ＣＯＳＯ『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』の内部監査での活用方法
～COSO ERM の２０の原則を活用したコンプライアンスリスク監査での７８の視点・着眼点・質問事項と事例・改善提言する際のポイント・留意点～

一般社団法人　日本内部監査協会
ＣＩＡフォーラム No. ａ３　ＥＲＭ研究会（第１２期）
2025 年９月 26 日

目　次

１．はじめに　…………………………………………………………………　**４**
（１）ＣＯＳＯ『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』について　……………………　４
（２）本報告書の目的……………………………………………………………　４
（３）改訂版ＣＯＳＯ・全社的リスクマネジメントに対する当研究会の取り組みの経緯……………………　４
（４）使用上の注意……………………………………………………………　４
（５）研究会メンバー（ＣＩＡフォーラムａ３　ＥＲＭ研究会（第 12 期））……………………　５
（６）本研究会の活動の経緯　…………………………………………………　７

２．本報告書の全体像（「視点・着眼点・質問事項」一覧）　……………………　**９**

３．ＣＯＳＯ全社的ﾘｽｸﾏﾈｼﾞﾒﾝﾄの 20 の原則に沿った内部監査での７８の視点・着眼点・質問と事項と事例・改善提言・・・・・　**１２**
（構成要素１　ガバナンスとカルチャー）
原則１　取締役会によるリスク監視を行う　……………………………１２
原則２　業務構造を確立する　…………………………………………１６
原則３　望ましいカルチャーを定義づける　……………………………１８
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　………………２０
原則５　有能な人材を惹きつけ、育成し、保持する…………………………２３
（構成要素２　戦略と目標設定）
原則６　事業環境を分析する　…………………………………………２５
原則７　リスク選好を定義する　………………………………………２７
原則８　代替戦略を評価する　…………………………………………２９
原則９　事業目標を組み立てる　………………………………………３２
（構成要素３　パフォーマンス）
原則１０　リスクを識別する　…………………………………………３４
原則１１　リスクの重大度を評価する　…………………………………３８
原則１２　リスクの優先順位づけをする　………………………………４０
原則１３　リスク対応を実施する　………………………………………４２
原則１４　ポートフォリオの視点を策定する　……………………………４４
（構成要素４　レビューと修正）

原則１５　重大な変化を評価する　……………………………………………………………４６
原則１６　リスクとパフォーマンスをレビューする　…………………………………………４９
原則１７　全社的リスクマネジメントの改善を追求する　……………………………………５１
（構成要素５　情報、伝達および報告）
原則１８　情報とテクノロジーを有効活用する　………………………………………………５３
原則１９　リスク情報を伝達する　………………………………………………………………５６
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　……………………６０

４．参考資料：全社的リスクマネジメントと内部統制とのおおよその関係　……………………６３

参考文献　……………………………………………………………………………………………６５

１．はじめに

（１）ＣＯＳＯ『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』(注) について

・同ガイダンスは、改訂版ＣＯＳＯ・全社的リスクマネジメント（以下、「COSO-ERM」という）を、**米国で広く認められたコンプライアンスと倫理のプログラムのフレームワーク**と連携させ、それぞれの**基礎となる概念を統合**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**することを目的としたガイダンスです。なお、同ガイダンスは 2020 年 11 月に公表されその後、公益財団法人日本内部監査研究所が 2022 年 6 月に邦訳し、日本内部監査協会のホームページ上で公開されています。

（注）*Compliance Risk Management: Applying the COSO ERM Framework*

（２）本報告書の目的

・本報告書の目的は、同ガイダンスから、**コンプライアンスリスクを監査する際の視点・着眼点・質問事項と、改善提言する際のポイント・留意点**を読み取り、整理することを通して、**同ガイダンスをコンプライアンスリスクに対する内部監査の実務で活用する方法**を提示することです。

・そのため、**20の原則ごとに、合計78の視点・着眼点・質問事項と、改善提言する際のポイント・留意点を例示**することにより、**20の原則を我が国におけるコンプライアンスリスクに対する内部監査の実務で活用**するという観点から作成しました。

・なお、コンプライアンスは良質な企業統治体制の基盤の一つであり、監査役はガバナンスの観点からコンプライアンス体制の監視・監督を行っていることから本報告書は、取締役の職務執行を監査する**監査役監査にも活用**できる内容となっています。

（３）改訂版ＣＯＳＯ・全社的リスクマネジメントに対する当研究会の取り組みの経緯

・当研究会は、**2018年４月に邦訳が公表された改訂版COSO-ERMで示された20の原則を内部監査の実務に活用するための手法を提示**するために、**2019年11月**に***『改訂版ＣＯＳＯ・全社的リスクマネジメントの内部監査での活用事例　～全社的リスクマネジメントの20の原則に沿った内部監査での73の「質問・確認事項」と「課題・改善提言」および61の「具体例」～』***を日本内部監査協会のホームページ上で公開しました**（第１０期）**。

・さらに、**2018年12月にCOSO-ERMを補完するものとして、どのように実務に適用すればよいかの理解に役立つ事例集**の邦訳が、一般社団法人日本内部監査協会から公表されたことを受けて、**2022年９月**に***『「ＣＯＳＯ全社的リスクマネジメント　事例の解説篇」の内部監査での活用方法　～２０の原則の内部監査での８１の視点・着眼点と確認事項～』***を日本内部監査協会のホームページ上で公開しました**（第１１期）**。

・今回の報告書は、上記２点の報告書に続いて、**COSO-ERMの内部監査の実務での活用方法を、コンプライアンスリスクの監査の視点から示したもの**です。**（第１２期）**

（４）使用上の注意

①本報告書は、同ガイダンスで示された内容について、COSO-ERM の観点からコンプライアンスリスクに対する内部監査の実務に資する視点や知見・ノウハウの提供を試みたものであり、**同ガイダンスそれ自体の解説を目的としたものではありません。**

②**紹介した内容はあくまでも一例**であり、それ以外にも多くのものがあることにご留意願います。

③**本報告書に記載した内容を全て使用する必要はなく、自社で活用できるものから活用し、自社の現在のコンプライアンスリスクマネジメントの状況**

を出発点として、高度化していくことが大切です。
④本報告書の記載内容に関する責任は、すべて本研究会にあることにご留意願います。

（５）研究会メンバー　（ＣＩＡフォーラムａ３　ＥＲＭ研究会（第 12 期））

（2025 年 9 月 26 日時点）

No.	氏名	会社名等	所属・役職
1	吉野 太郎 （座　長）	（株）エスエーティ	常勤監査役
2	野口 正文 （副座長）	損害保険ジャパン（株）	監査等委員会室・主査
3	新藤 和政 （座長補佐・Web 会議担当）	NIPPON EXPRESS ホールディングス（株）	内部監査室・専任部長
4	坂井 香苗	日本電気（株）	グループ内部監査部門　監査企画グループ・シニア監査プロフェッショナル
5	紀谷 倫有	個人会員	
6	真柳 元	個人会員	
7	丹羽 珠希	三井住友フィナンシャフグループ（株）	監査部・上席考査役
8	有村 祥一	アジア太平洋トレードセンター（株）	監査役
9	伊藤 裕美子	ＮＥＣネッツエスアイ（株）	営業統括本部　業務改革推進本部　営業タスク改革部・担当部長
10	宇田 文顕	シナネンホールディングス（株）	IT 戦略部・チーム長
11	大島 誠	（株）アシスト	顧問
12	和田 有弘	出光興産（株）	内部監査室
13	青木 博史	（株）三菱 UFJ フィナンシャルグループ	監査部・上席調査役
14	佐藤 伸吾	のむら産業（株）	内部監査室・室長
15	桐山 勝	（株）SkyDrive	常勤監査役
16	村上 裕子	明治安田生命相互会社	監査部・上席内部監査役
17	野々山 一郎	東芝ライフスタイル(株)	法務部　監査担当・グループ長
18	神山 典子	合同会社オズ	代表社員
19	小関 清久	個人会員	
20	岡田 芳明	三菱地所ハウスネット（株）	監査役

21	五十嵐 英知	東京海上ディーアール（株）	常勤監査役
22	加藤 彰子	（株）ラック	グループ経営推進部・企画推進室
23	福山 武雄	特別民間法人　企業年金連合会	コンプライアンス・業務監査室　コンプライアンスオフィサー　室長
24	栗城 雄太	楽天グループ（株）	内部監査部
25	中村 由紀子	損害保険ジャパン（株）	内部監査部・課長代理
26	高田 晋也	（株）レスター	統制監査室・マネージャー
27	洪 史詩	PayPay（株）	内部監査室・スタッフ
28	正能 佳子	クオールホールディングス（株）	内部監査部・部長
29	小島 至久	日本空港ビルデング(株)	監査室・主任
30	安村 誠巨	セガサミーホールディングス(株)	経営監査本部　監査企画推進部　監査企画推進課
31	今井 晃基	株式会社フェアコンサルティング	会計コンサルティング部・アシスタントマネージャー
32	大島 理	(株)チェンジホールディングス	内部監査室・室長
33	田中 恵太	農林水産省	検査・監察部・係長
34	永田 勝久	(株)りそなホールディングス	内部監査部・シニアインターナルオーディター
35	槙 絵美子	SOMPO ビジネスサービス(株)	取締役会長

（６）本研究会の活動の経緯

本研究会は 2004 年 4 月から活動を開始し、12 期 21 年にわたり一貫して、全社的リスクマネジメント（ＥＲＭ）を内部監査に活用する手法を研究し、内部監査の質的向上に微力ながらも貢献していきたいとの思いで活動を続けてきました。その間の研究成果とその概要は以下のとおりです。

活動期間	研究成果（報告書）	概　　要
第１期 2004 年 4 月 ～2005 年 2 月	**ＥＲＭのよくある質問集（ＦＡＱ）**	ＥＲＭについて理解を促進するためのＦＡＱ。
第２期 2005 年 4 月 ～2006 年 3 月	**使えるＥＲＭ（全社的リスクマネジメント）導入チェックポイント集** ～ 一目でわかるＥＲＭと内部統制の基本的要素の具体例 ～	ＥＲＭの８つの構成要素が有効に機能しているかどうかのチェックポイントと、その具体的な事例。
第３期 2006 年 4 月 ～2007 年 4 月	**ＥＲＭ実施体制を構築するために必要な１０の要件**	ＥＲＭ実施体制構築の要件と、その具体的事例、および中小企業であっても行うべきＥＲＭの最低要件。
第４期 2007 年 5 月 ～2008 年 7 月	**法対応の内部統制から価値創造のＥＲＭ（全社的リスクマネジメント）へ** ～ 会社法と金融商品取引法対応の内部統制を活かしたＥＲＭづくりへの提言 ～	内部統制法制化への対応で得られた成果のＥＲＭ実施体制構築への活用。
第５期Ａ分科会 2008 年 10 月 ～2010 年 1 月	**ＥＲＭ的な視点を取り入れた内部監査の手法** ～ ＥＲＭの視点を活用して、企業目標の達成に寄与し付加価値を提供する内部監査を行うためのノウハウ ～	内部監査にＥＲＭ的な視点を取り入れ、内部監査の質を高め､企業目標の達成に寄与するための手法･ノウハウ。
第５期Ｂ分科会 2008 年 10 月 ～2010 年 1 月	**格付会社のＥＲＭ確認項目を用いた事業会社向けＥＲＭチェックリスト** ～ 事業会社の目線に立った格付会社のＥＲＭ確認項目の読替と解説 ～	格付会社が公表している情報を参考に我が国の一般事業会社を対象としたＥＲＭの取組状況を確認するための項目についての解説。
第６期 2010 年 4 月 ～2012 年 6 月	**「ＣＯＳＯ　内部統制モニタリングガイダンス」に基づいた ＥＲＭモニタリング事例集**	「ＣＯＳＯ内部統制モニタリングガイダンス」の手法や考え方を反映させたＥＲＭのモニタリング事例集。
第７期 2012 年 8 月 ～2014 年 10 月	**全社的リスクマネジメント（ＥＲＭ）を活用した内部監査手法の研究** ～「リスク選好・リスク許容度」､「主要リスク指標」､「戦略的優位性を確保するＥＲＭ」についての業種別事例とリスクベース内部監査への活用事例～	「リスク選好・リスク許容度」､「主要リスク指標」､「戦略的優位性を確保するＥＲＭ」に関するＣＯＳＯの３つのレポートから、それらの業種別の具体的事例、および内部監査における確認事項と内部監査の実務で役立つ視点をまとめたもの。
第８期 2015 年 2 月 ～2015 年 11 月	**改訂版ＣＯＳＯ内部統制フレームワークの内部監査での活用事例** ～改訂版 COSO の 17 の原則の観点から見た内部監査において留意すべき問題事例と改善提言のための確認事項～	17 の原則ごとに「具体的視点」を例示し､「内部監査において留意すべき問題事例」と「改善提言のための確認事項／改善提言」を説明。

第９期 2016 年 2 月 ～2016 年 11 月	**リスク評価手法の内部監査での活用事例** ～内部監査での活用方法・改善提言のための確認事項～	リスク評価の具体的なノウハウ、問題のある事例、および良好な事例について、「具体的事例」を紹介すると共に、「内部監査での活用方法・確認事項・改善提言」を紹介。
第１０期 2017 年 4 月 ～2019 年 11 月	**改訂版ＣＯＳＯ・全社的リスクマネジメントの内部監査での活用事例** ～全社的リスクマネジメントの 20 の原則に沿った内部監査での 73 の「質問・確認事項」と「課題・改善提言」および 61 の「具体例」～	20 の原則ごとに、全社的リスクマネジメントに対する内部監査で質問・確認すべき事項を例示し、課題とその改善提言を紹介。
第１１期 2020 年 1 月 ～2022 年 9 月	**「ＣＯＳＯ全社的リスクマネジメント　事例の解説篇」の内部監査での活用方法** ～２０の原則の内部監査での 81 の視点・着眼点と確認事項～	事例の解説篇から全社的リスクマネジメントに対する内部監査での視点・着眼点と質問事項を読み取り 20 の原則ごとに紹介。
第１２期（当期） 2023 年 1 月 ～2025 年 9 月	**ＣＯＳＯ『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』の内部監査での活用方法** **～COSO ERM の２０の原則を活用したコンプライアンス・リスク監査**での７８の視点・着眼点・質問事項と事例・改善提言する際のポイント・留意点～	コンプライアンス・リスク監査での視点・着眼点・質問事項と事例・改善提言する際のポイント・留意点を 20 の原則ごとに紹介。

（注）上記報告書はすべて、一般社団法人日本内部監査協会のホームページ上で公開されています。

・第１期～８期報告書　　:「研究・活動」→「ＣＩＡフォーラム」→「活動実績」（右上）→「過去の活動実績」（最下段）→**研究会 No.15**（第１期～第８期）
＊https://www.iiajapan.com/leg/kenkyu/forum/report_past.html

・第９期～１２期報告書　　:「研究・活動」→「ＣＩＡフォーラム」→「活動実績」（右上）→ａ３（第９期以降）
＊https://www.iiajapan.com/leg/kenkyu/forum/report.html

２．本報告書の全体像（「視点・着眼点・質問事項」一覧）

＊合計７８項目

構成要素	原　則	当研究会で考察した視点・着眼点・質問事項
構成要素１ ガバナンスとカルチャー	原則１ 取締役会によるリスク監視を行う	（１）コンプライアンスに関する基本規程・取組方針の取締役会による決議・承認 （２）コンプライアンス委員会、コンプライアンス部門の実質的な機能発揮 （３）取締役会のコンプライアンスリスクに係る重要情報や専門知識の確保 （４）コンプライアンスに関する取締役会への報告
	原則２ 業務構造を確立する	（１）コンプライアンスリスク管理の仕組と所管部門 （２）取締役会に対する報告経路 （３）平時の体制と有事の体制 （４）意思決定の支援 （５）複数のコンプライアンス関連機能間の調整
	原則３ 望ましいカルチャーを定義づける	（１）認識の共有 （２）問題提起・相談ができるカルチャーの醸成 （３）カルチャーの浸透状況や課題のモニタリング （４）望ましいカルチャーの明示
	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	（１）トップからの行動指針の表明と社内伝達 （２）コンプライアンスを限定的に考えない （３）トップからの発信 （４）不正事案の早期把握と迅速な報告・通報体制の整備 （５）内部通報制度が機能するための体制整備
	原則５ 有能な人材を惹きつけ、育成し、保持する	（１）プリンシプルベースで考えることのできる人材の育成 （２）過去に発生した不祥事を風化させない啓発 （３）不祥事を自分事として捉えることのできる人材の育成
構成要素２ 戦略と目標設定	原則６ 事業環境を分析する	（１）組織戦略を踏まえたコンプライアンスリスクの管理 （２）コンプライアンスリスクに及ぼす環境要因の変化の確認 （３）他のリスク対応策によるコンプライアンスリスクへの影響の検討
	原則７ リスク選好を定義する	（１）コンプライアンスに関するリスク選好の誤解 （２）コンプライアンス委員会の議題 （３）国・地域や部門により異なるコンプライアンスリスクの検討 （４）戦略遂行に伴うコンプライアンスリスクがリスク選好の範囲内にあるかの確認

	原則８ 代替戦略を評価する	（１）CCO（最高コンプライアンス責任者）及びコンプライアンス部門の組織戦略への関与 （２）M&A のコンプライアンスリスクに関するデューデリジェンス （３）戦略の評価
	原則９ 事業目標を組み立てる	（１）事業目標の策定や達成自体により発生するコンプライアンスリスクの理解 （２）自部門の事業目標の設定・変更 （３）コンプライアンスリスクに関する業績評価指標
構成要素３ パフォーマンス	原則１０ リスクを識別する	（１）コンプライアンスリスクの識別プロセス （２）コンプライアンスリスクの可視化・体系化と更新頻度 （３）エマージングリスクの識別 （４）グループ会社を含めたリスクの識別 （５）複数のアプローチを活用したリスクの識別
	原則１１ リスクの重大度を評価する	（１）コンプライアンリスクの重大度の評価方法 （２）評価に関するバイアスの排除と一貫性の確保
	原則１２ リスクの優先順位づけをする	（１）リスク対応の優先順位の決定 （２）リスク対応の優先順位づけにおける他の評価基準の使用 （３）リスクの優先順位に応じた経営資源の配分 （４）経営層が参加する会議体での議論
	原則１３ リスク対応を実施する	（１）リスク対応改善の PDCA サイクルの実施 （２）リスク対応の形骸化防止 （３）リスク対応策追加のメリットとコストの比較検討
	原則１４ ポートフォリオの視点を策定する	（１）コンプライアンスリスク対応と他のリスクとの相互関係の考察 （２）各種のコンプアライアンスリスクのマネジメントと全社的リスクマネジメントとの統合
構成要素４ レビューと修正	原則１５ 重大な変化を評価する	（１）内部環境と外部環境の変化の識別 （２）環境変化の評価 （３）環境変化評価の頻度 （４）新たな戦略の実施によるコンプライアンスリスクへの影響の評価 （５）上級職員の交代がコンプライアンスリスクに与える影響の評価
	原則１６ リスクとパフォーマンスをレビュ	（１）コンプライアンスリスク評価・更新のしくみ （２）優先順位の高いコンプライアンスリスクへの対応状況の確認

	ーする	（３）コンプライアンスプログラムのレビューと取締役会への報告 （４）高リスク領域の監査とモニタリングの計画 （５）議論に資するリスクのレビュー結果の報告
	原則１７ 全社的リスクマネジメントの改善を追求する	（１）類似会社のコンプライアンスプログラムの調査・活用 （２）類似会社のコンプライアンスリスク事例やコンプライアンスリスクマネジメント手法の調査 （３）コンプライアンス部門やリスク管理部門など第２ラインのモニタリング機能の改善
構成要素５ 情報、伝達および報告	原則１８ 情報とテクノロジーを有効活用する	（１）テクノロジーを活用したコンプライアンス関連情報へのアクセス （２）モニタリングおよび監査におけるテクノロジーの活用 （３）テクノロジーを活用したコンプライアンス研修の管理 （４）テクノロジーを活用したモニタリングの効率性・正確性の検証
	原則１９ リスク情報を伝達する	（１）コンプライアンスと業務効率の最適なバランスの確保 （２）環境変化に伴うリスクの変化への対応 （３）経営者によるコンプライアンス意識向上に向けた継続的な発信 （４）戦略決定の際のコンプライアンスリスクの報告受領 （５）コンプライアンス部門と全事業部門との定期的で深度ある双方向のコミュニケーション （６）取締役会でのコンプライアンス関連議題の議論
	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	（１）不適切事案の背景となるカルチャーに関する報告 （２）コンプライアンスに関連するカルチャーの現状と変化の定期的な取締役会への報告 （３）各階層の役割・責任やニーズに合わせた報告 （４）外部委託先で発生するリスクを含めた報告 （５）過去に発生したリスク事案関連文書の適正保管

（注）構成要素と原則は、トレッドウェイ委員会支援組織委員会（COSO: Committee of Sponsoring Organizations of the Treadway Commission）著　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「ＣＯＳＯ全社的リスクマネジメント　ー戦略およびパフォーマンスとの統合ー」（2018 年 4 月　同文舘出版）74 頁他から引用。

３．ＣＯＳＯ全社的リスクマネジメントの 20 の原則に沿った内部監査での７８の視点・着眼点・質問事項と事例・改善提言

≪凡例≫
・*イタリック体*は、**表題**、もしくは**表題と関係する記載**
・青字は【問題ある事例】や「監査での視点・着眼点・質問事項」の記載のうち特に参考となる部分（手段）
・緑字は【問題ある事例】から生じるデメリットの記載のうち特に参考となる部分（結果）、もしくは【ポイント・留意点】のうち特に参考となる部分

・赤茶字は【良好な事例】や「監査での視点・着眼点・質問事項」の記載のうち特に参考となる部分（手段）
・濃い茶色の字は【良好な事例】から生じるメリットの記載のうち特に参考となる部分（結果）

・は特に監査で参考となる**事例と改善提言**
・は特に監査で参考となる**質問**

構成要素１　ガバナンスとカルチャー

原則１　取締役会によるリスク監視を行う

取締役会は、**戦略を監視**し、**ガバナンスの責任を果たす**ことにより、経営者が**戦略と事業目標を達成できるよう支援**する。

※以下の①、②…は原著に記載されている見出（以下同じ）。
①説明責任と執行責任
②スキル、経験および業務知識
③独立性
④全社的リスクマネジメントへの適合
⑤組織が持つバイアス

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）コンプライアンスに関する基本規程・取組方針の取締役会による決議・承認 ①基本規程 ・*コンプライアンスに関する基本規程*が策定され、*取締役会の決議*を得ているか。 ②取組方針 ・*コンプライアンスに関する年度の取組方針*が策定され、*取締役会の承認*を得ているか。	【ポイント・留意点】 (a) *コンプライアンスに関する基本規程*が策定されていない場合、**㋐コンプライアンス推進に関する基本的な考え方が不明確となり**、また、**㋑社内各階層における責任・権限が不明確となり**、適切なコンプライアンスの推進が図られない可能性がある。 (b) また、*取締役会が基本規程を決議*していない場合、取締役会が社内のコンプライアンスの状況に対して、**基本規程に基づく一貫した監視・監督を行えない**能性がある。 (a) *コンプライアンスに関する年度の取組方針*が策定されていない場合、**㋐コンプライアンス推進体制の適切な整備・運用のために解決すべき課題の明確化や、㋑必要な人材等の経営資源の確保がなされず**、適切なコンプライアンスの推進が図られない可能性がある。 (b) また、*取締役会の承認*を得ていない場合、取締役会は社内のコンプライアンス推進のための取組に対して、**年度の取組方針に照らした一貫した監視・監督を行えない**可能性がある。
（２）コンプライアンス委員会、コンプライアンス部門の実質的な機能発揮 ①コンプライアンス委員会 ・取締役会のコンプライアンスリスクマネジメントの監視・監督機能を補佐するコンプライアンス委員会は、*コンプライアンスリスクを調査・管理し、必要な施策を企画・調整するなど実質的に機能*しているか。	【問題のある事例】 ・コンプライアンス委員会は設置されているが、**形式的、事務的、前例踏襲的な議論が中心であり、*実質的な議論*がなされていない**。その結果、取締役会では**コンプライアンスリスクマネジメントの整備・運用状況の実態把握が不十分となり、同リスクマネジメントの監視・監督機能を十分に発揮できていない**。 【改善提言】 ・**コンプライアンス委員会の*議論で不足する事項*や課題を具体的に提示し**、その改善を提言する。

②コンプライアンス部門 ・コンプライアンス部門は、***必要な人員・予算等の資源、及び権限が付与され、実質的に機能***しているか。	【問題のある事例】 ・コンプライアンス部門は設置されているが、期待される機能に比較して***人員・予算等の資源***が不足しており、また***権限***が曖昧、もしくは不十分であるため、***実質的に機能***していない。そのため、取締役会がコンプライアンスリスクマネジメントの整備・運用状況を適切に監視・監督できていない。 【改善提言】 ・コンプライアンス部門の***人員・予算等の資源、及び権限***について不足する事項や課題を具体的に提示し、その改善を提言する。
（３）取締役会のコンプライアンスリスクに係る重要情報や専門知識の確保 ①重要な法改正や判例等に係る最新情報 ・弁護士等の専門家により、***重要な法改正や自社に関連した判例等に係る最新状況が常に把握***され、必要な事項が取締役会に適時に報告されているか。（弁護士等の専門家が取締役会に***法的情報を提供する体制***が整備されているか。）	【問題のある事例】 ・取締役会による***法改正や自社に関連した判例等の把握***が不十分で、重要なコンプライアンスリスクについて見落としが起こりかねない。 【改善提言】 ・取締役会が弁護士等の専門家から***法改正等について最新情報を提供される体制***を整備する。
②取締役会とCCO（最高コンプライアンス責任者）とのコミュニケーション・ルート ・取締役会とCCOとの直接的なコミュニケーション・ルートが設定され、コンプライアンスリスク情報が取締役会に適切に提供されているか。それにより、取締役会が自社の実態に即した***コンプライアンスリスクに対する専門知識を十分に習得***しているか。	【問題のある事例】 ・取締役会が自社の実態に即した***コンプライアンスリスクに対する専門知識を十分に習得***していない。 【改善提言】 ・取締役会とCCOとの直接的なコミュニケーション・ルートを設定し、取締役会が自社の実態に即した***コンプライアンスリスクに対する専門知識を習得***する体制を整備する。
（４）コンプライアンスに関する取締役会への報告 ①取組状況の報告	【ポイント・留意点】

・コンプライアンスに関する年度の取組方針に基づく**取組の進捗状況が定期的に*取締役会に報告***されているか。	・進捗状況が定期的に***取締役会に報告***されていない場合、取締役会は**コンプライアンスの取組を適切に監視・監督できない**可能性がある。
②重大事象の報告 ・重大なコンプライアンス上の事象が発生した時には、***遅滞なく取締役会に報告***されているか。	・コンプライアンス上の重大事象について、***取締役会に適時に報告***されない場合、**取締役会は状況を適時に把握できず、対応を適時、適切に監視・監督できない**可能性がある。

原則２：業務構造を確立する

組織は、**戦略と事業目標を達成するために**、業務構造を確立する。
①業務構造と**報告経路**
②**権限**と**責任**
③**進化する事業体**での全社的リスクマネジメント

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）コンプライアンスリスク管理の仕組と所管部門 ①仕組 ・*コンプライアンスリスクを管理する仕組*が存在するか。 ②所管部門 ・その仕組を運用し、*コンプライアンスリスクの管理を推進する所管部門*が存在するか。	【問題のある事例】 ①*コンプライアンスリスクの管理に焦点を絞った仕組*はなく、コンプライアンスリスクは多くのリスクの一つとして管理されている。 ②*所管部門*はない、もしくは曖昧である。 【改善提言】 ・コンプライアンスリスクの管理に責任を持つ*所管部門*を指定、もしくは設置し、同部部門に*コンプライアンスリスクを管理する仕組*を構築させる。
（２）取締役会に対する報告経路 ・コンプライアンス部門は*取締役会に対する直接的な報告経路*を持っているか。	【問題のある事例】 ・コンプライアンスリスク所管部門は社長に報告する仕組となっており、*取締役会に対する直接的な報告経路*を持たない。 【改善提言】 ・内部監査部門は、コンプライアンス部門が*取締役会に対する直接的な報告経路*を持つよう経営者、もしくは取締役会に具申する。
（３）平時の体制と有事の体制 ・コンプライアンスリスク所管部門の体制について、**コンプライアンスプログラムの推進や啓発活動などの*平時の体制の詳細*の他に、重大不祥事発生時の指揮命令系統や対応決定権限など*有事の体制の詳細***が定められているか。	【問題のある事例】 ・平時の体制の詳細が定められているが、*有事の体制の詳細*は定められておらず、*有事対応*も*平時の体制*をベースに行われている。 【改善提言】 ・*有事の体制の詳細*を定めておくことが、有事対応が機能するために必要であることを、コンプライアンスリスク所管部門長に提言する。なお、検討は有事の定義と判断基準の検討から開始する。

（４）意思決定の支援 ・コンプライアンスプログラムは、コンプライアンスリスクの評価・対応に関する**情報を統合**し、**経営者や取締役会が統合された情報をもとにした*同リスクに対する意思決定を支援***するものとなっているか。	【留意点】 ・コンプライアンスプログラムが、**㋐法令遵守の監視に偏向・偏重している場合や、㋑事業計画と関連したコンプライアンスリスクを想定していない場合、*経営者や取締役会の的確な意思決定を支援***できない場合があることに留意する。
（５）複数のコンプライアンス関連機能間の調整 ・社内に複数のコンプライアンス機能が存在する場合、コーポレートのコンプライアンス部門は、***各コンプライアンス機能のリスク対応を調整***しているか。	【改善提言】 ・業種・業界や地域により、会社が関与する規準（国内法令、域外法令、業界自主規制等）に対応するコンプライアンス機能が会社全体で複数存在する場合、**リスク対応が重複、欠落し、コンプライアンスリスク対応の有効性や効率性が損なわれる**可能性がある。 ・そのため、内部監査部門がコンプライアンス部門に対して**会社全体におけるコンプライアンス機能の重複や欠落がないかを検証するため、各機能の担当や役割を明確にした組織図やレイシー図**（RACI diagram:役割と責任をメンバーに振り分けた表）**を作成**するよう提言する。重複や欠落がある場合には、改善のために***各機能と調整***を行うことを提言する。

原則３　望ましいカルチャーを定義づける

組織は、事業体の**望ましいカルチャーを特徴づける望ましい行動**を定義づける。
①カルチャーと望ましい行動
②判断する
③カルチャーの影響
④コアバリュー，意思決定および行動を結びつける
⑤カルチャーを変える

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）認識の共有 ・自社の***コンプライアンスの目指す姿について、社内で認識が共有***されているか。	【改善提言】 ・自社のコンプライアンスの目指す姿は、一方的に発信するだけではなく、**議論や対話の場を設けることにより、経営層、ミドル層、現場の*各階層の目線を一致させる***ことが望ましい。
（２）問題提起・相談ができるカルチャーの醸成 ・各事業部門は、コンプライアンスの**重要性を繰り返し具体的に説明**し、社員がコンプライアンスリスクを目にした時、もしくはその予兆を認識した時に、自ら***問題提起を行う、または周囲に相談できるカルチャーを醸成***しているか。	【問題のある事例】 ・某金融機関では、危機対応業務にかかる融資において、「危機事象に起因する減収、減益」等といった融資等の要件をクリアするために、複数の支店において、稟議に使用する試算表や雇用維持証明書の改ざん等を伴う不正融資が多数実行されていた。 ・平時においても、コンプライアンスを意識して業務遂行し、違和感があれば***問題提起や相談ができるカルチャーが醸成***されていれば、未然に防げた可能性が高い。 【改善提言】 ・**年に一度など定期的に、職層・職種に応じたコンプライアンス上の問題についての教育、研修、ワークショップ、もしくはロールモデルの紹介を実施する**ことにより、コンプライアンスリスクを目にした時、もしくはその予兆を認識した時に、自ら***問題提起を行う、または周囲に相談できるカルチャーを継続的に醸成***していくことが必要である。

（３）カルチャーの浸透状況や課題のモニタリング ・各事業部門は、*コンプライアンスを重視するカルチャーの浸透状況や課題を把握するために*、定期的に*モニタリング*を行っているか。	①㋐コンプライアンス意識の現状、及び、㋑意識の希薄化などカルチャー面での変化を定期的に***モニタリングし、コンプライアンスを重視するカルチャーの浸透状況や課題を評価・検討***することにより、望ましいカルチャーの浸透のために効果的な各事業部門の特性と親和性の高い対応を行うことが必要である。 ・モニタリング方法には、㋐従業員のアンケート調査、㋑ワークショップ、㋒CSA（統制自己評価）、及び、㋓フィードバックセッション（参加者が協力して生まれたアイデアを説明し、率直な感想や疑問点を受け取るプロセス）などがある。 ②定期的に行う社員意識調査に*コンプライアンスを重視するカルチャーの浸透度合いを含めて行い*、分析結果をコンプライアンス委員会で公表すると共に、職場ごとの浸透度合いをフィードバックすることにより、カルチャーの浸透を職場レベルで促進する。
（４）望ましいカルチャーの明示 ・運営理念、行動規範に*望ましいカルチャーを明示*しているか。	【改善提言】 ・運営理念、行動規範は、コンプライアンス上の問題が発生したときに指針となる考え方を含むことが必要である。 ・この考え方には、㋐自らがコンプライアンスを重視すること、及び、㋑自分がコンプライアンス上の問題の兆候を認識したときに進んで懸念を表明することを、自社の*カルチャーとして明示*することが必要である。

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

組織は、事業体のコアバリューに対するコミットメントを表明する。
①組織全体にコアバリューを**反映**させる
②**リスクを認知するカルチャー**を奨励する
③**説明責任**を果たしている
④自らに説明責任を持たせる
⑤**開かれたコミュニケーション**を維持し，不利益な扱いをしない
⑥コアバリューと望ましい行動に対する**逸脱に対応**する

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）トップからの行動指針の表明と社内伝達 ①トップからのコミットメントによる指針の**表明** ・*経営トップからのコミットメント*に、*コンプライアンスと倫理的な事業行動への行動指針*が示されているか。	【問題のある事例】 ・*経営トップからのコミットメント*に、*コンプライアンスと倫理的な事業行動への行動指針*が示されていないため、コミットメントが機能していない。 【改善提言】 ・*コンプライアンスと倫理的な事業行動への指針*が示されるよう、**コミットメントに自社の具体的な事象を含むように、経営トップに提言**する。
②トップの気風の伝達 ・*経営トップの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*が、社内各層の管理者層を通じて、*会社全体に伝達*されているか。 ・また、*コミットメントを確実に伝達できるための仕組み*を構築しているか、その仕組みを活用しているか。	【問題のある事例】 ・*経営トップの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、社内各層の管理者を通じて*伝達*できていないため、自社のコンプライアンスリスク管理が機能しない。 ・Web サイトや研修などの*伝達体制*の構築を進めておらず、また仕組みがあっても活用できていないため、違反事例が発生してしまう。 【改善提言】 (a)社内の各管理者層の**目標管理制度の項目に、職場実態に即したコミットメントの部下への伝達を含める**よう、人事部門が検討するよう経営トップに提言する。 (b)コンプライアンスプログラムに準拠した研修を、社内各層の管理者に実施し、コミットメントの徹底をはかる。

	(c)経営トップのコミットメントの具体的な内容を記載したカードを作成し、社員証と共に付属させる。
（２）コンプライアンスを限定的に考えない ・コンプライアンスを*限定的に考え*、*社会の期待や意識の変化に対応できていない*ことはないか。	【問題のある事例】 ・会社のバリュー・ステートメント等の行動指針で、品質や安全の確保をはじめとするコンプライアンスの重視が謳われているが、法令や社内ルールを形式的に遵守すればよいと*限定的に考え*、*社会の期待や意識の変化に対応できていない*。 【改善提言】 ・バリュー・ステートメント等の行動指針について、コンプライアンスを幅広く認識し、社会の目線に合わせるよう、望ましい行動の実例を定期的に周知する。
（３）トップからの発信 ・経営トップが、コンプライアンスへのコミットメントとして、*望ましい行動を発信*しているか。 ・また、*コンプライアンス違反から学んだ教訓を会社全体に伝達*しているか。	【問題のある事例】 ・経営トップが違反事案発生時に、当該事案を踏まえた望ましい行動の徹底を会社全体にコミットメントとして発信していない。 ・そのため、自社でコンプライアンスに違反する重大事案が発生しても社内では、当該部門の問題と限定して受け取られたり、他人事と捉えたりして、会社全体の教訓となっていない。 【改善提言】 ・経営トップが、重大な違反事例が発生する都度、コンプライアンスへのコミットメントとして*望ましい行動を発信*する。 ・経営トップが、*コンプライアンス違反から学んだ教訓を自分の言葉で社内に発信*すると共に、社員がいつでも参照できるようにする。
（４）不正事案の早期把握と迅速な報告・通報体制の整備 ①各層の管理者による不正事案の**早期把握** ・各層の管理者が経営トップからのコミットメントに基づいて、*不正事案を早期に把握し*しかるべき階層の経営者に、*迅速に報告*しているか、その能力を有しているか。 ②不正事案を覚知した各個人からの**報告・通報体制**	【問題のある事例】 ・各層の管理者が*不正事案を早期に把握し、迅速に報告*できないため、不正への対応が遅延する。 【改善提言】 ・㋐各層の管理者へのコンプライアンス研修に*不正事案の早期把握と迅速な報告*を含めること、及び、㋑研修の確実な実施を経営トップに提言する。 【問題のある事例】 ・*不正事案の報告・通報体制*が機能していないため、会社が不正事案を把握できない。

(a) 不正事案を**直属の管理者に*迅速に報告***しているか。 (b) 不正事案を直属管理者に報告することが難しい場合には、その**上位の管理者へ*迅速に報告***しているか。 (c) **職制のライン以外に通報する*制度***があるか。	【改善提言】 (a) 社員が不正事案の覚知した時にためらいなく報告、通報できるよう、**リスク事案の報告規程や内部通報規程に、覚知した時には*速やかに報告*すべきことを明確に規定**する。また、**そのこと（速やかに報告すべきこと）をWebサイトや携帯用カードなどにより周知**する。 (b) その旨を内部通報規定で定める。 (c) ***内部通報窓口を設置***するよう提言する。
（５）内部通報制度が機能するための体制整備 ①**通報窓口**の整備 ・内部通報制度が機能しているか。また、従業員が不正行為を幅広く通報できるために、***社内外に通報窓口を複数設置し、周知***しているか。	【問題のある事例】 ・内部通報窓口はあるが**通報されない状態が続いている。通報されても人間関係の不満に限定され**、不正の発見・防止につながらない。 【改善提言】 ・**経営トップが内部通報を重視し、通報者の保護と適時適切な調査を実施する姿勢を折に触れ示すとともに、必要な資源（人員、予算）を確保**する。
②**適時適切な調査と公正さ**の確保 (a) 内部通報があった場合、コンプライアンス部門は***適時適切に調査を実施***しているか。 (b) 不正行為が確認された場合、過去の懲戒事例や弁護士意見をふまえて、***公正で一貫した懲戒処分***を行っているか。	【問題のある事例】 (a) 内部通報の窓口担当者が対応に不慣れで、通報者保護や***適時適切な調査***ができず、**内部通報制度への社員の信頼感が失われている**。 (b) ***懲戒処分が恣意的で、公平でない***と社内で受け取られている。 【改善提言】 ・**㋐事実確認、㋑弁護士相談、及び㋒懲罰委員会等、*懲戒処分の公正さと一貫性を担保する手続*を整備、運用**する。

原則５　有能な人材を惹きつけ、育成し、保持する

組織は、戦略と事業目標にふさわしい**人的資本の形成**にコミットメントする。
①**業務遂行能力**を，確立し評価する
②人材を惹きつけ，育成し，保持する
③パフォーマンスに対して**報奨**を与える
④**プレッシャー**に対処する
⑤**後継者**を準備する

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）プリンシプルベースで考えることのできる人材の育成 ・遵守すべき法令の制定目的・背景を理解し、*プリンシプルベースで考えることで、コンプライアンスリスクに対応できる人材*を育成しているか。	【問題のある事例】 ・日本の自動車メーカーは 2016 年以降、燃費データや検査に関する不正が相次いでいる。2023 年度も某自動車メーカーで車両の型式認証に関する不正が報道された。 【改善提言】 ・法令（例えば、道路運送車両法など）の制定目的・背景を理解し、*プリンシプルベースで考え、自律的に業務に法令違反のリスクがないか検討し、必要な対応をとれる人材*を育成する。
（２）過去に発生した不祥事を風化させない啓発 ・節目ごとにコンプライアンス研修を実施することにより、*過去の不祥事を風化させない継続的な啓発*が行われているか。	【改善提言】 ・㋐新入社員研修、㋑管理職研修、㋒部店長研修、及び、㋓役員研修などの**制度研修で、自社で過去に発生した不祥事について、発生の背景、真因、再発防止策についてグループ討議をする**など、*過去の自社での不祥事を風化させない実効性のある啓発*を継続的に行う。 【参考】 (a)某航空会社では、大規模墜落事故の教訓を風化させないため、**「安全啓発センター」を開設し、後世に語り次ぐため、機体の一部を展示する**など、社員教育に活かしている。 (b)型式認証不正が発覚した某自動車メーカーは**「正しい仕事学習館」を開設**した。

（３）不祥事を自分事として捉えることのできる人材の育成 ・**コンプライアンスリスクを効果的に認識し、管理する個人の能力**を高めることにより、自分の担当業務以外で発生した***不祥事を自分事として捉え***、***影響を分析し、防止策を立案できる人材***を育成しているか。	【問題のある事例】 ・約 20 年にわたりエンジンの排出ガスや燃費に関する認証申請において広い範囲で不正が行われてきた実態が、某自動車メーカーで明らかになった。 【改善提言】 (a)**自社で過去に発生した事案を事例とするグループ討議を中心とした研修**を行うことにより、***不祥事を自分事として捉え***、コンプライアンスリスクを適切に認識して管理する個人の能力を高める。 (b)なお、不祥事の再発防止策の立案と実施は**全社的な業務プロセスの改善の契機**ともなる。上記自動車メーカーでは再発防止のため、開発、認証、品質保証の領域ごとに業務プロセスを改善した。

構成要素２　戦略と目標設定

原則６　事業環境を分析する

組織は、**リスクプロファイルに対する事業環境の潜在的影響**を検討する。
①事業環境を**理解**する
②**外部環境**と外部のステークホルダーを検討する
③**内部環境**と内部のステークホルダーを検討する
④事業環境がどのように**リスクプロファイル**に影響を及ぼすか

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）**組織戦略を踏まえたコンプライアンスリスクの管理** ①コンプライナンスリスク管理の**対象とする領域を決定**する際に、㋐***組織戦略***、㋑その意思決定プロセス、及び、㋒その変更***を考慮***しているか。	【改善提言する際の留意点】 ・同左 （注）「事業戦略」は**特定の事業についての戦略**、「組織戦略」は人事やIT戦略、更にはパーパスやビジョン、カルチャーなども包含した**企業全体にかかわる戦略**といったニュアンスがあります。当研究会では、コンプライアンス・リスクマネジメントにおいて認識すべき戦略は後者と考え、「**組織戦略**」という用語を用いています。
②(a)***組織戦略の変更に伴うコンプライアンスリスクの変化へ対応***できているか。(b)変化への**対応策を計画し実行する部門**は決められているか。また、(c)当該部門に***戦略の変更に関する情報***がタイムリーに**伝達・共有**され、必要な対応がとられているか。	・(a)(b)コンプライアンスリスクの所管部門を定め、当該部門が***組織戦略の変更に伴うリスク変化への対応***を講じる位置付けとすること。(c)当該部門に***戦略の変更に関する情報***をタイムリーに伝達・共有するプロセスを作ること。

（２）コンプライアンスリスクに及ぼす環境要因の変化の確認 ・コンプライアンスリスクに影響を及ぼす*内部の環境要因と外部の環境要因の変化を確認*し、影響の大きいリスク要因の変化を識別しているか。	【留意点】 ・コンプライアンスリスクに影響を及ぼす環境について、*内部の環境要因*(注１)*と外部の環境要因*(注２)*を洗い出して一覧化*し、定期的に*変化を確認*し、一覧を更新する。 （注１）内部の環境要因→㋐社員の構成や雇用・契約形態、㋑プロセス、㋒技術、㋓組織のカルチャー、及び、㋔トップのメッセージなど （注２）外部の環境要因→㋐法規制、㋑競合などの市場環境、㋒政治・経済動向、㋓事業を展開する国や地域など
（３）他のリスク対応策によるコンプライアンスリスクへの影響の検討 ・*他のリスクへの対応策を実施することによる、コンプライアンスリスクへの影響が検討*されているか。	【留意点】 ・同左。

原則７　リスク選好を定義する

組織は、価値の創造、維持、実現の観点からリスク選好を定義する。
①リスク選好を**適用**する
②リスク選好を**決定**する
③リスク選好を**明確に表現**する
④リスク選好を**活用**する

【参考：リスク選好の定義】
・当研究会では、リスク選好を以下のように定義する。
リスク選好とは、企業が**企業価値向上のために受け入れるリスクの種類と量**である。

【参考：リスク選好の事例】
(a)**製薬会社**では、**薬機法**（医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律）**違反**するリスク選好はゼロである。
(b)**鉄道会社**では、**鉄道事故に起因する死亡事故**に対するリスク選好はゼロである。

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）コンプライアンスに関するリスク選好の誤解 ・コンプライアンスリスクに対する選好を、***既知のコンプライアンス違反を意図的に受け入れることと誤解***していないか。	【問題のある事例】 ・**コンプライアンス違反のリスクを、損得勘定で天秤にかけて安易に取ってしまい**、重大なコンプライアンス違反が発生している。 【改善提言】 ・コンプライアンス違反は基本的に取るべきではなく、もしくはリスク許容度が低いため、**損得勘定で安易に天秤にかけて取らない**ように指摘する。
（２）コンプライアンス委員会の議題 ・***コンプライアンス委員会の議題***に、***コンプライアンスリスクに関連するリスク選好***が入っているか。	【問題のある事例】 ・***コンプライアンス委員会の議題***に、***コンプライアンスリスクに関連するリスク選好***が入っておらず、**(a)リスク選好を事業目標の達成との関係を踏まえて評価できない、もしくは、(b)リスク選好をコンプライアンスリスクの変化に基づいて更新できないリスク**がある。 【改善提言】 ・***コンプライアンス委員会の議題***に、コンプライアンスリスクに関連するリスク選好を入れる。これはコンプライアンス違反の予防と発見のツールになる。

（３）国・地域や部門により異なるコンプライアンスリスクの検討 ①*国・地域によるコンプライアンスリスクの違い*を考慮せず、過重な統制や統制不足になっていないか検討したか。 ②*ある部門に重大な影響を与えるコンプライアンスリスクへの対応を*、*他の部門に対しても同じように対応させる*ことで業務効率を阻害していないか。	【問題のある事例】 ・例えば、設備投資の実施に際して、*国・地域で異なる自然災害リスクへの対応規制*を考慮せず、一律な水準を適用したために、過剰な設備投資（オーバースペック）を行う、逆に投資が不足し規制を満たせない。 【改善提言】 ・設備投資の水準は、国や地域の規制を確認したうえで判断する。 【問題のある事例】 ・*ある部門に重大な影響を与えるコンプライアンスリスクへの対応を*、*他の部門に対しても同じように対応させる*ことで業務効率を阻害している。 【改善提言】 (a)当該部門が関係するコンプライアンスリスクを洗い出し、当該部門の業務目標の達成に与える影響を検討した上で、対応を決定する。 (b)なお、コンプライアンス部門は各部門で検討したリスク対応を集約し、その判断の妥当性について定期的に検証する。
（４）戦略遂行に伴うコンプライアンスリスクがリスク選好の範囲内にあるかの確認 ・組織戦略を審査する際に、*戦略の遂行に伴い想定されるコンプライアンスリスクが、リスク選好の範囲内にあるか確認*しているか。	【問題のある事例】 ・確認していない場合には、会社のリスク選好を上回るコンプライアンスリスクが発生する可能性がある。 【改善提言】 ・組織戦略の取締役会審議資料には、*戦略遂行に伴い想定されるコンプライアンスリスクが**リスク選好の範囲内にあることの説明***の記載を必須とする。

原則８　代替戦略を評価する

組織は、**代替戦略**と**リスクプロファイル**に対する**潜在的影響**を評価する。
＊注：戦略が**リスクプロファイルに与える影響**を評価するという意味。
①**戦略と結びつける**ことの重要性
②選択された**戦略からの示唆**を理解する
③戦略を**リスク選好**と結びつける
④戦略を**変更**する
⑤**バイアス**を減らす

【参考：リスクプロファイル】
・リスクとパフォーマンスとの関係。
・COSO-ERM では、**縦軸をリスク、横軸をパフォーマンス**とした**リスク曲線**により、**リスクとパフォーマンスの関係**が示されている。なお、一般的には、パフォーマンスが大きくなるほど、リスクが大きくなる。

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）CCO（最高コンプライアンス責任者）及びコンプライアンス部門の組織戦略への関与 ①CCO は、***組織戦略を検討する会議に出席し***、**組織戦略がコンプライアンスリスクに及ぼす影響**について、***経営者に意見を述べ***ているか。	【問題のある事例】 ・組織戦略が既決事項として取り扱われ、***CCO が*****戦略がコンプライアンスリスクに及ぼす影響について、*****経営者に意見を述べる機会*****が与えられない。** 【改善提言】 ・***CCO は***、検討される組織戦略で想定されるリスクについて、**コンプライアンスの観点から*****経営者に意見を述べ***、経営者がコンプライアンスリスクを認識したうえで意思決定できるように支援する。
②CCO は***コンプライアンス部門に、組織戦略を適宜に説明し、組織戦略を理解させて***いるか。	【問題のある事例】 ・***CCO がコンプライアンス部門に対して、組織戦略を適宜に説明せず***、***コンプライアンス部門が戦略を知る***ことが遅れて、適切なスキルを有する担当者のアサインやコンプライアンスリスクに対処する準備が遅延する。

	【改善提言】 ・CCO は組織戦略の検討段階から、*コンプライアンス部門に組織戦略を説明し、理解させる*。
（２）M&A のコンプライアンスリスクに関するデューデリジェンス ①*コンプライアンスリスクに係るデューデリジェンス*を適切に実施しているか。 ②M&A チームは、必要な*コンプライアンスリスクに係るデューデリジェンスを実施*し、コンプライアンスの側面から、経営者が M&A の実行可否や受入れ可能な契約条件などを検討する情報を提供しているか。 ③*M&A 実施時のデューデリジェンスで確認されたコンプライアンスリスク情報がコンプライアンス部門に引き継がれて*いるか。	・左に同じ 【問題のある事例】 ・M&A チームによる M&A 対象企業からの情報収集や対象企業の経営者とのコミュニケーションが不十分な場合には、同チームによる必要な*コンプライアンスリスクに係るデューデリジェンス*が行われず、経営者がコンプライアンスリスクを適切に検討できない。 【改善提言】 ・M&A チーム*のデューデリジェンス担当者が情報収集や相手先企業とのコミュニケーションが図れるよう*、自社の経営者、及び相手先企業の経営者に要請する。 【問題のある事例】 ・デューデリジェンスで確認されたコンプライアンスリスク情報がデューデリジェンス実施チーム内にとどまっており、コンプライアンス部門に引き継がれていない。そのため、M&A 実施後にコンプライアン部門が当該会社のコンプライアンスリスクを把握できない。 【改善提言】 ・M&A のプレスリリース後速やかに、*デューデリジェンスで確認されたコンプライアンスリスクをコンプライアンス部門に伝達する*ことを社内規程に定める。
（３）戦略の評価 ①コンプライアンス部門は、戦略策定部門とコミュケーションをとり、*組織戦略の遂行で想定されるコンプライアンスリスクを適切に評価*しているか。	【問題のある事例】 ・コンプライアンス部門と戦略策定部門とのコミュニケーションが不十分なため、戦略の目標や実施内容についてのコンプライアンス部門の理解が不十分となっている。そのため、コンプライアンス部門が*組織戦略の遂行で想定されるコンプライアンスリスクを適切に評価*できず、戦略策定部門に対してリスクのモニタリング方法や対応策について必要な助言、もしくは協議が行えない。

②コンプライアンス部門は、**組織戦略の変更**に際して、もしくは**コンプライアンスリスクのモニタリング結果**に基づき、必要な***リスク評価の見直し***を行い、新たなリスクや重大度が増したリスクを識別しているか。	【改善提言】 ・コンプライアンス部門は、戦略策定部門とコミュニケーションを取り、事業戦略の目標や実施内容を理解し、***戦略の遂行で想定されるコンプライアンスリスクを適切に評価***し、必要な指導をする。 【問題のある事例】 ・コンプライアンス部門が、組織戦略の変更に際して、もしくはコンプライアンスリスクのモニタリング結果に基づき、***リスク評価の見直し***を行っておらず、新たなリスクや重大度が増したリスクを識別できない。 【改善提言】 ・コンプライアンス部門は、組織戦略の変更やモニタリング結果に基づいたリスク評価の見直しを行うためのレビュー計画を策定し、***リスク評価の見直し***を行う。

原則９　事業目標を組み立てる

組織は、戦略と結びつき、かつ、戦略を支える**事業目標**をさまざまな階層において**設定する際にリスクを検討**する。

①事業目標を**設定**する
②事業目標を**結び**つける
③選択された事業目標からの**示唆**を理解する
④事業目標を**分類**する
⑤**パフォーマンス指標**と**ターゲット**を設定する
⑥**許容度**を理解する
⑦パフォーマンス指標と設定された許容度

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）**事業目標の策定や達成自体により発生するコンプライアンスリスクの理解** ・事業部門は、***事業目標の策定やその達成自体がコンプライアンスリスクを生み出す***場合があることを**理解**しているか。	【監査での留意点】 ・事業目標について、 (a)その**事業目標を策定することによりもたらされる**コンプライアンスリスクがある (b)その**事業目標を策定しないことによりもたらされる**コンプライアンスリスクがある (c)**それが達成されることによりもたらされる**コンプライアンスリスクがある (d)**それが達成されないことによりもたらされる**コンプライアンスリスクがある ・このような***事業目標に関連するコンプライアンスリスク***について、事業部門が**特段の注意を払っていない**場合があることに留意する。
（２）**自部門の事業目標の設定・変更** ・***自部門の事業目標を設定・変更***することが、**他部門のコンプライアンスリスクに影響**を及ぼすことを理解しているか。	【監査での留意点】 ・***自部門の事業目標の設定・変更***が、他部門、もしくは全社のコンプライアンスリスクに対し影響を及ぼす場合があることを、**当該部門が理解していない場合がある**。 ・内部監査では、***部門の事業目標の設定・変更***では、**部分最適ではなく全体最適に留意すべき**ことを提言する。

（３）コンプライアンスリスクに関する業績評価指標 ①*事業目標を設定することにより増加することが想定されるコンプライアンスリスク*に*業績評価指標*が設定されているか。	【監査での留意点】 ・*事業目標を設定することにより増加するコンプライアンスリスク*について、*業績評価指標*を設定しモニタリングすることは、コンプライアンスプログラムが有効に機能するために有効である。
②業績評価指標は、*客観的*で**比較可能**か。	【監査での留意点】 ・「設定した指標が*客観的*であるということは、どのような状態か」という点について社内で共通の認識を持てるようにしておくことが必要である。

構成要素３　パフォーマンス

原則１０　リスクを識別する

組織は、**戦略**および**事業目標のパフォーマンスに影響を及ぼすリスク**を識別する。
①リスクを識別する
②リスク**一覧表**を利用する
③リスク識別の**アプローチ**
④**フレーミングリスク**

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）**コンプライアンスリスクの識別プロセス** ・㋐法律や規制の新設や変更、㋑組織戦略の変更、もしくは、㋒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など、会社が直面する多数のコンプライアンス***リスクを全社的にどのように識別、評価、対応***しているか。	【問題のある事例】 ・全社のビジネスから生じる様々なコンプライアンスリスクを戦略や事業目標を踏まえ、***会社全体で一貫性をもって識別、評価、対応***する必要があるが、**各部門は縦割りで独自に対応しており、重大な課題に直面するまでリスクの共有が進みにくい**。 【改善提言】 ・会社全体を対象にして関連法令の新設・変更情報の収集を行い、ビジネスから生じる様々なコンプライアンス***リスクを全社的に識別して体系的に評価、対応する枠組み*****を整備・運用**する必要がある。 ≪参考１≫商品・業務の**リスクチェック** ・Ａ社では、**新商品・新規業務を開始する際に**業務所管部とリスク管理部門と協働してコンプライアンスリスクを含む**全てのリスクを洗い出しチェックするプロセス**を導入している。 ・また、**既存の商品・業務についてもリスクプロファイルに変化があった場合、同様のチェック**を行っている。既存リスクの変化・新しいリスクを含むリスクの全体状況を定期的に識別して経営に報告している。

	例：生成 AI の業務活用におけるリスク検討 ≪参考２≫**経営レベルでのリスク識別**の取り組み ・Ｂ社では、**経営会議メンバー**で**構成される**リスク管理委員会で、㋐戦略、及び事業目標の達成に係る経営に重大な影響を及ぼすリスクの変化、㋑新たに発生したリスク、及び、㋒高まりを見せるエマージングリスクに関する事項等についての審議を経て、重要なコンプライアンス**リスクを識別**している。
（２）**コンプライアンスリスクの**可視化・体系化と更新頻度 ・識別された全社リスクの中からコンプライアンス***リスクを可視化して体系的に把握***するためにどのような方法をとっているか。また、識別したリスクを***どのような頻度で更新***しているか。	【問題のある事例】 ・全社リスクの中からコンプライアンス**リスクを識別するプロセス**が明確に定められていない。**識別されたコンプライアンス*リスクが体系化・階層化*されておらず、*可視化して把握*することができない。*更新の頻度*についても担当者の裁量に任されており、*定期的な更新*が行われていない。** 【改善提言】 ・コンプライアンス**リスクの識別プロセスを明確に定め文書化**することが必要である。**識別したコンプライアンスリスクについてリスク一覧表を作成するなど*可視化・体系化*して把握し、*定期的*（例えば、半年毎）*に更新*すること**が必要である。 ≪参考３≫リスクの識別のアプローチ ・**リスクの識別**には多様な**アプローチ**が利用可能であり、事業の規模、拠点および複雑さに応じて、複数の手法を用いられる。 ・例えば、リスクの種類を次のように３分類（既存のリスク、新しいリスク、エマージングリスク）し、㋐簡単なアンケート、㋑ワークショップ、㋒インタビュー、㋓過去の事象からのデータ追跡、㋔リスクの変化を識別するための主要指標、㋕ワークフロー表などによるプロセス分析、もしくは、㋖コグニティブコンプ―ティング[注] などの**アプローチ**を活用することが考えられる。 （注）コンピュータ自身が自ら学習し、考えて、大量のデータを瞬時に統合し、分析するシステム。
（３）エマージングリスクの識別 ・***エマージングリスク***が、㋐戦略や組織目標の達成に影響を及ぼし得る**脅威**や、㋑事業目標を達成するのに役立つ**機会*をどのように識別***しているか。	【問題のある事例】 ・***エマージングリスク***は、環境変化等により新たに現れてくるリスクであって従来リスクとして認識されていなかったものや、リスクの程度が著しく高まったものであり、**㋐その定義や、㋑リスク（脅威・機会）を識別するためのプロセス、及び、㋒検討に関与する者などが決まっていない。**

	【改善提言】 ・*エマージングリスク*についての ㋐**定義** ㋑戦略や事業目標の達成に影響を及ぼし得る*脅威や機会の識別プロセス* ㋒**関係する業務管理者**やリスクオーナー　など、 *エマージングリスクにおけるコンプライアンスリスク識別のためのフレームワーク*を明確化する。 ≪事例４≫エマージングリスクの選定とモニタリング・調査研究 ・Ｃ社は、**エマージングリスクを「環境変化などにより新たに発現または変化し、当社に大きな影響を及ぼす可能性のあるリスク」と定義し**、重大リスクへの変化の予兆を捉えて管理をしている。 ・洗い出したエマージングリスク候補から想定される**影響度が一定以上のものをエマージングリスクに選定**している。 ・現在「AI の活用拡大」「地球温暖化」「人権重視対応の遅れ」など 10 件程度をエマージングリスクとして選定し、**損失軽減**の観点だけではなく、新たな商品・サービスなどの**ビジネス機会**の観点から**モニタリング**および**調査研究**を実施している。
（４）**グループ会社を含めたリスクの識別** ・事業計画に関するリスクの一覧表は、バリューチェーンを構成する*グループ会社のリスクを含めたリスクの識別*活動に基づき作成されているか。	【問題のある事象】 ・リスクを識別するにあたり、**自社内**のパフォーマンスレビュー、プロセス分析は実施したものの、当社事業の一部の**業務を委託しているグループ会社Ａに対してはそれらを実施しなかった**。 ・サービスや製品の品質が低下したため、原因を調査したところ、委託元部門は目標を達成するためにグループ会社Ａに対して納期の**短縮**や委託費の**削減**を要請していた一方で、グループ会社Ａの業務プロセスの効率化に向けた**支援・指導**を実施していなかったことが判明した。 【改善提言】 ・リスクの識別活動の対象に、バリューチェーンを構成する*グループ会社も含めてパフォーマンスレビュー、プロセス分析*を実施する。
（５）**複数のアプローチを活用したリスクの識別** ・*リスクの識別にあたっては*、㋐過去の事象からのデータ追跡やプロセス分析といった**書類・データの閲覧**に加え、㋑インタビュー	【問題のある事象】 ・新規事業について、㋐各種会議資料や、㋑法令、社内規程の閲覧、及び、㋒会計・人事・業績等のデータ分析などの**書類・データ閲覧のみでリスクを識別**し

やワークショップといった人の知見を聴取するなど***複数のアプローチを活用***しているか。	た。そのため、**インタビューやワークショップを実施すれば把握可能であった海外異業種からの参入の可能性を見落としてしまった。** 【改善提言】 ・リスクの識別にあたっては、書類・データ閲覧に加えて、**その分野に知見を持つ人へのインタビュー、ワークショップを通じて、最近の懸念事象、過去の経験を踏まえた懸念事象を把握**するなど。 ・なお、環境が整えば、**コグニティブコンピューティング**(注)により、人では気づきづらいリスクを把握する。 （注）コンピュータ自身が自ら学習し、考えて、大量のデータを瞬時に統合し、分析するシステム。

原則１１　リスクの重大度を評価する

組織は、リスクの重大度を評価する。
①リスクを評価する
②事業体における**異なる階層での重大度**を評価する
③重大度の**測定基準**の選択
④評価アプローチ
⑤固有リスク、目標（とする残余）リスクおよび（実際の）残余リスク　＊（　）内は追記
⑥評価結果を**描写**する
⑦**再評価のトリガー**（契機）を識別する
⑧評価における**バイアス**

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）**コンプライアンリスクの重大度の評価方法** ①**重大度の評価基準**の設定 ・***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***が採用されているか。	【問題のある事例】 ・コンプライアンスリスクの重大度の評価を「大・中・小」や「1 から 5 の 5 段階」としているものの、***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***がなく、**評価者の主観だけに依存しており、体系的な判断ができていない。** 【改善提言】 ・コンプライアンスリスクの重大度を発生可能性と影響度に基づいて評価する。 ・発生可能性と影響度を***評価する統一された基準***を設定する。例えば、 (a)**発生可能性**については精度を高める方法として「コンプライアンス違反の**頻度**」と「存在する**統制**」**の２つの要因を考慮**して基準を定義する。また、 (b)**影響度**については、㋐「法務（罰金や刑罰）」だけでなく、㋑「**財務**（調査や是正に係るコスト）」、㋒「**業務**（中断の可能性）」、及び、㋓「**評判**（レピュテーション）」**なども考慮**して**基準**を定義する。
②評価の尺度や測定方法の***カスタマイズ*** ・評価基準は外部の事例をそのまま使うのではなく、会社に合わせて***カスタマイズ***されているか。	【問題のある事例】 ・評価基準が設定されているものの、**外部の参考事例を単純に流用しており、会社の実態にそぐわない評価結果**となっている。

	【改善提言】 ・評価基準を外部の事例を参考にして設定する場合、単純に流用することを避け、会社特有のニーズや環境の状況、及び、会社の戦略や事業目標に照らして*カスタマイズ*することが必要である。
（２）評価に関するバイアスの排除と一貫性の確保 ①評価の**バイアス**の排除 ・評価結果について、各リスクの主管部門の自己評価だけを拠り所としており、各部門の*バイアスがかかった評価*となっていないか。	【問題のある事例】 ・リスクの重大度評価の全社的な取りまとめにおいて、各リスクの主管部門の自己評価をそのまま使用しており、各部門の*バイアスが残っており*、*全社的な整合性がとれていない*評価となっている。 【改善提言】 ・重大度の評価は、各リスクの主管部門の自己評価だけに依存するのではなく、リスク管理部門や経営企画部門など、さまざまな分野や経験を持つ複数の評価者のレビューを受けて*バイアスを最小限に抑え*、*全社的に整合性がとれたもの*に調整することが必要である。
②評価の**一貫性**の確保 ・評価において、評価者は*一貫した測定基準*を適用しているか。	【問題のある事例】 ・評価のたびに測定基準を変えており、過去の評価結果との比較分析ができない。 【改善提言】 ・**過去の評価結果との比較分析**を行うためには、評価する基準がブレないことが大切であり、評価者は*測定基準を一貫して適用*することが必要である。

原則１２　リスクの優先順位づけをする

組織は、**リスク対応選択の基礎**として、リスクの優先順位づけを行う。
①**規準**を設定する
②リスクを優先順位づけする
③**リスク選好**を活用したリスクの優先順位づけ
④**すべての階層**における優先順位づけ
⑤優先順位づけにおける**バイアス**

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）リスク対応の優先順位の決定 ・コンプライアンスリスクの重大度を発生可能性と影響度の観点から評価し、対応すべき事項の***優先順位を決定***しているか。	【問題のある事例】 ・Ａ社はコンプライアンスリスクの重大度を発生可能性と影響度の観点から評価しているが、対応すべき事項の***優先順位づけ***を**部門ごとに行い**、実行している結果、**経営資源が効率的に使用されていない**。 【改善提言】 ・コンプライアンスリスク対応の***優先順位を決定***する際には、**経営資源を効率的に使用**できるように、コンプライアンス部門やリスク管理部門が中心となり、**会社全体で統一的に行う**ことを提言する。
（２）リスク対応の優先順位づけにおける他の評価基準の使用 ・コンプライアンスリスク対応の優先順位付けにおいて、重大度だけで判断できない場合は、***他の要因も考慮***しているか。	【問題のある事例】 ・Ｂ社はコンプライアンスリスクの重大度を発生可能性と影響度の観点からそれぞれ３段階で評価しているが、発生可能性と影響度が**中程度のものが多く**、対応すべき事項の優先順位付けに至っていない。 【改善提言】 ・コンプライアンスリスクの重大度**評価が同程度のもの**については、***㋐速度、㋑影響の持続性、及び、㋒回復度等の評価基準***を使用して、対応すべき事項の優先順位を決定する。
（３）リスクの優先順位に応じた経営資源の配分 ・会社として優先して対応すべきコンプライアンスリスクは、**リスクベース**の考え方に基づき、***優先順位付に応じて経営資源が配分***されているか。	【問題のある事例】 ・**リスク評価の見直しが定期的に実施されていない**ため、環境の変化により過去と比較し重大度が増加している***優先順位の高いリスクに対して、十分な資源が配分***されていない。

・つまり、全てのコンプライアンスリスクへ対応するのではなく、***重大度の高いリスクに重点的に経営資源が配分***されているか。	【改善提言】 ・***リスクの優先順位に応じて、リスク対応のための経営資源を配分***する。 ・例えば、対応の優先順位が高いリスクに対しては、経営資源を追加するなど**重点的に資源を配分**する。他方で、**優先順位が低いリスクに対しては、現状の資源配分の見直しを検討する、もしくは現状の資源配分でモニタリングを継続する。**
（４）経営層が参加する会議体での議論 ・優先順位が高いコンプライアンスリスクは、コンプライアンス委員会等の***経営層が参加する会議体に報告され***、対応計画、及びモニタリングの状況について***十分な議論***がされた上で、当該リスクへの対応の決定権者（リスクオーナー）が対応を決定しているか。	【問題のある事例】 ・コンプライアンス委員会は定期的に開催されているが、コンプライアンスリスクに関しては**リスクの報告にとどまり、対応計画、及びモニタリングの状況についての*議論がなされていない***、もしくは不足している。 【改善提言】 ・***経営層が参加する会議体で議論***することにより、**(a)会社の方針や戦略を踏まえた対応の意思決定（資源配分を含む）を行うことができ、また、(b)リスクオーナーの責任を明確化できる。**それにより、優先順位の高いリスクへの確実な対応が推進される。

原則１３　リスク対応を実施する

組織は、リスク対応を**識別**し、**選択**する。
①リスク対応を**選択**する
②リスク対応を選択し**採用**する
③リスク対応の**費用**と**効果**を考慮する
④その他の留意点

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）リスク対応改善の PDCA サイクルの実施 ・コンプライアンスリスクを***改善するための PDCA サイクル***を回しているか。	【問題のある事例】 ・Ａ社は、苦情削減を年間コンプライアンスプログラムに掲げているが、苦情年間受付件数は削減に向かっていない。 【改善提言】 ・苦情発生の要因を社員の行動レベルで分析して**改善策を作成**し（Ｐ）、改善の**実施**（Ｄ）による改善状況を計る管理指標（KPI）を策定する。そのうえで、管理指標をもとに**フォローアップ**や継続的なモニタリング（Ｃ）を行い、必要な**改善**を行う（Ａ）という***PDCA サイクルを回しながら改善***を進める。
（２）リスク対応の形骸化防止 ・コンプライアンスリスク***対応が形骸化しないためにどのような施策***を講じているか。	【問題のある事例】 ・Ｂ社は、個人情報漏えいの撲滅に向け、㋐メール誤送信・資料誤送付注意喚起ポスターの掲示、㋑メール社外送信の際の注意喚起ボックスの表示、及び、㋒資料送付の際の二重チェックなどの防止対策を導入して取り組んでいるが、個人情報漏えいの年間件数は削減に向かっていない。 【改善提言】 ・上記事例では、防止対策の形骸化の懸念がある。***形骸化を回避するため***、個人情報漏えい対策の研修を実施し、防止対策を共有すると共に、グループ討議による原因の深掘り（根本原因の解明）を行う。それにより、社員に漏えい防止に対する説明責任を持たせ、***形骸化しない実効性のある防止対策***を実現する。
（３）リスク対応策追加のメリットとコストの比較検討 ・リスク対応策の追加は、***改善メリットと、***改善に要する財務的・非財務的***コストとを比較検討***したうえで判断されているか。	【問題のある事例】 ・Ｃ支店は、個人情報漏えい対策のため、二重チェックを実施していたが、内部監査において、個人情報漏えいが引き続き発生し、対応策が不十分であると指

	摘され、その対策として、**三重チェック**を実施する旨と、そのための**新たなパート社員を採用**する旨を内部監査部に回答した。 【改善提言】 ・上記事例では、㋐三重チェックのための社員の新たな**業務負荷**によるモチベーションの低下、㋑業務時間をさらなるチェックに割くことによる**生産性の低下**、及び、㋒パート社員の**人件費**などの***対応策のコストと、改善メリットとを比較検討***したうえで、実施を判断すべきである。 ・すなわち、**リスク対応策の追加によるメリットとコストとは、トレードオフの関係になる場合が多い**ことに留意し、***改善によるメリットと改善に要するコストを比較検討***し、**現実的か否かを検討したうえで判断**する必要がある。

原則１４　ポートフォリオの視点を策定する

組織は、**リスクのポートフォリオの視点**を策定し、評価する。
①ポートフォリオの視点を**理解**する
②ポートフォリオの視点を**策定**する
③ポートフォリオの視点を**分析**する

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）コンプライアンスリスク対応と他のリスクとの相互関係の考察 ・現場レベルでは、***コンプライアンスリスクへの対応***（例：検査の緻密化・増加）***と他のリスク***（例：生産効率の低下・コスト増）***との相互関係***を考察し、その結果に基づいた**ポートフォリオ的な見方による調整**を行い、**リスク対応の部署間での対立や非効率**を防いでいるか。	【問題のある事例】 ・某自動車メーカーでは、衝突試験や排出ガス、燃費試験でのデータ改ざんなどのコンプライアンスリスクが顕在化した。原因は、㋐**開発部門と検査部門が同一部署**に属していたため長年に亘り独立した検査が行われなかったこと、㋑**短期間での成果**を求められる現場の過度な負担、及び、㋒「絶対に合格しなければならない」という強い**プレッシャー**が挙げられた。 【改善提言】 (a) コンプライアンス違反の再発防止のため、全社レベルでは、検査部門の独立性を確保して、開発部門からのプレッシャーを排除し、独立した立場から検査が行えるようにする。 (b) また、現場レベルでは、***コンプライアンスリスクへの対応***（例：検査の緻密化・増加）***と他のリスク***（例：生産効率の低下・コスト増）***との相互関係***を考察し、**ポートフォリオ的な見方による調整を行う**ことにより、**リスク対応の部署間での対立や非効率を防ぐ**。
（２）各種のコンプアライアンスリスクのマネジメントと全社的リスクマネジメントとの統合 ・経営レベルで、***各種のコンプライアンスリスクのマネジメントと全社的リスクマネジメント（ERM）と統合して、リスク全体をポートフォリオの視点から管理***しているか。 ※これにより、**ポートフォリオの視点から全社レベルでリスクの重大度や対応策を一元的に把握し、各リスクの相互作用を認識**した上で、全社的リスクマネジメントの実施が可能となり、**各部門が単独でコンプライアンスリスクを管理**	【問題のある事例】 ・上記（１）の事案による被害は、当該部署に留まらず、㋐部品調達やサプライチェーン等（親会社も含む）全体の生産停止、㋑地域経済面では雇用の一時喪失など広範に及んだ。 ・経営者に対しては、㋐検査部門が開発部門から独立していないこと、㋑全社的なリスクに関するポートフォリオ管理の欠如、㋒内部統制の不備、及び、㋓監査の不備などの問題点が指摘された。

するより、効率的、効果的にコンプライアンスリスクを管理できる。	・その結果、当局による生産停止措置は約半年となり、改善策と共に、経営陣の退陣やメンバーの入れ替え（監査役、外部監査法人、内部監査部門長を含む）を表明するに至った。 【改善提言】 ・㋐開発部門と検査部門の分離、㋑内部統制の強化、㋒外部監査の強化、及び、㋓経営陣のコンプライアンス教育などを検討・実施する。検討・実施に際しては、上記の各種対応策を経営者がポートフォリオの視点から全社レベルで管理することにより、*各種のコンプライアンスリスクのマネジメントと全社的リスクマネジメント（ERM）とを統合し、*全社的リスクマネジメントによる一貫性のあるコンプライアンスリスクの管理を実施する。

構成要素４　レビューと修正

原則１５　重大な変化を評価する

組織は、**戦略や事業目標に重大な影響**を与え得る変化を認識し、評価する。
①レビューを事業活動に統合する
②内部環境
③外部環境

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）内部環境と外部環境の変化の識別 ・コンプライアンスリスクに重大な影響を与える可能性がある***内部環境、及び外部環境の重要な変化を識別***しているか。	【問題のある事例】 ・Ａ社は業務プロセス効率化のために**第三者を利用**（業務の外部委託）したが、このことを**コンプライアンスリスクの*変化要因として識別*しなかった**。 ・また、**環境変化の識別手法を、外部業界団体からの情報提供（外部要因の識別）、及び重要会議の資料のレビュー（内部要因識別）に限定**していたため、**重要な*変化要因として*識別すべき法規制の変化や社内プロセスの変更を*識別*できなかった**。 【改善提言】 ・コンプライアンスリスクに重大な影響を与える可能性がある***内部環境の変化***（㋐業務プロセスの第三者利用、㋑プロセス及びテクノロジー変化、㋒上級職員の交代、㋓M&A 等）***と、外部環境の変化***（㋐法律・規制・エンフォースメントの優先順位の変化、㋑社会規範や価値観の変化等）***をカテゴリー別に一覧化し***、それぞれの変化をどのような手法で***識別***するかを定める。
（２）環境変化の評価 ・識別した内部環境と外部環境の***変化がコンプライアンスリスクに与える影響を***適切に***評価***しているか。	【問題のある事例】 ・Ｂ社のコンプライアンス部門は、各部門からのコンプライアンスリスクの発生報告の受領や、経営会議資料の閲覧を通じて、**形式的に**コンプライアンスリスクの変化を**評価**していた。そのため、実際の***内部環境と外部環境の変化がコンプライアンスリスクに与える影響の評価***が**不十分**となっている。

	【改善提言】 (a)コンプライアンスリスクの評価担当者に、コンプライアンスリスク評価の外部トレーニングを受講させ、㋐**評価スキル**を向上させると共に、㋑**内部環境と外部環境の変化を把握する手法**（他社事例を含む）を習得させる。 (b)上記トレーニングをベースとして、内部環境と外部環境の**変化を把握**する自社に適した手順と、これらの**変化がリスクに及ぼす影響**を評価する枠組みを作成させる。
（３）環境変化評価の頻度 ・*重要な内部環境と外部環境の変化を適時に評価*し、**経営者と取締役会に報告**しているか。	【問題のある事例】 ・Ｃ社はコンプライアンス規程に則り、コンプライアンス部門**がコンプライアンスプログラム**を年度ごとに改定し、**重要な内部環境と外部環境の変化に対する評価**と合わせて、経営者に報告した上で、取締役会に報告している。しかし、**重要な環境変化の評価は、プログラムの年度改定時の１回のみ**である。 【改善提言】 ・半期もしくは四半期ごとに*内外の環境変化の評価*を実施することとし、重要な*環境変化*を認識した場合には都度、*評価*を実施し、経営者と取締役会に報告する体制とする。
（４）新たな戦略の実施によるコンプライアンスリスクへの影響の評価 ・*新たな戦略の実施によるコンプライアンスリスクへの影響を評価*しているか。	【問題のある事例】 ・Ａ社は、傍系である住宅のメンテナンス事業の事業規模を３倍に強化する*新たな戦略を実施*し、これまで内製中心だった**施工を外注中心**に切り替えた。 ・しかし、**外注先の管理が不十分**だったため、電気工事や廃棄物処理で必要な**資格を持たない個人事業主が当該業務を行って**おり、コンプライアンスリスクの顕在化が確認された。 【改善提言】 (a)戦略実施のための事業計画を分析し、*外注施工量の急激な増加（新たな戦略）が*無資格施工などの*コンプライアンスリスクに及ぼす影響を評価*する。 (b)**外注施工量の急激な増加に対応した外注管理体制**が必要な水準まで整備されているか検証する（リスク評価結果に基づく対応策の検証）。 (c)外注先で法令違反などコンプライアンスリスクの有無を把握するために、**外注先の管理状況や外注先での作業実態**について定期的に施工管理部門にヒアリングを行う。

（５）上級職員の交代がコンプライアンスリスクに与える影響の評価 ・*経営者の変更によるカルチャーやリスク許容度の大きな変化*がコンプライアンスリスクに及ぼす影響を**評価**しているか。	【問題のある事例】 ・Ｂ社は*他業種から業界知識のない社長が就任*し、株主に将来の飛躍的な成長を示すために、会社として知見・経験のない海外での新規エネルギー事業への投資案件を実施した。しかし数年後に、海外での法規制が遵守できないこと（＝コンプライアンスリスクの顕在化）が判明して、巨額の損失を計上した。 【改善提言】 (a)*経営者の交代により、会社のカルチャーとリスク許容度に大きな変化*が生じていないか、以下を確認することにより**評価**する。㋐取締役会報告事項、㋑決裁書記載内容、㋒組織戦略の変更や管理職の異動、及び、㋓社外からの中途採用の状況など。 (b)上記評価の結果、コンプライアンスリスクの発生が想定される場合には、内部監査部門長(CAE)が経営者に新規投資案件のコンプライアンス**リスクの評価と対応について説明**し、リスク認識ついての経営者の意見を聞く。 (c)コンプライアンスリスクの許容度が経営者の交代によって影響を受けないように、投資管理規程の例外運用は社外取締役・社外監査役によって構成される**独立した委員会での承認**を要することを定める。

原則１６　リスクとパフォーマンスをレビューする

組織は、事業体のパフォーマンスの結果をレビューし、**リスクを考慮**する。
①レビューを**事業活動に統**合する
②事業体の**能力**を検討する

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）コンプライアンスリスク評価・更新のしくみ ①*コンプライアンスリスクについて評価する仕組み*はあるか。 ②**評価を定期的**に行い、*評価結果を定期的に更新*しているか。	【問題のある事例】 ・コンプライアンスリスクを洗い出し、リスクの発生可能性と顕在化した場合の影響度について評価しまとめたが、年度末に担当者が退職し引継ぎが行われなかったため、**翌年度には*評価が行われず*、前年度の評価結果がそのまま使用された**。 【改善提言】 ・**コンプライアンスリスクは**事業環境の変化等により優先的に対応すべきリスクが変わってくるため、***評価を定期的に更新***する必要がある。
（２）優先順位の高いコンプライアンスリスクへの対応状況の確認 ・優先順位の高いコンプライアンス*リスクへの対応策の実施状況について実績や進捗を確認*し、施策の有効性を定期的にレビューしているか。	【問題のある事例】 ・Ａ社はコンプライアンスリスク評価に基づきリスクマップを作成し、重点対応リスクを定めている。今年度の最優先対応リスクはサイバーセキュリティである。 ・リスク主管部門はリスク対応策として、Web 研修を行うと共に訓練メールを従業員に不定期に送付する計画を策定し実行したが、***研修受講者数や訓練メールでのクリック数の集計*を行っていなかった**。 【改善提言】 ・***リスク対応策に対する実績測定***を行い、施策の有効性を定期的にレビューする必要がある。
（３）コンプライアンスプログラムのレビューと取締役会への報告 ・コンプライアンスプログラムのパフォーマンスと有効性を定期的にレビューし、*取締役会に報告*しているか。	【問題のある事例】 ・Ａ社では CCO（最高コンプライアンス責任者）が、コンプライアンスプログラムのレビュー結果をコンプライアンス委員会に定期的に報告しているが、***取締役会に対する報告***がされていないため、取締役会がコンプライアンスリスクに対する**監督責任**を果たすことができていない。

	【改善提言】 ・CCO 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、***取締役会への直接の報告ラインを確保***することが必要である。
（４）高リスク領域の監査と**モニタリングの計画** ・優先順位の高いコンプライアンスリスクに対する***モニタリング計画***を策定しているか。	【問題のある事例】 ①***モニタリング計画***が策定されていない。 ②モニタリング計画は策定されているが、**実施責任の所在や具体的な実施方法が不明確**であるため、十分に運用されていない。 【改善提言】 ①***モニタリング計画***の策定はコンプライアンス部門が主導する。なお、策定には、㋐リスクオーナー、㋑内部監査部門、㋒リスクマネジメント部門、及び、㋓関係する可能性のある部門が関与する。 ②モニタリング計画には、**実施責任の所在や具体的な実施方法を明確にするため、㋐モニタリングの責任者、㋑有効性の測定方法なども記載**する。
（５）**議論に資するリスクのレビュー結果の報告** ・取締役会に報告されるコンプライアンスリスクのレビュー結果は、取締役会が監督責任を遂行するための***議論に資する内容***となっているか。	【問題のある事例】 ・リスクのレビュー結果は取締役会に報告されているが、**表層的な測定結果を羅列した形式的報告にとどまっており、*議論に資する内容*になっていない**。そのため、コンプライアンスと倫理の機能に対して、**取締役会が監督責任を遂行するための議論が行われていない**。 【改善提言】 ・**議論すべき優先順位の高いコンプライアンスリスクに絞ってわかりやすく論点整理し、リスクの根本原因分析を実施**する等、取締役会での***議論に資する情報***を提供する。

原則１７　全社的リスクマネジメントの改善を追求する

組織は、全社的リスクマネジメントの改善を追求する。
・改善を追求する

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）類似会社のコンプライアンスプログラムの調査・活用 ・コンプライアンス部門は、*類似会社のコンプライアンスプログラム*を**調査**し、自社のコンプライアンスプログラムの改善に活用しているか。	【問題のある事例】 ・自社内の知見、事例のみにもとづいてコンプライアンスプログラムを策定しており、類似会社と比較してコンプライアンスプログラムが未熟である。 【改善提言】 ・類似会社のコンプライアンス部門との情報交換、もしくは、コンプライアンス・コンサルタントの活用を行い、*類似会社のコンプライアンスプログラム*の**情報を収集**し、自社のコンプライアンスプログラムの改善に活用する。
（２）類似会社のコンプライアンスリスク事例やコンプライアンスリスクマネジメント手法の調査 ・内部監査部門は、*類似会社のコンプライアンスリスク事例*や*コンプライアンスリスクマネジメントの手法*を**調査**し、自社のコンプライアンスリスクマネジメントの改善に資する提言を行っているか。	【問題のある事例】 ・内部監査部門の業務は基本的に J-SOX の監査であり、COSO フレームワークに基づいた内部監査はほとんど実施していない。そのため、**自社のコンプライアンスリスクを把握しておらず、コンプライアンスリスクマネジメントの手法も理解していない**。内部監査部門はそれを課題認識しているが、改善の仕方がわからず困っている。 【改善提言】 ・類似会社の内部監査部門との情報交換、もしくは、コンプライアンス・コンサルタントの活用を行い、*類似会社のコンプライアンスリスクの事例*や*コンプライアンスリスクマネジメントの手法*を**情報収集**し、自社での改善に活用にする。
（３）コンプライアンス部門やリスク管理部門など第２ラインのモニタリング機能の改善 ・内部監査部門は、コンプライアンス部門やリスク管理部門など*第２ラインによる、事業部門など第１ラインに対するモニタリングの状況*を**検証**し、不十分な点がある場合には改善を提言しているか。	【問題のある事例】 ・コンプライアンス部門やリスク管理部門など*第２ラインによる、事業部門など第１ラインに対するモニタリング*が**機能しておらず**、内部監査部門が第１ラインを直接モニタリングしている。（第２ラインが機能していない）

	【改善提言】 ・内部監査部門は、コンプライアンス部門やリスク管理部門など***第２ラインに対し、所管するリスクのモニタリング状況***についてヒアリングを行う。**各部門にヒアリング結果をフィードバックし、課題を明確にした上で、自部門のモニタリングの有効性について自己評価してもらい**、モニタリング機能を高めるよう改善提言する。なお、自己評価では、CSA（Control Self Assessment：統制自己評価）の手法を活用することも有効である

構成要素５　情報、伝達および報告

原則１８　情報とテクノロジーを有効活用する

組織は、**全社的リスクマネジメントをサポート**するために、事業体の情報とテクノロジーシステムを有効活用する。

①**関連性のある情報**を利用する
②情報の進展
③データソース
④リスク情報を**分類**する
⑤データを管理する
⑥情報をサポートするためにテクノロジーを利用する
⑦要求の**変化**

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）テクノロジーを活用したコンプライアンス関連情報へのアクセス ・内部監査部門や品質管理部門などのモニタリング部門は、機能不全を発見するために、モニタリング対象部門の**コンプライアンス*関連情報へテクノロジーを活用してアクセス***できるか。	【問題のある事例】 ・モニタリング部門である内部監査部門や品質管理部門は、開発部門の品質評価の実施状況の検証で、同部門が作成した品質評価報告書を査読するのみで、同部門の品質評価の*生データにアクセス*できない。 【改善提言】 ①**開発部門の品質評価*データへのアクセス権***を内部監査部門や品質管理部門が保有し、**常時モニタリング**できるようにする。 ②データの**アクセスログ**を残す。 【留意点】 ・開発部門内でのデータ改竄を防ぐために、データのアクセスログを残し、同部門の品質評価担当者以外のデータへのアクセス状況を、内部監査部門や品質管理部門がリアルタイムで調査できるようにする。

（２）モニタリングおよび監査におけるテクノロジーの活用 ・内部通報制度で報告された被通報者の情報を、*テクノロジーを活用して重要度を初期評価*しているか。	【問題のある事例】 ・*テクノロジーを活用*せず、通報内容の信ぴょう性が確認できないまま、大掛かりな調査を開始している。その結果、限られた監査資源を重要性の低い案件に振り当てている。 【改善提言】 ・マンパワーを要さないPCモニタリングや電子メール評価などの*テクノロジーを活用して初期評価*を行い、重要度の高い案件から調査を行う。 【ポイント】 ・限られた監査資源を有効活用するため、*テクノロジーを活用して重要度を初期評価*し、重要度の高い案件を優先的に調査する。
（３）テクノロジーを活用したコンプライアンス研修の管理 ・コンプライアンス研修で、*テクノロジーを活用した受講状況の管理*が行われているか。	【問題のある事例】 ・オンラインでコンプライアンス研修を実施しているが、*テクノロジーを活用した受講状況の管理*が行われていないため、未受講者を把握できず、受講を促せない。 【改善提言】 ・*テクノロジーを活用した受講状況の管理*を行い、自動的に未受講者に対して受講を促すシステムを整備する。 【ポイント】 ・対面でない場合は、リアルタイムでの受講の把握ができないことから*テクノロジーを活用して受講状況を管理*する必要がある。
（４）テクノロジーを活用したモニタリングの効率性・正確性の検証 ・整備された内部統制のモニタリングシステムが*効率的かつ適切に機能*しているか。	【問題のある事例】 ・職務分離やデータへのアクセス権管理の適切性などの内部統制のモニタリングをテクノロジーを活用して行っているが、人事システムと連携していないため、承認者、監督者、及びアクセス権限者など人の面でのデータ登録を手作業で行っている（非効率）。 ・そのため、承認者等の㋐登録漏れ、㋑異動の反映が遅れる、もしくは、㋒異動が反映されないなどにより権限のない者が承認、監督、もしくはアクセスするケースが発生する（適切性に欠ける）。 【改善提言】 ・人事部と連携して、内部統制のモニタリングシステムを最新の人事データと連携させることにより、承認者、監督者、及びアクセス権者との照合を自動化する（効率化）と共に、登録漏れの防止やタイムリーな更新が確実に行えるようにする（正確性の確保）。

	【ポイント・留意点】 ・テクノロジーを活用して承認者や監督者による**承認や監督が電子的に行われる**場合、以下の３点でそれらの者が**正しく登録**されることが重要になる。 (a)**権限のない承認者による承認を防止**する。 (b)**権限のない監督者による監督を防止**する。 (c)**アクセス権のない者によるアクセス**やデータの改ざん等の不正**を防止**する。

原則１９　リスク情報を伝達する

組織は、**全社的リスクマネジメントをサポート**するために、**コミュニケーション経路を利用**する。
①***ステークホルダー***とのコミュニケーション
②**取締役会**とのコミュニケーション
③コミュニケーションの***方法***

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）**コンプライアンスと業務効率の最適なバランスの確保** ・コンプライアンスプログラムは、***コンプライアンスと現場の業務効率の最適なバランス***を確保し、現場の実態と乖離しないものとなっているか。	【問題のある事例】 ・コンプライアンス部門は、コンプライアンスプログラムを推進する際、**本社業務所管部門と**所管業務に関連するコンプライアンスリスクの管理について**十分な対話を行っていなかった**。そのため、**プログラムの内容が現場の業務実態と乖離**しており、現場の納得感が得られず、**形骸化**し、忘れられていた。 【改善提言】 ・コンプライアンスプログラムを推進する際には、コンプライアンス部門は**本社業務所管部門と**コンプライアンスリスクの管理について、**十分な対話を行い**、***コンプライアンスと業務効率の最適なバランス***を**確保**することによって、現場と乖離しないプログラムを推進する。
（２）**環境変化に伴うリスクの変化への対応** ・コンプライアンスプログラムは、***社内外の環境変化に伴うコンプライアンスリスクの変化に対応***したものとなっているか。	【問題のある事例】 ・コンプライアンス部門は、コンプライアンスプログラムを推進する際、**本社業務所管部門と**所管業務に関連するコンプライアンスリスクの管理について**定期な対話を行っていなかった**。そのため、**プログラムの内容が*社内外の環境変化に伴うコンプライアンスリスクの変化に対応*したものとなっておらず、陳腐化**し、忘れられていた 【改善提言】 ・コンプライアンスプログラムを推進する際には、コンプライアンス部門は**本社業務所管部門と**コンプライアンスリスクの管理について、**定期な対話を行い**、プログラムが***社内外の環境変化に伴うリスクの変化に対応***したものとなっているかを確認する。その上で、***リスクの変化に応じたプログラムの見直し***を行う。

（３）経営者によるコンプライアンス意識向上に向けた継続的な発信 ・経営者は、会議、研修、開示資料、もしくは社内資料など、*さまざまな場面を通して継続的にコンプライアンス意識向上に向けた発信*を行っているか。	【問題のある事例】 ・経営者のコンプライアンス意識向上に向けた発信が年に１度の年頭挨拶に留まっている。その結果、**経営者トップの意思の表明**によるコンプラアインス**意識の醸成**が進んでいない。 【改善提言】 ①内部監査部門は経営者への監査報告の際に、コンプライアンスは会社存在の前提条件であり、その徹底は経営の重要課題であるため、コンプライアンス意識醸成のために、経営者は*さまざまな場面で継続的にコンプライアンス意識向上に向けた発信*を行うことが必要であることを提言する。 ②社員各人が**日頃目にする身近な範囲に経営者から発信されるコンプライアンスに関するメッセージが掲示される職場環境**を構築することをコンプライアンス部門に提言する。 例：㋐イントラネットトップページ、㋑電子看板、㋒デジタルサイネージ(注)、㋓社内メールマガジン、及び、㋔メッセンジャーアプリなど （注）ディスプレイやプロジェクターなどの電子表示媒体を用いて、情報や広告を表示するシステム（デジサネ）。 ・近年のテレワーク推進、フリーアドレス化、及び、ポスター廃止などにより、**デジタル化や職場環境の大きな変化に対応した細やかな周知活動**が望ましい。
（４）戦略決定の際のコンプライアンスリスクの報告受領 ・事業戦略や重要な施策を取締役会で決議する際に、*コンプライアンス担当役員から想定されるコンプライアンスリスクについて報告を受け*、必要な場合には**リスク対応についての論議**を行っているか。	【問題のある事例】 ・取締役会で事業戦略を決議した際に、**戦略の遂行に伴い発生が想定されるコンプライアンスリスクの検討が不十分**であったため、リスク対応策が未策定もしくは不完全であった。そのため、対応策を事前に作成していれば防止できたコンプライアンスリスクが顕在化し、対応が遅れ、損失が拡大した。 【改善提言】 ・取締役会での重要な組織戦略や施策の決議に際しては、*コンプライアンス担当役員から想定されるコンプライアンスリスクについて報告を受ける*ことを取締役役会規則、もしくはその細則に規定する。
（５）コンプライアンス部門と全事業部門との定期的で深度ある双方向のコミュニケーション ・コンプライアンス部門は、*全ての事業部門*と、コンプライアンスリスクマネジメントについて、*定期的に深度ある双方向のコミュニケーション*を実施しているか。	【問題のある事例１】（「全ての事業部門」について） ①コンプライアンス部門は、**主要な特定事業部門**に対してのみ、コンプライアンスプログラムや個別の施策を伝えることに止まっており、**全くコミュニケーションを取っていない事業部門**が存在する。

【改善提言１】
・コンプライアンス部門は、***全ての事業部門とコミュニケーションの機会を設ける***ことで、**全社の重大なコンプライアンスリスクを把握**することができる。
・**一部の事業部門**に対してのみ実施した場合、**除外された事業部門**でのコンプライアンス施策の実施状況やそのモニタリングが不十分になるなど、**全社的なコンプライアンスリスクマネジメントの機能**が損なわれる可能性がある。
・**売上高の大小とコンプライアンスリスクの大小は比例しない場合がある**ことに留意することが必要。例えば大手上場会社において、**傍流の小規模子会社で安全上の重大なコンプライアンス違反**が発生し、社長が辞任した事案がある。
・なお、売上高は少ないが**リスクが高い**と評価された、あるいは重大リスクが発生した事業部門には**コミュニケーションの機会を増や**すことが必要（**リスクアプローチ**の観点から）。

【問題のある事例２】（「定期的」について）
②コンプライアンス部門と事業部門との***コミュニケーションが定期的に実施***されていない。
【改善提言２】
・***不定期なコミュニケーション***では、**一過性な効果に限られ、また、継続的なモニタリングが行えず、コンプライアンスリスクマネジメントの継続的な改善が行えない**可能性がある。そのため、***定期的なコミュニケーション***が必要である。

【問題のある事例３】（「深度ある双方向のコミュニケーション」について）
③(a)コミュニケーションが、コンプライアンス部門からのコンプライアンスプログラムや個別の施策の**資料説明に止まっており**、事業部門との**質疑がなく、実質的な意見交換が行われていない**など***双方向***になっていない。
・(b)また、**事業部門からの報告は、**㋐インシデントや事故件数、㋑研修受講率、及び、㋒セルフチェック実施回数などの**形式的・定例的な報告に限られて**おり、コンプライアンス部門はインシデント件数が少なければよい、受講率が高ければよいとの**形式的な評価に止まって**いる。
・このように、***コミュニケーションの深度***が浅く、**形式的な説明・報告**に止まっている。

	【改善提言３】 ・*深度ある双方向のコミュニケーション*を通して、双方の考えるコンプライアンス上の課題やその対応策について、**対応のための実質的な議論**を行いながら、**リスク認識を共有し、議論を通して実効的かつ効率的な対応策を見出す**ことが必要である。
（６）取締役会でのコンプライアンス関連議題の議論 ・取締役会において、コンプライアンスプログラム等のコンプライアンスに関する重要議題は、***必要な議論がなされた上で決議***されているか。	【問題のある事例】 ・毎年、コンプライアンスプログラムは、取締役会の**書面開催で決議**されている。 【改善提言】 ・コンプライアンスに対するガバナンスの実効性を向上させるため、取締役会において、重要なコンプライアンスに関する議題は**実開催の上、必要な議論を行ったうえで決議**すべきことを**取締役会規則の細則**で規定する。

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

組織は、リスク、カルチャーおよびパフォーマンスを複数の階層に、また、全社にわたって報告する。
①報告の**利用者**とその役割を認識する
②報告の**特質**
③報告の**種類**
④**取締役会**へのリスク報告
⑤**カルチャー**に関する報告
⑥主要な**指標**
⑦報告の**頻度**と**質**

監査での視点・着眼点・質問事項	問題のある事例と改善提言、もしくは改善提言する際のポイント・留意点
（１）**不適切事案の背景となるカルチャーに関する報告** ・コンプライアンスにかかる不適切事象に関する**取締役会への報告**の際に、***原因として考えられるカルチャー***についても報告しているか。	【問題のある事例】 ・社内で発生したコンプライアンスに関する不適切事象を取りまとめ、定期的に**取締役会宛に報告**しているが、その***背景となるカルチャー***に関して報告されていなかった。 ・かかる中、社内で不適切な窃盗事件が複数発生していたが、個人的な犯罪事象として報告され、***職場における個人の非公式なコミュニケーションに否定的なカルチャー***が発見を遅らせた可能性については報告されなかった。 ・そのため、**カルチャーとその改善に対する取締役会の監督**が行き届いていなかった。 【改善提言】 ・不祥事などのコンプライアンス事案についての取締役会への報告に際しては、**㋐カルチャー上の問題点がないか検証すること、及び、㋑カルチャー上の問題点がある場合には当該問題点について報告すること**を、コンプライアンスプログラムやコンプライアンス規程で定める。これにより、**取締役会によるカルチャーとその改善に対する監督**が十分に行える体制とする。

（２）コンプライアンスに関連するカルチャーの現状と変化の定期的な取締役会への報告 ・コンプライアンスに関連する*カルチャーの現状と変化が定期的に取締役会へ報告*されているか。	【問題のある事例】 ・コンプライアンス部門は、毎年従業員へのカルチャーを含むコンプライアンス全般について調査を行っているが、その結果については特に問題がある場合にのみ報告することとしており、**カルチャーについての定期的な報告**は行われていなかった。 ・そのため、特段の問題がない限り、**人事制度や採用方針の変更に伴う**、コンプライアンスに関する*カルチャーの変化*を**取締役会は把握していなかった**。 【改善提言】 ・コンプライアンスに関連する*カルチャーの現状と変化*の**調査結果を、年に一度、取締役会へ報告**するようコンプライアンスプログラム、もしくはコンプライアンス規程で定め、コンプライアンスに関する*カルチャーの現状とその変化*を**取締役会が把握**できるようにする。
（３）各階層の役割・責任やニーズに合わせた報告 ・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、及び、パフォーマンスに関する**報告**は、取締役会、監査役会、及び、事業部門などの*各階層の役割・責任やニーズに合わせてカスタマイズ*され、**各階層が必要とするもの**に焦点を当てているか。	【問題のある事例】 ・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、及び、パフォーマンスに関する報告は、取締役会、監査役会、及び、事業部門などの各階層に対して行われている。しかし、**報告内容が各階層一律の内容となっており、*階層ごとに異なる役割・責任やニーズ*と一致しておらず**、その役割・責任を果たすために必要とするものとなっていない。 【改善提言】 ・**取締役会、監査役会への報告では**例えば、全社のコンプライアンスに対する資源配分の状況や、カルチャーの変化の傾向など、その役割・責任である**コンプライアンス全体を監督するために必要な事項を含める**。 ・他方、**事業部門への報告では**例えば、所管事業のコンプライアンスリスクとその対応状況や、同リスクの管理指標の動向など、事業部門長がその役割・責任である**自部門のコンプライアンスリスクマネジメントを適切に実施するために必要な事項を含める**。
（４）外部委託先で発生するリスクを含めた報告 ・会社にリスクをもたらす可能性のある第三者サプライヤーや販売代理店など*外部委託先で発生するリスク*の状況について経営者や取締役会に**報告**されているか。	【問題のある事例】 ・*部品の仕入れ先が性能検査結果を改ざん*しており、当社が安全基準を満たさない部品を使用していたことが判明した。当該仕入れ先は、所管事業部門の**コンプライアンスリスクマネジメントの評価対象外**だったため、リスクを事前に把握できていなかった。

	【改善提言】 ・事業部門におけるコンプライアンスリスクマネジメントの**報告対象には**、社内だけでなく、***外部委託先***も含める。 ・そのうえで、㋐第三者サプライヤー、㋑販売代理店、及び、㋒外部ベンダーその他の***外部委託先のコンプライアンスリスクマネジメントの状況***を、定期的に評価し、評価結果を経営者や取締役会に**報告する**。
（５）過去に発生したリスク事案関連文書の適正保管 ・***過去に発生したコンプライアンスリスク事案の***調査報告書や重要な関連資料・記録などの***関連文書***は、主要部分が**洩れなく保管され、随時閲覧可能**な状態に維持されているか。また、保管責任部門は明確になっているか。	【問題のある事例】 ・Ａ工場で食品安全基準未達食品の製造事案が判明し、再発防止策を策定、実行したが、***調査報告書や重要な関連資料・記録などの関連文書***が**散逸**しており、**教訓が伝承・共有されておらず、類似事案が**５年後にＢ工場で**再発**した。 【改善提言】 ①***発生したコンプライアンスリスク事案の調査報告書や重要な関連資料・記録などの関連文書***は、**保管責任部門を明確にした上で**、定められた期間、主要部分が**洩れなく保管され、随時閲覧可能**な状態を維持することを**文書保管規則で規定**する。 ・これにより、(a)**教訓が伝承・共有され、類似事案の再発防止**に活用できる。また、(b)過去に発生したコンプライアンス事案の**教訓の風化防止のための教育・研修資料**として活用できる。

４．参考資料：全社的リスクマネジメントと内部統制とのおおよその関係

・全社的リスクマネジメントの20の原則と表面上概ね対応していると見える内部統制の17の原則とのおおよその対応関係は下表の通りです。なお、これは両者の関係の理解の一助として記載したものです。

全社的リスクマネジメント（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　2017年9月公表）		内　部　統　制（ＣＯＳＯ・内部統制の統合的フレームワーク　2013年5月公表）	
構成要素	**原　　則**	**構成要素**	**原　　則**
構成要素１ **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**	構成要素１ **統制環境**	**監督責任の遂行**　（原則２）
	２．業務構造を確立する		**組織構造、権限・責任の確立**　（原則３）
	３．望ましいカルチャーを定義づける		**誠実性と倫理観に対するコミットメントの表明**（原則１）
	４．コアバリューに対するコミットメントを表明する		**説明責任の履行**　（原則５）
	５．有能な人材を惹きつけ，育成し，保持する		**業務遂行能力に対するコミットメントの表明**　（原則４）
構成要素２ **戦略と目標設定**	**６．事業環境を分析する**		※対応すると思われる内部統制の構成要素はない。
	７．リスク選好を定義する		※対応すると思われる内部統制の構成要素はない。
	８．代替戦略を評価する		※対応すると思われる内部統制の構成要素はない。
	９．事業目標を組み立てる		※対応すると思われる内部統制の構成要素はない。
構成要素３ **パフォーマンス**	**１０．リスクを識別する**	構成要素２ **リスク評価**	**適合性のある目的の特定**　（原則６）
	１１．リスクの重大度を評価する		**リスクの識別と分析**　（原則７）
	１２．リスクの優先順位づけをする		**不正リスクの評価**　（原則８）
	１３．リスク対応を実施する		**重大な変化の識別と分析**　（原則９）
	１４．ポートフォリオの視点を策定する		

構成要素3 **統制活動**	**統制活動の選択と整備**　（原則１０）
	テクノロジーに関する全般的統制活動の選択と整備（原則１１）
	方針と手続を通じた展開　（原則１２）

構成要素４ **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

構成要素5 **モニタリング活動**	**日常的評価および／または独立的評価の実施**（原則１６）
	不備の評価と伝達　（原則１７）

構成要素5 **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

構成要素４ **情報と伝達**	**関連性のある情報の利用**（原則１３）
	組織内における情報伝達　（原則１４）
	組織外部との情報伝達　（原則１５）

引用文献

・トレッドウェイ委員会支援組織委員会（COSO:Committee of Sponsoring Organizations of the Treadway Commission）著　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**「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」**（2018年4月同文舘出版）74頁他。

・トレッドウェイ委員会支援組織委員会（COSO:Committee of Sponsoring Organizations of the Treadway Commission）著　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**「内部統制の統合的フレームワーク　フレームワーク篇」**（2014年2月日本公認会計士協会出版局）40～42頁他。

参考文献

・トレッドウェイ委員会支援組織委員会（COSO: Committee of Sponsoring Organizations of the Treadway Commission）著　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新COSO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』　（2018年4月　同文舘出版）

・トレッドウェイ委員会支援組織委員会著　八田進二、橋本尚監訳　堺咲子訳
・『ＣＯＳＯ　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』　（2022 年６月　日本内部監査協会）

以　上