banks Grapple with Conduct Risk Rules.” May 13, 2018. https://www.risk.net/risk-management/5595381/asia-pacific-banks-grapple-with-conduct-risk-rules.

Yuen, Arthur. Hong Kong Monetary Authority. “Bank Culture Reform.” March 2, 2017, letter to the chief executive of all authorized institutions. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2017/20170302e2.pdf.

謝辞

ガイダンス策定チーム

Jose Esposito, CIA, CRMA, Peru（Chairman）

Stacey Schabel, CIA, United States（Project Lead）

Mark Carawan, CIA, QIAL, United States

Trevor Brookes, CIA, CRMA, Bermuda

Ian Stuart Lyall, CIA, CCSA, CGAP, CRMA, Australia

John J. Mickevice, CIA, CRMA, United States

Juergen Rohrmann, CIA, Germany

Teis Stokka, CIA, CRMA, Norway

グローバル・ガイダンス策定協力者

Tan Dang, CIA, Vietnam

Najeeb Haq, CIA, CFSA, Canada

David Hill, CIA, QIAL, United Kingdom

Adrian Kyburz, CIA, CRMA, Switzerland

Silvia Tapia Navarro, CIA, Mexico

Thomas Bang van Dijk, CIA, CFSA, CRMA, Denmark

ＩＩＡ国際およびガイダンス作成委員会

Jeanette York, CCSA, FS Director（Project Lead）

Jim Pelletier, CIA, CGAP, Vice President

Anne Mercer, CIA, CFSA, Director

P. Michael Padilla, CIA, IT Director

Chris Polke, CGAP, PS Director

Shelli Browning, Technical Editor

Lauressa Nelson, Technical Editor

Geoffrey Nordhoff, Content Developer, Technical Writer

Christine Janesko, Content Developer, Technical Writer

Vanessa Van Natta, Standards and Guidance Specialist

ＩＩＡは次の監督機関の支援に感謝する。Financial Services Guidance Development Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

内部監査人協会（ＩＩＡ）について

内部監査人協会（ＩＩＡ）は、内部監査という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。

免責事項

ＩＩＡは、この文書を情報提供および教育目的で公表しているのであって、特定の状況に対する決定的な解決策を提供することを意図している訳ではなく、ガイドとして使われることを意図しているだけである。ＩＩＡは、特定の状況に対応する場合は常に、独立した専門家からその状況に直接関係した助言を求めることをお勧めする。ＩＩＡは、このガイダンスのみに依拠した者に対し責任を負うものではない。

著作権

2020 年 5 月

The Institute of Internal Auditors | Global

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org