COSO

トレッドウェイ委員会支援組織委員会

全社的リスクマネジメント

コンプライアンス リスクマネジメント： COSO ERM フレームワークの適用

SCCE Society of Corporate Compliance and Ethics

企業のコンプライアンスと倫理協会

HCCA Health Care Compliance Association

医療コンプライアンス協会

著　者

企業のコンプライアンスと倫理協会および医療コンプライアンス協会（ＳＣＣＥ＆ＨＣＣＡ）

トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）理事

ポール・J．ソーベル
ＣＯＳＯ会長

ダグラス・F．プラット
米国会計学会

ロバート・D．ドーラ―
米国公認会計士協会

ダニエル・C．マードック
国際財務担当経営者協会

ジェフリー・C．トムソン
管理会計士協会

パティ・K．ミラー
内部監査人協会

序　文

本プロジェクトは、トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）から委嘱されたものである。ＣＯＳＯは、組織のパフォーマンスや監督を改善するとともに、組織における不正を減らすために立案された内部統制、全社的リスクマネジメントおよび不正抑止に関する包括的なフレームワークとガイダンスの開発を通じて先進的な考え方を提供することに取り組んでいる。ＣＯＳＯは、次の団体の協賛と資金提供によって運営されている民間部門主導の団体である。

米国会計学会（American Accounting Association）

米国公認会計士協会（American Institute of Certified Public Accountants）

国際財務担当経営者協会（Financial Executives International）

管理会計士協会（Institute of Management Accountants）

内部監査人協会（Institute of Internal Auditors）

COSO
トレッドウェイ委員会
支援組織委員会
coso.org

全社的リスクマネジメント

コンプライアンス リスクマネジメント： ＣＯＳＯ ＥＲＭ フレームワークの適用

調査委嘱者

COSO

トレッドウェイ委員会支援組織委員会

2020 年 11 月

Design and production: Sergio Analco.

目　次

ページ

1．はじめに

本稿が必要とされる理由

コンプライアンスリスクは、組織の目標を達成する上で一般的なリスクであり、重大なリスクであることが多い。長年にわたり、コンプライアンス専門家は、コンプライアンス違反やその他の不正行為を予防し、また、適時に発見するために、広く認められたコンプライアンスと倫理（C＆E）プログラムのフレームワークを使用してきた。C＆Eプログラムのフレームワークは、付録1に記載している（読者がC＆Eプログラムの要素にまだ精通していない場合、先に進む前に付録1を読むことを検討されたい）。一方、トレッドウェイ委員会支援組織委員会（COSO）の全社的リスクマネジメント（ERM）フレームワークは、コンプライアンスリスクを含むさまざまな組織のリスクを識別して軽減するために、リスク専門家などに利用されてきた。

本稿は、COSO ERMフレームワークをC＆Eプログラムのフレームワークと連携させ、これらの貴重なフレームワークのそれぞれの基礎となる概念を統合する強力なツールを作成することにより、コンプライアンスリスクの識別、評価および管理に適用するためのガイダンスを提供することを目的としている。

コンプライアンスリスクおよびコンプライアンス関連リスクとは何か

COSOは、リスクを「事象が発生し、戦略と事業目標の達成に影響を及ぼす可能性」と定義している。この定義で考慮するリスクには、コンプライアンスを含むすべての事業目標に関連するものが含まれる。コンプライアンスリスクとは、適用される法律、規制、契約条件、基準または内部方針などに違反する可能性に関するリスクであり、その違反により、組織や従業員に直接的または間接的な金融負債、民事・刑事罰、規制上の制裁またはその他の悪影響が生じる可能性である。本稿では、コンプライアンスリスクに関連する「事象」を「コンプライアンス違反」[i]と表記する。

コンプライアンス違反は、基本的には個人の作為（または不作為）であるが、組織の従業員や代理人が通常の職務として行った場合は、組織に帰属すると考えるのが一般的である。組織に帰属する行為の正確な範囲は、状況により異なる。また、場合によっては、従業員が個人としての責任を負うこともある。

コンプライアンス違反の大部分は、個人、地域社会または組織に潜在的に害を及ぼすか、直接的な害を及ぼす可能性がある。コンプライアンス違反によって被害を受ける可能性のある当事者の例には、顧客（例：個人情報の漏洩や盗難につながる個人情報保護法違反やデータセキュリティ法違反、怪我につながる製品安全法違反、価格高騰につながる独占禁止法違反）、従業員（例：労働者の怪我につながる労働安全規則違反、差別禁止法違反や公益通報者保護法違反）、一般市民（例：病気や死亡につながる環境法違反）などがある。

コンプライアンスリスクの大部分は、特定の法令に関連するものであるが、そうでないものもある。このようなその他のリスクは「コンプライアンス関連リスク」と呼ばれ、職業上の基準、（行動規範や企業倫理を含む）組織の内部方針および契約上の義務の違反に関連するリスクが含まれる場合がある。例えば、利益相反は、（政府の関係者やプログラムが関与することが多い）限定的な場合にのみ、法令違反となる。利益相反は、職業上の基準、契約条件や補助金協定または内部方針によって禁止されていることが多く、開示や管理がされないと組織に損害を与えると考えられる。そのため、利益相反は一般的にコンプライアンスリスクの母集団に含まれる。

したがって、本稿では、法令に直接関連するリスク、またはその他の基準、組織の方針、倫理的な期待やガイドラインに関連するコンプライアンス関連リスクを指して「コンプライアンスリスク」という用語を使用している。

この議論が示すように、組織がコンプライアンスリスクの範囲を捉えるための厳密な体系的方法はないものの、大部分の組織では、各領域における具体的なコンプライアンスリスクは異なっていても、プログラムの対象領域として類似のリスト（例：環境、贈収賄、汚職）を使用している。C＆Eプログラムの厳密な範囲を決定することは、通常、プログラム開発の初期段階であると同時に、リスクの状況が変化し、コンプライアンス、法務、上級幹部[ii]および取締役会からの情報が考慮されるにつれて、継続的に行われる作業でもある。

---

[i] 訳注：原文は「"noncompliance" or "compliance violations"」であるが、日本語では両方とも「コンプライアンス違反」と訳されることが多いため、ここでは両方を合わせて「コンプライアンス違反」とし、以後も同様とした。

[ii] 訳注：本稿では「senior leader」「senior executive」を「上級幹部」と訳した。

コンプライアンス違反は、しばしば罰金、科料、民事上の和解金または類似の金融負債につながる。しかし、すべてのコンプライアンス違反に直接の財務的な影響があるわけではない。場合によっては、当初の影響は純粋に評判に関わることもある。しかし、評判の低下は、顧客の喪失から従業員の喪失、競争上の不利益またはその他の影響（例：事業停止や契約からの排除）に至るまで、将来の財務的または非財務的な損害につながることが多い。

コンプライアンス違反の大部分は、内部関係者である従業員、経営者または組織の取締役による行為に起因している。リスクはまた、その行為が組織に影響を及ぼす請負業者やその他の第三者から生じることがますます増えている。最も一般的な例では、組織のサプライチェーンに関わるベンダー（例：エジプト綿の寝具を供給する大手小売業者数社が、エジプト産ではない品質等級の低い綿を使用していたことが判明し、小売業者が顧客に対して多額の債務を負った）、または販売サイクルに関わる第三者（例：組織にとって有利な契約を得るために政府関係者に賄賂を支払う可能性のある仲介業者）が関与している。

プログラムの範囲を決定する上で最後に考慮すべきことは、合併や買収（M＆A）に起因するリスク継承の可能性である。M＆Aが行われると、組織が曝されるコンプライアンスリスクの対象領域が大幅かつ瞬時に変化する可能性がある。これらのリスクは、合併前に発生した事象に関連する場合もあれば、買収者がそれまで直面していなかった、合併後の企業が直面する特有のリスクに起因する場合もある。

コンプライアンスと倫理のプログラムの進化

コンプライアンスは長年にわたって期待されてきたが、専門職としての、また組織内の別個の機能としてのコンプライアンスと倫理は、比較的最近になって発展してきたものである。これは、C＆Eプログラムが組織管理にとって価値があり、頻繁に必要とされる要素として、同様に最近浮上したことに起因している。

米国では 1980 年代に一連の事件が発生し、1991 年に米国量刑委員会（U.S. Sentencing Commission）が法律に違反した組織に対する処罰のガイドラインを発表した。その条項の中で、組織に対する量刑ガイドラインは、組織が効果的なコンプライアンスプログラムを整備している場合、刑事罰が非常に大きく軽減されることを規定している。2004 年と 2010 年には、効果的なプログラムの特徴を明確にして拡大するために、重要な改正が行われた。

現行の米国連邦量刑ガイドライン（U.S. Federal Sentencing Guidelines：USSG）では、効果的なC＆Eプログラムの7つの要素を以下のように定めている。

1. 基準と手続
2. ガバナンス、監督および権限
3. 権限委譲におけるデューディリジェンス[iii]
4. コミュニケーションと研修
5. モニタリング、監査および通報制度
6. インセンティブとエンフォースメント[iv]
7. 不正行為への対応

これとは別に、USSGは、組織がコンプライアンス違反のリスクを定期的に評価することと、C＆Eプログラムを改善する方法を継続的に模索することも求めている。この2つの要件は、効果的なプログラムの8番目の要素と呼ばれることが多い。これらの各要素については、付録1でさらに詳しく説明している。

また、USSGは、組織は倫理的な行動と法律の遵守を奨励するカルチャーを促進すべきであると述べている。このように、組織のカルチャーや企業倫理がコンプライアンスリスクマネジメントに不可欠な役割を果たすと認識されていることが、「コンプライアンスと倫理のプログラム」または「C＆Eプログラム」という用語が一般的に使われるようになった要因の1つである。

USSGは、いかなる組織に対してもC＆Eプログラムを義務づけているわけではないが、組織が連邦法に違反した場合に生じ得る多額の罰金を軽減する手段として、そのようなプログラムの確立にインセンティブを与えている。法律違反を伴う刑事事件の場合、一部では効果的なC＆Eプログラムの存在によって、組織の罰金が決定された基準額から大幅に減額されることがある。量刑ガイドラインに関連した判例法が発展したことで、特に規制の厳しい企業においてC＆Eプログラムの重要性がさらに強調されており、裁判所は、効果的なC＆Eプログラムを実施しないことは受託者義務違反となる可能性があると結論づけている。さらに、米国司法省やその他の機関が発行したガイダンスも、C＆Eプログラムの重要性を強調している。

USSGは、組織に対してC＆Eプログラムを義務づけていないが、個々の政府機関がC＆Eプログラムを義務づけることがある。例えば、特定の医療機関は、メディケア[v]への参加資格条件としてコンプライアンスプログラムを持たなければならず、また、連邦調達規則（Federal Acquisition Regulations）は、特定の政府請負業者にコンプライアンスプログラムを持つよう求めている。

[iii] 訳注：「due diligence」は、国際法では「相当の注意」の意味。企業などに要求される当然に実施すべき注意義務および努力のこと。ビジネス用語では、投資や取引を行うにあたって、対象先の価値やリスクなどを調査すること。

[iv] 訳注：「enforcement」は、法や規則の執行のこと。罰則を科すことをエンフォースメントと呼ぶ場合もある。また、違反に対する是正や制裁といった実効性確保の仕組みを指す場合もある。

[v] 訳注：「Medicare」は、米国の高齢者向け医療保険制度。

最後に、コンプライアンス部門は、法務部門や規制担当部門から独立した存在とすべきである。この独立性は一般的には要求されていないが、2つの機能の責任は異なり、時には相反することもあるため、望ましい慣行として急速に広まってきている。例えば、米国保健福祉省監察総監室（Office of Inspector General of the U.S. Department of Health and Human Services：HHS OIG）が発行したガイダンスでは、コンプライアンス部門は独立した存在とすべきとされている。HHS OIGの医療不正防止およびエンフォースメント活動チーム（Health Care Fraud Prevention and Enforcement Action Team：HEAT）は、2012年の「医療機関の理事会のためのツールキット（*A Toolkit for Health Care Boards*）」の中で、「コンプライアンス責任者を法務顧問や上級経営者とは別の者にすることで、その独立性を確保しなければならない。コンプライアンス責任者の雇用に影響を与えたり、コンプライアンスプログラムの範囲を制限したりするすべての決定は、事前に理事会の承認を得るべきである」と述べている。

コンプライアンスと倫理のプログラムに関する国際的なガイダンス

C&Eプログラムに関する法律上、規制上および規制以外の最も広範囲なガイダンスは米国から発せられているが、他の多くの国々もC&Eプログラムに関するさまざまな形式の要件やガイダンスを発表している。一部の例として、米国外のC&Eプログラムに関するガイダンスは、贈収賄や汚職または独占禁止や競争のように、法律の特定領域に限定して適用されている場合がある。また、米国と同様に、より広範で多くの法律領域に適用されている場合もある。国際的に発表されているガイダンスの多くは、USSGに記載されている概念や要素の多くを反映している。

米国外のガイダンスをいくつか見てみると、規制当局がC&Eプログラムに期待することは、ほぼ一貫していることがわかる。例えば、英国法務省（Ministry of Justice）は2010年贈収賄禁止法（Bribery Act 2010）に関するガイダンスを示し、贈収賄のリスクを最小限にするために営利組織が整備できる手続について説明している。これらの手続は、以下の6つの原則にまとめられており、USSGと整合している。

1. 相応の手続
2. トップレベルのコミットメント
3. リスク評価
4. デューディリジェンス
5. （研修を含む）コミュニケーション
6. モニタリングとレビュー

ガイダンスは、国際標準化機構（ISO）からも発表されている。2016年版ISO 37001「贈収賄防止マネジメントシステム」規格には、プログラムに対する次の期待が含まれている。

1. 贈収賄リスク評価の実施
2. 贈収賄防止マネジメントシステムに対するリーダーシップとコミットメント
3. 贈収賄防止コンプライアンス機能の確立
4. 贈収賄防止マネジメントシステムのための十分な資源の提供
5. 従業員の能力
6. 贈収賄防止に関する方針についての認識と研修
7. 第三者の取引関係者と従業員に関するデューディリジェンス
8. 贈収賄防止統制の確立と導入
9. 贈収賄防止マネジメントシステムの内部監査
10. 統治機関による贈収賄防止マネジメントシステムの定期的なレビュー

贈収賄以外にも、ISOはISO 19600:2014という形で、より広くコンプライアンスマネジメントシステムに関するガイダンスを発表している。最近では、ISO 19600に代わるものとして、2020年にISO/DIS 37301が提案された。この新規格案では、コンプライアンスマネジメントシステムの以下の5つの要素について説明している。

1. コンプライアンス義務（新規および変更されたコンプライアンス要件の識別）
2. コンプライアンスリスク評価
3. コンプライアンス方針
4. 研修とコミュニケーション
5. パフォーマンス評価

C&Eプログラムに直接言及しない他のさまざまな法律や規制の進展であっても、C&Eプログラムに影響を与える。例えば、内部通報者に対して新たな保護を提供することを目的とした2019年の欧州連合の規制は、効果的なC&Eプログラムの重要な要素を支援するのに役立っている。同様に、データ保護法や個人情報保護法は国によって異なるのが一般的であるが、C&Eプログラムに直接的または間接的な影響を及ぼすことがよくある。

C&Eプログラムに関する国際的なガイダンスのその他の例は、付録2に記載している。ここからわかるのは、C&Eプログラムの適用範囲が異なる（すなわち、ある法域では贈収賄と汚職に限定し、別の法域ではより広範囲に適用するなど）としても、C&Eプログラムに関する国際的なガイダンスは、相違点よりも類似点の方がはるかに多いということである。これらのさまざまなガイダンスに共通するテーマは、このCOSOのガイダンスのベースとなる要素に対する認識を共有することである。

コンプライアンス、内部統制および全社的リスクマネジメントの関係

ＣＯＳＯは、「内部統制の統合的フレームワーク」（2013 年）、「全社的リスクマネジメント－戦略およびパフォーマンスとの統合」（2017 年）の中で、内部統制を以下のように定義している。

> *業務、報告およびコンプライアンスに関連する目的の達成に関して合理的保証を提供するために整備された、事業体の取締役会、経営者およびその他の構成員により実行される１つのプロセス。*

この定義が明確に指摘しているように、内部統制は会計や財務だけの問題ではない。コンプライアンスは、組織の内部統制システムの３つの基本的な目的の１つである。内部統制の次の５つの構成要素は、３つのカテゴリーの目的すべてを支えている。

- 統制環境
- リスク評価
- 統制活動
- 情報と伝達
- モニタリング活動

３つの目的、５つの構成要素および事業体の関係を図１．１で示す。

図１．１　2013 年版ＣＯＳＯフレームワーク

出典：COSO Internal Control Framework ©2013（邦訳は、八田進二・箱田順哉監訳、日本内部統制研究学会新ＣＯＳＯ研究会訳『ＣＯＳＯ 内部統制の統合的フレームワーク』日本公認会計士協会出版局、2014 年）

ＣＯＳＯは、ＥＲＭを以下のように定義している。

> *組織が価値を創造し、維持し、および実現する過程において、リスクを管理するために依拠する、戦略策定ならびにパフォーマンスと統合されたカルチャー、能力、実務。*

ＣＯＳＯのＥＲＭフレームワークは、内部統制フレームワークと同様に、相互に関連する５つの要素で構成されている。

- ガバナンスとカルチャー
- 戦略と目標設定
- パフォーマンス
- レビューと修正
- 情報、伝達および報告

図１．２　リスクマネジメントの構成要素

出典：COSO Enterprise Risk Management – Integrating with Strategy and Performance（邦訳は、一般社団法人日本内部監査協会・八田進二・橋本　尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会ＣＯＳＯ - ＥＲＭ研究会訳『ＣＯＳＯ全社的リスクマネジメント－戦略およびパフォーマンスとの統合』同文舘出版、2018 年）

ＥＲＭは、内部統制とは異なるが関連している。ＥＲＭは、内部統制の概念の一部を取り入れている。実際、内部統制の導入は、リスクを低減するための最も一般的なアプローチである。しかし、ＥＲＭは、内部統制の中では考慮されない特定の概念も含んでいる。例えば、リスク選好、許容度、戦略および事業目標の概念は、ＥＲＭ内で設定されるが、内部統制では前提条件として捉えられている。ＥＲＭは、内部統制よりも戦略との整合性がより高い。

ＥＲＭの重要な側面は、価値の創造、維持および実現に焦点を当てていることである。Ｃ＆Ｅプログラムは、これら３つの目標それぞれを支援する。効果的なＣ＆Ｅプログラムによって、組織はより自信を持って新たな価値創造の機会を追求できるようになる。なお、組織が創造した価値は、法令違反を伴うとすぐに損なわれる可能性がある。効果的なＣ＆Ｅプログラムは、組織がこの価値を維持して十分に実現することを可能にする。

したがって、コンプライアンスリスクの管理は、組織の内部統制および広範なＥＲＭの機能やプロセスの両方の重要な要素である。

組織内でのコンプライアンス機能の範囲と位置づけ

前述のとおり、コンプライアンスリスクには、一般的に法令違反のリスクが含まれるが、契約条項、職業上の基準、組織の方針および倫理的な問題が扱われる場合もある。しかし、コンプライアンスプログラムの範囲に含まれる法令は、業種や組織によって異なる場合がある。例えば、海外腐敗行為防止法（Foreign Corrupt Practices Act）に違反するリスクは、明らかに企業のＣ＆Ｅプログラムの範囲に含まれる可能性がある。しかし、米国証券取引委員会（ＳＥＣ）への提出書類で要求される会計基準の遵守は、経理・財務機能内で対応され、Ｃ＆Ｅプログラムの範囲外と考えられる可能性もある。人事や雇用法のリスクは、完全に人事機能が管理する場合もあれば、コンプライアンス機能もこれらのリスクの管理に関与する場合がある。

組織のＣ＆Ｅプログラムの範囲については、普遍的に受け入れられている定義はない。組織によって異なる場合がある。その結果、一部の法令の遵守は、主として別の機能の監督の対象となる可能性があるが、別の機能がリスクを適切に管理できない、または管理する意思がない場合、コンプライアンス機能は常に包括的な役割を果たすか、支援や問題解決のために介入できるように備えておくべきである。

もう１つの組織間の違いは、コンプライアンス機能が組織内のどこに「位置する」かである。Ｃ＆Ｅプログラムは、すべての機能領域の従業員や管理者が関与する組織全体のものであるが、コンプライアンスと倫理の専門家からなる専任チームで構成されるコンプライアンス機能は、組織図内のさまざまな場所に配置される可能性がある。大部分の組織では、コンプライアンスは独立した機能であり、これがベストプラクティスと考えられている。別の組織では、法務、内部監査、リスクマネジメントまたはその他の機能の一部であったり、その直属であったりする場合もある。コンプライアンス機能が組織図のどこに位置づけられるかにかかわらず、Ｃ＆Ｅプログラムの成功には、前述の各機能とのコミュニケーションと協働が不可欠である。

同様に、倫理はコンプライアンスとは別の機能であると考えられるかもしれない。しかし、多くの組織では、コンプライアンスと倫理は、コンプライアンス・倫理責任者の監督下に位置づけられている。

事実上、全従業員がリスクを管理する役割を担っているが、コンプライアンスリスクの管理や軽減は、主に全階層の経営者の責任であることを理解することが重要である。コンプライアンス機能は、Ｃ＆Ｅプログラムの開発を主導するが、プログラムを実施するのは最終的には経営者の仕事であり、それを監督するのは取締役会である。コンプライアンス・倫理責任者の役割は、経営者がリスクを理解するのを助け、それらのリスクを軽減して管理するためのプログラムの開発を主導し、プログラムがどの程度うまく実施されているかを評価し、対象範囲のギャップ、実施状況、あるいは上級幹部によるものを含む重大なコンプライアンス違反の事案について経営幹部に報告することである。

要するに、コンプライアンスリスクの管理は、さまざまな構造モデルの下で効果的に行うことができる。本稿は、組織構造や責任の分担方法にかかわらず、効果的なＣ＆Ｅプログラムを設計して運用するためのガイダンスを提供する。

本ガイダンスについて

本稿の対象読者には、以下が挙げられる。

1. 組織のＥＲＭプログラムをコンプライアンスリスクに適用することに携わる、リスクマネージャーや内部監査人などの専門家。
2. Ｃ＆Ｅプログラムを組織全体のＥＲＭプログラムと整合させたり統合したりすることを目指すコンプライアンス専門家。
3. コンプライアンスリスクとＣ＆Ｅプログラムをよりよく理解したい上級経営陣。
4. 取締役会の監督役割を支援する取締役。

ＵＳＳＧが策定されたとき、そして効果的なＣ＆Ｅプログラムの要素が進化してきたとき、ＥＲＭフレームワークの中に７つの要素を当てはめることは大きな関心事でも目的でもなかった。実際、この進化の多くは、2004 年にＣＯＳＯが最初のＥＲＭフレームワークを発表する前に起こった。

本ガイダンスの残りの部分では、図１．３に示すＣＯＳＯ ＥＲＭフレームワークの 20 の原則のそれぞれを、効果的なＣ＆Ｅプログラムの具体的な要件と新たな実務に対応させている。第２章では、まず、ガバナンスとカルチャーの構成要素と、それに関連する５つの原則を説明する。第３章から第６章では、その他の構成要素とそれに関連する原則をそれぞれ取り上げる。各章では、ＥＲＭの各原則について、効果的なＣ＆Ｅプログラムを導入して維持するための重要なステップを紹介する。

図１．３　リスクマネジメントの構成要素－ 20 の原則

ガバナンスとカルチャー

1. 取締役会によるリスク監視を行う
2. 業務構造を確立する
3. 望ましいカルチャーを定義づける
4. コアバリューに対するコミットメントを表明する
5. 有能な人材を惹きつけ、育成し、保持する

戦略と目標設定

6. 事業環境を分析する
7. リスク選好を定義する
8. 代替戦略を評価する
9. 事業目標を組み立てる

パフォーマンス

10. リスクを識別する
11. リスクの重大度を価する
12. リスクの優先順位けをする
13. リスク対応を実施する
14. ポートフォリオの視点を策定する

レビューと修正

15. 重大な変化を評価する
16. リスクとパフォーマンスをレビューする
17. 全社的リスクマネジメントの改善を追求する

情報、伝達および報告

18. 情報とテクノロジーを有効活用する
19. リスク情報を伝達する
20. リスク、カルチャーおよびパフォーマンスについて報告する

出典：COSO *Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、一般社団法人日本内部監査協会・八田進二・橋本　尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会ＣＯＳＯ - ＥＲＭ研究会訳『ＣＯＳＯ全社的リスクマネジメント－戦略およびパフォーマンスとの統合』同文舘出版、2018 年）

本稿で示すガイダンスを個々のコンプライアンスリスクに適用した例は、corporatecompliance.org/coso で見ることができる。

図１．４　よく使われる用語と略語

	本稿では、以下の用語や略語を頻繁に使用している
取締役会	取締役会、または必要に応じて取締役会からコンプライアンスの監督責任を委任された取締役会レベルの委員会
Ｃ＆Ｅプログラム	コンプライアンスと倫理のプログラム
ＣＣＯ	最高コンプライアンス責任者、最高コンプライアンス・倫理責任者、またはＣ＆Ｅプログラムの監督を担当する最高位の従業員に関する同等の肩書
コンプライアンス委員会	組織内のさまざまな部門や機能の従業員で構成される内部委員会であり、組織の運営を通じてコンプライアンス機能を伝達して拡大するために、ＣＣＯに助言し、情報を提供し、協力することを使命とする組織
コンプライアンスリスク	適用される法律、規制、契約条件、基準または内部方針に違反し、組織に財務的または非財務的な悪影響を与える可能性
ＤＯＪ	米国司法省
ＵＳＳＧ	米国連邦量刑ガイドライン

2．コンプライアンスリスクのガバナンスとカルチャー

本章では、ＣＯＳＯ ＥＲＭフレームワークの「ガバナンスとカルチャー」の構成要素を、コンプライアンスリスクの管理に適用することについて説明する。ＣＯＳＯフレームワークでは、この構成要素の根底にある次の５つの原則を説明している。

1. 取締役会によるリスク監視を行う
2. 業務構造を確立する
3. 望ましいカルチャーを定義づける
4. コアバリューに対するコミットメントを表明する
5. 有能な人材を惹きつけ、育成し、保持する

原則１－取締役会によるリスク監視を行う

取締役会は、組織のＣ＆Ｅプログラムを監督する責任があり、経営者は、プログラムの設計と運用に責任がある。取締役会の監督に対する期待は、数か国で公布されたＣ＆Ｅプログラム基準で強化されている。例えば、ＵＳＳＧ 第８章パートＢ２．１サブセクション（ｂ）（２）（Ａ）～（Ｃ）は、企業の「統治機関は、コンプライアンスと倫理のプログラムの内容と運用について知識を有するものとし、また、合理的な監督を行うものとする」と述べている。

組織のＣ＆Ｅプログラムが複雑である可能性を考慮すると、一般に監査の監督が監査委員会に委ねられるのと同様に、取締役会がこの監督責任を取締役会レベルの常任委員会に委ねることが望ましい場合が多い。これにより、委員会は、取締役会全体では不可能と思われる監督に十分な時間を割くことができるようになる。前述のとおり、「取締役会」という用語は、取締役会またはＣ＆Ｅプログラムの監督責任を持つ取締役会レベルの委員会のいずれかを指すものとして使用されている。

監督が適切に行われるためには、ＣＣＯと取締役会の間にオープンで直接的なコミュニケーションラインがなければならない。このコミュニケーションには、取締役会が他の上級経営者を同席させずにＣＣＯと個人的に会う会合のような、一定の間隔で予定される定期的な会合を含めるべきである。

取締役会にコンプライアンスの専門知識があることは、非常に価値があり、プログラムの監督が強化できる。理想的には、この専門知識が、関連性のあるコンプライアンス問題に関する業界特有の経験や、効果的なコンプライアンスプログラムの開発と管理の経験からもたらされるとよい。

また、取締役会は、Ｃ＆Ｅプログラムを支援するために、十分な人員と資源、およびプログラムの目的を達成するための適切な権威と権限付与を含む、効果的なコンプライアンス監督のためのインフラが整備されるようにすべきである。このインフラには、内部のコンプライアンス委員会が含まれることもある。多くの場合、主要な機能や事業部門から成る内部コンプライアンス委員会は、ＣＣＯがオープンなコミュニケーションラインを維持し、エマージングコンプライアンスリスク領域を適時に認識し、リスクを軽減して対処する方法について重要な意見と賛同を得るのに効果的な方法である。

表２．１　取締役会によるリスク監視を行う

主要な特徴	• 取締役会に対して、コンプライアンスと倫理の基本規程の承認を含む、コンプライアンスリスクマネジメントとＣ＆Ｅプログラムの監督を義務づける • 取締役会がＣ＆Ｅプログラムについて熟知して、その監督を実際に行うようにする（議題の定例化、コンプライアンス指標のモニタリング、ＣＣＯ等との定期的なエグゼクティブ・セッション[vi]の開催） • 取締役会にコンプライアンスに関する専門知識を持つ者を含めることを要求する • Ｃ＆Ｅプログラムに対する取締役会の監督の証拠を議事録に記録する • ＣＣＯの任命・解任・配置転換について意見を述べたり承認したりして、独立性を確保する • Ｃ＆Ｅプログラムに十分な資源が確実に提供されるようにする • ＣＣＯから定期的に報告を受ける • 重要な調査と是正措置について、取締役会が確実に情報を入手して意見を述べる

[vi] ＣＣＯ以外の上級経営者を含まない会合。

原則２－業務構造を確立する

組織内でのコンプライアンス機能の位置づけは、プログラムの有効性に重要な影響を与える。コンプライアンス機能は、効果的に機能するように位置づけられた人物が率いるべきであり、それは通常、他の上級幹部と同格の者であることを意味する。さらに、コンプライアンス機能は、その任務を効果的に果たすために、実質的な権限、資源およびツールを持たなければならない。最後に、コンプライアンス機能は、他の機能、特に規制当局から相反する義務や優先事項を持つと思われがちな機能（例：法務、財務など）とは、職務上、分離して独立させるべきである。コンプライアンスと倫理の機能を他の部門内に位置づけることで効果が上げられる可能性もあるが、望ましい実務は、内部監査と同様に、コンプライアンスが職務上分離されて取締役会に報告することである。コンプライアンス機能が取締役会に報告しない場合、取締役会への直接的かつ自由なアクセスを含む、適切な資源と十分な自律性を確保するための特別な注意を払わなければならない。

業務構造には、Ｃ＆Ｅプログラムに関連するガバナンスと意思決定プロセスも対象にした、文書化された方針と手続も含めるべきである。ガバナンスの観点から、Ｃ＆Ｅプログラムの監督が取締役会から取締役会レベルのコンプライアンス委員会に委任されている場合、同委員会は取締役会が承認した基本規程に従って運営されるべきである。基本規程には、委員会の責任と主要な運営手続（例：会議の頻度と内容、取締役会への報告）および委員の資格も詳細に記述する。

規制当局やエンフォースメント機関は、Ｃ＆Ｅプログラム、ひいてはコンプライアンスが組織内でどれほど重視されているかを示すシグナルとして、他の執行機能とコンプライアンス機能との相対的な地位を一層考慮するようになってきている。コンプライアンス機能は、組織図の下層に埋もれているか。それとも、非常に高い経営幹部層に位置づけられているか。また、地位については、ＣＣＯと組織の他の上級幹部との相対的な位置づけも考慮している。

業務構造には、コンプライアンスリスク評価の方法とパフォーマンス、組織全体から代表者を集めた内部コンプライアンス委員会の設置の検討、重要なリスク事象が発生した場合の上申手続など、その他の主要なコンプライアンス方針と手続も含めるべきである。

表２．２　業務構造を確立する

主要な特徴	• ＣＣＯおよびコンプライアンスと倫理の機能の独立性を維持する • ＣＣＯが取締役会に直接報告し、定期的にコミュニケーションをとるようにする • ＣＣＯとＣ＆Ｅプログラムが、他の機能リーダーに比べて高い地位にあるようにする • Ｃ＆Ｅプログラムを効果的に管理するために、ＣＣＯに十分な権限を付与する • Ｃ＆Ｅプログラムが効果的に機能するために、十分な資源を提供する • Ｃ＆Ｅプログラムの監督を基本規程に明記する（該当する場合、指定した委員会への委任を含む） • Ｃ＆Ｅプログラムの運用に特化した方針と手続を文書化する • 重大なコンプライアンスリスク事象の上申のための手順や手続を確立する

原則３－望ましいカルチャーを定義づける

コンプライアンスとインテグリティのカルチャーを確立して維持することは、組織にとって非常に重要である。これがなければ、細心の注意を払って設計したコンプライアンスの統制でさえ、機能不全を起こしやすくなる。カルチャーは、コンプライアンスと倫理に対するリーダー層の真摯なコミットメントから始まる。このコミットメントは、期待される行動を明確に記述して行動規範や企業倫理規範に盛り込むことから始まり、いくつかの方法で反映される。また、リーダーは、他のコミュニケーションを通じてこのカルチャーを強化して明確にできる。このカルチャーへのコミットメントは、重要なコンプライアンス指標の採用や、特にリーダー層では、コンプライアンスを業績評価や報酬・インセンティブ支払いプロセスに有効に組み込むことによって、より一層反映させるべきである。

カルチャーに対する期待を設定するのに役立つ作業は、上級経営者が、コンプライアンスリスクと組織のリスク選好やリスク許容度との関係についてしっかりと議論することであるが、これは次章で詳しく説明する。法令やその他の要件の遵守自体がすべての組織の主要な事業目標の１つであるはずなので、特に、事業目標の達成に関連するパフォーマンスの許容可能なレベルの差異を考慮する許容度については、コンプライアンスリスクの潜在的影響を考慮すべきである。

コンプライアンスのカルチャーのもう１つの側面は、リスクの認知である。コンプライアンスを重視するカルチャーがあることは、１つのポイントである。しかし、そのような環境に不可欠なのは、従業員が気を緩めず、リスクの兆候を見つけたら進んで懸念を表明するような、リスクを認知するカルチャーである。

コミュニケーションと研修は、コンプライアンスとインテグリティに関する全般的な考え方を強化し、同時に重要なコンプライアンス問題に対する意識を向上させるため、倫理的なカルチャーを促進するための重要な手段でもある。そのため、研修では、行動規範を定期的に議論するだけでなく、自身の業務に関連するコンプライアンスリスクに曝されている個々の従業員グループに合わせた具体的なコンプライアンス問題についての研修も行うべきである。

表2.3　望ましいカルチャーを定義づける

主要な特徴	• 行動・倫理規範およびその他の主要なコンプライアンス方針を、取締役会が熟知して承認するようにする • 行動・倫理規範の中で、倫理とコンプライアンスに関連する期待を説明する • （取締役を含む）全職員に、行動規範と倫理的な意思決定に関する研修を実施して義務づける • 組織のカルチャーの継続的なモニタリングや評価を実施する • 客観的に測定可能なコンプライアンス指標を開発し、必要に応じて業績評価や報酬と関連づける • C＆Eプログラムの一貫した実施を推進するために、有効なインセンティブを採用する • リーダーからのコミュニケーションの中で、組織の価値観、期待および倫理の重要性に言及する

原則4－コアバリューに対するコミットメントを表明する

コアバリューに対するコミットメントは、コンプライアンスと倫理的な事業行動へのコミットメントを示すバリュー・ステートメントやその他の一連の指針に表されるべきである。倫理的なカルチャーと組織のパフォーマンスとの間に相関関係があることを示す研究はますます増えており、価値の創造というERMの目標とも一致している。

トップからの気風は、コンプライアンスリスクの管理において重要な役割を果たす。経営陣が示す気風は、コンプライアンスと倫理的行動の模範となるものでなければならない。このようなコミットメントは、組織全体に落とし込まなければならないため、「トップの」気風ではなく「トップからの」気風と表現している。組織内の各リーダー層、すなわち他者の監督者や管理者は、コミュニケーションを取ってこの気風を下層に伝えなければならない。

しかし、コンプライアンスと倫理へのコミットメントは、気風を設定することよりはるかに多くのことを必要とする。従業員は、コンプライアンスリスクの管理における各自の役割に説明責任を持つべきであり、それは職務記述書、業績評価およびインセンティブに反映されるべきである。

コンプライアンス違反や倫理にもとる行為の疑義が浮上した場合は、真剣に受け止めなければならない。これは、個人が不正行為を通報することを求められ、通報するための複数の手段を持つべきであることを意味する。申し立てを受けたら、その申し立ての信憑性を評価するために、適切な調査手順に適時に従うべきである。さらに、この制度が効果的に機能するためには、不正行為に関する懸念を通報する個人が安心して発言でき、報復から保護されるようにしなければならない。

調査プロセスを通じて不正行為が確認された場合は、不正行為の程度に応じた懲戒処分を行うべきである。懲戒は、組織図上の職位や組織内での影響力のレベルに関係なく、不正行為の内容に基づいて一貫して行われるべきである。

表2.4　コアバリューに対するコミットメントを表明する

主要な特徴	• リーダーによる倫理的でコンプライアンスに基づいた気風の確立など、コンプライアンスリスクを認知するカルチャーを積極的に推進する • 業務上のインセンティブと重要なコンプライアンス上のインセンティブのバランスをとる • 特に上級職において、（1）コンプライアンスリスク、（2）コンプライアンスプログラムの導入、の管理に関する説明責任を、従業員の業績測定、昇進およびインセンティブ制度に組み込む • 不正疑義事案を通報した者を保護し、報復を一切許さない • 不正疑義事案の申し立てを真剣に受け止め、適時に調査する • 不正行為に対する説明責任、懲戒処分の公正さと一貫性および昇進の公正さなど、組織的な公正さを推進する • コンプライアンス違反や倫理違反から学んだ教訓を、適度な詳しさで組織全体に伝達する

原則５－有能な人材を惹きつけ、育成し、保持する

効果的なコンプライアンス機能は、適切な経験と資格を持つＣＣＯが率いるべきである。過去の経験やその他の資質の具体的な内容は、組織の性質、業種およびその他の多くの要因によって異なる可能性がある。

組織全体で、コンプライアンスを尊重し倫理的な判断ができる人材を採用することが、コンプライアンスリスクの管理には欠かせない。実際、コンプライアンスと倫理を重視する組織であると認識されることは、企業が優秀な人材を惹きつけて保持するのに役立つ。

Ｃ＆Ｅプログラムの世界標準となったＵＳＳＧのフレームワークでは、「組織は、デューディリジェンスの実施により、違法行為または効果的なコンプライアンスと倫理のプログラムに反するその他の行為に関与していることを組織が知っていた、または知っていたはずの個人を、組織の実質的権限者の中に含めないよう、合理的な努力を払うものとする」と述べている。このように、組織は、役職の責任に相応しく関連する雇用法に準拠した身元調査を行うべきである。ＣＣＯは、「実質的権限」を伴うと考えられる役職、つまり組織にコンプライアンスリスクを生じさせる可能性がある役職を特定するために、人事部などと協力することができる。

ＣＯＳＯのＥＲＭフレームワークでは、人材の育成と保持のためには、業績評価と適切なインセンティブの確立が２つの重要な要素であることが示されている。これらのツールは、コンプライアンスリスクの管理にも不可欠である。ＤＯＪは、「効果的に実施されているコンプライアンスプログラムの顕著な特徴は、コンプライアンスに対するインセンティブとコンプライアンス違反の阻害要因を確立していることである」と指摘している。

行動規範や広範な倫理問題に関する研修が組織の望ましいカルチャーを定義するのに役立つように（原則３）、具体的なコンプライアンスリスクに関する研修は、コンプライアンスリスクを効果的に認識して管理する個人の能力を一層高めるものである。さらに、コンプライアンスチーム自体も、Ｃ＆Ｅプログラムを管理するための新たな実務や、法規制を取り巻く環境の変化に関する研修によって、継続的に能力開発をすべきである。

近年、特にサプライチェーン、販売、配送などの重要な機能に関連して不可欠な役割を果たす第三者（非従業員）を引き金に、多くのコンプライアンス問題が発生している。したがって、組織のために活動する第三者（例：サプライヤー、販売代理店、外部委託先）を雇う場合にも、各第三者に関連するコンプライアンスリスクのレベルに基づいて、本章で説明するデューディリジェンスの概念を適用すべきである。身元調査、その他のデューディリジェンスおよびコンプライアンス関連のパフォーマンス指標の程度は、評価したリスクのレベルに応じて変えるべきであり、デューディリジェンスは、リスクの高い第三者との継続的な関係を維持する一環として、定期的に繰り返すべきである。特定の第三者との関係におけるデューディリジェンスと、第三者の継続的な研修とコンプライアンスパフォーマンスのモニタリングは、規制当局から期待されるようになってきており、この原則の不可欠な要素である。

表２．５　有能な人材を惹きつけ、育成し、保持する

主要な特徴	• Ｃ＆Ｅプログラムを指導する適切な経験や専門知識を持つＣＣＯを雇用して保持する • コンプライアンスチームに、専門知識を持つ人材を配置する • 各職位のリスクレベルに合わせて、コンプライアンスリスクのチェックを目的とした身元調査を実施する • 業績評価において、従業員がＣ＆Ｅプログラムの要件と期待事項を実行し、遵守していることを考慮する • 組織内の具体的な役割で生じるコンプライアンスリスクに基づいて、適切なコンプライアンス研修を実施する • 第三者に対してリスクベースのデューディリジェンスを実施する

3．コンプライアンスリスクの戦略と目標設定

本章では、COSO ERMフレームワークの「戦略と目標設定」の構成要素と、コンプライアンスリスクの管理に関連する以下の４つの原則の適用について説明する。

6. 事業環境を分析する
7. リスク選好を定義する
8. 代替戦略を評価する
9. 事業目標を組み立てる

原則６－事業環境を分析する

コンプライアンスリスクを理解して管理するためには、環境が重要である。事業上の意思決定は、コンプライアンスリスクの増減要因の１つであり、意思決定によって新しいリスクが生じたり、既存のリスクが変化したり、リスクが排除されたりすることがある。したがって、コンプライアンスリスクの対象領域を識別する際には、組織の戦略展開を考慮すべきである。CCOは、戦略設定プロセスに適切なレベルで関与すべきであり、コンプライアンス機能が戦略の変更から生じるコンプライアンスリスクを識別して管理するための計画を策定できるように位置づけられるべきである。同様に、組織が環境の変化に対応する際に生じ得る戦略の突然の変更についても、CCOは情報を得るべきである。

効果的なコンプライアンスリスクマネジメントのための環境には、コンプライアンスリスクの他の内部要因、すなわち、新しいリスクを生じさせたり既存のリスクを変化させたりする要因を考慮することが含まれる。コンプライアンスリスクの最も重要な内部要因には、人、プロセスおよびテクノロジーの変化が含まれる。コンプライアンスリスクのもう１つの増減要因は、経営者からのプレッシャーであり、特に、そのようなプレッシャーが、コンプライアンスへの期待に関する注意喚起やC＆Eプログラムを遵守するための適切なインセンティブと結びついていない場合である。さらに広い意味では、組織のカルチャーの変化は多くの要因から生じ、コンプライアンスリスクに影響を与える可能性がある。

コンプライアンスリスクの外部要因も、コンプライアンスリスクを識別して管理する上での環境の重要な要素である。最も明白な外部要因は、法律、規制およびエンフォースメントの状況に関わるものである。例えば、最近の個人情報保護法やセキュリティ法の改正により、一部の組織ではまったく新しいコンプライアンスリスクが発生している。外部要因には、コンプライアンスリスクに直接的または間接的に影響を及ぼす可能性のある競争、経済およびその他の要因も含まれる。外部要因には、マクロレベル（例：業界全体の競争、経済状況）のものもあれば、ミクロレベル（例：地元や地域の法令の変更）のものもある。

リスクの相互依存関係は、組織がコンプライアンスリスクを管理する方法にも影響を与える可能性がある。他のリスク（例：戦略リスク、財務リスク）に対する組織の対応は、コンプライアンスリスクにプラスまたはマイナスの影響を与える可能性がある。

表３．１　事業環境を分析する

主要な特徴	• コンプライアンスリスク評価の実施やコンプライアンスリスクの管理の際に、組織戦略を考慮して反映させる • 人、構造、プロセス、テクノロジーのような内部の変化が、コンプライアンスリスクに及ぼす影響を検討する • 外部要因（例：競合の動向、景気動向、エンフォースメントの傾向、環境的影響力、政治勢力、社会的勢力）が、コンプライアンスリスクに及ぼす影響を評価する • 戦略策定の際に、リスクの相互依存関係を識別して検討する • 組織が活動する場所に基づいて、法的枠組みの文化的・地域的な差異を考慮する

原則７－リスク選好を定義する

リスク選好という言葉に馴染みのない者にとって、コンプライアンスリスクに対する選好というと、既知のコンプライアンス違反を意図的に受け入れている組織を想起されることがたびたびある。コンプライアンスリスクの本質は、組織に財務的または非財務的な影響（例：罰金、事業停止や契約からの排除、評判の低下）のある法律違反が発生する可能性があることを意味している。事業目標や目的を追求する上で、コンプライアンスリスクをどの程度許容するかは、経営者と取締役会の間で議論されるテーマである (この議論は、既知の違反の受容とは関係がないことを明確に指摘しておく。ここでは、コンプライアンス違反という事象の発生可能性を排除することは不可能であるという現実的な仮定について述べている)。

ＣＯＳＯの定義によると、リスク選好とは、組織が価値追求において受け入れる、幅広いリスクの種類と量である。通常、リスク選好もリスク許容度（事業目標に関連するパフォーマンスの許容可能な差異のレベル）も、個々のリスクレベルで定義されることはない。

コンプライアンスリスクという単位では、リスク選好も許容度も表明されないが、個々のコンプライアンスリスク領域に関してリスクを中心に考えた文書が個別に存在する場合がある。一般的には、リスク選好と許容度の決定と表明に関連して、コンプライアンスリスクが事業目標の達成に及ぼす潜在的な影響を検討すべきである。前述のように、法令およびその他の要求事項の遵守は、それ自体が組織の事業目標であると考えるべきである。

コンプライアンスリスクとリスク選好や許容度との関係を見る現実的な方法として、事業部や拠点レベル、また、コンプライアンスリスクの種類別に見ることができる。事業部門（または機能）レベルでは、各グループが独自のコンプライアンスリスクを抱えていることが多く、違反した場合の潜在的な影響もそれぞれ大きく異なる。例えば、国際的な贈収賄の違反は、建築基準法違反よりもはるかに重大な財務的な罰をもたらす可能性がある。

消防法違反の場合は、罰金程度で済むかもしれないが、消防法違反で人命が失われた場合は、その影響は甚大なものになる可能性がある。建築基準法違反のような一見重要でないコンプライアンスリスクは、建築検査官からの賄賂要求のような他のリスクにつながる可能性がある。潜在的な影響をすべて考慮した上でリスク選好を検討することは、コンプライアンスリスクマネジメントの重要な要素である。

ＣＯＳＯが 2020 年５月に発表した「リスク選好－成功に不可欠なもの：変化する世界で成功するためにリスク選好を活用する（*Risk Appetite - Critical to Success: Using Risk Appetite to Thrive in a Changing World*）」では、リスク選好へのインプットとして、以下の３つを挙げている。

1. リスク選好に関する取締役会と経営者の見通し
2. 既存のリスクプロファイルの理解
3. 組織のカルチャー

リスク選好に関する取締役会と経営者の見通しは、ある程度、コンプライアンスリスクと事業目標の達成との関係を考慮して立てるべきである。これは、取締役会と経営者が、組織全体のリスクプロファイルの構成要素としてコンプライアンスリスクを十分に理解している場合にのみ達成され得る。同様に、前述のように、コンプライアンスのカルチャーを維持することは、Ｃ＆Ｅプログラムの不可欠な要素であり、したがって、一般的なリスクに対する組織全体のリスク選好を策定する際に考慮すべきである。

コンプライアンスリスクが事業目標の達成に対してどの程度の脅威を与えているかを理解することで、ＣＣＯは予防と発見のための資源の配置に効果的な優先順位をつけることができる。例えば、ある組織が、特定のカテゴリーのコンプライアンスリスクは事業目標の達成に重大な脅威を与えると判断した場合、そのリスクの管理により多くの資源を割り当てることができる。この領域の監査やモニタリングにより多くの注意を払うなど、さまざまな対応が考えられる。

組織は、現実的にはすべてのコンプライアンスリスクを排除したり、発生可能性をゼロにしたりはできないことも認識しなければならない。これは単に不可能である。そのため、コンプライアンスリスクに関連するリスク選好について議論することは、具体的なコンプライアンス違反の予防と発見を目的とした取り組みの優先順位を決定する上で貴重なツールとなる。規制当局のガイダンスはこの概念と一致しており、組織はコンプライアンスリスクを必ずしも排除するのではなく、低減し管理することが期待されている。

表３．２　リスク選好を定義する

主要な特徴	• リスク選好を決定する際に、組織のリスクプロファイルの一部として、コンプライアンスリスクを検討する • コンプライアンスリスクを、（１）リスクの種類（例：贈収賄防止）、（２）事業部門や組織機能（例：人事）、（３）場所や地域別、に検討する • コンプライアンスリスクと事業目標の達成との関係を判断して評価する • リスク選好について定期的に議論し、コンプライアンスリスクの変化に基づいて必要に応じて更新する • 組織のリスク選好と許容度の裏づけとして、コンプライアンスリスクに関して具体的なリスクを中心に考えたリスク選好文書を作成することを検討する

原則８－代替戦略を評価する

コンプライアンス機能は、（1）Ｃ＆Ｅプログラムがコンプライアンスリスクを適切に管理できるように戦略を理解する、（2）検討中の戦略に関連するコンプライアンスリスクの可能性について戦略の意思決定者に助言する、という観点から戦略の議論に参加すべきである。コンプライアンスリスクの評価と管理は、新たな戦略的施策に着手する前にコンプライアンス機能に十分な情報が提供されており、Ｃ＆Ｅプログラムが新たなコンプライアンスリスクや変化するリスクに積極的に対処する準備が整っている場合に最も効果的である。また、ＣＣＯ は、戦略やリスク選好の変化に対応した新たなコンプライアンスリスク低減手法の開発や、検討中の代替戦略に関連するコンプライアンスリスク問題の評価の支援という役割を担うべきである。

組織による戦略的意思決定がＭ＆Ａ活動に関わる場合、コンプライアンスリスクに焦点を当てた適切なデューディリジェンスを実施できるように、プロセスの初期段階からコンプライアンスが関与することが重要である。このデューディリジェンスは、Ｍ＆Ａの意思決定プロセスにおいて、Ｃ＆Ｅプログラムを統合する必要性や対処が必要なリスクを理解するだけでなく、取引の結果として継承する可能性のあるリスクのレベルを理解するためにも重要である。

一旦戦略が決定されたら、コンプライアンス機能は、組織のＣ＆Ｅプログラムへの影響を特定して理解すべきである。まず、コンプライアンスリスクを識別して評価し、コンプライアンスリスクの軽減を目的とした内部統制の修正を提案することから始める。Ｃ＆Ｅプログラムの研修、モニタリング、および監査計画の変更、ならびに主要なコンプライアンス指標や業績評価指標の策定を検討する。

戦略が実行されるにつれて、組織はその成功と失敗の評価に基づいて、戦略を継続的に変更する可能性がある。この評価は、ＣＣＯがＣ＆Ｅプログラムのモニタリング業務や監査業務に基づいて貴重な意見を提供するもう１つの機会であり、当初の予想とは異なるレベルのコンプライアンスリスクを明らかにする可能性がある。

表３．３　代替戦略を評価する

主要な特徴	• 戦略に関する議論の場に、ＣＣＯの席を確保する • 戦略がコンプライアンスリスクに与える影響について、ＣＣＯに意見と洞察を求める • 取引実行前のＭ＆Ａ対象企業にリスクベースのデューディリジェンスを実施する • Ｃ＆Ｅプログラムの設計において、（その後の戦略変更も含めた）戦略的意思決定の影響を検討する

原則９－事業目標を組み立てる

戦略と連動した事業目標は、組織や個々の事業部門を評価するための測定可能な規準である。戦略の採用がコンプライアンスリスクに影響を与えるのと同様に、事業目標の策定もまた、コンプライアンス違反の可能性を生み出したり、影響を与えたりすることが多い。さらに、他の事業目標でコンプライアンスを明示的に取り上げていない場合は、適用される法令、契約条件およびその他の要件を遵守すること自体を事業目標として検討すべきである。

事業部門用に策定された業績評価指標が、コンプライアンス要件に違反するインセンティブを不用意に生み出すことがある。増産に向けた積極的な新しい目標によって従業員が動機づけられている製造施設の簡単な例を見てみよう。この目標は、品質管理や検査の手抜きにつながるかもしれないが、製造チームがこれらのコンプライアンス要件違反を新しい目標を達成するために許容できる方法であると見なした場合、製品安全違反という結果になり得る。コンプライアンス機能は、原則８で述べたのと同様に、事業目標を設定する際に相談を受けて、好ましくない行動の促進を最小限に抑えるようなインセンティブが適切に構成されているか、あるいはそのようなインセンティブと適切なコンプライアンスのインセンティブとのバランスが取れているかを確認すべきである。理想的なのは、コンプライアンス機能が事業目標の設定に参加することであるが、最低でも、そのような目標や個人の評価に使用される業績評価指標について十分に知らされるようにする。

また、リスクの相互作用も考慮すべきである。組織のある領域で事業目標や業績評価指標が変更されると、同じ事業部門や組織の他の領域で、コンプライアンスリスクが影響を受ける可能性がある。

最後に、業績評価指標が事業部門にとって不可欠な特性であるのと同様に、コンプライアンス機能自体も業績評価指標を策定してモニターすべきである。これらの指標は、Ｃ＆Ｅプログラムとインフラが組織全体で実際に機能している程度とその全般的な有効性を取り上げて測定するものである。測定可能な指標と主要業績評価指標（ＫＰＩ）の例には、研修修了率、問題への対応、調査および是正措置計画の実施の適時性、組織の通報制度を通じて報告される問題の量、頻度および種類、長期にわたるカルチャーの調査の回答、ならびにリスクの高い事業所におけるベンダーへの支払いのようなさまざまなコンプライアンス内部統制のモニタリング指標などがある。Ｃ＆Ｅプログラムのすべての領域が客観的に測定しやすいわけではないが、コンプライアンス機能は、可能な限り客観的な指標を策定してモニターするための措置を講じるべきである。

表３．４　事業目標を組み立てる

主要な特徴	• 計画された事業目標に関連するコンプライアンスリスクを識別して評価する • コンプライアンスを独立した事業目標として設定することを検討する • コンプライアンスリスクマネジメントと説明責任を業績評価指標や関連評価に組み込む • 事業目標の変更に基づいて、コンプライアンスと他のリスクとの相互作用を検討する • 客観的に測定されたコンプライアンス指標を事業目標に含め、コンプライアンスリスクの管理とＣ＆Ｅプログラム実施の有効性を反映し、インセンティブやその他の報酬の決定に適切な重みを持たせる

4．コンプライアンスリスクのパフォーマンス

本章では、COSO ERMフレームワークの「パフォーマンス」の構成要素と、コンプライアンスリスクの管理に関連する以下の５つの原則の適用について説明する。

⑩ リスクを識別する
⑪ リスクの重大度を評価する
⑫ リスクの優先順位づけをする
⑬ リスク対応を実施する
⑭ ポートフォリオの視点を策定する

Ｃ＆Ｅプログラムが効果的であるためには、組織が法律、規制および方針へのコンプライアンス違反や倫理にもとる行為の潜在的脅威を定期的に評価し、これらのリスクを許容可能なレベルに管理するための措置を講じることが、規制当局などから期待されている。

原則 10 －リスクを識別する

Ｃ＆Ｅプログラムにとって最も困難な作業の１つは、組織が直面する無数のコンプライアンスリスクを識別することである。組織は、独占禁止、個人情報、詐欺および知的財産の権利義務から、地方消費税、許認可要件および環境基準に至るまで、何千もの法令の適用を受けている。さらに、これらの脅威は、法律や規制の要件の新設や変更、小売業者が医療サービス事業に参入するなどの組織戦略の変更および社会的な価値観の進化に伴う新たなコンプライアンスリスクの出現により、常に変化している。Ｃ＆Ｅプログラムが効果的に機能するためには、組織全体でこれらのさまざまなリスクを識別して追跡するためのプロセスを整備する必要がある。

従来、多くの組織は縦割りで法令遵守に取り組み、組織や業界内の他の組織が重大な課題に直面した際に、その問題に対処するためのプログラムを開発してきた。例えば、独占禁止、環境またはマネーロンダリングなどのリスクに直接関わる事業部門が、すべてではないにしても、これらの法律の遵守のほとんどの側面について責任を負うことになる。しかし、コンプライアンスプログラムが成熟するにつれて、組織は、繰り返したくない過去の特定の危機ではなく、組織とその環境を体系的に評価してコンプライアンスに対する現在と将来の脅威を識別する、より統合的で先を見越したアプローチに移行してきた。これと同じ動機が、組織をＥＲＭの導入に向かわせるのである。

コンプライアンスの脅威のすべてが、ＥＲＭという観点で優先事項と考えられるとは限らない。例えば、Ｃ＆Ｅプログラムが識別した最も重要な 10 件のコンプライアンスリスクのうち、コンプライアンスリスクとその他のリスクを統合した上で組織レベルのＥＲＭ機能が識別した最も重要な 10 件のリスクに入るのは、おそらく２～３件にとどまるであろう。しかし、Ｃ＆Ｅプログラムにとっては、コンプライアンスのカルチャーに影響を及ぼすことで深刻な脅威となり得るため、これらは重要である。規制当局は、Ｃ＆Ｅプログラムの一環として、コンプライアンスリスクの具体的な評価を期待している。このことは、組織が成熟した充実しているＥＲＭプログラムを持っている場合であっても、Ｃ＆Ｅプログラムは組織レベルのＥＲＭを補完すべきであり、また、組織レベルで重要かどうかにかかわらず、すべてのコンプライアンスリスクを識別して管理するよう努めるべきであることを示唆している。

コンプライアンスリスクのリスク一覧表の作成は、ＥＲＭのリスク一覧表の作成と同様のプロセスである。図４．１に示すように多くのアプローチがあり、新しいリスクやエマージングリスクを識別する上で、より効果的なアプローチもある。

コンプライアンスリスクの識別には、いくつかのアプローチが特に有用であることがわかっている。多くの組織は、類似の組織や業界団体が識別したリスク一覧表から始める。この一覧表は、出発点として捉える必要があり、その後、その組織に特有の業務を考慮して、組織に合わせて調整すべきである。別のよく用いられるアプローチは、主要な従業員にインタビューして業務内容をより深く理解し、彼らが日常的に扱っている適用法令を判断するという方法である。図４．１に示したように、この方法は、コンプライアンスリスクをもたらす既存の法令を識別するのに有効であり、エマージングリスクの指標となる可能性もあるが、従業員がまだ認識していない新しいリスクやエンフォースメント基準の変更を識別するのには、それほど有効でない可能性がある。また、アンケー

図４．１　リスク識別のアプローチ*

リスクの種類	コグニティブコンピューティング	データ追跡	インタビュー	主要指標	プロセス分析	ワークショップ
既存のリスク	✓	✓	✓	✓	✓	✓
新しいリスク	✓	✓			✓	✓
エマージングリスク	✓		✓	✓		✓

* 出典：COSO Enterprise Risk Management—Integrating with Strategy and Performance, Volume 1, p. 69.（邦訳は、一般社団法人日本内部監査協会・八田進二・橋本　尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会ＣＯＳＯ - ＥＲＭ研究会訳『ＣＯＳＯ全社的リスクマネジメント－戦略およびパフォーマンスとの統合－』154 頁、同文舘出版、2018 年。）

ト調査を利用して、主要な管理者に自身の担当領域で通常扱っている適用法令を識別してもらうこともできる[1]。

どのようなアプローチをとるにせよ、コンプライアンスリスクは多様で複雑なので、業務管理者やリスクオーナーがリスク識別プロセスに関与する必要がある。これを実現する方法の１つが、組織内のさまざまな階層にコンプライアンス委員会を設置することである。また、上級経営者と取締役会は、Ｃ＆Ｅプログラムのリーダーが組織の現在と将来の戦略に関連するコンプライアンスリスクを理解できるようにするために、彼らを戦略計画に参加させるように関与しなければならない。

規制当局の多くは、エマージングリスクやコンプライアンス上の懸念がある場所について警告を発しているため、規制当局から提供される情報も、新しいリスクやエマージングリスクを識別する上で有用である。例えば、ＳＥＣのコンプライアンス検査局（Office of Compliance Inspections and Examinations）は、特別なリスク警告を出しており、また、ＨＨＳ ＯＩＧは、作業計画を公表して高リスクと考えられる領域を組織に警告している。

さらに、コンプライアンスリスクは、組織の法的な境界を超えて広がっている。第三者の請負業者、サプライヤーおよび戦略的提携相手は重大なコンプライアンスや倫理上のリスクを引き起こす可能性がある。特に第三者リスクに関連する懸念事項には、以下のようなものがある。

1. 組織は通常、自社の従業員の場合よりも、第三者の仕事を統制または監督する能力が劣る。
2. 第三者は、従業員ほどコンプライアンスや倫理に関する期待に応えようとする強い動機を持っていないことが多い。
3. 第三者は、組織の本部から地理的に離れた地域で業務を行う場合があり、時には法律、規範および習慣が異なる場合がある。

これらの理由から、第三者が関与するリスク評価は複雑になるが、リスク評価は、第三者との契約時と以後定期的に実施すべきである。各リスク評価、デューディリジェンスプロセスおよび以後のモニタリングや監査の程度は、第三者が果たす役割、重要性および各第三者に関連するリスクのレベルに影響し得るその他の要因を考慮すべきである。

すべてのコンプライアンスリスクが全社レベルまで上がってＥＲＭリスク一覧表に記載されるわけではないが、大部分の組織では、規制変更のリスクはそのような全社レベルの一覧表に含まれるであろう。

表４．１　リスクを識別する

主要な特徴	• コンプライアンスリスクの識別と評価のプロセスを、方針と手続の文書の中で説明する • 計画した戦略と事業目標に関連するコンプライアンスリスクを識別する • リスクを識別するために、内部環境と外部環境を評価する • 新しいリスクとエマージングリスクを識別するプロセスを構築する • 第三者の利用に伴うリスクを検討する • 内部通報窓口、その他の通報経路および調査結果を通じて収集した情報を検討する

[1] Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 21-25, https://compliancecosmos.org/compliance-risk-assessments-introduction

原則 11 －リスクの重大度を評価する

コンプライアンスリスクの重大度は、通常、主に発生可能性と影響度に基づいて評価される。その他の要因も考慮されることがあるが、これについては後で説明する。

発生可能性とは、そのリスクが発生する確率のことである。コンプライアンスの場合、特定の法令を遵守しない確率や倫理にもとる行為が起こる確率を意味する。コンプライアンスリスクの発生可能性の評価は、大抵の場合、主観的な判断である。主観的であるにもかかわらず、体系的な判断が可能である。１つのアプローチは、コンプライアンス違反の発生頻度を考慮することである。その事象（例：営業担当者が契約を獲得するために政府関係者に違法な支払いを行う）は、１年に１回発生するのか、それとも５年に１回発生するのか。この判断は、経験または組織の過去のデータが利用可能であればそのデータに基づいて行われるであろう。この評価に入るもう１つの要因は、組織の状況である。通常、評価者は、違法な支払いを禁止する方針や支払いプロセスに関する統制など、整備されている統制を前提にしている。理論的には、統制がまったく整備されていないという前提で評価を行いたいところであるが、そのような「統制がない」状況を想像するのは難しい。一般的には、「通常の統制」またはある種の「最小限の統制」を想定して評価を行う。より精度を高めるために、図４．２に示すように、発生可能性評価を２つに分ける評価方法もある。すなわち、１つは発生可能性または頻度であり、もう１つは内部統制の有効性である。モデルによっては、予防的統制と発見的統制を２つの別個の要因として考慮し、予防的統制は発生可能性または頻度に、発見的統制は発見の適時性に基づいて事象の影響に、より大きな影響を与える可能性があるとする場合もある。

図４．２では、発生可能性は「めったにない」から「ほぼ確実」までの５段階で測定している。統制の想定と頻度には、評価者の意見に合うような説明文が示されている。

図４．２　発生可能性*

段階	存在する統制	コンプライアンス違反の頻度
5 **ほぼ確実**	• 統制は整備されていない • 方針や手続はない、責任者は特定されていない、研修は実施されていない、経営者によるレビューは実施されていない	ほとんどの状況で発生が予想される 年１回超
4 **起こりそう**	• 方針と手続は整備されているが、義務づけも定期的な更新もされていない • 統制はテストされていない、またはテストされていても満足のいく結果ではない • 責任者は特定されている • 公式・非公式な（ＯＪＴ）研修は実施されている • 経営者によるレビューは実施されていない	おそらく発生する 少なくとも１年に１回
3 **可能性あり**	• 方針は義務づけられているが、定期的に更新されていない • 統制は時々テストされるだけで、結果はまちまちである • 責任者は特定されている • 研修は必要に応じて実施されている • 経営者によるレビューは時々実施されるが、文書化されていない	いつかは発生する可能性がある 少なくとも５年に１回
2 **起こりそうもない**	• 方針は義務づけられており、定期的に更新されている • 統制はテストされ、大部分は良好な結果である • 特定された責任者に定期的な研修が実施されているが、文書化されていない • 経営者によるレビューは定期的に実施されているが、文書化されていない	いつかは発生するかもしれない 少なくとも 10 年に１回
1 **めったにない**	• 方針は義務づけられており、定期的に更新されている • 統制は定期的にテストされ、良好な結果である • 特定された責任者に定期的な研修が義務づけられており、その研修は文書化されている • 経営者によるレビューは定期的に実施され、文書化されている	例外的な状況でのみ発生する可能性がある 10 年に１回未満

* 出典：Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 30, https://compliancecosmos.org/compliance-risk-assessments-introduction

この方法は一例に過ぎない。すべての組織は、組織特有のニーズに合わせて、尺度や測定方法をカスタマイズすべきである。このカスタマイズは、コンプライアンス委員会やＣ＆Ｅプログラムの担当者が、経営者の意見を聞いて行うことになる。尺度が決まったら、評価者はそれを一貫して適用すべきである。

リスクの重大度の第２の構成要素は、影響度である。影響度とは、組織の戦略や事業目標に照らして、リスクがもたらす結果や影響のことである。コンプライアンスリスクというと、民事・刑事上の罰金や刑罰と、コンプライアンス違反がもたらす直接的な財務的影響がすぐに思い浮かぶ。別の重要な要素は、コンプライアンスや倫理の問題が評判に与える影響である。この影響やその他の影響（例：制裁、事業停止、契約からの排除）は、間接的に重大な財務的影響を及ぼす可能性があり、また、測定が困難なモラルやその他の要素にも影響を及ぼす可能性がある。

コンプライアンス違反や倫理違反の影響は、さまざまな測定カテゴリーを用いて評価できる。

- **法務**－民事・刑事の罰金や刑罰から成る
- **財務**－調査と是正に関連する内部と外部のコスト（例：弁護士費用、コンサルタント、調査員）
- **業務**－工場閉鎖、事業停止、契約からの排除、許認可喪失による業務運営の中断の可能性
- **評判（イメージ）**－マスコミ報道の影響、組織のイメージやブランドの毀損ならびに現在と将来の従業員、ビジネスパートナー、ベンダーおよび顧客にとってその後の魅力の低下
- **安全衛生**－従業員、患者、顧客
- **戦略目標の追求能力**－新規顧客開拓の禁止、許認可喪失

図４．３は、これらのカテゴリーを使用して、コンプライアンスリスクの影響を評価するための尺度を構築する方法を示している。

図４．３　コンプライアンスリスクの影響

段階	法務*	財務#	業務（中断の可能性）*	評判（イメージ）+	安全衛生*	戦略目標の追求能力*
1 **重要でない**	遵守	百万ドル未満	半日未満	マスコミ報道なし	負傷者なし	影響はほとんどまたはまったくない
2 **軽微**	罰金がほとんどまたはまったくない民事上の違反	１～５百万ドル	１日未満	（大口顧客１社の喪失のような）局所的な評判への悪影響はあるが回復可能	応急処置	軽微な影響
3 **深刻**	重大な民事上の罰金や刑罰	５百万～ ２千５百万ドル	１日～１週間	米国内の特定地域または外国における否定的なマスコミ報道	治療	大きな影響
4 **悲惨**	重大な違反、刑事訴追の可能性	２千５百万～ １億ドル	１週間～１か月	米国内外のマスコミによる否定的な報道（一面扱いではない）	死亡または重傷	重大な影響
5 **壊滅的**	重大な違反、前科がつく可能性、許認可喪失	１億ドル超	１か月超	米国内（および海外）のマスコミによる否定的な報道の継続（ビジネス欄の一面に掲載）	複数の死亡または複数の後遺症	許認可喪失

金額は一例であり、各組織はその規模や財務体質を考慮して金額を設定すべきである。
* 出典：Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 39, https://compliancecosmos.org/compliance-risk-assessments-introduction
\+ 出典：Deloitte, *Compliance risk assessments: The third ingredient in a world-class ethics and compliance program*, Deloitte Development LLC, 2015.

発生可能性の尺度と同様に、各組織は影響度の尺度や要因を自らの環境の状況に合わせることになる。また、説明文に使用する値を設定する際には、組織のリスク選好を反映させることになる。

重大度の評価を充実させるもう１つの要因として、場所や地域ごとに評価することが挙げられる。多拠点や多国籍の組織では、リスクはさまざまな要因に基づき、場所や地域によって異なる可能性がある。組織レベルで重大度を評価するよりも個別の尺度を決定する方が、評価の精度を高めることができる。

コンプライアンスリスク一覧表の中の各リスクの評価は、コンプライアンス担当者やコンプライアンス委員会が行うことができ、また、組織のさまざまなレベルで実施できる。評価の実施にあたっては、リスクが適切に評価されるように、自己評価を避け、さまざまな分野や経験を持つ複数の評価者を用いて、バイアスを最小限に抑えるための措置を講じるべきである。

表４．２　リスクの重大度を評価する

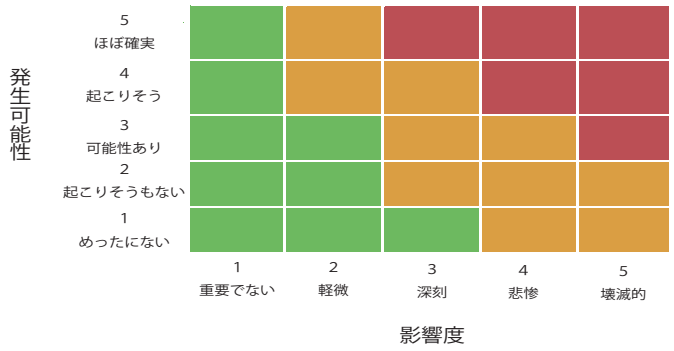
主要な特徴	• コンプライアンスリスクの重大度を測定するための統一された尺度やスコアリングシステムを採用する • 定性的・定量的な尺度を検討する • コンプライアンスリスク事象発生の影響度と発生可能性を評価する規準を設定する • 異なるレベル（組織、地域、関連会社など）でリスクの重大度を評価する • コンプライアンスリスク事象の発生を予防または発見することを目的とした内部統制の整備と運用を検討する • 重大度の評価においてバイアスや不十分な知識を最小限に抑える（例：自己評価を最小限に抑える、多くの専門分野にわたるチームを活用する）

原則 12 －リスクの優先順位づけをする

コンプライアンスリスクを発生可能性と影響度の観点から評価することで、組織全体での優先順位づけが可能となる。重大度評価を把握して要約するために用いられる方法の１つは、リスク一覧表のマトリクスを作成することである。

前述の段階の例を用いて、次のようなマトリクスが作成できる。

図４．４　発生可能性と影響度のマトリクス



これにより、組織は、いつどのように対処し、それぞれにどの程度の注意を払うかという観点から、リスクをグループ化できる。組織は、理想的にはすべてのコンプライアンスリスクに対処可能であると主張できるかもしれないが、現実的な観点からは、最も深刻なリスクに対してより直接的かつ即時に注意を払うことが必要である。これをどのように行うかは、組織のリスク選好と許容度、そして組織が利用できる資源次第である。例えば、この例では、緑色の領域のリスクは定期的に再評価するが、具体的なリスク対応措置や広範なモニタリング措置は取らないであろう。黄色の領域では、リスクオーナーは、多大な資源を追加せずに、リスクを低減または排除するためのリスク軽減計画を策定することが求められるであろう。赤色の領域に該当するリスクについては、コンプライアンス委員会は、リスクオーナーと協力して、リスクオーナーを明確に特定した詳細な対応計画を策定し、リスク対応の責任を割り当て、是正措置のモニタリングと監査の計画を策定する、という役割を与えられるであろう。

リスクの優先順位づけにおいて、重大度とリスク選好に加えて他の要因も考慮する組織がある。速度、持続性および回復度に基づいてリスクを調整することもある。速度とは、リスクが組織に影響を及ぼす速度のことで、例えば、食品加工工場の即時閉鎖を必要とするような重大な食品安全違反のようなものである。持続性とは、リスクが組織に影響を及ぼす期間であり、例えば、犯罪行為に関するマスコミ報道が４～５年続くような場合を指す。回復度とは、問題を解決するのに要する時間（すなわち、リスクを許容できるレベルに管理するのに要する時間）のことで、例えば、ペーパーカンパニーとの取引のリスクを低減するために、ベンダーのデューディリジェンスの規準やプロセスを改善するのに要する時間などを指す。

表４．３　リスクの優先順づけをする

主要な特徴	• 事業目標の達成に関連して評価されたリスクレベルに基づいて、コンプライアンスリスクの優先順位を決定する • 評価に基づく客観的なスコアリングを使用する • コンプライアンスリスクの優先順位づけにおいて、他の評価規準（傾向、速度など）の使用を検討する • 戦略や業務の計画変更に伴う影響を考慮する • リスク軽減のためのリスクベースの行動計画（次のステップで実施する、リスク対応）を策定する

原則 13 －リスク対応を実施する

リスク対応は、評価されたリスクレベルを管理するために設計されるものであり、多くの形態をとることができる。リスクレベルの上昇に対する最も明白な対応は、コンプライアンスに関する内部統制の改善を設計して導入することである。コンプライアンスリスクを効果的に軽減するには、各リスクに対するＣ＆Ｅプログラムの７つの要素すべて（例：方針、研修）を考慮する必要がある。

リスク特有の方針の多くには、内部統制が関わっている。コンプライアンスに関する内部統制は、予防的な性質のものと発見的な性質のものがあり、理想は、その両方が一緒に整

備されていることである。コンプライアンス違反や倫理にもとる行為は予防することが望ましいが、実務上の配慮から、特定のリスクについては適時に発見する統制に組織が重きを置くことになる場合もある。

内部統制を効果的に改善するためには、各リスクの主な要因を理解する必要がある。リスクの発生可能性や発生頻度によって評価される重大度が高まった場合、予防的な統制の改善が特に重要になる。他方で、影響度、特にリスクが発見されない期間と影響度が相関している場合は、発見的統制の改善によって軽減される可能性がある。

リスク対応には、手続き的な内部統制の改善以外にも、さまざまな措置が考えられる。例えば、脆弱な領域に的を絞った研修が有効な場合がある。研修は、内部統制の一形態であり、手続き的な統制の設計は適切であるが、統制の適用方法の理解不足や統制に対する一般的な認識不足によって統制に機能不全が起きている場合に、特に有効な対応となる。

また、より一般的な研修を行う場合もある。観察された行動がコンプライアンスのカルチャーの弱さに関わるものである場合、コンプライアンスの重要性に関する一般的な研修が有効な場合がある。だが、どのような種類の研修であっても、それだけで大きな改善につながることはほとんどない。しかし、統制プロセスの改善と組み合わせれば、改善が見られる可能性はより高くなる。

もう１つのリスク対応として、評価した特定のコンプライアンスリスクに関連する監査とモニタリングの機能を強化または改善することが考えられる。これは、モニタリングや監査の頻度を高め範囲を広げることによって行うことができる。あるいは、監査やモニタリングの新たな方法を導入することによっても実現できる。例えば、コンプライアンス違反の危険信号や内部統制の機能不全の危険信号を発見することを目的としたデータアナリティクスの利用拡大（ＥＲＭ原則 18 との関連でも議論）は、監査やモニタリングの機能にとって強力なツールとなり得る。

リスク対応について、さらに検討する価値があるのは、対応の精度の高さである。統制の対応には、プロセス全体に適用される非常に広範なものもあれば、より狭い範囲に適用されるものもある。これは、改善された内部統制の設計と一定の監査やモニタリング手続に特に適している。リスクと統制の評価によって、長いプロセスの中のある特定の部分の脆弱性が明らかになる場合がある。例えば、玩具メーカーの製品安全違反のリスクを評価した結果、組立ラインに導入された新しい機械には、これまでの機械にはなかった操作上の特有の脆弱性があり、安全でない製品を製造するリスクの増加につながることが判明する場合がある。このような場合、新しい機械の点検と保守の方法を変えて頻度を上げるという、同様に狭い範囲での対応となる可能性がある。

もちろん、内部統制やその他のリスク対応を追加または改善することのメリットは、常にその取り組みにかかる財務的・非財務的コストと比較検討されるべきものである。コンプライアンスリスクを極めて低いレベルまで低減することは可能かもしれないが、生産性を低下させるという点で、そのコストは過大かもしれない。したがって、リスク対応を設計して導入する際には、コストが現実的に考慮される。このように、コンプライアンスに関連する統制と業務効率との間に緊張が生じる可能性があることは、注意を要する重要なトレードオフとなることが多い。

リスク対応を適切に行うためには、説明責任を確立しなければならない。対応策の責任は、リスクに直接影響を受ける事業部門から、内部監査、人事、ＩＴ、コンプライアンスなど組織内の他の部門まで、さまざまなグループ間で共有されることが多い。このため、リスク対応の正確な内容は、その実施に役割を果たす全関係者によって合意されるべきである。これが達成されたら、許容レベルを最も超えていると識別されたリスクにより高い優先順位を与えて、実施のための具体的なスケジュールを作成すべきである。

リスク対応の最後は、その対応策の導入と運用の効果を評価するためのフォローアップである。優れた対応計画は、その実施があってこそのものである。対応計画の一部には、計画の中のすべての措置が適切に導入され、計画通りに運用されているかどうかを判断するためのフォローアップ評価と継続的なモニタリングを含めるべきである。

表４．４　リスク対応を実施する

主要な特徴	• リスク対応の設計時に、Ｃ＆Ｅプログラムの各要素の修正が必要となる可能性を考慮する • （コンプライアンス以外の）他のリスクやリスク対応への影響を考慮したコンプライアンスリスク対応を設計する • 各コンプライアンスリスク対応について、（スケジュール等を含めた）説明責任を割り当てる • コンプライアンスリスク対応が設計通りに適切に導入されたかを判断するためのフォローアップを行う • モニタリングと監査の計画策定時に、コンプライアンスリスク対応を検討する

原則 14 －ポートフォリオの視点を策定する

コンプライアンスリスク間の相互関係はもちろんのこと、コンプライアンスリスクと他の組織上のリスクとの関係を認識することも重要である。これらの相互関係は、リスクの評価だけでなく、リスク対応の設計と導入の両方において重要な考慮事項となり得る。また、このような考慮は、必ずしも新たなリスクを生じさせるわけではないが、他の行動や事象の結果として、あるリスク事象の可能性を高め得る要因、すなわち、リスクの一定の推進要因の特定につながることもある。

ここで簡単な例を示す。コンプライアンス違反のリスク低減を目的とした内部統制の強化は、特定の業務や生産プロセスの遅延リスクを増大させる可能性がある。生産チームもプロセスの遅れを対応すべきリスクとして認識していた場合、この懸念は増幅されるであろう。リスクの識別と軽減の両方に関してポートフォリオ的な見方がなされない限り、２つのリスクは互いに対立する可能性がある。

他のリスクを考慮せずにリスクを単独で管理すると、非効率、そして場合によっては対立が生じる可能性がある。このため、リスクを組織全体のリスクポートフォリオの一部として捉えることが不可欠である。

ポートフォリオの視点を展開する際のもう１つの考慮点は、コンプライアンスリスクが組織内のより高いレベルに統合されるにつれて、その重大度がどの程度増減するかである。事業部門レベルでは重大に見えるコンプライアンスリスクも、他のリスクと統合されて組織内のより高いレベルに集約された時点では、むしろ軽微なものになる可能性がある。反対に、単独では軽微なコンプライアンスリスクも、他の一見軽微なリスクと統合されると、はるかに大きなリスクとなる可能性がある。

表４．５　ポートフォリオの視点を策定する

主要な特徴	• リスクの相互作用を考慮する（すなわち、コンプライアンスリスクの軽減が他のリスクにどう影響するか） • コンプライアンスリスク対応と他のリスク対応との相互作用を考慮する • コンプライアンスリスクマネジメントとＥＲＭを統合する • コンプライアンス部門と事業部門との定期的な会議やコミュニケーションを行う

5．コンプライアンスリスクのレビューと修正

組織の法律、規制および倫理の環境は常に変化しており、頻繁に複雑さを増している。テクノロジーの進歩により、コミュニケーションと活動の速度が上がり、組織が影響を与えることができる個人の数は世界中に広がっている。小規模な組織であっても、複数の国や法域で事業を展開している場合があり、これらの場所の規制は急増している。組織の行動に対するステークホルダーの期待も高まり続けている。したがって、コンプライアンスリスクマネジメントを効果的に行うために、組織は、コンプライアンスリスクマネジメントの実務と能力を定期的にレビューし、C＆Eプログラムを継続的に改善するための措置を講じなければならない。

本章では、COSO ERMフレームワークの「レビューと修正」の構成要素と、コンプライアンスリスクの管理に関連する以下の3つの原則の適用について説明する。

⓯ 重大な変化を評価する
⓰ リスクとパフォーマンスをレビューする
⓱ 全社的リスクマネジメントの改善を追求する

原則 15 －重大な変化を評価する

組織の内部環境と外部環境の変化は、組織のコンプライアンスリスクプロファイルに重大な影響を与える可能性があるが、大抵、変化は非常に速いため、多くのコンプライアンスプログラムの基準は、定期的な再評価と修正が必要である。CCOは、コンプライアンスリスクを変化させ得る要因を特定する必要がある。それらの要因としては、大まかに以下が挙げられるが、これらに限定されるものではない。

- 組織の戦略や目標の変更
- 人、プロセスおよびテクノロジーの変化
- 規制要件および / または社会的期待の変化

原則6で述べているように、CCOは戦略設定プロセスに関与し、C＆Eプログラムが事業戦略や目標の大幅な変更に伴うコンプライアンスリスクの変化を識別して管理できるようにすべきである。例えば、あるテクノロジー企業が、医療システムの診療記録用にクラウドサービスを提供するなど、規制の厳しい環境下で新たな事業の開始や買収を決定した場合や、エンジニアリング企業が連邦政府との契約を開始しようとした場合などである。また、組織が業務プロセスに第三者を利用するという変更は、コンプライアンスリスクに大きな変化をもたらす可能性がある。

内部環境である人、プロセスおよびテクノロジーの変化も、コンプライアンスリスクに変化をもたらす可能性がある。例えば、上級職員[vii]の交代は、コンプライアンスカルチャーだけでなく、リスク許容度の大幅な変化をもたらす可能性がある。（コスト、売上、生産性、効率などの）パフォーマンスに対するプレッシャーの増大は、リスクに影響を与える可能性がある。M＆Aも、コンプライアンスリスクの変化を促すことがある。プロセスやテクノロジーの変化も、コンプライアンスリスクに変化をもたらす可能性がある。例えば、自動化によって、企業はより速く作業を実行できるようになる可能性があるが、これは失敗した場合の影響も大きくなる可能性があることを意味している。

外部環境の変化は、法律、規制、エンフォースメントの優先順位および社会規範や価値観の変化を通じて、組織のコンプライアンスリスクに影響を与える。コンプライアンスリスクへの影響の評価は、法令が法域を超えて拡散しており、しばしば矛盾する要件が存在するため、複雑さを増してきている。C＆Eプログラムは、業界団体や専門家グループからの情報だけでなく、エンフォースメントの傾向や規制当局が提供するガイダンスを調査して、規制環境の変化を常に把握しておく必要がある。また、C＆Eプログラムの識別と追跡を支援する規制変更管理アプリケーションも、洗練さを増してきている。

[vii] 訳注：本稿では「senior personnel」「high-level personnel」を「上級職員」と訳した。

表５．１　重大な変化を評価する

主要な特徴	• コンプライアンスリスクの内部と外部の変化要因を特定する • 新たな戦略的施策の実施がコンプライアンスリスクに与える影響を検討する • 上級職員の交代がコンプライアンスリスクおよび / またはリスク許容度に与える影響を検討する • 法令の変更を評価する • エンフォースメントの展開、規制当局のガイダンスおよびその他の動向を検討する • 地元や地域の環境の変化を評価する

原則 16 －リスクとパフォーマンスをレビューする

原則１の議論でも述べたように、取締役会は組織のＣ＆Ｅプログラムのパフォーマンスについて監督責任があり、ＣＣＯと経営者はプログラムの設計と導入について責任がある。取締役会と経営者がその責任を果たすためには、コンプライアンスリスクが許容範囲内で管理されているというアシュアランスを提供するための仕組みが必要である。

Ｃ＆Ｅプログラムのパフォーマンスをレビューする目的は、取締役会と経営者がコンプライアンスリスクを許容可能なレベルに管理する責任を果たすために必要なアシュアランスを提供するだけではなく、Ｃ＆Ｅプログラムを継続的に改善することにもある。規制当局は、効果的なコンプライアンスプログラムの重要な要素として、Ｃ＆Ｅプログラムのパフォーマンスをレビューすることに対する期待をより明確にしている。前述のように、ＵＳＳＧの効果的なコンプライアンスプログラムの７つの要素の１つには、「組織のコンプライアンスと倫理のプログラムの有効性を定期的に評価すること」に対する期待が含まれている。Ｃ＆Ｅプログラムのパフォーマンス評価に関する同様の期待は、世界中のさまざまな規制当局のガイダンスにも見られる。

期待されるのは、２種類のレビューである。すなわち、（１）コンプライアンス違反の発生可能性と影響度の評価に基づいて優先順位が高いと考えられるコンプライアンスリスクのレビュー、（２）Ｃ＆Ｅプログラムの全般的なパフォーマンスと有効性の定期的なレビュー、である。監査やモニタリングによるレビューに加えて、Ｃ＆Ｅプログラムのパフォーマンスに関するフィードバックを提供する別の仕組み、特に従業員などが不正行為の可能性について通報したりガイダンスを求めたりできる信頼できる制度の利用が期待されている。

優先順位の高い各コンプライアンスリスクについて、組織は、教育と研修の戦略策定に加えて、モニタリングと監査の計画を策定すべきである。このような計画の策定は、コンプライアンス機能が主導的に行うこともできるが、コンプライアンス機能だけの責任で行うべきではない。計画の策定には、リスクオーナー、内部監査、リスクマネジメントおよび関係する可能性のある人々が関与すべきである。計画の役割を明確にすることは、努力の重複やアシュアランスのギャップを最小限に抑えるために不可欠である。計画には、計画したリスク対応、対応の責任者、対応の有効性の測定方法およびパフォーマンスレビューの責任者なども記載すべきである。

役割の明確化に役立つモデルとして、内部監査人協会が2020 年７月に改訂した「３ラインモデル[viii]」（旧「３つのディフェンスライン」）がある。このフレームワークは、効果的なリスクマネジメントに関わる以下の３つのグループ（すなわち、ライン）を区別している。

第１ラインの役割（経営管理者）：

- （リスクの管理を含む）活動と資源の活用を主導し指示して、組織体の目標を達成する
- 統治機関と継続的に対話して、組織体の目標に関連する、計画された、実際の、および期待された成果、ならびにリスクについて報告する
- 業務と（インターナル・コントロールを含む）リスクを管理するために、適切な構造とプロセスを確立して維持する
- 法規制上のおよび倫理的な期待事項への遵守を確実にする

第２ラインの役割（経営管理者）：

- 以下のような、リスクの管理に関連する補完的な専門知識、支援、モニタリングを提供し、また、異議を唱える
  - プロセス、システム、および全社レベルでの（インターナル・コントロールを含む）リスク・マネジメント実務の策定、導入、および継続的な改善
  - 法規制および許容される倫理的行動の遵守、インターナル・コントロール、ＩＴセキュリティ、持続可能性、および品質保証のような、リスク・マネジメント目標の達成
- （インターナル・コントロールを含む）リスク・マネジメントの妥当性と有効性に関する分析とレポートを提供する

[viii] 日本語訳は、『月刊監査研究』2020 年 8 月号（37-41 頁）に掲載。本稿の翻訳でも、『月刊監査研究』掲載の訳語を引用。

第３ラインの役割（内部監査）：

- 統治機関に対する一義的なアカウンタビリティ、および経営管理者の責任からの独立性を維持する
- ガバナンスと（インターナル・コントロールを含む）リスク・マネジメントの妥当性と有効性について、経営管理者と統治機関に独立にして客観的なアシュアランスと助言を伝達することにより、組織体の目標達成を支援し、継続的な改善を奨励して促進する
- 独立性と客観性の侵害を統治機関に報告し、必要に応じてセーフガードを実行する

この３ラインの上にあるのが、組織の統治機関である。「３ラインモデル」では、統治機関の責任として次のようなものを挙げている。

経営管理者に責任を委ね資源を提供して、法規制上および倫理的な期待を確実に満たしながら、組織体の目標を達成する。

より簡単に言えば、取締役会は、コンプライアンスと倫理の機能を監督する責任がある。ＣＣＯが位置する経営者の最高位層は、コンプライアンスの確保を目的とした構造とプロセスの確立に責任を負う。次のレベルの経営者は、コンプライアンスと倫理の期待事項を達成するために、専門知識、支援およびモニタリングを提供する責任を負う。

図５．１は、このモデルを用いて、高リスク領域（大学病院における利益相反[ix]）の監査とモニタリングの計画を策定したものである。

図５．１　高リスク領域の監査とモニタリングの計画

	第１ライン	第２ライン	第３ライン
リスク領域	**経営管理者**	**経営管理者**	**内部監査**
リスク評価で識別した通り	構造と方針	モニタリングと支援	独立した監査
利益相反（ＣＯＩ）	• ＣＯＩ方針と手続の策定 • ＣＯＩ方針に関する職員教育 • ＣＯＩマネージャーへのコンプライアンス違反の報告 • 未承認のベンダーによる代理行為や展示物の報告 • 質問がある場合は、コンプライアンスに連絡するよう職員に助言 • ＣＯＩ年次開示のレビュー	• ＣＯＩの年次開示 • 購買先や医薬品ベンダーの登録 • 支払データベースの開設 • 医師・研究者の利益相反チェック用データベースの照合	• 出張旅費支払の 10%をサンプリングして、立替旅費の精算金額を検証する監査 • ＣＯＩ開示の２次レビュー •「開示すべきものなし」の 10%をサンプリングして検証する監査 •「正当な理由」の内容調査

高リスク領域の監査やモニタリングに加えて、Ｃ＆Ｅプログラム全体のレビューは、取締役会や上級経営者が求めるアシュアランスを提供するために必要であり、また、これは原則 17 の一部であり、Ｃ＆Ｅプログラムを継続的に改善する取り組みでもある。このレビューには、Ｃ＆Ｅプログラム全体の有効性を定期的に評価することが含まれる。とることができるアプローチはいくつかある。このレビューは、自己レビューとしてコンプライアンスと倫理の機能の者が、組織の内部監査機能が、あるいは外部のサービスプロバイダが実施できる。少なくともこのレビューでは、Ｃ＆Ｅプログラムが付録１に記載されている効果的なコンプライアンスプログラムのすべての要素（または他の適用可能な基準）を組み込んでおり、それらが効果的に運用されていることを確認すべきである。

Ｃ＆Ｅプログラムの有効性を評価するために利用できる別の資料には、ＤＯＪが連邦検察官に提供した「企業コンプライアンスプログラムの評価（Evaluation of Corporate Compliance Programs）[2]」というガイダンスがある。このガイダンスでは、組織のＣ＆Ｅプログラムに関して、次の３つの基本的な質問をしている。

1. 組織のＣ＆Ｅプログラムは適切に設計されているか。
2. プログラムは真剣かつ誠実に適用されているか。言い換えれば、プログラムは十分な資源を備えており、効果的に機能する権限を与えられているか。
3. Ｃ＆Ｅプログラムは実際に機能しているか。

これら３つの質問に対する答えを見つけるには、効果的なプログラムの各要素をさらに詳しく調べることに加えて、Ｃ＆Ｅプログラム全体を評価する必要がある。

[2] U.S. Dept. of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (updated June 2020), http://bit.ly/2Z2Dp8R.

[ix] 米国の医療分野では、医師や研究者と製薬会社や医療機器メーカーとの金銭的利害関係に関して厳しい規制があり、大学や病院では、医師や研究者個人が情報を開示するだけでなく、製薬会社や医療機器メーカーが個人に対して行った支払いについても、データベースで管理している。また、医師や研究者の出張旅費を製薬会社や医療機器メーカーが一部を負担していないかを、立替旅費の精算金額などでチェックしている。

ＤＯＪのフレームワークで注目すべき問題の１つは、Ｃ＆Ｅプログラムの全体的なレビューに、組織のコンプライアンスカルチャーの測定を含めることが期待されている点であり、これには、上級経営者と中間管理者のコンプライアンスへの取り組みについて、全階層の従業員がどう認識しているかを確認するための意見を求めることが含まれている。

最後に、モニタリングと監査に加えて、Ｃ＆Ｅプログラムのパフォーマンスに関するフィードバックを提供する別の仕組みがある。従業員などが、組織に関わる不正疑義事案を通報できる内部通報制度は、調査や是正が必要な具体的な事案を特定し、また、プログラムを改善する機会をもたらす可能性がある。従業員はこの制度を利用して、自身の仕事や職場環境について指導を受けたり質問をしたりすることもできる。

通報された不正行為の申し立ての調査によって、実際に不正行為があったと結論づけられた場合、組織は、Ｃ＆Ｅプログラムの適切な修正を含む、対応と同様の不正行為の再発防止のために適切な措置を講じるべきである。（モニタリングと監査の結果やその他のデータも含めた）内部通報制度のデータの傾向分析は、Ｃ＆Ｅプログラムの設計や実施におけるギャップを特定するために使用すべきである。しかし、多くの組織では、内部通報制度を通じて通報される不正行為事案はごく一部に過ぎないため、他のフィードバックやデータポイントも考慮しなければならないことが調査によって一貫して判明している。例えば、多くの従業員は、内部通報制度を利用するのではなく、監督者に不正行為を報告している。大半の場合、これらは監督者や組織内の他の者によって処理されるが、データは必ずしも追跡されずコンプライアンスに報告されないため、Ｃ＆Ｅプログラムのパフォーマンスに関するフィードバックはない。このフィードバックを得るために、一部の組織では、コンプライアンスが追跡と分析を行えるようにするために、監督者がこのような事案をコンプライアンスに報告することを義務づける方針を取っている。

その他の仕組みには、組織内で不正行為を目撃したかを尋ねる退職時面談からの情報、定期的な従業員へのアンケート調査およびコンプライアンス研修の受講者からのフィードバックがある。

表５．２　リスクとパフォーマンスをレビューする

主要な特徴	• コンプライアンスと倫理に関する指標に対するパフォーマンスをモニターし、経営者や取締役会レベルに報告する • コンプライアンスリスク評価を定期的に更新する • 優先順位の高いリスクに対するモニタリング計画を策定し、３ライン間でアシュアランスの責任を明確に割り当て、パフォーマンスに対する明確な期待を設定する • 内部監査は、組織のリスクとパフォーマンスのレビューに関連して、コンプライアンスリスクを考慮するようにする • 組織のコンプライアンスカルチャーを定期的に評価する • Ｃ＆Ｅプログラムの年次作業計画にリスク評価を反映させる（相互参照する） • モニタリングや監査を容易にするために、第三者との契約にしかるべき監査権条項を盛り込む • コンプライアンス研修の参加者、内部通報の報告書、従業員へのアンケート調査および退職時面談からフィードバックを得る • 是正措置計画の実施を、経営者と取締役会がモニターする重要な指標とすることを義務づける • 経験したコンプライアンスリスク事象の根本原因分析を実施する

原則 17 －全社的リスクマネジメントの改善を追求する

効果的なＣ＆Ｅプログラムの重要な指標の１つは、継続的な改善へのコミットメントである。原則 15 と 16 では、組織内と組織を取り巻く環境の重大な変化を識別してプログラムの有効性におけるギャップを特定するために、さまざまな仕組みを利用することの重要性を説明している。しかし、単に問題を特定するだけでは十分ではない。Ｃ＆Ｅプログラムを調整して改善するための措置を講じなければならない。規制当局は、Ｃ＆Ｅプログラムをレビューして、陳腐化させないような措置を講じる努力を組織が示すことの重要性を一層強調するようになってきている。多くの規制当局は、組織による積極的な取り組みに対して、解決の合意や起訴の判断において罰金や要件の低減という形で報いる可能性がある。

ＣＣＯは、取締役会と、そして組織内にコンプライアンス委員会が存在する場合はその委員会と、定期的に会合を持つべきである。その際、Ｃ＆Ｅプログラムのパフォーマンスレビューの結果やＣ＆Ｅプログラムのパフォーマンスにおけるギャップに対処するための行動計画案に加えて、プログラムの積極的な改善についても共に話し合うべきである。さらに、不正行為が発見された場合には根本原因を究明するために調査結果を分析し、Ｃ＆Ｅプログラムにどのような調整が必要かを判断し、各委員会と協議すべきである。

Ｃ＆Ｅプログラムの調整と改善が必要な場合は、適切な行動計画を策定してスケジュールと具体的な責任を割り当てるべきである。行動計画の進捗は追跡すべきであり、適切なフォローアップを行うべきである。

Ｃ＆Ｅプログラムの改善は、実際は、すべてが反応的に行われるわけではない。継続的改善の重要な側面は、先を見越した対策を講じることである。組織は、プログラムのパフォーマンスと有効性を向上させる可能性のある新しいツールや改良されたツールはもちろん、革新的なアプローチについても常に最新情報を入手すべきである。

Ｃ＆Ｅプログラムの継続的な改善に貢献するもう１つの活動は、他の組織の実務に対するベンチマーキングである。多くの場合、これは同じ業界内で行われるが、業界内でもコンプライアンスプログラムの成熟度には大きな差があるため、あまりにも限られたものになる可能性がある。他の業界、特に規制環境のためにかなりの期間コンプライアンスリスクの高まりに対処してきた業界を見ることで学べることは多い。

表５．３　全社的リスクマネジメントの改善を追求する

主要な特徴	• （研修、規制当局のガイダンスの確認などを通じて）コンプライアンスリスクマネジメントに関する最新動向を把握し続ける • コンプライアンス機能がＣ＆Ｅプログラムのパフォーマンスを定期的に自己評価するようにする • 共有したコンプライアンスリスク情報の質と有用性について、取締役会からフィードバックを得る • Ｃ＆Ｅプログラムの定期的な独立評価の取得を検討する • 類似の組織とのＣ＆Ｅプログラムのベンチマーキングを検討する • コンプライアンスリスクの評価プロセスの有効性を定期的にレビューする • Ｃ＆Ｅプログラムの有効性を定期的に評価するために、内部監査が積極的な役割を果たすようにする

6．コンプライアンスリスクの情報、伝達および報告

本章では、COSO ERMフレームワークの「情報、伝達および報告」の構成要素と、コンプライアンスリスクの管理に関連する以下の３つの原則の適用について説明する。

⑱ 情報とテクノロジーを有効活用する
⑲ リスク情報を伝達する
⑳ リスク、カルチャーおよびパフォーマンスについて報告する

原則 18 ―情報とテクノロジーを有効活用する

コンプライアンス機能がC＆Eプログラムを効果的に管理するためには、C＆Eプログラムの各要素に関連する情報へ適時にアクセスできなければならない。例えば、モニタリングと監査の機能を効果的に遂行するためには、コンプライアンス機能がコンプライアンス違反やコンプライアンス関連の内部統制の機能不全を発見するために、すべての情報にアクセスできなければならない。

テクノロジーは、C＆Eプログラムのいくつかの側面に関して、重要な財産となり得る。例えば、テクノロジーを活用したコンプライアンス意識向上研修は、さまざまな方法と形式で実施することができ、教室での集合研修のような他の方法と比較して、双方向な機能によって学習効果を高めることができる。また、テクノロジーを利用した研修は、新しい問題に迅速に対応したり単に研修の鮮度を保ったりするために、簡単に更新できる場合が多い。

C＆Eプログラムのモニタリングと監査という要素ほど、テクノロジーがコンプライアンスに役立つ所はない。監査に対するサンプリングというアプローチとは異なり、適切に設計されたデータアナリティクスでは、危険信号があるかについて取引や活動の母集団を 100%分析できる。これらのテストは、（1）コンプライアンス違反を予防するために設計された内部統制の機能不全、（2）コンプライアンス違反の事案やパターン、（3）コンプライアンス違反を発見するために設計された内部統制の機能不全、（4）コンプライアンス違反のその他の指標や影響、を対象とすることができる。データアナリティクスでは、これら４つの対象のいずれかに一致する異常を特定するために、デジタル記録を調べる。さらに、適切に設計されたデータアナリティクスは、リスク評価に基づいて、優先順位の高いコンプライアンスリスク領域に焦点を当てた形で展開できる。

例えば、デジタルマーカーは、コンプライアンスに関する特定の内部統制が設計通りに機能しているかを示せる（例：監督者によるレビューや承認が電子的に行われる場合に、レビューや承認に対する期待にデジタル証拠が一致しているか）。また、デジタル証拠によって、取引が完了したはずの後に記録が変更されたりすり替えられたりしたことを示すなど、コンプライアンス違反と一致するその他の異常も明らかにできる。アナリティクスは、コンプライアンス関連の異常を特定するために、非構造化データにも適用できる。テクノロジーによって、組織は電子通信（例：電子メール、テキストメッセージなど）やその他のテキスト（例：発注書の説明、仕訳入力など）をスキャンしたり積極的にモニターしたりして、不正な活動の兆候を見つけることを可能にする。例えば、従業員が重要なコンプライアンス統制を無効にするリスクを高める、期限を守ることへの極端なプレッシャーの兆候が、管理者と部下とのコミュニケーションから明らかになる可能性がある。

情報とテクノロジーのもう１つの用途として、組織の内部通報制度によって提供された情報の初期評価を行うことが挙げられる。

表６．１　情報とテクノロジーを有効活用する

主要な特徴	• コンプライアンスリスクを効果的に管理するために、関連するすべての情報にコンプライアンスがアクセスできるようにする • コンプライアンスに、関連するＩＴやデータアナリティクスのスキルを提供するか、そのようなスキルが利用できるようにする • モニタリングや監査でデータアナリティクスを活用する（コンプライアンスと内部統制のパフォーマンスのモニタリング） • コンプライアンスのモニタリングのために、自動化されたダッシュボードやレポートを作成する • コンプライアンスと倫理の研修を効果的に実施するために、テクノロジーを活用する • リスク評価プロセス（スコアリング、レポーティング等）を促進するために、テクノロジーを活用する

内部通報窓口への通報は、具体的なコンプライアンス違反や職場での倫理にもとる行為に関する申し立てについての貴重な情報源となり得る。本格的な調査や従業員への聞き取りに先立ってデータアナリティクスを活用すると、申し立ての信憑性を評価したり調査範囲の絞り込みに役立てたりできる。

また、情報とテクノロジーを活用して、事業部門ごとにカスタマイズしたダッシュボードやその他のレポートを管理者に提供することもできる（原則 20 で詳しく説明）。コンプライアンス関連の活動やモニタリングの取り組み結果について適時な情報を得ることで、管理者は迅速に行動して特定された問題の影響を最小限に抑えることができる。

原則 19 －リスク情報を伝達する

C＆E プログラムにとって有益な特徴の中でも、コミュニケーションは最も重要なものである。コンプライアンス機能は、事実上、組織内のすべての事業部門や機能と交流して、組織を脅かすコンプライアンスと倫理のリスクを識別して管理し、コンプライアンスと倫理のリスクに関する質の高い研修と情報を提供し、コンプライアンス事項に関する申し立てや懸念へ対応する上で、パートナーとして活動すべきである。

C＆E プログラムが効果的であるためには、コンプライアンスと各事業部門とのパートナーシップが不可欠である。事業部門が自らの業務を誰よりもよく知っているように、CCOとコンプライアンスチームほど、事業部門がコンプライアンスと倫理の問題の影響を理解するのを支援する立場にある者はいない。したがって、コンプライアンスリスクの管理は、コンプライアンスと各事業部門との間で定期的に対話が行われ、その結果、コンプライアンスと業務効率のバランスをとるというミッションが共有された場合に最も効果的となる。このコミュニケーションは、単にコンプライアンスから業務へのコミュニケーションではなく、双方向のものである。業務部門は、解決策が効果的かつ実用的であり、業務部門のリーダーがもたらす現実的な洞察に基づいて構築されることを確実にするような方法で、コンプライアンスに関与することができなければならない。

コンプライアンスに関する効果的なコミュニケーションには、重要なカスケード効果もある。倫理観やコンプライアンス意識に関する広範な声明は、最高経営者層や取締役会から発信すべきである。その後、管理者や監督者は、C＆E プログラムにおいて従業員が果たす役割をより個人に合ったものにするために、各部門、各機能、さらには具体的な職務に合わせたコミュニケーションを策定して提供すべきである。このプロセスにおいてCCOとコンプライアンスチームは、ガイダンスを提供したり、組織が経験したコンプライアンス違反から学んだ教訓に言及するメッセージを含めた特定のメッセージの作成を支援したりすることさえあり、重要な役割を果たす。

コミュニケーションは、電子メール、ポスターおよびその他の定期的な手段から、タウンホールミーティング、会議およびその他のイベントまで、さまざまな形式でとることができる。管理者や監督者からの非公式なコミュニケーションは、C＆E プログラムに関連する従業員の役割と責任を明確にするためのもう 1 つの効果的な手段である。まとめると、これらのさまざまなコミュニケーション方法によって、原則 5 に関連して説明した、より正式なコンプライアンスと倫理の研修を強化すべきであり言及すべきである。

コンプライアンスに関するコミュニケーションで見落とされがちな領域の 1 つは、上申の方針や手順に関連する部分である。ある種の申し立て、問題、発見または調査は、その問題の調査を担当するチーム以外にも開示すべきである。例えば、不正行為の申し立てが組織の下級社員に向けられたものである場合、そのような問題の調査を担当するチームは、組織内の他の多くの人々に知らせる必要はない。しかし、申し立てが経営陣の 1 人に対するものであった場合、または非常に深刻な問題に関わるものであった場合は、取締役会に対してある程度の情報開示が必要である。

コミュニケーションの最終ステップには、原則 1 で紹介したように、取締役会または取締役会の委員会が関与する。このコミュニケーションの多くは、原則 20 で説明される報告を通じて行われる。コンプライアンスリスクマネジメントの重要な側面は、取締役会とCCOの間で行うべきリスクに関する議論であり、取締役会がCCOに対して、内外のすべてのコンプライアンス要因が考慮されていることを確認することも含まれる。どんなに詳細な内容であっても報告書を提出するだけでは十分ではなく、プログラムの有効性を示すことはできない。それでは、規制当局が期待するレベル、あるいはコンプライアンスリスクを効果的に管理するために不可欠なレベルの監督を示すことはできない。報告書で取り上げた問題について直接説明し、有意義な情報を提供し、プログラム改善のための実行可能な計画について話し合うことは、いずれもコンプライアンスリスクを効果的に管理するための重要なステップである。

表 6．2　リスク情報を伝達する

主要な特徴	• C＆E に関する各自の役割について、従業員が明確かつ定期的なコミュニケーションを受けるようにする • CCOによる取締役会への定期的な報告を義務づける • 上申の手順を確立し、上申方針が明確に理解されるようにする • 研修と職責に関連し、それらを支援するような、コンプライアンスリスクのコミュニケーションを提供する • 業務部門の経営者とコンプライアンスとの間で効果的な双方向コミュニケーションをとる

原則 20 －リスク、カルチャーおよびパフォーマンスについて報告する

リスク情報の伝達と密接に関連するのは、コンプライアンス関連リスクに関わるリスク、カルチャーおよびパフォーマンスに関する報告である。報告先となるステークホルダーには、取締役会、（存在する場合は）コンプライアンスリスクの監督を委任された取締役会レベルの委員会、上級幹部チーム、（存在する場合は）内部コンプライアンス委員会および組織内のしかるべき管理職と部門や機能の責任者などが含まれる。これらのグループへの報告は、報告の頻度と同様に、各グループ特有のニーズと責任に合わせて行うべきである。

例えば、取締役会への報告は、C＆Eプログラム全体を効果的に監督するために必要なものに焦点を当てるべきである。すなわち、リスク評価プロセスに関する情報、最も重要なリスクの識別とそれらのリスクに対応するために取られた措置、プログラムの構造的なパフォーマンスと実質的なパフォーマンスの両方に対応する有意義なコンプライアンス指標、コンプライアンス関連の調査、資源配分およびニーズの情報などである。取締役会への報告は、コンプライアンスと倫理に関連するカルチャーについても定期的に取り上げるべきである。カルチャーは評価が難しい領域であるが、コンプライアンスと倫理に関連する組織のカルチャーの展望と傾向を取締役会に提供するよう努力すべきである。これは、従業員へのアンケート調査、カルチャーに関連するデータおよびインタビューやフォーカスグループのような、あまり正式でない方法によって達成できる。

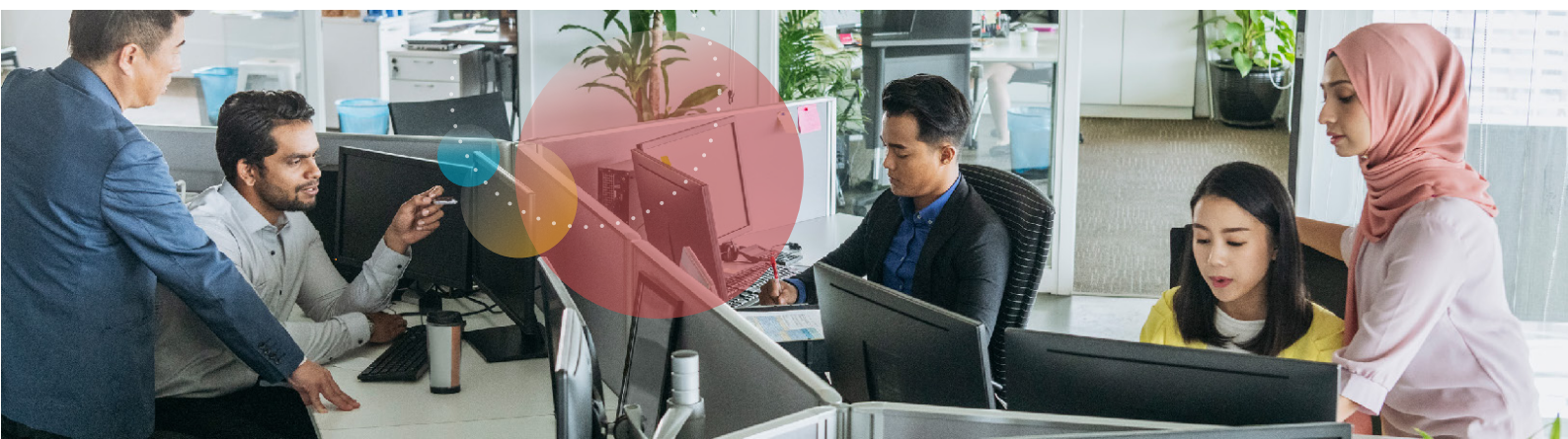
報告書は組織図の階層ごとに設計されるため、含める情報はより細かくすべきであり、また、各階層のニーズに合わせてカスタマイズすべきである。組織全体のリスクに関する定期的な報告が有用な背景情報をもたらす場合があるものの、部門長や管理者層が報告を受け取る時点の情報は、担当領域のコンプライアンスリスクを管理するために必要なものに焦点を当てるべきである。

コンプライアンスリスクマネジメントに関する報告は、内部のリスク対象領域（例：従業員の行為）に起因するリスクだけでなく、外部で発生したリスクも取り上げるべきである。第三者のリスクマネジメントは、C＆Eプログラムの重要な要素の１つである。したがって、組織にリスクをもたらす可能性のある第三者のサプライヤーや販売代理店などの状況について、報告書を作成してしかるべきステークホルダーに配付すべきである。これらの報告書は、ベンダーやその他の第三者の選定や継続的な使用を判断するための第三者によるデューディリジェンスの結果、現地視察、監査とモニタリングの手続、第三者に対する研修およびこの領域のリスクの管理に関連するその他の事項に焦点を当てるべきである。

C＆Eプログラムの有効性に不可欠な報告の最後の側面は、文書化である。通常、調査に関わる文書は、コンプライアンス、法務および / または調査チームによってのみ維持されレビューされる。法的措置や政府からの照会があった場合に備えて、これらの資料や記録は適切に扱い、保存し、維持することが極めて重要である。コンプライアンスに関連する各調査は、事象の時系列とその過程で行われた主要な手順や行動を含めて十分に文書化すべきであり、また、あらゆる是正措置も要約すべきである。正式な事案管理ソフトウェアツールを使用するにしても、もっと簡単なものを利用するにしても、この記録を維持することは、C＆Eプログラムの重要な部分である。これらの記録から、コンプライアンスリスクマネジメントの調査の要素の必要性と有効性を理解するための有用な報告書が作成できる。

表６．３　リスク、カルチャーおよびパフォーマンスについて報告する

主要な特徴	• コンプライアンスと倫理のリスク評価と関連する是正措置について、主要なステークホルダーのニーズに合わせた定期的な報告書を提供する • C＆Eプログラムの有効性に関連する有意義な業務上の指標と実質的な指標を策定して報告する • 管理者に対して、直属の部下の研修の修了状況と結果を報告する • 調査と結果を管理するために、事案管理・報告システムを利用する • すべての重要な是正の取り組みについて、報告の内容を明確にした方針を策定して従う



付録１.
効果的なコンプライアンスと倫理のプログラムの要素

はじめに

効果的なコンプライアンスと倫理のプログラムの７つの要素は、米国連邦量刑ガイドライン（ＵＳＳＧ）第８章パートＢ２.１、サブセクション(ｂ)に以下のように記載されている。

（１） 組織は、犯罪行為を予防および発見するための基準と手続を確立するものとする。

（２）（Ａ）組織の統治機関は、コンプライアンスと倫理のプログラムの内容と運用について知識を有するものとし、また、コンプライアンスと倫理のプログラムの導入と有効性に関して合理的な監督を行うものとする。

（Ｂ）組織の上級職員は、本ガイドラインに記載されているように、組織が効果的なコンプライアンスと倫理のプログラムを有していることを確実にするものとする。上級職員の中の特定の者に、コンプライアンスと倫理のプログラムに対する全般的な責任を負わせるものとする。

（Ｃ）組織内の特定の個人に、コンプライアンスと倫理のプログラムの日常的な運用責任を委ねるものとする。運用責任を有する個人は、コンプライアンスと倫理のプログラムの有効性について、定期的に上級職員に、また、必要に応じて統治機関または統治機関のしかるべき下位グループに報告するものとする。このような運用上の責任を果たすために、当該個人には、適切な資源、適切な権限および統治機関または統治機関のしかるべき下位グループへの直接のアクセスが与えられるものとする。

（３） 組織は、デューディリジェンスの実施により、違法行為または効果的なコンプライアンスと倫理のプログラムに反するその他の行為に関与していることを組織が知っていた、または知っていたはずの個人を、組織の実質的権限者の中に含めないよう、合理的な努力を払うものとする。

（４）（Ａ）組織は、効果的な研修プログラムを実施するか、その他の方法で個人の役割と責任に適した情報を広めることにより、サブパラグラフ（Ｂ）で言及する個人に、組織の基準と手続およびコンプライアンスと倫理のプログラムのその他の側面を、定期的かつ実用的に伝えるための合理的な手段を講じるものとする。

（Ｂ）サブパラグラフ（Ａ）で言及された個人とは、統治機関の構成員、上級職員、実質的権限者、組織の職員および必要に応じて組織の代理人である。

（５）組織は、以下について合理的な手段を講じるものとする。

（Ａ）犯罪行為を発見するためのモニタリングや監査など、組織のコンプライアンスと倫理のプログラムの遵守を確実にすること

（Ｂ）組織のコンプライアンスと倫理のプログラムの有効性を定期的に評価すること

（Ｃ）組織の職員と代理人が、報復を恐れずに犯罪行為の可能性または現実の犯罪行為に関して通報するまたは指導を求めることができる、匿名または極秘を可能にする仕組みを含む制度を保有し公表すること

（６）組織のコンプライアンスと倫理のプログラムは、（Ａ）コンプライアンスと倫理のプログラムに従って業務を遂行するための適切なインセンティブ、（Ｂ）犯罪行為に関与した場合および犯罪行為を予防または発見するための合理的な措置を講じなかった場合の適切な懲戒措置、を通じて組織全体で一貫して推進して実施するものとする。

（７）犯罪行為が発見された後、組織は、犯罪行為に適切に対応し、さらに同様の犯罪行為の再発を防止するために、組織のコンプライアンスと倫理のプログラムに必要な修正を加えることを含む、合理的な措置を講じるものとする。

第８章パートＢ２．１、サブセクション（ｃ）には、次のように記載されている。

サブセクション（ｂ）を実施するにあたり、組織は、犯罪行為のリスクを定期的に評価するものとし、また、このプロセスを通じて識別された犯罪行為のリスクを低減するために、サブセクション（ｂ）に定める各要件を設計、導入または修正する適切な措置を講じるものとする。

2004 年に追加された、コンプライアンスリスクの定期的な評価とＣ＆Ｅプログラムの継続的な改善を求めるこの最終条項は、Ｃ＆Ｅプログラムの８番目の要素と呼ばれることが多い。

Ｃ＆Ｅプログラムが効果的であると見なされるためには、Ｃ＆Ｅプログラムの７つのすべての要素が定期的なリスク評価と継続的なプログラムの改善とともに整備され、適切に機能しなければならない。なお、7 つの要素を定めたＵＳＳＧは、連邦裁判官のためのガイドラインであるが、組織にとっては「ガイドライン」をはるかに超えている可能性があることに注意すべきである。要素に関連して「するものとする（shall）」という言葉が 17 回出てくるが、このガイドラインは、少なくとも米国で活動する米国の組織やその他の企業、および米国を拠点とする多国籍企業にとって、効果的なＣ＆Ｅプログラムを構築するための最低基準であるとの見方が強い。

この付録は、これらの各要素の概要を説明し、本稿の前の章にあるＥＲＭへの適用に関するガイダンスを理解するための基礎を形成している。

基準と手続

行動基準は、倫理的な職場と法令を遵守するカルチャーに対する組織のコミットメントを示すものである。これは、行動・倫理規範から始まる。その規範は、すべての従業員、経営者および取締役会に適用されるように設計すべきである。規範は、多くの方針と手続によって支えられている。規範は、ベンダーやサプライヤーなどの一定の第三者にも適用すべきであるが、この規範は、従業員に適用される規範とは異なり、より簡略化されたものになることが多い。

Ｃ＆Ｅプログラムには、構造的なものと実質的なものという、２種類の方針と手続が不可欠である。構造的な方針は、プログラムがどのように運用されるかというフレームワークを作るものである。実質的な方針は、事業活動に適用される主要な法律、規制および基準に対する組織の立場を示すものである。

構造的な方針と手続の例には、コンプライアンス責任者、コンプライアンス委員会および取締役会の役割と責任、不正疑義事案の報告方法、監査とモニタリングに用いるプロセス、調査の責任と手続、その他多くの事項を定めるものがある。

実質的な方針は、個々のリスク領域に関連する従業員の行動に対する組織の期待事項を伝えることにより、具体的なコンプライアンス違反（例：贈収賄、不正請求、独占禁止、環境、記録保持）の予防と発見に焦点を当てるものである。

ガバナンス、監督および権限

コンプライアンスと倫理の機能は、取締役会、経営者およびコンプライアンス責任者のレベルでの、効果的な監督の対象とすべきである。

取締役会は、効果的なＣ＆Ｅプログラムを確実に整備し、プログラムの内容や運用について知識を持つことによってプログラムの適切な監督を行うという明確な責任がある。また、取締役会は、ＣＣＯを組織内の上級階層に位置づけ、プログラムを効果的に管理するための十分な資源と権限を持たせなければならない。

取締役会レベルでのコンプライアンスの監督は、監査委員会やコンプライアンス委員会などの委員会に委ねられる場合もある。また、取締役会全体としてコンプライアンスの監督を行う場合もある。いずれにせよ、ＣＣＯは、最高経営責任者（ＣＥＯ）などの別の経営幹部職への報告ラインがある場合であっても、取締役会または取締役会の委員会と報告関係を持つべきである。

この点で、コンプライアンス機能は内部監査機能に似ており、独立性と自律性が重要である。日常業務の観点からは、コンプライアンス専門家の責任者は、他の上級経営者に報告する場合があるが、コンプライアンス責任者が他の経営者から干渉されることなく率直な議論ができるように、常に取締役会への直接の報告ラインも確保すべきである。

取締役会は監督を行うが、経営者は、従業員が研修を修了し、懸念を報告し、問題を解決し、プログラム要件に合致した業務活動を行うようにするなど、プログラムの実施に責任を負う。ＵＳＳＧは、プログラムが効果的であることを確実にする責任を負うのは、最終的には経営者であると認めた。

ＣＣＯは、Ｃ＆Ｅプログラムの運用に日常的な責任があり、プログラムの運用に必要な資源と情報へのアクセスを持たなければならない。ＤＯＪは、2020 年 6 月に改訂した「企業のコンプライアンスプログラムの評価（Evaluation of Corporate Compliance Programs）」ガイダンスの中で、コンプライアンスプログラムを評価する際に考慮する要因のリストに「十分な資源」を追加した。

また、主要な機能領域および / または事業部門からの代表者で構成される内部コンプライアンス委員会が存在する場合もある。ＣＣＯはＣ＆Ｅプログラムの最も歴然たるリーダーであるが、内部コンプライアンス委員会は、各事業部門が同

じようにコンプライアンスに取り組むことを確実にする、非常に効果的なプログラム管理方法となり得る。このようなコンプライアンス委員会のもう１つの利点は、Ｃ＆Ｅプログラムの全般的な目標を支えるための、機能領域を超えた協働とインプットによって生み出される価値である。

コンプライアンスの監督の最後の重要な要素は、これらの機能や委員会のそれぞれの役割と責任について、明確かつ書面による理解を得ることである。これは、基本規程や方針の形で文書化できる。

権限委譲におけるデューディリジェンス

組織は、新たに従業員を雇用する前に身元調査を行い、法律で許可または要求されている場合には、さらに定期的な調査を行うべきである。さらに、組織は、従業員をより大きな権限のある職位に昇進させる場合、その者が過去に組織のＣ＆Ｅプログラムを支援した（または支援や実行をしなかった）ことを考慮すべきである。身元調査のレベルと種類は、コンプライアンスリスクに関連してその者が担う、または担う予定の役割に基づいて、各従業員の職位に対応したものとすべきである。

ＵＳＳＧは、この期待を「実質的権限者」に関連して言及しているが、この用語は、適用上の注意の中で「組織のために行動する際に、その権限の範囲内で実質的な裁量を行使する個人」と定義しており、これらの個人は経営者と考えられる場合もあれば、そうでない場合もあると指摘している。このことから、責任の度合いが大きくなるにつれて、注意義務の範囲も大きくなることが明らかに推測される。コンプライアンスは、これらの判断をするために人事やその他の機能の協力を望む場合がある。

ＵＳＳＧには明示されていないが、規制当局は、組織にコンプライアンスリスクを生じさせる、またはコンプライアンスリスクに関与する第三者に対して、適切なレベルのデューディリジェンスを実施することを期待するようになった。例えば、ある企業が他国にいる第三者を組織の代表として利用する場合や、その国の顧客に販売する場合、関連するコンプライアンスリスクの評価レベルに基づいて適切な規模の身元調査を行うことが期待される。

コミュニケーションと研修

コミュニケーションと研修は、効果的に行われると、コンプライアンス問題の予防と発見に貢献する。すべての従業員と取締役は、プログラムにとって重要な一般的なテーマに関する研修を受けるべきであり、各コンプライアンスリスクに関連する業務に携わる者には、具体的なコンプライアンス事項により焦点を絞った研修を行うべきである。

少なくとも年１回、すべての従業員と取締役を対象に行われる一般的な研修は、強固で効果的なプログラムの象徴である。一般的な研修は、行動規範、コンプライアンスと倫理のカルチャーの維持、不正疑義事案の指導の求め方と通報方法、組織の報復禁止方針、コンプライアンス問題疑義事案が通報された場合の組織の対応およびその他全員に影響を与えるプログラムのあらゆる関連側面が網羅されている。

焦点を絞った研修は、具体的なコンプライアンスリスク領域、重要な内部統制および特定のリスクに関連するその他の手続について深く掘り下げるものである。そのため、通常、これらのリスク領域に関わる重要な役割を担う従業員のみが、この種の研修に参加することを義務づけられる。焦点を絞った研修の例には、国際的企業の営業担当者を対象とした海外腐敗行為防止法遵守のための研修がある。全従業員が同法の違反について理解する必要はないが、国際的な営業に携わる従業員（および関連する支援チームや財務チーム）は、このリスクと、不正行為を予防するために組織が導入した統制と手続を正しく理解することが重要である。

研修が効果的であるためには、単に教育内容を伝えるだけでは不十分である。2020 年 6 月のガイダンスの中で、ＤＯＪは、（1）研修中に従業員が質問できるようにすること、（2）研修が従業員の行動に影響を与えたかを評価すること、の重要性を強調した。

コンプライアンスをテーマとした研修の多くは、従来の教室でのプレゼンテーションやオンラインのウェブベースのプログラムの形で行われているが、研修には他の形態の教育やコミュニケーションも含まれることがある。例えば、電子メールや社内報を利用して、コンプライアンス要件の新設や変更について従業員に知らせたり、従来の研修を強化したりできる。また、コミュニケーションは、組織が経験したコンプライアンス違反から学んだ教訓を取り上げることもある。

組織は、第三者のコンプライアンス違反について説明責任を負う場合がある。したがって、関連するコンプライアンスリスクの種類とレベルの評価に基づいて、各第三者を対象とした研修を検討すべきである。

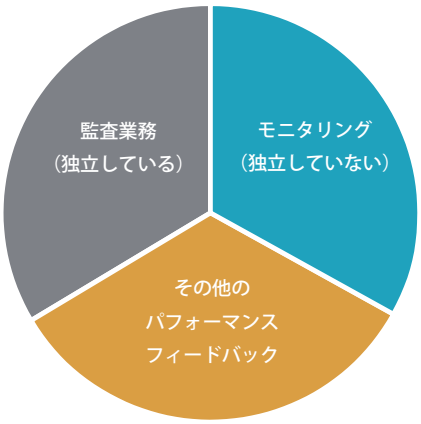
最後に、その他の一般的なコミュニケーション形式も、コンプライアンスと倫理のカルチャーを創造して維持するのに役立つ。例えば、ＣＥＯからの応援メッセージ、社内報の情報提供記事など、さまざまなものがある。

モニタリング、監査および通報制度

モニタリングとは、広義には、システムの改善に向けて、プロセスが意図したとおりに動いているかを評価することである。「監査」がシステムから独立した個人による評価を指すのに対して、「モニタリング」という言葉は、より狭義に使われることもある。監査とモニタリングは、同じ手法や技法で

行われ、システムのパフォーマンスの質について長期的にアシュアランスを得て、その継続的な改善に貢献することを目的としている（図A．1参照）。

図A．1　監査、モニタリングおよび報告



したがって、監査は、レビュー対象の機能から独立した個人によって行われる。監査は、内部監査部門やその他の第三者、あるいは独立性を維持するように構成されている場合はコンプライアンス機能内の個人によって行われることがある。モニタリングは、品質保証機能によって、あるいはレビュー対象機能内の管理者、監督者およびその他の従業員によって行われることが多い。

モニタリングと監査の計画は、コンプライアンスプログラムの有効性を高める重要な推進力であり、定期的なリスク評価に基づいて設計して更新すべきである。モニタリング業務や監査業務は、（1）コンプライアンス違反（またはその兆候）の発見、（2）予防的または発見的な統制が設計どおりに機能していない領域のようなコンプライアンスに関する内部統制の機能不全の識別、の両方を目的とすべきである。モニタリングと監査には、多種多様な手法が用いられることがある。例えば、観察や現地訪問、アンケート調査、質問票やチェックリスト、インタビュー、取引や書類のレビュー、データアナリティクスおよびデジタル証拠のレビューなどである。また、監査機能は、C＆Eプログラムの全般的な有効性について、取締役会にアシュアランスを提供することもある。

効果的なC＆Eプログラムのもう1つの重要な仕組みは、従業員（およびその他の人々）が不正疑義事案を通報したり指導を求めたりするための信頼のある制度を維持することである。従業員は、コンプライアンスと倫理の問題について指導を求めたり、法律、規制または組織の方針や手続に違反する可能性があると思われることを通報したりするための手段を複数持つべきである。

従業員には事案を監督者に報告することが奨励されるかもしれないが、それが望ましくない、あるいは現実的でない状況があることを組織は認識しなければならない。したがって、従業員が通報のための別の選択肢を知っていることが重要である。別の選択肢としては、（社内または独立した第三者が運用する）電話や電子メールによる制度、あるいは人事、コンプライアンス、内部監査、調査部門、上級経営者の特定の者、さもなければ取締役会や監査・コンプライアンス委員会など、組織内の他者に直接通報することが考えられる。

効果的な通報制度の特徴には、次のことを可能にする利用者のための選択肢がある。

1．**匿名の通報**－（法律で認められている場合）報告者の身元を明らかにせず、内部通報や類似の仕組みで実現されることが多い
2．**極秘の通報**－報告者の身元が一部の者にのみ知られ、その一部の者は、問題を追及する間、機密を保持するために合理的な措置を講じることが期待されている
3．**オープンな通報**－通報者は制限なしに自身の身元を開示する用意があるか、それを望んでいる

これらおよびその他の通報方法は、通報制度を運用する国や地域の連邦法、州法、地元法を考慮して作成すべきである。

どのような通報でも、効果的であるためには信頼されなければならない。信頼は多くの要因によってもたらされるが、最も重要な2つは、（1）組織が申し立てや懸念を真剣に受け止め、それに対して適切な評価を行うと信じられること、（2）通報者が観察や懸念を誠実に通報した後に報復を受けないことが期待できること、である。

最後に、DOJは、従業員に加えて第三者にも通報制度を公表することを奨励している。ベンダー、サプライヤーおよびその他の第三者は、従業員がすぐには観察できない可能性のある違反の兆候を観察する独特の立場にあることが多い。

通報されたすべての事案は、適時に検討され評価されなければならない。通報の評価は、通報者から提供された情報、考えられる違反の内容と重大性および通報に関連するその他の既知の情報に基づいて、さらに調査が必要かを検討すべきである。

どんなに信頼されている制度であっても、組織を離れるまでは不正行為を通報することに抵抗を感じる従業員もいる。そのため、退職時面談では、従業員が不正疑義事案を報告したりC＆Eプログラムに関連するその他の領域について意見を述べたりする、最後の機会を提供すべきである。

調査は、通報制度を通じて得た情報に起因する場合もあるが、組織の監査業務やモニタリング業務、あるいは外部者（例：顧客、競合他社、サプライヤー）に起因する場合もある。どのような事象が懸念の引き金となったかにかかわらず、調査

は、迅速かつ徹底的に、そして影響を受ける機能や個人から独立して行うべきであり、また、書面による方針と手続に従って実施すべきである。事案ファイルやその他の文書は、各調査の完全性を確保するように維持して保護すべきである。調査については、「不正行為への対応」の項目でさらに詳しく説明する。

重要なのは、疑義事案の調査や解決が、これらの通報制度の唯一の目標ではないということである。同様に重要な目標は、C＆Eプログラムのパフォーマンスに関するフィードバックを提供してプログラムを改善できるようにすることである。そのためには、C＆Eプログラムの効果を高めるための適切な措置が講じられるように、通報された問題の傾向や指導を求められている領域を、追跡して分析する必要がある。

インセンティブとエンフォースメント

コンプライアンス違反は、まったく意図的でない場合もあり、効果的でない統制、効果的でない研修や新入社員のオリエンテーション、手続の誤解、カルチャーの悪化または単なる不注意が原因であることが多い。プロセスや内部統制が一貫して実施されていない限り、時間の経過とともにプロセスや内部統制の自然な劣化が起こる。また、コンプライアンス違反は意図的な場合もあり、組織の方針に違反していることを知っている従業員や、プロセスの中で法令に違反していることを理解している可能性のある従業員によって行われることもある。

ＵＳＳＧは、C＆Eプログラムへの一貫した参加および/または実施を推進するために、インセンティブや同様のツールを利用するよう求めている。取締役会や経営幹部が、売上、安全成果、顧客満足、従業員満足およびその他の戦略目標を達成するために金銭や表彰のインセンティブを用いるように、ＵＳＳＧは、インセンティブを組織のコンプライアンスの取り組みの一部として用いるべきと述べている。インセンティブは、コンプライアンスプログラムを取り入れて実施するリーダーの動機づけに特に効果的であるが、組織内のあらゆる階層でも効果的に使用できる。インセンティブには、実際には金銭的なものと金銭的でないものがあり、組織のパフォーマンス管理システムと効果的に統合できる。

エンフォースメントの説明の中で、ＵＳＳＧは、コンプライアンス義務の無視や法律や方針への違反に対して、しかるべき措置を講じることを推奨している。このような懲戒は、作為または不作為のコンプライアンス違反が意図的か否か、また、コンプライアンス違反の重大度も考慮すべきである。組織は、口頭や書面による戒告から解雇に至るまで、さまざまな懲戒処分の可能性を規定すべきである。

C＆Eプログラムの成功には、組織的な公正さが不可欠である。したがって、エンフォースメントと懲戒は、組織の全階層、おそらく最も重要なのは最高位層において一貫していなければならない。もしも、大きな成功を収めた営業担当者や経営幹部、あるいは影響力のある従業員のコンプライアンス違反を容認する一方で、別の従業員が同じ違反で懲戒処分を受けた場合、C＆Eプログラムの信頼性が損なわれ、組織のカルチャーに悪影響を及ぼす可能性がある。

C＆Eプログラムのすべての要素と同様に、懲戒は常に現地や地域の法的環境と契約条項や労働組合の規定を考慮すべきである。

法的責任をもたらす可能性のあるベンダー、サプライヤーおよびその他の第三者に関わるインセンティブやエンフォースメントに関して、組織は、適切なコンプライアンス義務を課すとともに、罰則条項や契約解除条項のような、コンプライアンス違反の結果に対処するしかるべき契約条項があることを確認すべきである。

不正行為への対応

どのようなC＆Eプログラムであっても、組織のコンプライアンスを終生保証するものではない。組織が十分長く存続しているか十分な規模であれば、プログラムがいかに効果的であってもコンプライアンス違反は避けられない。

コンプライアンス違反に対して組織が何をするかは、効果的なプログラムと効果的でないプログラムを区別する重要な要因である。不正行為への対応には、調査と是正という２つの重要な側面がある。

コンプライアンス調査は、迅速かつ徹底的に、全関係者に対して公正に行わなければならず、また、対象者から独立しており他の点で対立していない者が行わなければならない。その他、コンプライアンス調査を実施する上で考慮すべき重要な点は以下のとおりである。

1. **通知**－調査について誰に通知すべきか（例：リーダー、法務、外部の関係者）。
2. **専門知識**－組織には調査を実施するために必要な専門知識がすべてあるか、それとも外部の支援を受けるべきか。
3. **コンプライアンスの関与**－コンプライアンス責任者が調査を行うかどうかにかかわらず、コンプライアンス責任者は、調査の過程で情報を与えられ、関与すべきである。
4. **文書化**－調査の一環として収集した証拠やその他の文書を収集し、保護し、保存する。
5. **監督と管理**－調査が大規模になればなるほど、（必要に応じて弁護士の関与を含む）適切な指揮系統を確立し、全関係者の作業を監督し、レビューし、調査の範囲を適切に管理することが重要である。

6．**調査範囲**－調査の範囲を最初から理解し、それに合わせて調査計画を立てる。

調査には多くの段階がある（例：文書の収集、電子記録の特定、関係者への聴取）。そして最終的には、書面による報告書の必要性や要望がある場合もない場合もある。しかし、事案ファイルは常に適切に閉じるべきである。

調査の結果、コンプライアンス違反が判明した場合は、根本原因分析を行い、内部統制のどこで機能不全や不備が生じたのか、あるいは内部統制の設計に弱点がなかったかを十分に把握すべきである。これが終わったら、組織は根本的な問題の是正に目を向けなければならない。既存の方針と手続が適切に設計されていたにもかかわらず、それらの統制の実施が失敗した場合、その是正は、それらの統制に関わる特定の従業員グループへの研修（または再研修）と、適切なモニタリングプロセスの復活または導入だけで済むかもしれない。

それ以外の場合、是正には一層の取り組みが必要である。方針と手続の修正、予防的統制の改善、業務プロセスまたはインセンティブの変更およびその他の是正の取り組みは、すべて特定のコンプライアンス違反行為が再発しないようにすることを目的とすべきである。予防にコストがかかるか現実的でない場合には、今後コンプライアンス違反が発生した場合に、より早く発見し、修正し、損失や罰則が減るように、発見的統制を追加または変更することが是正につながるかもしれない。計画された措置の内容にかかわらず、是正計画を完全に実施するために説明責任を確立してモニターすべきである。

リスク評価とプロフラムの改善

規制当局は、研修、モニタリング、監査およびその他のC＆Eプログラムの要素について、リスクベースのアプローチをとることの重要性を一貫して強調している。そのため、適切なリスク評価プロセスが重要である。コンプライアンスと倫理に関する事象のリスクを評価するためのアプローチと考慮事項は、一般に他の種類のリスクの評価と非常によく似ている。例えば、典型的なアプローチには、以下のステップが含まれる。

1．組織の活動に固有のコンプライアンスリスクを識別する
2．コンプライアンスリスクと既存の内部統制を対応させる
3．内部統制の有効性を評価する
4．各コンプライアンスリスクの発生可能性と影響度を評価する
5．その評価に基づいて、（スコアリング、ヒートマップ等を用いて）コンプライアンスリスクを優先順位づけする
6．リスクを許容水準まで低減するためのリスク対応策（例：内部統制の改善、研修）を設計する
7．リスク対応の責任を分担して実施状況をモニターする

これらは典型的なリスク評価の中核的要素であるが、リスク評価の質をさらに高めるために、多くの追加的要素が考慮できる。リスク評価は、一定の時間間隔で、またはリスクに影響を及ぼすような変化が生じた可能性があることを示す関連する新たな情報が明らかになったときに、定期的に更新すべきである。

2004年にUSSGに追加されたもう1つの項目は、C＆Eプログラムを継続的に改善する取り組みがなされることを期待するものである。定期的なリスク評価は、プログラムに必要な改善点を特定する方法の1つである。しかし、改善点を特定する方法は他にも多くあり、調査終了時の徹底的な根本原因分析、フィードバックの仕組み、監査とモニタリングなどが挙げられる。また、他の組織とのベンチマーキングも、プログラムの有効性を評価する効果的な方法である。プログラムの有効性評価は、内部で行うことも、第三者（例：コンサルティング会社）に依頼することも可能である。さらに、カンファレンスに出席し、出版物を読み、政府のガイダンスをモニタリングするなど、組織の外部に目を向けることは、プログラムを改善するために採用できる新たな実務を見つける優れた方法である。

付録２．
コンプライアンスと倫理のプログラムに対する認識と要件の国際的な高まり

第１章で述べたように、近年、Ｃ＆Ｅプログラムに対する国際的な認識がかなり高まってきている。この付録では、さらにいくつかの例を紹介する。

フランス

2016 年のフランスのサパン II 法（Sapin II Law）に伴い、フランス腐敗行為防止庁（French Anticorruption Agency：ＡＦＡ）の腐敗防止コンプライアンスプログラムに関するガイダンスが 2017 年に発行され、その後 2019 年 12 月に改訂された。このガイダンスでは、コンプライアンス責任者の任務は腐敗行為防止にとどまらず、反マネーロンダリング、独占禁止、個人情報保護など、プログラムの範囲として適切と考えられる他の法律も含まれ得ると述べている。ＡＦＡのガイダンスでは、プログラムで期待される領域として、以下の 8 つを挙げている。

1. 方針と手続、組織の最高位にまで及ぶプログラムに対するガバナンス、従業員や外部パートナーとのプログラムに関するコミュニケーションなど、最高経営者によるコミットメント
2. 行動規範
3. 内部通報制度
4. リスクの評価、優先順位づけおよび管理を含むリスクマッピング
5. 第三者のデューディリジェンス
6. 会計統制
7. リスクに曝されている管理者と従業員へのリスク研修
8. 内部のモニタリングと評価

ブラジル

2014 年に施行されたブラジルのクリーンカンパニー法（Clean Companies Act）は、贈収賄、マネーロンダリング、契約のための公共入札における不正など、特定の行為を行った場合の罰則を定めている。この法律は、政府がこの法律に関する規則を発行することを要求し、それは 2015 年の政令（8.420/15）の形で行われた。この政令では、プログラムの存在と適用について、以下のパラメータにしたがって評価するとしている。

1. プログラムに対する明確で疑う余地のない支援によって証明される、評議会を含む法人の最高経営者によるコミットメント
2. 職位や機能に関係なく、すべての従業員と管理者に適用される行動基準、倫理規範、方針および手続
3. 必要に応じて、サプライヤー、サービスプロバイダ、仲介業者および取引関係者のような第三者にも適用される行動基準、倫理規範および方針
4. プログラムに関する定期的な研修
5. プログラムに必要な調整を行うための定期的なリスク分析
6. 企業の取引を完全かつ正確に反映した会計記録
7. 企業の報告書や財務諸表の迅速な作成と信頼性を確保するための内部統制
8. 入札手続、行政契約の締結または公共部門とのあらゆるやり取りという状況で、たとえ第三者が介在する場合でも、納税、検査対応、あるいは認可、ライセンス、許可および証明書の取得などにおいて不正や不法行為を予防するための具体的な手続
9. プログラムの実施とその遵守のモニタリングに責任を有する内部組織の独立性、構造および権限
10. 従業員や第三者に公開され広く浸透している内部通報の経路と、通報者を保護するために設計された制度
11. プログラムに違反した場合の懲戒措置
12. 発見された不正や違反の迅速な中断と、発生した損害の適時な救済を確実にする手続
13. サプライヤー、サービスプロバイダ、仲介業者および取引関係者のような第三者との契約と、場合によっては、その監督に関する適切な手続
14. 合併、買収および企業再編の過程で、不正行為や違法行為が行われていないか、あるいは関係する企業の脆弱性が存在しないかの検証
15. 法律で禁止されている行為の発生を予防、発見および撲滅するために、プログラムの改善を目的とした継続的なモニタリング
16. 議員候補者や政党への寄付に関する企業の透明性

政令では、コンプライアンスプログラムの評価にあたっては、従業員数、拠点数、事業を展開している国、業種、複雑さおよび第三者の利用など、組織に独自の特徴を考慮するよう述べている。

この規定は、C＆Eプログラムには「万能」のアプローチは存在しないとする米国のガイダンスと整合している。すべてのプログラムは、組織特有のニーズに合わせて調整すべきである。

コスタリカ

コスタリカも、（2018年のアルゼンチン、ペルーおよびチリとともに）最近コンプライアンスプログラムに対応する法律を制定したラテンアメリカの国である。2019年のコスタリカの法律の範囲は、国内および国際的な贈収賄と汚職、そしてそのような汚職を隠すための帳簿や記録の改ざんとなっている。企業がコンプライアンスプログラムを整備していれば、重大な罰則が軽減される可能性がある。法律に記載されているC＆Eプログラムへの期待事項は以下のとおりである。

1. コスタリカでの事業活動に関するリスク評価を実施する
2. 犯罪を予防するための行動規範を導入し、具体的な規則やプロセスを採用する
3. 公共入札契約、ライセンス取得およびその他行政に関連する活動に関する犯罪を予防するための具体的な方針と手続を確立する
4. 第三者に対するこれらの方針の適用範囲を決定する
5. 不正行為の予防を目的とした適切な財務統制と財務記録を確立する
6. 第三者に対する研修を含む、定期的な腐敗防止研修を実施する
7. 定期的にリスク評価を実施して、それに応じてプログラムを修正する
8. コンプライアンス違反に対する懲戒モデルを策定する
9. コンプライアンス責任者を任命し、プログラムのために十分な能力と資源を提供する
10. 外部者による会計監査を実施する

ニュージーランド

2013年7月、マネーロンダリングおよびテロ資金供与対策法（The Anti-Money Laundering and Countering Financing of Terrorism Act）が施行された。この法律の要件の1つは、コンプライアンス責任者の任命と、報告プログラムとコンプライアンスプログラムの策定である。

コンプライアンスプログラムの主要な要素には、以下を含めなければならない。

1. 包括的なリスク評価
2. 管理者に対する身元調査と教育の義務づけ
3. 報告手続
4. 記録の保持
5. デューディリジェンス
6. その他不正使用リスクを最小限にするためのプロセス

シンガポール

シンガポールの汚職調査局（Corrupt Practices Investigation Bureau）は、2017年、組織が腐敗防止法（The Prevention of Corruption Act）を遵守する支援をするために、「シンガポールにおける企業のための実践的汚職防止ガイド（PACT - A Practical Anti-Corruption Guide for Businesses in Singapore）」を発表した。このガイドでは、企業が汚職を防止するためにとることのできる以下の4つのステップ（その頭文字をとってPACTと呼ばれている）が説明されている。

1. **誓約（Pledge）**－トップからの気風、腐敗防止方針および行動規範
2. **評価（Assess）**－定期的なリスク評価の実施
3. **統制と伝達（Control and communicate）**－内部統制、監査チェック、研修とコミュニケーションおよび強固な通報制度
4. **追跡（Track）**－腐敗防止システムの評価と改善

スペイン

2015年7月1日に施行されたスペイン刑法の改正により、企業のコンプライアンスプログラムの規制が規定された。改正法では、企業が以下の6つの要素を含むコンプライアンスプログラムを採用している場合、その役員または従業員が実行した犯罪に対する刑事責任を免除することを定めている。

1. リスク評価
2. 発見された犯罪リスクを軽減するための基準と統制
3. 犯罪を予防するための財務統制
4. 基準や統制に違反した場合のコンプライアンス機関への通報義務（内部通報の経路）
5. 役員や従業員のコンプライアンスプログラム違反に対する懲戒制度
6. コンプライアンスプログラムの定期的な見直しと、重大な違反の発生時や組織的、構造的または経済的な変化があった場合の必要な調整

要約

この付録の要約は完全なものではなく、コンプライアンスと倫理のプログラムに関する何らかの要件やガイダンスを公布している多くの国々の中の、一握りの国同士の類似点と相違点を説明するためにのみ提供しているものである。組織は、さらにガイダンスを得るために、事業を行う各法域の法令を常に参照すべきである。

謝辞

企業のコンプライアンスと倫理協会および医療コンプライアンス協会
（The Society of Corporate Compliance and Ethics & Health Care Compliance Association：ＳＣＣＥ＆ＨＣＣＡ）

corporatecompliance.org

本稿は、ＥＲＭのコンプライアンスリスクへの適用に関するＳＣＣＥ＆ＨＣＣＡワーキンググループ（SCCE & HCCA Working Group on the Application of ERM to Compliance Risk）の成果物である。

共同委員長
米国ケンタッキー大学フォン・オールメン会計学部、ディレクター兼ＥＹ教授
アートン・アンダーソン
ＳＣＣＥ＆ＨＣＣＡ最高経営責任者　ゲリー・ザック

寄稿編集者
オプタム 360 社、最高コンプライアンス責任者、ダン・ローチ
コンプライアンス・インテグリティ・ソリューションズＬＬＣ、プリンシパル、グレッグ・トリグバ

寄稿者
以下の方々のご意見、ご感想およびご寄稿に謝意を表したい。

Deborah L. Adleman, Ernst & Young LLP
Joseph Agins, Institutional Compliance Officer, Sam Houston State University
Jeffrey Driver, Faculty, Arizona State University & Principal, Soteria Risk Works
Margaret Hambleton, President, Hambleton Compliance LLC
Samantha Kelen, Chief Ethics and Compliance Officer, Cardinal Innovations Healthcare
Gwendolyn Lee Hassan, Managing Counsel – Global Compliance & Ethics, CNH Industrial
Walter Johnson, Assistant Privacy Officer, Regulatory Compliance, Inova Health System
Caroline McMichen, Principal, McMichen Consulting and former Vice President, GlobalEthics and Compliance, Molson Coors (Retired)
Robert Michalski, Chief Compliance Officer, Baylor Scott & White Health
Rebecca Walker, Kaplan & Walker LLP

企業のコンプライアンスと倫理協会（Society of Corporate Compliance and Ethics：ＳＣＣＥ）および医療コンプライアンス協会（Health Care Compliance Association：ＨＣＣＡ）について

企業のコンプライアンスと倫理協会および医療コンプライアンス協会（ＳＣＣＥ＆ＨＣＣＡ）は、1996 年に医療のコンプライアンス専門家のために設立され、2004 年にはあらゆる業界のグローバルなコンプライアンスと倫理のコミュニティーのために拡大された。世界 100 か国に２万人の会員を擁するＳＣＣＥ＆ＨＣＣＡは、専門職の利益を促進する最大の協会である。ＳＣＣＥ＆ＨＣＣＡはミネソタ州ミネアポリスに本部を置き、倫理的実務とコンプライアンスの基準を支持し、倫理とコンプライアンスの専門家に必要な研修、出版物、認定資格およびその他の資源を提供するために存在している。

ＣＯＳＯについて

1985 年に設立されたＣＯＳＯは、5 つの民間団体の共同イニシアチブであり、全社的リスクマネジメント（ＥＲＭ）、内部統制および不正抑止に関するフレームワークとガイダンスの開発を通じて、先進的な考え方を提供することに取り組んでいる。ＣＯＳＯの支援団体は、内部監査人協会（ＩＩＡ）、米国会計学会（ＡＡＡ）、米国公認会計士協会（ＡＩＣＰＡ）、国際財務担当経営者協会（ＦＥＩ）、管理会計士協会（ＩＭＡ）である。

一般社団法人日本内部監査協会

内部監査および関連する諸分野についての理論および実務の研究、ならびに内部監査の品質および内部監査人の専門的能力の向上を推進するとともに、内部監査に関する知識を広く一般に普及することにより、わが国の産業、経済の健全な発展に資することを目的に活動。

また、国際的な内部監査の専門団体である内部監査人協会（The Institute of Internal Auditors：ＩＩＡ）の日本代表機関として世界的な交流活動を行うとともに、内部監査人の国際資格である“公認内部監査人（Certified Internal Auditor：ＣＩＡ）”等の認定試験を実施している。1957（昭和 32）年創立。

公益財団法人日本内部監査研究所

内部監査に関する研究調査を推進するとともに、わが国の内部監査の普及発展に貢献することにより、わが国経済、社会の健全な発展に資することを目的として、2020 年 7 月に設立。2021 年 7 月に公益財団法人としての認定を受け「公益財団法人日本内部監査研究所」となった。

監訳者

八田　進二　（大原大学院大学　会計研究科　教授　／　青山学院大学　名誉教授）
橋本　　尚　（青山学院大学大学院　会計プロフェッション研究科　教授）

訳　者

堺　　咲子　（内部監査人協会（ＩＩＡ）国際本部理事　専門職資格担当　／　インフィニティコンサルティング　代表　／
プレミアアンチエイジング株式会社　社外取締役　／　ＣＩＡ，ＣＲＭＡ，ＣＣＳＡ，ＣＦＳＡ）

全社的リスクマネジメント

COSO

トレッドウェイ委員会
支援組織委員会

coso.org

コンプライアンス リスクマネジメント： COSO ERM フレームワークの適用

COSO

トレッドウェイ委員会支援組織委員会

coso.org