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」～

一般社団法人　日本内部監査協会
ＣＩＡフォーラム№．ａ３　ＥＲＭ研究会（第１０期）
２０１９年１１月３日

「ＣＩＡフォーラム」は、ＣＩＡ資格保持者の研鑽及び相互交流を目的に活動する、一般社団法人日本内部監査協会の組織上の研究会の一つです。各ＣＩＡフォーラム研究会は、担当の座長が責任をもって自主的に運営し、研究期間、目標成果を設定し、研究成果を発信しています。

本報告書は、本研究会（CIA フォーラムａ３　ＥＲＭ研究会）が、その活動成果として取りまとめたものです。本報告書に記載された事例は、すべて本研究会メンバーが会合・合宿等で合議して作成したものであり、研究会メンバーが所属する個別企業の事例ではありません。報告書に記載された意見・コメント・その他の記載も同様に、すべて本研究会としての見解であり、メンバー、およびメンバーが属する組織の見解ではありません。また、協会の見解を代表するものではありません。

目　次

１．はじめに

（１）改訂版ＣＯＳＯ・全社的リスクマネジメントの特徴

・周知の通りＣＯＳＯ（トレッドウェイ委員会支援組織委員会）は2017年9月、13年ぶりに『全社的リスクマネジメント　－統合的フレームワーク』を全面改訂した『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』を公表し、2018年4月にはその邦訳が公表されています(注)。

（注）さらに2018年1月には、改訂版ＣＯＳＯ・全社的リスクマネジメントの『事例の解説篇』が公表され、2018年12月にはその邦訳が公表されています。

・改訂版フレームワークの最大の特徴は、内部統制など他のＣＯＳＯのフレームワークと同様に、全社的リスクマネジメントの**５つの構成要素に関連する基本的な概念である20の原則**を提示したことです。**20の原則は事業体の全社的リスクマネジメント（ＥＲＭ：Enterprise Risk Management）の実務として行われると考えられる事項を記載したもの**であり、**内部監査で全社的リスクマネジメントの有効性評価を行う際の視点として活用できるもの**です。

・従来、内部監査での全社的リスクマネジメントの有効性評価には、主観的な判断に陥りやすい側面がありましたが、20の原則を参照することにより、より客観的に行うことができ、20の原則は内部監査の品質を向上させるための有力なツールとしての活用が期待されます。

（２）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（参考）

・**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）
	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。

構成要素２ **戦略と目標設定**	**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**	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）
	１６．リスクとパフォーマンスをレビューする		**不備の評価と伝達**　（原則１７）
	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 **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**	構成要素４ **情報と伝達**	**関連性のある情報の利用**（原則１３）
	１９．リスク情報を伝達する		**組織内における情報伝達**　（原則１４）
	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組織委員会（COSO:Committee of Sponsoring Organizations of 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組織委員会（COSO:Committee of Sponsoring Organizations of 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。

（３）本報告書の目的と特徴

①本報告書の目的は、改訂版ＣＯＳＯ・全社的リスクマネジメントで示された 20 の原則を内部監査に活用するための手法を提示することです。そのため、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 73 の事項および、それに対する課題と改善提言を例示しました。また、必要に応じて関連する 61 の「具体例」を記載しました。

改訂版ＣＯＳＯ・全社的リスクマネジメントで提示された 20 の原則は、全社的リスクマネジメントの設計、適用および運用、ならびに全社的リスクマネジメントの有効性評価という幅広い目的で作成されているため、概念的な記載が多く、内部監査に直接活用しにくい面があります。そのため、本報告書では 20 の原則を内部監査で活用するという観点から事例中心で作成しました。

②各事例には「見出し」を付けてあります。合計 73 個の「見出し」は「質問・確認事項」、および「課題・改善提言」の内容を反映しており、全社的リスクマネジメントを監査する際の着眼点を検討する参考となるようにしています。「見出し」は「質問・確認事項」、および「課題・改善提言」の３つを読むことにより、20 の原則を全社的リスクマネジメントの内部監査に活用する方法をイメージできるように作成しました。

③「本報告書の全体像（「見出し」・「具体例」一覧）」に「見出し」と「具体例」を一覧表形式でまとめましたので、それを読めば、比較的短時間で 20 の原則の内部監査での活用方法のおおよそのイメージが把握できるようになっています。

④全体を通して、20 の原則を事例に即して理解できるように努めました。また、監査対象部門の内部統制を含めた全社的リスクマネジメントを評価し、改善提言するという内部監査の実務に活用できるように努めました。

（４）使用上の注意

①本報告書は、改訂版ＣＯＳＯ―ＥＲＭで示された 20 の原則に従い、ＥＲＭの観点から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、20 の原則の解説を目的としたものではありません。

②各原則についての記載内容はあくまでも一例であり、それ以外にも多くの質問・確認事項や課題・改善提言があることにご留意願います。

③本報告書に記載した事項のすべてを満たす必要はなく、自社で活用できる項目から活用し、自社の現在のリスクマネジメントやＥＲＭ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 10 期）

（2019 年 10 月 13 日時点）

No.	氏名	会社名等	所属・役職
1	吉野 太郎 （座長）	東京ガス（株）	リビング企画部ライフパル監査役チーム
2	野口 正文 （副座長）	損害保険ジャパン日本興亜（株）	監査役室・主査
3	藤枝 繁	みずほ情報総研（株）	業務監査部・参事役
4	坂井 香苗	NEC マネジメントパートナー（株）	リスクアドバイザリー事業部・監査シニアエキスパート
5	紀谷 倫有	個人会員	
6	宮内 隆行	住友化学（株）	内部統制・監査部・主席部員
7	村井 直樹	個人会員	コンサルタント
8	真柳 元	個人会員	
9	丹羽 珠希	三井住友 DS アセットマネジメント（株）	内部監査部・シニアマネージャー
10	有村 祥一	（株）日本政策投資銀行	監査部・参事　内部監査担当
11	小堀 真	大和証券（株）兼（株）大和証券グループ本社	内部監査部・次長
12	伊藤 裕美子	ＮＥＣネッツエスアイ（株）	経営監査部・担当課長
13	宇田 文顕	ＳＣＳＫ（株）	部門統括部・課長
14	大島 誠	第一屋製パン(株)	常勤監査役
15	石井 学	Supership ホールディングス（株）	内部統制推進室
16	和田 有弘	出光興産（株）	内部監査室・室長付
17	鈴木 均	オリンパス（株）	内部統制　ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑﾃﾞﾍﾞﾛｯﾌﾟﾒﾝﾄｻﾎﾟｰﾄ ｸﾞﾛｰﾊﾞﾙ
18	髙橋 和弘	曙ブレーキ工業(株)	企業年金基金・健康保険組合・常務理事
19	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
20	佐藤 伸吾	のむら産業（株）	内部監査室・室長
21	小林 竹幸	第一生命保険（株）	内部監査部・上席内部監査員
22	桐山 勝	(株)クレハ	常勤社外監査役
23	新藤 和政	三井物産(株)	内部監査部企画業務室・次長
24	村上 裕子	明治安田ライフプランセンター(株)	内部監査部・執行役員内部監査部長
25	野々山 一郎	日本郵船(株)	グループ経営推進グループ・部長代理

（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、10 期 15 年にわたり、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（当期） 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方法** ～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。

（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。（研究・活動　CIA フォーラム）

第１０期報告書　　:「研究・活動：ＣＩＡフォーラム」→「活動実績」→ａ３

第１期～９期報告書　　:「研究・活動：ＣＩＡフォーラム」→「活動実績」→「過去の活動実績」→ａ３（第９期）、研究会 No.15（第１期～第８期）　（http://www.iiajapan.com/kenkyu/forum/report_past.html）

２．本報告書の全体像（「見出し」・「具体例」一覧）

※「見出し」の数：73 項目　　「具体例」の数 61 個

構成要素	原　則	見出し・具体例
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）全社的リスクマネジメントに対する役割・責任の明確化
		（２）取締役会がリスク監視責任を遂行できる体制の整備 *【具体例】全社リスクマネジメント委員会によるリスク監視*
		（３）取締役会と経営者との対話の促進 *【具体例】経営会議情報の社外取締役への提供・共有*
	原則２ 業務構造を確立する	（１）全社的リスクマネジメントが戦略と事業目標を達成できる業務構造の確立
		（２）業務構造に応じた報告経路の設定
		（３）権限と責任の明確化 *【具体例】職務分掌規程および決裁権限規程等の整備*
		（４）事業体の進化に応じた全社的リスクマネジメントの見直し *【具体例】全社的リスクマネジメントの見直し*
	原則３ 望ましいカルチャーを定義づける	（１）望ましいカルチャーの定義 *【具体例１】望ましい行動（行動基準）の再定義* *【具体例２】タスクフォースを活用した全社共通のミッション・ビジョン・コアバリューの明確化* *【具体例３】各部署単位でのミッション・ビジョン・コアバリューの明確化とカルチャーの定義づけ* *【具体例４】カルチャーを伝える社長メッセージの掲載*
		（２）望ましいカルチャーを形成するプロセスの整備 *【具体例】リスクアペタイトをベースとした全社リスクマネジメントの運用体制*
		（３）コアバリューを意思決定・行動と結びつける *【具体例１】SDGs（持続可能な開発目標）に基づく事業転換* *【具体例２】誠実性をコアバリューとして全社に浸透*
		（４）望ましいカルチャーの醸成とリスクテイク哲学との整合 *【具体例】マテリアリティ基準（持続的成長を遂げるための重要な経営課題）での新規事業の投資判断*
		（５）望ましいカルチャーの浸透 *【具体例】経営者自らによる望ましいカルチャーの浸透*
	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）コアバリューを含めたコミットメントの表明 *【具体例】経営者によるコミットメントの表明*
		（２）コアバリューに基づいた行動基準の策定
		（３）経営者のコアバリューに対するコミットメントの表明と周知徹底 *【具体例】コアバリューに対するコミットメントの周知徹底*
		（４）コアバリューを認識した行動基準の遵守
		（５）事業体全体のコアバリューの明確化と伝達 *【具体例】コアバリューの取締役会決議*
		（６）説明責任の明文化を通したリスクを認知するカルチャーの醸成

		（７）報酬・インセンティブとコアバリューとの整合性の確保 *【具体例】期待される行動の評価への反映*
		（８）コアバリューや望ましい行動からの逸脱への対応 *【具体例】不適正事象判明時の社内周知*
		（９）行動基準の逸脱に対する適切な相談窓口の設置 *【具体例】行動基準の逸脱に対する相談窓口の設置*
	原則５ 有能な人材を惹きつけ、育成し、保持する	（１）採用時の望ましい行動・業務スタイル等の明確化と候補者との共有 *【具体例】採用時の望ましい行動・業務スタイル等の明確化と候補者との共有*
		（２）行動基準遵守状況の評価 *【具体例】顧客本位への取組み状況の評価*
		（３）行動基準遵守状況のモニタリング *【具体例】顧客本位の徹底とそのモニタリング*
		（４）必要な人材の定義と評価
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）事業環境変化の監視 *【具体例】事業環境変化の把握・確認*
		（２）事業環境変化の社内伝達と分析 *【具体例】事業環境変化の企画部門への報告と同部門による評価*
		（３）事業環境変化を検討した上での意思決定 *【具体例】事業環境変化を踏まえた意思決定*
	原則７ リスク選好を定義する	（１）リスク選好の策定 *【具体例】リスク選好方針によるリスク選好の明示*
		（２）リスク選好の取締役会承認 *【具体例】リスク選好の取締役会承認*
		（３）リスク選好の事業体全体への伝達 *【具体例】リスク選好の伝達・周知*
		（４）リスク選好に基づいた資源配分 *【具体例】リスク選好の資源配分への活用*
	原則８ 代替戦略を評価する	（１）ミッション・ビジョン・コアバリューおよびリスク選好と整合した戦略の策定 *【具体例】ミッション・ビジョン・コアバリューおよびリスク選好に適合する新キャンパスへの移転*
		（２）リスクの識別とリスクが及ぼす影響の評価 *【具体例】識別したリスクとその影響の評価に基づく最適な教務体制の構築*
		（３）戦略がリスク選好に適合していることの確認
		（４）戦略のモニタリングと変更
	原則９ 事業目標を組み立てる	（１）事業目標の適切な設定
		（２）事業目標の各階層への落とし込み
		（３）測定可能なパフォーマンス指標と適切なターゲットの設定 *【具体例１】働き方改革に対応した労働時間の測定* *【具体例２】不適切な利益評価指標の改善*

		（４）パフォーマンスの許容度の設定とモニタリング *【具体例】法令順守や健康管理に対応した労働時間の測定*
構成要素３ パフォーマンス	原則１０ リスクを識別する	（１）新しいリスク・エマージングリスク・変化する既存のリスクの識別 *【具体例】経営者によるリスク識別の取り組み*
		（２）リスク識別プロセスの統一・明確化 *【具体例】ボトムアップおよびトップダウンアプローチによるリスク評価*
		（３）リスク一覧表の作成によるリスクの可視化
	原則１１ リスクの重大度を評価する	（１）リスクを評価する時間軸の明確化と統一 *【具体例】リスク評価の時間軸と戦略および事業目標の時間軸との整合性確保*
		（２）事業内容の変化に応じたリスク測定基準の見直し
		（３）最適なリスク評価のアプローチの選択 *【具体例】定量的アプローチと定性的アプローチを組合せたリスク評価*
	原則１２ リスクの優先順位付けをする	（１）リスクの優先順位付けを行う規準の設定 *【具体例】優先的に対応すべきリスクと優先順位付けの規準の周知*
		（２）リスクの優先順位付けの実施 *【具体例】全社および各部門でのリスクの優先順位付けの実施*
		（３）リスク選好に沿ったリスクの優先順位付け *【具体例】リスク選好に基づいたリスクの優先順位付けと資源配分*
	原則１３ リスク対応を実施する	（１）所定のプロセス（検討事項・評価項目・決裁レベル）に則ったリスク対応の選択 *【具体例１】リスク対応における「共有（移転）」の決定* *【具体例２】リスク対応における「活用」の決定*
		（２）リスク対応の費用対効果の検証と戦略および事業目標の変更
	原則１４ ポートフォリオの視点を策定する	（１）リスク・リターンの相関関係をポートフォリオの視点から検討する *【具体例】部門間の相反するリスク・リターンの相関関係を踏まえた投資判断*
		（２）より高次の次元からリスクテイクの判断を行う *【具体例】経営者による高次の視点からのリスクテイク*
		（３）定量評価も含めてリスクのポートフォリオ分析を行う *【具体例】定量的な基準に基づく判断*
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）傍流部門を含めた網羅的な事業環境変化のモニタリング *【具体例】ネット通販への需要拡大の把握とそれに対応した投資シフト*
		（２）外部環境の変化を評価できる人材の確保 *【具体例】サイバーセキュリティをモニタリングする専門人材の配置*
		（３）カルチャー変化による影響のモニタリング *【具体例】カルチャーの変化が買収先企業の定着率に及ぼす影響のモニタリング*
	原則１６ リスクとパフォーマンスをレビューする	（１）パフォーマンスをレビューする際に未達成項目を十分分析する *【具体例１】中期経営計画の業績の振り返りと修正* *【具体例２】買収事業の成果の振り返りと翌期の事業計画への反映*
		（２）パフォーマンス目標の修正

		（３）パフォーマンスの継続的モニタリング *【具体例１】重要リスクのモニタリング結果のパフォーマンスターゲット設定への活用* *【具体例２】財務パフォーマンスの継続的モニタリング*
	原則１７ 全社的リスクマネジメントの改善を追求する	（１）経営者による日常的モニタリング活動の結果のレビュー
		（２）中長期的な視点での全社的リスクマネジメントの改善
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）意思決定に有用な情報の収集と活用 *【具体例】情報の有効活用を通じた競争優位の構築*
		（２）新たなテクノロジーの導入に伴うリスクの検討 *【具体例】リスクの検討を踏まえた効果的なシステムの構築*
		（３）事業環境の変化に対応した情報システムの変更 *【具体例】事業環境の変化に対応した情報システムの変更*
	原則１９ リスク情報を伝達する	（１）リスク情報伝達の責任部門と適切な伝達経路を設定する *【具体例】全社リスクマネジメント統括部門への情報伝達管理責任の付与*
		（２）受け手のリスク対応に役立つ情報を伝達する *【具体例】全社リスクマネジメント統括部門による情報モニタリング*
		（３）情報が必要な階層に伝達されていることを検証する *【具体例】企業理念と行動基準の理解の定期的な検証*
		（４）社外に発信する各種情報の整合性を確保する *【具体例】各部門の社外発信情報はリスクマネジメント統括部門と協議*
		（５）経営者の意図に沿わない情報の社外発信を防止する *【具体例】経営レベル情報の社外発信時におけるリスクマネジメント統括部門による調整*
	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）取締役会への報告を戦略・事業目標・リスク・パフォーマンスに関連付ける
		（２）報告の利用者とその役割を認識する *【具体例】報告の利用者に応じた情報提供の仕組みの構築*
		（３）利用者のニーズに合った報告の内容と時期

（注）構成要素と原則は、トレッドウェイ委員会組織委員会（COSO:Committee of Sponsoring Organizations of 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 頁他から引用。

３．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」

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

質問・確認事項	課題・改善提言 （注）“⇒”は改善提言を示す（以下同じ）
（１）全社的リスクマネジメントに対する役割・責任の明確化 ①取締役会および経営者それぞれのリスク監視に対する役割や責任を定めた規程が整備されているか。	①「取締役会規程」、「経営会議規程」（以下、規程等）が作成されていないため、取締役会および経営者のリスク監視に対する役割や責任が決まっていない。
②規程等がある場合それには、㋐取締役会の監督（リスク監視を含む）責任、㋑取締役の選任要件、㋒取締役の適格性、㋓取締役会の独立性および客観性の評価、㋔その他リスク監視に必要な事項について明記されているか。	②規程等はあるが、リスク監視に必要な事項についての記載がない、または内容が曖昧なため、リスク監視に対する役割や責任が明確になっていない。
③「取締役会規程」、「経営会議規程」は、定期的に見直しがされ、常に最新のものとなっているか。	③規程等の定期的見直しがされていないため、その内容が陳腐化しており、実態に合わないところがある。 ⇒「取締役会規程」、「経営会議規程」における取締役会と経営者のリスク監視に対する役割・責任の明確化とそれらの定期的な見直しを実施する。（①～③共通）
（２）取締役会がリスク監視責任を遂行できる体制の整備 ①取締役会によるリスク監視体制はどのように構築されているか。	①～③リスク監視に必要な体制、プロセスならびにオペレーションが構築されていないため、実態として取締役会によるリスク監視が適切に行われていない。

②経営者によるリスクとコントロールに対するモニタリング、および経営者から取締役会への報告体制はどのように構築されているか。 ③取締役会および経営者は、その運用状況と有効性を定期的に評価しているか。 ④取締役会が意思決定をする上で必要な情報は共有されているか。 ⑤モニタリングの評価結果についての取締役会の経営者への指示や助言は適切に行われているか。 ⑥取締役会を支える体制、たとえば、取締役会や監査委員会事務局の体制（要員、スキル等）に不備はないか。	④～⑤必要な情報がタイムリーに報告されない、客観的な裏付けとなる資料が不十分などの理由から、取締役会での議論が十分にされず、意思決定が適切に行われていない。 ⑥取締役会や監査委員会事務局の要員、スキルが不足しているため、支援体制が十分でない。 ⇒経営者による㋐リスクのモニタリングおよび報告体制の構築、㋑モニタリング結果の取締役会への定期報告の実施、および、㋒スタッフの支援体制を拡充する。（①～⑥共通） **【具体例】全社リスクマネジメント委員会によるリスク監視** ・A社では、取締役会から委任を受けた全社リスクマネジメント委員会が、経営者から重要リスクに対するコントロールの進捗状況や有効性の評価などについて報告を受け、取締役会はその内容を確認または審議し、是正または改善すべき事項があれば必要な指示や助言を行っている。
（3）取締役会と経営者との対話の促進 ①取締役会は経営者との間で、㋐会社のミッション・ビジョン・コアバリュー、㋑戦略と事業目標ならびに、㋒会社が有するリスクに関する管理体制、㋓その他戦略や事業目標達成上の重要情報の共有を行っているか。 ②対話は定期的に行われているか。対話は取締役会の意思決定に役に立っているか。	①～②会社のミッション・ビジョン・コアバリューなど会社の統制環境や企業風土、カルチャーに影響する情報の共有がないため、取締役会と経営者の間で価値観の共有のための対話が行われていない、または形骸化している。 ⇒リスク情報のみならず、取締役会の意思決定に有益な情報を共有する場（例：社外取締役への事前説明会や取締役の懇談会）の開催、経営者と社外取締役との個別面談を実施する。

	【具体例】経営会議情報の社外取締役への提供・共有. ・Ｂ社では、取締役会に先立つ社外取締役への事前説明会において、議案に関連する経営会議の議論の内容や決定事項が共有されている。 ・また、経営会議の議事録や関連資料は、各取締役が必要な時に自由に閲覧できる環境が構築されている。その上で、経営者と取締役会が自由闊達な意見交換を行っている。

原則２　業務構造を確立する

質問・確認事項	課題・改善提言
（１）全社的リスクマネジメントが戦略と事業目標を達成できる業務構造の確立 ・全社的リスクマネジメントが戦略と事業目標を達成できるように、業務構造が、法的な枠組みや経営の枠組みとの関連で適切に確立されているか。	・業務構造を通して戦略と事業目標に関するリスクの管理が十分出来ていないため、戦略と事業目標を達成できない。 ⇒戦略と事業目標に関するリスクの管理が十分に行われ、それらの達成が図られるように、事業構造を法的な枠組みや経営の枠組みに適合したものに見直すことを経営者に具申する。
（２）業務構造に応じた報告経路の設定 ・分散した業務構造か統合した業務構造かなど、確立された業務構造に応じ、責任を明確に定めた報告経路が適切に設定されているか。	・事業体の戦略と事業目標を達成するために分散した業務構造を確立した。報告経路の責任は明確に設定されているものの、報告経路が分散した業務構造に適した形で設定されていないため、リスクの全体像等を把握するのに十分な報告が経営者に上げられていない。 ⇒分散した業務構造の場合、統合した業務構造に比べ、リスク把握のチャネルをしっかりと固める必要があるため、それに適した報告経路に設定し直すことを経営者に具申する。
（３）権限と責任の明確化 ・戦略と事業目標が達成されるように、事業体全体や事業体内のそれぞれの階層における各業務単位について、役割や権限と責任が明確に定められているか。	・事業体の各階層で役割や権限と責任が明確に定められていないため、戦略と業務目標の達成が難しい。 ⇒戦略と事業目標が達成されるように、事業体の各階層で役割や権限と責任が、規程・手続等により明確に定めることを、取締役会や経営者に具申する。 **【具体例】職務分掌規程および決裁権限規程等の整備** ・Ａ社においては、戦略と事業目標が達成されるように、役割やその役割に応じた権限と責任が、職務分掌規程および決裁権限規程等において明確に定められており、毎年取締役会による規程見直しと経営者による最新の規程内容の周知徹底が実施されている。

（４）事業体の進化に応じた全社的リスクマネジメントの見直し ・事業体の事業の性格や戦略は進化し、業務構造も変化するが、それらの動きに即して、全社的リスクマネジメントが、事業体の能力を勘案のうえ、継続的に見直されているか。	・事業体が進化し、業務構造も変化しているにもかかわらず、それに即した全社的リスクマネジメントの見直しが行われていないため、経営者が戦略と事業目標の遂行に伴うリスクを適切に把握できていない。 ⇒事業体の進化に即して、全社的リスクマネジメントが見直され、経営者がリスクを適切に把握できるように全社的リスクマネジメントの見直しを行う体制の整備を取締役会や経営者に具申する。 **【具体例】全社的リスクマネジメントの見直し** ・Ｂ社においては、内外の経営環境の変化や戦略の進化等に即して、リスク管理委員会および内部監査委員会の審議のうえ、毎年取締役会による全社的リスクマネジメントの見直しと経営者による最新の内容等の周知徹底が実施されている。

原則３　望ましいカルチャーを定義づける

質問・確認事項	課題・改善提言
（１）望ましいカルチャーの定義 ①組織が戦略と事業目標を達成するため、**事業体全体およびあらゆる従業員が尊重し、適時適切に行動するカルチャーを醸成するための望ましい行動を定義**しているか。	①当社の行動基準は、主にコンプライアンスの観点から行為規制を中心に策定されている。**ミッション、ビジョン、コアバリューを踏まえた望ましいカルチャーが定義されていない**ため、**従業員が適時適切に行動するカルチャーを醸成し望ましい行動に結びつけられる行動基準**になっていない。 ⇒㋐**望ましいカルチャー**を取締役会での審議を経て定義すること、㋑行動基準を組織の**意思決定と行動が望ましいカルチャーに基づき行われることを促す内容**に見直すこと、および㋒行動基準の作成においては、わかりやすさに配慮して**トップからのメッセージやキーワードの解説**などを盛り込むことを提言する。
②定義した望ましい行動は**適切な頻度で見直し**が行われているか。	②行動基準は制定以降一度も見直されていないため、陳腐化している。 ⇒行動基準の**定期的な見直しを実施する枠組み**の導入を提言する。 **【具体例１】望ましい行動（行動基準）の再定義** ・Ａ社では、不適切行為の発覚に伴い実施した根本原因分析のなかでカルチャー（組織文化・風土）の課題を認識し、課題を踏まえて 10 年ぶりに**企業理念、行動基準などの見直し**を行い**望ましい行動の再定義**を行った。
③組織が戦略と事業目標を達成する際に、事業機会を捕捉し、リスクを最小化するために、**各人が適時適切に行動するカルチャーを醸成**しているか。	③組織の**ミッション・ビジョン・コアバリューが明確になっていない**ため、それらを反映したカルチャーが醸成されておらず、ポジティブ・ネガティブ両面の**リスクに対する姿勢、行動、およびリスクの理解**ができない。 ⇒全社横断型のタスクフォースを設置して、全社共通の**ミッション・ビジョン・コアバリューを明確化**し、その上で**望ましいカルチャーを定義づける**ことを経営者に具申する。 **【具体例２】タスクフォースを活用した全社共通のミッション・ビジョン・コアバリューの明確化**

④経営者はこの望ましいカルチャーを定義づけているか。	・Ｂ社では、経営企画部が中心となって全社横断型のタスクフォースを設置、全社共通のミッション・ビジョン・コアバリューを起案し、経営会議での審議を経て、取締役会で決議した。 **【具体例３】各部署単位でのミッション・ビジョン・コアバリューの明確化とカルチャーの定義づけ** ・Ｃ社では、不正事案発生の再発防止策として、各営業部署単位でワークショップを開催し、全社共通のミッション・ビジョン・コアバリューを元に、各部署の事業の特性に沿ったミッション・ビジョン・コアバリューを明確化し、それに基づいて各部署のカルチャーを定義づけた。 ④経営者は望ましいカルチャーを定義づけていないため、各人が認識する組織のカルチャーが複数ある。 ⇒望ましいカルチャーを定義づけし、会社全体に周知することを経営者へ具申する。 **【具体例４】カルチャーを伝える社長メッセージの掲載** ・Ｄ社では、カルチャーを伝える社長メッセージを、毎年新年度を迎えるにあたりイントラネットと社内広報誌に掲載している。

（２）望ましいカルチャーを形成するプロセスの整備 ①カルチャーと望ましい行動は、組織体内のどのような会議体で議論され、どのようなプロセスを経て合意されているか。 ②そのプロセスおよび**責任・権限**は、明確に定められているか。	①～②取ろうとする行動と、自社の望ましいカルチャーを反映したリスクテイク姿勢（リスク選好）との整合性を踏まえた議論を行う公式な会議体がなく、検討プロセスや責任・権限も規定されていないため、組織内部の変化や外部からの影響、従業員へのインタビューやアンケート結果など、組織の実態を踏まえた議論を経て合意されるプロセスとなっていない。 ⇒望ましい行動がリスク選好や事業体の実態を踏まえ、適切に検討・定義される枠組みの整備を提言する。 **【具体例】リスクアペタイトをベースとした全社的リスクマネジメントの運用体制** ・Ｅ社では、社外取締役を委員長とした全社リスクマネジメント委員会を設置し、戦略と事業目標を達成するため、リスクカルチャーに立脚したリスクアペタイト（進んで引き受けようとするリスクの種類と量）を審議している。 ・また、行動基準（コアバリュー）との一貫性を確保しながらリスクアペタイトを明示･説明する文書を社内に配布・周知し浸透を図っている。
（３）コアバリューを行動・意思決定と結びつける ・戦略と事業目標の達成のために、組織の行動と意思決定がそのコアバリューと結びついているか。	・組織の行動と意思決定がそのコアバリューと結びついてないため、戦略と事業目的が達成できない。 ⇒コアバリューと結びついた組織の行動と意思決定を実現するために、新規投資案件を取締役会や経営会議で審議する際に、案件がコアバリューと結びついているか検討することを経営者へ具申する。 **【具体例１】ＳＤＧｓ（持続可能な開発目標）に基づく事業転換** ・Ｆ社では、ＳＤＧｓをコアバリューと掲げ、火力発電事業を順次売却し、太陽光発電事業へと事業の軸足を移した。 **【具体例２】誠実性をコアバリューとして全社に浸透** ・Ｇ社では、社会規範に則り、自社に対する社会の期待に応える誠実な企業行動を浸透させるために、誠実性をコアバリューとし、全営業部署・食堂にポスターを掲示するとともに、弁護士を講師としたセミナーなどを通じて全社への浸透を進めている。

（４）望ましいカルチャーの醸成とリスクテイク哲学との整合 ・取締役会と経営者は、リスクテイク哲学に整合したカルチャーを醸成しているか。	・リスクテイク哲学に整合したカルチャーを醸成しておらず、リスクマネジメントに対する望ましいアプローチを推進できない。 ⇒リスクテイク哲学に適合したカルチャーの醸成を、取締役会や経営者へ具申する。 **【具体例】マテリアリティ（持続的成長を遂げるための重要な経営課題）基準での新規事業の投資判断** ・H社では、望ましいカルチャーの醸成の一環としてマテリアリティ基準を経営会議で討議し、取締役会での決議を経て社外へ開示した。 ・このマテリアリティ基準に基づき、翌期の事業計画を制定し、新規事業案件の優先投資順位を判断している。
（５）望ましいカルチャーの浸透 ①経営者は、望ましいカルチャーに基づく行動について組織全体にどのように伝えているか。	①経営者が自らの姿勢や言葉を社内に直接伝える機会がなく、従業員の直接の上司となるミドルマネジメントも望ましいカルチャーを正しく理解していないため、部下への伝達が不十分となっている。また、浸透のための研修内容・ツールが画一的であり、職位階層別に設計されていないため、組織全体への浸透が不十分となっている。 ⇒浸透の実効性向上のため、タウンホールミーティング(注)や社内イントラネットでの発信など経営者が自ら伝える機会（Tone from the Top）やミドルマネジメントへの教育の新設など階層に応じた研修の充実を提言する。 （注）経営者と、現場の従業員とが一堂に会して、直接対話できるような形で進められるミーティング。対話集会ともいう。
②その浸透状況について、どのようにモニタリングが行われており、取締役会にどのような頻度で報告が行われ、実効的な審議が行われているか。	②望ましい行動の浸透に関する取締役会への報告の頻度が決まっておらず、判断や意思決定をするうえで必要な情報の内容も曖昧で、具体的でないため、実効的な審議が行われていない。 ⇒望ましいカルチャーの浸透状況に対する経営者によるモニタリングの実効性向上のため、報告事項の具体化など体制の整備を行い、取締役会への定期報告を提言する。

	【具体例】経営者自らによる望ましいカルチャーの浸透 ・Ｉ社では、望ましいカルチャーに基づく行動基準について、経営者自らが現場に足を運び従業員との対話集会を開催したり、社内報やイントラネットで発信するなど、経営者自らが伝える機会を定期的に設け、継続的に実施している。

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

質問・確認事項	課題・改善提言
（１）コアバリューを含めたコミットメントの表明 ①事業体は戦略と事業目標の達成のためのコミットメントを表明しているか。	①事業体として戦略と事業目標の達成のためのコミットメントが表明されていないため、戦略と事業目標の達成を目指す事業体の気風が醸成されない。 ⇒戦略と事業目標の達成のためのコミットメントを表明するように提言する。
②コミットメントには、コアバリューとして物事の善悪や許容の有無をどのように含んでいるか。	②コミットメントにコアバリューとして物事の善悪や許容の有無を含んでいないため、事業体の行動基準が十分に機能せず、リスクの認知ができずに意思決定される恐れがある。 ⇒コアバリューとして物事の善悪や許容の有無を含むコミットメントを表明するように提言する。 **【具体例】経営者によるコミットメントの表明** ・Ａ社では、経営者が戦略と事業目標を達成するために、コアバリューに沿った事業運営を行うというコミットメントをホームページで表明し、ステークホルダーにも明確にしている。
（２）コアバリューに基づいた行動基準の策定 ①事業体の行動基準がコアバリューに基づいて策定されているか。	①事業体の行動基準がコアバリューに基づいて策定されていないため、リスクの認知と意思決定が効率的に行えず、事業体の戦略と事業目標が達成されない。 ⇒行動基準をコアバリューに基づくものとすることを提言する。
②それらの行動基準は首尾一貫してコアバリューに基づいているか。	②事業体のコアバリューと行動基準が首尾一貫していないため、従業員やステークホルダーと望ましい行動について共通の理解が得られず、戦略や事業目標の達成に支障を来たす。 ⇒行動基準をコアバリューと首尾一貫したものとすることを提言する。
（３）経営者のコアバリューに対するコミットメントの表明と周知徹底	

①事業体のコアバリューは経営者によってコミットメントが表明されているか。 ②また、それらは事業体の各階層に周知徹底がされているか。 ③どのような方法で周知徹底を図っているか。 （㋐従業員への説明、㋑ホームページへの掲載、㋒カードなどで周知徹底されているか。）	①経営者によるコアバリューに対するコミットメントの表明がないため、事業体の行動基準がステークホルダーと共有できず、戦略と事業目標の効率的な達成ができない。 ⇒経営者がコアバリューに対するコミットメントを表明するように提言する。 ②経営者によるコミットメントの表明が事業体の各階層に周知徹底がされていないため、表明したコミットメントに沿った行動が十分実施されず、戦略と事業目標の達成に齟齬をきたす。 ⇒経営者が表明したコミットメントが事業体の各階層に周知徹底させるよう提言する。 ③コミットメントの表明方法が不十分のため周知徹底が図られていない。 ⇒経営者によるコミットメントの表明を、㋐従業員への説明会の開催、㋑ホームページへの掲載、㋒解説書やカードなどの作製・配布などを通して行うように提言する。 **【具体例】コアバリューに対するコミットメントの周知徹底** ・Ｂ社ではコミットメントの表明を、㋐ホームページへの掲載だけでなく、㋑説明会の開催、㋒解説書の配布および、㋓常時携帯できるコアバリューをまとめたポケットカードの配布を通して行っている。
（４）コアバリューを認識した行動基準の遵守 ①事業体の各階層においてコアバリューが認識され、行動基準からの逸脱が防止されているか。 ②ルールが明確化されていない場合を含めたコンダクトリスクに対するマネジメントがどのように行われているか。	①事業体の各階層において、コアバリューが認識されていないため、行動基準からの逸脱が発生する恐れがある。 ②コンダクトリスクに対するマネジメントが不十分なため、行動基準からの逸脱が発生する。 ⇒事業体の各階層において、コアバリューの認識度合いと、行動基準の遵守状況についての監査の実施を提言する。（①、②共通）

（５）事業体全体のコアバリューの明確化と伝達 ①事業体のコアバリューは明確になっているか。	①事業体全体のコアバリューが明文化されていないため、一部の部門においては当該部門のコアバリューを明文化していた。しかし、部門間での共通の理解が得られていなかったため、事業体全体のコアバリューが不明確になっていた。 ⇒事業体全体としてのコアバリューを明文化し、取締役会に上程するように提言する。 **【具体例】コアバリューの取締役会決議** ・Ｃ社では、中期経営計画策定時に自社のコアバリューに関する討議を重ね、取締役会にて「お客さま志向」をコアバリューとすることを決議した。
②経営者は、首尾一貫したコミットメントを通じてコアバリューを組織に伝達しているか。	②コアバリュー含むコミットメントは、コミットメントを決定した際に社内に周知されたが、その後は四半期ごとに開催される会議時のみの発信であり、コアバリューから外れた業務運営が散見される。 ⇒従業員がコアバリューを自分事としてとらえて日常業務に反映するようになるように、㋐経営者から従業員にメッセージを発信する際には、可能な限りコアバリューについてのコミットメントを含めること、および、㋑ホームページやイントラネット、掲示等を使ってそのコミットメントが従業員の目に触れる頻度を増やすことを提言する。
（６）説明責任の明文化を通したリスクを認知するカルチャーの醸成 ・経営者はリスクを認知するカルチャーを醸成するために、説明責任に関する方針を文書等で示しているか。	・説明責任に関する方針がなく、説明責任を求められるケースも少ないため、従業員にリスクを認知しようという意識が希薄である。 ⇒説明責任に関する方針を明文化し、㋐説明責任の欠如は許されないこと、および、㋑説明責任を果たすことによって適切な報奨が与えられることを明確にすることを通して、リスクを認知するカルチャーを醸成することを経営者に具申する。
（７）報酬・インセンティブとコアバリューとの整合性の確保 ・報酬とインセンティブのプログラムは、組織のコアバリュー、すなわち、㋐期待される行動、㋑行動基準の遵守、㋒リスクを認知し	・コアバリューを反映した期待される行動および行動基準は明文化されていたが、人事評価に反映する仕組みがなく、精神論に止まっている。

た意思決定と判断、および㋓説明責任を、**それぞれの従業員が自分事化することを推進**するように定められているか。	⇒**期待される行動および行動基準順守の状況を人事制度の枠組みの中で評価し、処遇等に反映**させる仕組みの構築を提言する。 **【具体例】期待される行動の評価への反映** ・Ｄ社では、**業績を評価するパフォーマンス評価とコアバリューに沿った行動や姿勢の評価の二本立て**で従業員を評価し、**後者の結果を昇進・昇格に反映**することを通じて、組織のコアバリューの浸透を図っている。
（８）コアバリューや望ましい行動からの逸脱への対応 ・**コアバリューや望ましい行動からの逸脱**が判明した場合、事実関係と**何が許されない行為なのかを明確にし、社内に周知**しているか。	・不適正事象が発覚して社内処分が行われた際に、**処分の内容や処分の理由を社内で共有するルールとなっておらず**、対象となった不適正事象と原因を同じくする事象が他の部門で発生するケースが散見される。 ⇒コアバリューや望ましい行動からの逸脱を防止するために、不適正事象が判明した場合には、**事実関係および逸脱が許されない理由を明確にし、社内に周知**することを提言する。 **【具体例】不適正事象判明時の社内周知** ・Ｅ社では、**不適正事象**に対する社内処分が実施された場合、㋐発生事象の概要と㋑その中の許されない行為、㋒社内処分の内容、㋓社内外への影響を**イントラネットで周知**することで、組織内へのコアバリューの浸透と望ましい行動からの逸脱の防止を図っている。
（９）行動基準の逸脱に対する適切な相談窓口の設置 ①**行動基準の逸脱に対する相談窓口**が設置されているか。 ②相談窓口は、**匿名性を持ってアクセスしやすく**なっているか。	①**行動基準の逸脱に対する相談窓口が設置されていない**ため、行動基準の逸脱の発見が遅れ、損失が拡大する。 ②**行動基準の逸脱に対する相談窓口が匿名性を持っておらず**、アクセスしにくいため、行動基準の逸脱の発見が遅れ、損失が拡大する。 ⇒**行動基準の逸脱に対する匿名性のある相談窓口**の設置を提言する。（①、②共通）

	【具体例】行動基準の逸脱に対する相談窓口の設置 ・Ｆ社では、「内部通報制度」以外に、行動規範の逸脱に対する相談を、**日常的に上司以外にも相談できる窓口**(注) を別途設置し、行動基準の逸脱の未然防止を強化している。 （注）「日常的に上司以外にも相談できる窓口」とは、実際に目にした逸脱以外に、逸脱していることが明確でないことや疑問に思うことなどを抵抗感なく気楽に相談できるセカンドオピニオン的な窓口をいう。

原則５　有能な人材を惹きつけ、育成し、保持する

質問・確認事項	課題・改善提言
（１）採用時の望ましい行動・業務スタイル等の明確化と候補者との共有 ・採用にあたり、㋐自社のカルチャー、㋑望ましい行動、㋒業務スタイル、㋓組織のニーズ、および㋔期待する業務遂行能力を明確化し、候補者と確認・共有した上で候補者を選考しているか。	・有能な人材を採用したにも関わらず、退職が続くケースが認められた。退職理由は、㋐業績評価基準への不満、㋑生活スタイルのギャップ（自由な休暇取得・時間外勤務の長さ・テレワーク環境などの会社の業務スタイルや制度が希望に対応していないこと）、および㋒転居を伴う転勤内示等のため、退職が続くケースが認められた。 ・これらの退職理由は、採用時点で十分な説明や意向確認をしていれば避けられた内容であった。 ⇒採用する際に考慮している要素が業務遂行能力に偏っていることから、㋐自社のカルチャー、㋑望ましい行動、㋒業務スタイル、㋓組織のニーズを明確化した上で、採用時に候補者と十分確認・共有する選考プロセスを検討する。 **【具体例】採用時の望ましい行動・業務スタイル等の明確化と候補者との共有** ・Ａ社では業務上ハイレベルの給与水準の中途採用を行うことから、採用する前に㋐自社のカルチャーや望ましい行動、㋑業務スタイル、㋒組織としてのニーズ、㋓期待する業務遂行能力を明確化しておき、採用候補者にそれらをどのように確認・共有するかを選考プロセスの中に折り込んで、想定外の退職を防いでいる。 ・また、過去退職の動機となった㋐人事制度（転勤の有無）、㋑勤務環境・福利厚生（テレワークの可否、平均時間外勤務状況）、および㋒業績評価のポイントなどを取りまとめ、採用候補者の最終面接前に具体的に説明・確認している。
（２）行動基準遵守状況の評価 ・個人の業務目標の設定や評価において、収益のみならず、行動基準の遵守についても適切に評価しているか。	・会社の行動基準としては「顧客本位」であることが謳われているものの、業績評価において「顧客本位」の実行を評価する項目が設定されていなかったため、営業現場では収益のみを評価し、顧客クレームが多くあっても業績評価上考慮されていなかった。 ⇒業績評価項目として、顧客本位を推進するＫＰＩ（主要業績指標）を定め、評価するよう改定する。また、顧客クレームの増加などがあった場合、内容を確認の上必要に応じて業績評価に加味するプロセスを追加する。

	【具体例】顧客本位への取組み状況の評価 ・Ｂ社では、行動指針として「顧客本位」を追加した時に、**業績評価項目にも「顧客本位の推進」を入れ**、**営業店で行う顧客満足度アンケート結果を評価**で考慮することを明確化した。 ・また**本部でも別途、顧客満足度アンケート**を行い、営業店での評価結果との差異をモニタリングの上**評価**している。
（３）行動基準遵守状況のモニタリング ・**倫理的行動として行動基準に掲げられていることが、現場で徹底**されているか。 ・また、それが**実施しやすい環境**となっているか。 ・**本部は現場での行動基準の実施状況をモニタリング**しているか	・業務目標（ノルマ）を支店および支店の営業部員に割り当てて業務管理をしているが、その業務目標の定め方がトップダウンであり、かつ現実的な達成可能性を十分検討していない過大なものだった。 ・そのため、強いプレッシャーが支店および支店営業部員にかかり、多くの支店では業者経由で紹介された個人顧客の**リスク認識が不十分な不動産投資への融資**が行われ、中には**改ざんされた個人資産の証跡**（年収や通帳の改ざん等）が使用されていた。加えて、それらの不適切行為を支店のマネジメント層自らが助長し、あるいは看過していた。 ・また、突出して業績の良い支店への**モニタリングは特段行われていなかった**ため、本部は実態を把握しておらず、**顧客クレームに関する所管部署とその他の本部との情報共有も不十分**であったことも加わり、経営者が把握できていなかった。 ⇒業務目標の定め方、および支店への割り当てについて、**現実性と達成可能性**を加味する。 　また、業務目標の達成状況をモニタリングする際には、現場の実態把握を行い、**行動指針に沿ったものとなっているかを検証**する。併せて、**顧客満足度調査や顧客からのクレームなどもモニタリング**する。 **【具体例】顧客本位の徹底とそのモニタリング** ・金融機関Ｃ社では、業務における**顧客本位を徹底**するため、個人に割り当てられる**業務目標（ノルマ）を撤廃**し、**長期的視野で顧客と向き合えるよう業務のあり方を変更**した。 ・また上記とは別に、本部は支店の**業績が期末に急に良くなる等一定の事象がある場合は具体的にその要因の内容を確認**する等の管理を行い、ノルマ達成への対応が行き過ぎていないか確認している。

	・加えて、**顧客アンケート結果や、顧客からのクレームなどをモニタリング**し、現場の**顧客本位への対応**が適切か確認している。
（４）必要な人材の定義と評価 ①経営者は戦略と業務目標を検討する際に、そのために**必要な人材や業務遂行能力を明確に**しているか。 ②また、経営者は業務目標の達成度合いを評価する際に、**人材や業務遂行能力も評価**しているか。 ③それらは**取締役会に報告**されているか。	①社内で新規事業部門を立ち上げる際に、必要なマネジメントができる人材を社外から招くこととしたが、**どのような業務経験や能力の人を探すか明確にしない**まま、新規事業と同じ業界の人物を新規業務のリーダーに迎え、戦略も一任することとした。 ②また、その戦略の業績評価を行う際に、その人物の**業務遂行能力を評価しなかった**。そのため、目標に届かず赤字となっていたにも関わらず、その業務の一時的特殊事情というそのリーダーの**説明を鵜呑み**にして放置してしまった。 ③加えて、それらの内容は**取締役会に報告されていなかった**。 ⇒経営者は、新規事業・新規業界ということで特別扱いをすることなく、その内容や必要な**人材の適性、業務遂行能力を明確にし**、またそれらの達成度合いをモニタリングの上、そのリーダーの**能力を評価**する。 　また、**取締役会にも**戦略や業務目標策定および人材の評価について**報告**する。（①～③共通）

構成要素２　戦略と目標設定

原則６　事業環境を分析する

質問・確認事項	課題・改善提言
（１）事業環境変化の監視 ①社内外を問わず、パフォーマンスに影響を与える事業環境を網羅的に特定しているか。 ②特定した事業環境の変化を監視する体制を整備しているか。	①監視対象が網羅的でないために、重要な環境変化を見落としている。 ②監視体制が整備されていないために、環境変化に気づかない。 ⇒多くの情報源を活用して、また情報源毎にモニタリング担当部署を取り決め、幅広く、かつ定期的に環境変化を監視する。（①、②共通） **【具体例】事業環境変化の把握・確認** ・Ａ社は、専業中堅エンジニアリング企業である。リーマンショック以降、顧客である製造業の海外進出が増加し、国内における工事件数の伸びが鈍化する環境変化への対応に迫られていた。 ㋐営業部門では、日々の営業活動の中で、新設工事は頭打ちする一方で、改造・保全工事が増加する傾向にあることに気づいた。 ㋑企画部門では、各種調査資料から、顧客である製造業では保全に関わる技術者不足が課題となっている情報を得た。 ㋒人事部門では、技術者不足が工事受注の制約になることから、全社での資格取得状況を定期的に確認している。
（２）事業環境変化の社内伝達と分析 ①環境変化に関する情報を適時に関係部署へ伝達しているか。 ②環境変化が長期的な受注見込み等のパフォーマンスに与える影響を分析しているか。	①～②モニタリング担当部署から事業環境変化の情報が伝達されず、環境変化への対応が後手にまわる。 ⇒定期的な会議体で環境変化の情報を社内で共有化すると共に、パフォーマンスに与える影響を分析する。 **【具体例】事業環境変化の企画部門への報告と同部門による評価** ・Ｂ社では、

	㋐全部門が参加する月次定例会議において、工事進捗・受注実績だけでなく、各部門のＫＰＩ（主要業績指標）の進捗状況、および事業環境変化に関する情報を企画部門に報告している。 ㋑企画部門では、各部署からの情報に基づき、年度計画の達成見込みを評価している。
（３）事業環境変化を検討した上での意思決定 ・進行している環境変化、将来想定される環境変化の影響等を検討したうえで、事業戦略の意思決定を行っているか。	・環境変化を適切に織り込まず事業戦略を決定してしまい、期待したパフォーマンスを得られない。 ⇒中期計画、年度計画を策定する際には、事業環境想定を十分に議論した上で、各部門の事業戦略を決定する必要がある。 **【具体例】事業環境変化を踏まえた意思決定** ・Ｃ社では、事業環境の変化を踏まえて、㋐有望な東南アジア市場に進出すること、㋑改造・保全工事の受注に力を入れることおよび、㋒それらの戦略に必要な技術の資格習得に奨励金を支給することを、年度計画承認の取締役会で決定した。

原則７　リスク選好を定義する

質問・確認事項	課題・改善提言
（１）リスク選好の策定 ①価値の創造、維持、実現の観点から**リスク選好を検討する際に、考慮すべき要素を明確にして**いるか。明確にしている場合、どのような要素を考慮しているか。	①**リスク選好を検討する際に考慮すべき要素の整理が不十分**のため、**重要な要素が明確になっていない**。あるいは**一部の重要な要素が欠落**し、考慮されていない。 ⇒**リスク選好の検討**に際しては、**㋐ミッション・ビジョン・コアバリュー、㋑過去の戦略、㋒リスクプロファイル、㋓リスクキャパシティ、㋔全社的リスクマネジメントの能力と成熟度を考慮**するように提言する。特に㋐、㋑が重要である。
②策定されたリスク選好において、**価値追求のために受け入れるリスクの種類および量を明示**しているか。	②リスク選好として策定されたが、**受け入れるリスクの種類および量が明示されていない**ため、本来のリスク選好の役割を果たしていない。 ⇒リスク選好においては、**受け入れるリスクの種類および量を明示**するように提言する。また、量の表現においては、㋐戦略・事業目標との関係性や㋑全社的リスクマネジメントの能力と成熟度等を考慮するように提言する。 **【具体例】リスク選好方針によるリスク選好の明示** ・Ａ社では、**リスク選好フレームワーク**(注1)**とリスク選好方針**(注2)**を一体で定め**、リスク選好方針において、事業区分ごとに**受け入れる主なリスクの種類および量を明示**している。 （注１）㋐資本配賦運営、㋑リスク・リターン運営、㋒自己資本充実度評価運営など、会社がリスクテイクを行う上での運営の枠組みを定めたもの （注２）会社としてのリスクテイクの方針を定めたもの
（２）リスク選好の取締役会承認 ・**リスク選好は取締役会によって承認**されているか。	・リスク選好の承認は経営者とする運用になっているため、**取締役会が承認プロセスに関与していない**。 ⇒リスク選好は戦略と密接な関係にあることから、**取締役会の承認**が必要である。

	【具体例】リスク選好の取締役会承認 ・Ｂ社では、一体化したリスク選好フレームワークとリスク選好方針を取締役会が承認している。
（３）リスク選好の事業体全体への伝達 ・承認されたリスク選好は、事業体全体に伝達され、周知されているか。	・リスク選好の伝達が事業体の一部にとどまっている結果、研修も行われていないなど、事業体全体から見て周知に至っていない。 ⇒リスク選好を事業体全体に伝達するとともに、定期的な研修等を通じて周知する。 【具体例】リスク選好の伝達・周知 ・Ｃ社では、リスク選好を定めたリスク選好方針をイントラネットを通じて全社に伝達するとともに、定期的に開催する階層別のリスク管理研修の中で説明を行い周知している。
（４）リスク選好に基づいた資源配分 ・リスク選好に応じて全社および事業区分ごとに経営資源を配分することで、リスク選好を経営資源の配分に活用しているか。	・リスク選好の活用方法について整理がされていないため、リスク選好を反映した経営資源の配分が行われていない。 ⇒リスク選好に応じて全社および事業区分ごとに経営資源を配分することで、リスク選好を経営資源の配分に活用する。 【具体例】リスク選好の資源配分への活用 ・Ｄ社では、㋐戦略（経営計画）と連動したリスク選好に応じて全社および事業区分別・リスク種類別に自己資本(注)を配賦し、事業区分ごとのリスク量の上限にすると共に、㋑リスク選好を事業区分別の要員配置にも活用している。 （注）自己資本は時価ベースの資産から時価ベースの負債を控除したもの

原則８　代替戦略を評価する

質問・確認事項	課題・改善提言
（１）ミッション・ビジョン・コアバリューおよびリスク選好と整合した戦略の策定 ①選択対象の戦略は、組織のミッション・ビジョン・コアバリューと整合的であるか。	①コアバリューである建学の精神(注１)に基づき、国際的感性とコミュニケーション能力ある人材の養成をミッション・ビジョンとして標榜しているが、かつて国際感覚からは程遠いロケーションにキャンパスを新設し学部移転したため、アドミッション・ポリシー（入学者方針）に適合する学生の応募が漸減している。（選択した戦略がミッション・ビジョン・コアバリューと整合していない） （注１）私立大学のコアバリュー ＝ 「建学の精神」 ⇒国際感覚のイメージに合う立地にキャンパスを移転する。（選択した戦略をミッション・ビジョン・コアバリューと整合させる） リスク　　：土地取得費用・建設費の確保、現キャンパス跡地利用 リスク対応：新キャンパス開設に必要な基本金(注２)を確保する。 （注２）学校法人は、教育研究の基盤となる土地・建物・設備などの資産を保持・維持し、または新校舎・キャンパスを新設するための資産を「基本金」として留保している。
②戦略は、組織のミッション・ビジョン・コアバリューおよびリスク選好と整合的であるか。	②国際的人材の養成という観点から、実務英語の能力が高い教員の確保により、実務英語教育を中心とした授業運営をアピールすべきであるが、そのような教員確保のための人件費がネックとなり実現に至っていない。（選択した戦略がミッション・ビジョン・コアバリューに基づくリスク選好と整合していない）
（注）（１）～（３）は戦略設定のためのプロセス。	⇒実務英語能力の高い教員確保に伴う人件費の上昇というリスクを、財務基盤の強化によりリスク選好の範囲内に抑制しながら、ハイクォリティの実務英語教員を多数確保して実務英語授業の体制を整備することにより、真に実務英語能力を修学したい学生の応募につなげる。（ミッション・ビジョン・コアバリューおよびリスク選好と整合的な戦略の選択） リスク　　：人件費の上昇 リスク対応：㋐卒業生（資産家・企業経営者）からの奨学寄附金の大募集、㋑授業料のアップ、㋒教育活動支出の見直し等により、財務基盤を強化する。

	【具体例】ミッション・ビジョン・コアバリューおよびリスク選好に適合する新キャンパスへの移転 ・Ａ大学では、 (a)県北部の人口減少地域にあるキャンパスを閉鎖し関連する学部を廃止する一方、公的な長期資金の調達により、インターナショナルな企業が多く国際感覚の醸成が期待される南部港湾地域のキャンパスを拡充し（ミッション・ビジョン・コアバリューと整合的な戦略の選択)、 (b)また、長期資金計画の見直しにより教員人件費の課題をクリアして（リスク選好の範囲内でのリスクテイク)、 実務英語教育を中心とした新学部を開設した結果、志願者が増加した。(戦略目的の達成)
（２）リスクの識別とリスクが及ぼす影響の評価 ①戦略の基盤となる仮定、および戦略のパフォーマンスに関連するリスクを、全体俯瞰して識別しているか。 ②識別した仮定、およびリスクが組織に及ぼす影響を評価しているか。	①～② ・新キャンパス投下資金を回収すべく授業料をアップしたが、実務英語教員の新規採用が進捗せず教務体制が不十分との評価のため、アドミッション・ポリシーに合致する志願者が増えず、偏差値の低下傾向に歯止めがかからない。 ・少しでも優秀な学生を獲得するための奨学金支出が増加し、更に収益が悪化している。 ⇒長期資金計画においては、授業料の値上げにより収支尻を合わせるだけでなく、最適なポートフォリオの教務体制に要する人件費を見積もる必要がある。併せて、景気動向の想定に沿った実質収益（変数；休・退学率、奨学金を考慮した実質授業料）および人件費・減価償却費などのシナリオ分析に基づいて影響を評価する。 【具体例】識別したリスクとその影響の評価に基づく最適な教務体制の構築 ・Ｂ大学では、新規募集する実務英語教員の処遇向上（准教授、教授への昇任）と在籍している教員の継続雇用に伴うリスクとその影響を評価した上で、本学教員職としての将来性に希望が持てる処遇条件を提示した結果、優秀なネイティブ教員が確保でき、実務英語の授業運営が高く評価され、アドミッション・ポリシーに合致する志願者が増加した。

（３）戦略がリスク選好に適合していることの確認 ①戦略に関連するリスクは、組織のリスク選好に適合しているか。 ②リスク選好に適合しない場合の戦略最適化プロセス(注)を明確にしているか。 （注）当該戦略の修正、他の戦略の採用、リスク選好の見直し。	①～② ・長期収支計画の全ての要素が学校法人の望むようになる前提であるため、想定が崩れると、教育活動収支が一気に悪化し財務基盤に影響するリスクがある。 ・業務のスクラップ・アンド・ビルドが行われていないため、人海戦術もしくは安易な業務外注（派遣会社）により、実質的な人件費の膨張が止まらない。 ・教職員の定年まで定期昇給が保証される終身雇用制度、かつ役職定年、人事評価もないことから、人件費アップ圧力が強い人事制度となっている。 ⇒㋐ＲＰＡ（ﾛﾎﾞﾃｨｯｸ・ﾌﾟﾛｾｽ・ｵｰﾄﾒｼｮﾝ）の導入による業務軽減、㋑専門的技術・業務の外部委託、㋒硬直的人事制度の見直しによる固定費削減など、各戦略が財務基盤に与える影響を評価し、リスク選好に適合した優先戦略を選択する。
（４）戦略のモニタリングと変更 ・最高戦略委員会は、採用した短期戦略および長期戦略を定期的にモニタリング(注)しているか。 （注）パフォーマンス指標の評価、リスク許容度の適合状況、経営資源の調達可否。	・新キャンパスの設置および新学部の開設後、日常業務の諸調整に追われ定期的なモニタリングを先延ばしにした結果、以下の課題が明らかになっている。 (a)新キャンパス開設が公表された年の志願者は大幅に増加したが、新学部の概要が明らかになるにつれ、教務体制整備が不十分との評価が広まったため、志願者増加の勢いが鈍化している。 (b)単に既存教職員の雇用を確保することに重点が置かれ、目新しい授業がない。全学的に教職員・学生の要望を集約し、新キャンパスの全体像をデザインして建築計画に反映したものの、工事進捗につれて、完成時期、コストとの見合いが優先されたため、志願者増加に結びつくような斬新さが削がれてしまった。 ⇒最高戦略委員会は、戦略遂行上の課題を適時に把握し解決するため、長期戦略および短期戦略の遂行状況を定期的にモニタリングし、必要に応じて戦略の変更を検討する。 (a)建学の精神（コアバリュー）に基づき、国際的感性とコミュニケーション能力ある人材の養成という本来のミッションに立ち戻り、学生および志願者目線で全体俯瞰してシラバス（講義概要）を再検討する。 (b)ハイクォリティの実務英語教員の採用（高額給料支払）および最新の教育機器導入に必要な資金確保の可否判断のため、経営資源自体を再検証する。

原則９　事業目標を組み立てる

質問・確認事項	課題・改善提言
（１）事業目標の適切な設定 ①組織が設定する事業目標は、**測定することが可能**なように考慮されているか。	①設定された**事業目標の記載があいまいで抽象的**であるため、達成度合いを測定することができず、事業目標の修正や廃止などの**意思決定が困難**となっている。
②組織が設定する事業目標は、**達成することが可能**なように考慮されているか。	②市場規模・外部環境および内部環境など自組織の**身の丈に比べて過大な目標**が設定されているため、達成を求めるあまり**過剰なリスクを受容**してしまっている。
	⇒事業目標の**策定基準の明確化**および**経営者によるレビュー**を行う。（①、②共通）
③組織が設定する事業目標は、**戦略およびミッション・ビジョン・コアバリューと関連性**を持つように考慮されているか。	③－１　組織の**戦略やミッション・ビジョン・コアバリューと関連性のない事業目標**が設定されているため、目標を達成しても組織の**戦略およびミッション・ビジョンの支えとはならない**。また、かえって事業体の**リスクプロファイルに不必要なリスクを持ち込んで**しまう可能性もある。
	⇒経営者による**事業目標と戦略およびミッション・ビジョン・コアバリューとの整合の確認**を行う。
	③－２　**事業目標が戦略と結び付いておらず**、事業体のミッションやビジョンの達成に役立っていない。
	⇒事業目標の持つ意味を執行部門の幹部に教育し、**事業目標の設定については戦略と整合するように経営者によるレビュー**を実施する。
④組織が設定する事業目標は、**リスク選好と関連性**を持つように考慮されているか。	④組織の**リスク選好と関連性のない事業目標が設定**されているため、**組織は過剰なリスクを受容**するかまたは、**過少のリスクしか受容しない**ことになる。
	⇒経営者による**事業目標とリスク選好との整合の確認**を行う。

（２）事業目標の各階層への落とし込み ・事業目標は事業体の各階層に段階的に落とし込まれているか。	・部門単位の事業目標は設定されているが、各課の目標にまで落とし込まれていないため、各課でどんな目標を達成すべきか明らかになっていない。 ⇒部門長は、部門の事業目標の達成のために各課が行うべき役割を明確に伝え、各課の目標達成によって部門の目標が達成されるような各課の目標設定を行う。
（３）測定可能なパフォーマンス指標と適切なターゲットの設定 ・事業目標には、達成度を把握できるように測定可能なパフォーマンス指標と適切なターゲットが設定されているか。	㋐パフォーマンス指標が測定可能な指標でないため、達成度が客観的に判断できない。 ㋑ターゲットが過大あるいは過少であり目標として適切でないため、過剰なリスクを受容している、もしくは過少のリスクしか受容しない。 ㋒ターゲットが適切ではないため、想定した結果と違う結果になっている。 ⇒部門長が設定したパフォーマンス指標とターゲットの適切性を、経営者および財務部門長がレビューする。 **【具体例１】働き方改革に対応した労働時間の測定** ・Ａ社では月間平均残業時間を働き方改革のパフォーマンス指標とし、20 時間以下をターゲットとして事業目標に掲げている。全社員の勤怠管理システムを一元化し、出退勤の打刻と日次の承認を徹底している。 ・補完的にリモートアクセスの実績ログや社員証ＩＣカードによる入退館履歴も取得し、測定可能な限り適正な勤怠データを登録させている。 ・人事部門は、毎月部署別の残業時間を集計し、経営会議で報告している。 **【具体例２】不適切な利益評価指標の改善** ・Ｂ社は二つある主力部門の一つで赤字が常態化していた。その部門では利益率の向上のために、限界利益率をパフォーマンス指標としそれ一定レベル以下の顧客には値上げを要請し、要請を断られた顧客との取引を断念することにした。 ・その結果、この部門の限界利益率は向上したが、売上が減少したため赤字からは脱却できなかった。

	・部門長会で管理部門長から限界利益率をパフォーマンス指標にした事業目標が誤りであることを指摘され、損益分岐点をパフォーマンス指標とした事業目標に変更し、管理を行うことにした。
（4）パフォーマンスの許容度の設定とモニタリング ①組織の事業目標には、パフォーマンスの許容可能な差異（許容度）があらかじめ定義されているか。 ②組織のパフォーマンスがモニタリングされ、許容度の範囲内であることが確認されているか。	①パフォーマンスの許容度（ポジティブ差異・ネガティブ差異）が設定されていないため、許容度を逸脱しているのかどうかが判断できない。 ・そのため、リスクを許容できないレベルにまで高いパフォーマンスを追求しており、過剰なリスクを受容している。 ⇒経営者によるリスク選好とパフォーマンスの許容度のレビューを行う。 ②組織のパフォーマンスがモニタリングされていない、またはパフォーマンスが許容度の範囲内であることを確認されていないため、気付いた時には非常に大きなリスクを許容していることが後になって発覚する。 ⇒組織のパフォーマンスが許容度の範囲内にあるかを確認するモニタリングプロセスを設計・実施する。 **【具体例】法令順守や健康管理に対応した労働時間の測定** ・C社では 36 協定や罰則付き残業規制の対策として、年間平均 60 時間/月以内を許容範囲として設定した。組織的にモニタリングを浸透させるために残業時間管理に以下の通り段階的な許容度を設定し、月末の勤怠締めの承認権限の階層を定義している。 ㋐20 時間以下：課長承認、　㋑40 時間以下：部長承認、 ㋒60 時間以下：執行役員承認、㋓60 時間超：取締役承認 ・人事部門は、毎月部署別の残業時間を集計し、単月および年間平均 60 時間/月超の発生状況を経営会議で報告している。

構成要素３　パフォーマンス

原則１０　リスクを識別する

質問・確認事項	課題・改善提言
（１）新しいリスク・エマージングリスク・変化する既存のリスクの識別 ①戦略および事業目標の達成に関連するリスクについて、その**識別のために**、既知のリスクに加えて、**どのような要素を考慮**しているか。	①リスクの識別について、**既知のリスクのみを対象**としているため、リスク識別の要素としては不十分となっている。 ⇒リスクの識別に際しては、既知のリスクだけではなく、戦略や事業目標の達成に影響を与える可能性がある**㋐新しいリスク、㋑エマージングリスクおよび、㋒変化する既存のリスクを考慮**する。 **【具体例】経営者によるリスク識別の取り組み** ・Ａ社では、リスクの識別について、経営者自ら**㋐新しいリスク、㋑エマージングリスクおよび、㋒変化する既存のリスクの洗い出し**を行い、経営会議等で検討を行っている。
②リスクの識別において、事業目標の達成を阻害する可能性がある脅威だけでなく、**事業目標を達成したり超えたりするのに役立つ可能性がある機会**も考慮しているか。	②リスクの識別について、**脅威のみを対象**としており、事業目標を達成したり超えたりするのに役立つ可能性がある**機会が考慮されていない**。 ⇒リスクの識別に際しては、脅威のみを対象とするではなく、事業目標を達成したり超えたりするのに役立つ可能性がある**機会も考慮する**。
（２）リスク識別プロセスの統一・明確化 ・**リスクを識別する**ために、どのような**アプローチ**（**リスク評価プロセス**）を検討しているか。また、そのリスク評価プロセスは**文書化**されているか。	・**リスクの識別について、その評価プロセスは明確に定められておらず、**リスク管理部門の担当者の裁量に任されているため、**担当者によって評価プロセスが異なって**おり評価結果に統一性がない。 ⇒**リスク評価プロセスを明確に定め**、**文書化**する。また、その評価プロセスでは以下のアプローチの組み合わせを検討する。 ㋐インタビュー、㋑ワークショップ、㋒データ追跡、㋓主要指標、 ㋔プロセス分析、㋕コグニティブコンピューティング

	【具体例】ボトムアップおよびトップダウンアプローチによるリスク評価 ・Ｂ社では、㋐リスク管理部門がファシリテーターとなって各部門とワークショップを開催し、**ボトムアップアプローチによるリスク評価**を行うとともに、㋑各担当役員へのインタビューによる**トップダウンアプローチによるリスク評価**も行い、その組み合わせにより総合的なリスク評価を実施している。また、その評価プロセスは**リスク評価マニュアルとして文書化**されている。
（３）リスク一覧表の作成によるリスクの可視化 ①識別された**リスクを可視化**して把握するためにどのような**方法**を取っているか。 ②識別したリスクを**どのような頻度で更新**しているか。	①識別した**リスクが体系化・階層化されていない**ため、**可視化して把握することができない**。 ⇒識別されたリスクを**一覧表の作成により体系化・階層化し、可視化**する。 ②**定期的なリスクの更新を行っていない**。このため、経営者が**リスクの最新の状況を認識できない**。 ⇒識別した内部および外部のリスクの変化に対応して、**定期的**（例えば、半年ごとなど）**に更新**する。

原則１１　リスクの重大度を評価する

質問・確認事項	課題・改善提言
（１）リスクを評価する時間軸の明確化と統一 ・リスクを評価するための時間軸は、戦略および事業目標の策定で使用した時間軸（対象期間）と同一であるか。	・リスク評価を毎年年度初めに実施しているが、対象とする時間軸を明確に示していない。 ・一方、戦略および事業目標については、毎年年度末に、翌年度１年間の戦略および年間事業目標を策定しており、さらに３年に１度、翌年度以降３年間の中期戦略および中期事業目標を策定している。 ・そのため、リスク評価の結果が、翌年度１年間の戦略および事業目標に影響を与えるものなのか、翌年度以降３年間の中期戦略および中期事業目標に影響を与えるものなのかが曖昧になっている。 ⇒リスク評価の実施に当たっては、対象とする時間軸を明示し、翌年度１年間の戦略および事業目標に対するリスク評価なのか、翌年度以降３年間の中期のそれらに対するリスク評価なのかを明確に示す。 【具体例】リスク評価の時間軸と戦略および事業目標の時間軸との整合性確保 ・Ａ社では、リスク評価を単年度および中期の戦略および事業目標設定時に実施し、戦略および事業目標の策定で使用した時間軸（対象期間）に対するリスクとして明確にしている。
（２）事業内容の変化に応じたリスク測定基準の見直し ・経営者は、リスクの評価に際し、現在の事業内容に合致した測定基準(注)を選択しているか。 （注）事業内容に合致した測定基準とは、事業環境に基づいて選択されるものであり、事業体の㋐規模、㋑性質、㋒複雑さを考慮し、なおかつ㋓リスク選好と一致している必要がある。	・かつては機械製造が中心であったが、現在は、Ｍ＆Ａなどで事業を拡大し、㋐機械設備保守、㋑コールセンター運営、㋒システム開発、㋓アプリ開発、および㋔人材派遣など多様な業態をかかえている。 ・毎年リスク評価を実施しているが、リスク評価で用いる測定基準は、機械製造事業が殆どであった時代から踏襲しているものを使用している。 ・そのため、機械製造事業以外のメンバーからは、評価がしづらい、評価結果が実感とあわない、という声が上がっている。 ⇒リスク評価の測定基準は、事業体の㋐規模、㋑性質、㋒複雑さに鑑み、また、㋓リスク選好に一致するよう、事業内容が変化する都度見直す。 ・異なる性質の事業ごとに、それらに合致した測定基準を設けたうえで、全社のリスク評価を行う。

（３）最適なリスク評価のアプローチの選択 ・経営者は、リスクの評価に際し、**最適なアプローチ**(注)**を使用**しているか。 （注）リスク評価のアプローチには、定性的アプローチ、定量的アプローチそれぞれがあり、定性的アプローチは「インタビュー」「ワークショップ」「調査」「ベンチマーキング」などがあり、定量的アプローチには「モデリング」「デシジョンツリー」「モンテカルロシミュレーション」などがある。	・毎年リスク評価を実施しているが、**リスク評価のアプローチは**、部門長がリスク測定基準に基づきアンケート回答する方法のみが取られており、リスク評価を開始した時から**長年見直されていない**。 ・そのため、リスク評価に活用できる有益なデータを効率的に（容易に・短時間で・安価に）取得できるようになったにもかかわらず、**リスク評価の精度が向上しない**事態を招いている。 ⇒**リスク評価のアプローチは**、経営者が様々な手法の中から、実用性や費用対効果の側面を検討した上で、**適切なものを単独あるいは複数組み合わせて使用**する。 **【具体例】定量的アプローチと定性的アプローチを組合せたリスク評価** ・Ｂ社では**リスク評価のアプローチ手法を継続的に検討**している。すなわち、㋐製造ラインの故障発生率、㋑営業車 100 台あたりの事故発生率、㋒情報漏えいリスクにおける最大漏洩時の損害金額など、**定量的なデータが効率的に得られるようになった段階で評価アプローチに取り入れ**てきた。 ・同時に、責任者へのインタビューやマネジメント層へのワークショップといった**定性的**アプローチも取り入れ、定量・定性両面でのアプローチを組み合わせて**リスク評価の精度を高めて**いる。

原則１２　リスクの優先順位付けをする

質問・確認事項	課題・改善提言
（１）リスクの優先順位付けを行う規準の設定 ・リスクの優先順位付けを行う規準を設定し、周知しているか。	・会社は全社で**優先的に対応すべきリスクを定め従業員に周知しているが、規準が明確になっておらず**、結果としてなぜこのリスクの優先度が高いのか、従業員は納得できていない。 ・このため、全社のリスク教育のアンケートでは、多くの従業員が「このリスクの優先順位が高いことに対する納得感がない」と回答している。 ⇒**リスクの優先順位付けを行う規準を設定し**、周知する。 **【具体例】優先的に対応すべきリスクと優先順位付けの規準の周知** ・Ａ社では全社リスク委員会での審議および経営会議での審議を経て、**優先的に対応すべきリスクを定め**、イントラネット上で従業員に周知している。 ・同時に、**リスクの優先順位付けの規準も周知**し、従業員の納得感を高めている。
（２）リスクの優先順位付けの実施 ・リスクの重要度やリスク選好、およびリスクの優先順位付けの規準を踏まえ、**リスクの優先順位付けを行って**いるか。	・全社および各部門では、関連するリスクは洗い出して評価していたが、**優先順位付けを行っていない**。 ・このため、洗い出したリスクすべてに対応策を策定したものの、**実行されていない施策**や**運用上に不備のある施策**が見られる。 ⇒リスクに対応できる資源は限られていることから、**定期的にリスクの優先順位付けを行う**。 **【具体例】全社および各部門でのリスクの優先順位付けの実施** ・Ｂ社では、毎年、全社のリスクの洗い出しと評価に加えて、**リスクの優先順位付けを行い**、優先的に対応すべきリスクを識別している。 ・各部門や子会社においても、同様に自部門や自社に関連するリスクの洗い出しと評価に加えて、**リスクの優先順位付けを行い**、優先的に対応すべきリスクを識別している。

（３）リスク選好に沿ったリスクの優先順位付け ・リスクの優先順位付けの際にリスク選好と比較し、事業目標のリスク選好に接近または超過するリスクは対応の優先順位を高めているか。	・優先順位付けされたリスクを確認したところ、評価したリスク一覧の中に事業目標のリスク選好を超過しているリスクがあったが、その優先順位は他に比べて低くなっている。 ⇒リスクの優先順位付けの際には、事業目標のリスク選好を考慮する。 【具体例】リスク選好に基づいたリスクの優先順位付けと資源配分 ・安全・安心な都市・行政基盤システムを社会に提供することを使命としているＣ社は、セキュリティ事件・事故や品質問題の増加が自社の価値を大きく損なうことを十分に認識している。（リスク選好に基づいてリスクを優先順位付けしている） ・このため、リスクを評価する際には情報セキュリティと品質に関するリスクを最優先に考え、従業員に周知徹底し、対応策の実施に十分な資源を優先的に配分している。（リスク選好に基づいて資源配分を行っている）

原則１３　リスク対応を実施する

質問・確認事項	課題・改善提言
（１）所定のプロセス（検討事項・評価項目・決裁レベル）に則ったリスク対応の選択 ①識別されたリスクに対する次のカテゴリー、すなわち㋐受容、㋑回避、㋒活用、㋓軽減、㋔共有を考慮したリスク対応の選択プロセス（規程・手続等）は整備されているか。 ・または、リスク対応の選択プロセスに、㋐事業環境、㋑費用と効果、㋒義務と期待、㋓リスクの優先順位づけ、㋔リスク選好、㋕リスクの重大度等に対する評価項目や決裁レベルが明定されているか。	①リスク対応の選択プロセスが整備されていない。または、プロセスはあるが、検討すべき項目の漏れやリスクの重大度に対応した決裁レベルが規定されていないため、リスク対応の選択が曖昧になっている。 ⇒識別されたリスクの重大度に応じ、対応の実効性を確保できるように、リスク対応の選択に必要な検討項目や決裁レベルを定めたプロセスを整備する。
②リスク対応の選択が、㋐評価すべき項目や対象とすべき関係部署を網羅して検討されまた、㋑決裁者の承認を得ているか。	②リスク対応の選択において、評価すべき項目や対象とすべき関係部署に漏れがある。または、リスクの重大度に応じた決裁レベルが明記されておらず、そのため不十分なリスク対応となっている。 ⇒リスク対応が形骸化したり、実効性が棄損しないように、㋐評価すべき項目や対象とすべき関係部署および、㋑リスクの重大度に応じた決裁レベルを含めたプロセスを明定する。 **【具体例１】リスク対応における「共有（移転）」の決定** ・インターネットに接続し、ＷＥＢサービスを提供する情報処理Ａ社では、サイバー攻撃の激化と高度化に対応した防衛策の実装が急務となっている。 ・サイバー攻撃による情報漏洩やサービス停止時の経営インパクトを踏まえ、これまでのソフトウェアによる多重防御に加え、費用対効果を検証のうえ、経営会議の承認を得てサイバー保険に加入するリスク移転の決定を行った。 **【具体例２】リスク対応における「活用」の決定** ・Ｂ社では、これまで膨大なコストと期間をかけて堅牢なハードウエアとソフトウェアを独自開発してきた。 ・近年の厳しい事業環境を踏まえ、リスクを許容し、パブリッククラウド(注1)の採用による特定ベンダーへのロックイン(注2)等のリスクとコスト削減効果を検証し、取締役会での承認を得て、基幹システムにパブリッククラウドの採用を決定した。

	（注１）広く一般のユーザーや企業向けにクラウドコンピューティング環境をインターネット経由で提供するサービス。 （注２）情報システムなどの中核部分に特定の企業の製品やサービスなどを組み込んだ構成にすることで、他社製品への切り替えが困難になる。
（２）リスク対応の費用対効果の検証と戦略および事業目標の変更 ①リスク対応は、㋐リスクの重大度と優先順位や㋑戦略および事業目標の達成との兼ね合いを踏まえ、**費用とその効果について検証**されているか。 ②リスク対応の検討の結果、選択したリスク対応が**費用対効果の観点から許容できない**場合は、**戦略および事業目標の変更**の要否の可能性について検討されているか。	①**リスク対応の選択において、費用対効果についての検討が不十分**なため、**リスク低減による効果以上に過大な対応費用を要し**、事業効率が低下した。 ⇒リスク対応の選択においては、戦略および事業目標の達成との兼ね合いも含め、**費用対効果についての検証**が必要である。 ②選択したリスク対応について、**費用対効果の観点から容認できず、リスク対応が不十分、または実施されない**。 ⇒**費用対効果の観点からリスク対応の選択が容認できない**場合、リスクの重大度に応じ、**戦略および事業目標の変更**について検討する。

原則１４　ポートフォリオの視点を策定する

質問・確認事項	課題・改善提言
（１）リスク・リターンの相関関係をポートフォリオの視点から検討する ・リスク・リターンの相関関係について、ポートフォリオの視点から検討しているか。	・リスク・リターンについて、各部署の判断に任せているため、ダイナミックな経営判断ができない。 ⇒リスクを考慮する際は、**リスク・リターンの相関関係を、部門横断的にポートフォリオの視点から検討**する。 　その際、各部門で捉えているリスクは、㋐同時多発的に起こる可能性のないものや（相関関係の認められないリスク）、㋑一つのリスクが起きた場合他方のリスクは起きる可能性がないもの（マイナスの相関）や、㋒逆に一つのリスクが起きた場合他方のリスクも必ず発生するリスク（プラスの相関）など、様々である点に注意する。 **【具体例】部門間の相反するリスク・リターンの相関関係を踏まえた投資判断** （上記㋑の**マイナスの相関**があるケース） ・事業環境の変化に対して、Ａ社のある部門では、**事業環境が変化しなかった場合**のリスクを考慮して、投資を躊躇していた。また別の部門では、逆に**事業環境が変化した場合**を考慮して、投資を躊躇していた。 ・経営者はこの状況を調整し、両部門それぞれに相応の経営資源を割り当てた結果、**事業環境が変化してもしなくても、一定の利益を確保出来る経営態勢**を整えることができた。
（２）より高次の次元からリスクテイクの判断を行う ・リスクの特徴を十分理解して、より高次のリスクテイクの判断をすることにより、リスクの本質に迫り、適切な経営判断を行っているか。	・リスクテイクの判断を現場レベルに任せているため、保守的になってビジネスチャンスを逃している、あるいは過度にリスクを取っている。 ⇒リスクテイクの判断は現場レベルの認識・対応に委ねるだけでなく、より高次の次元からも判断をする。 　その際、組織としてのリスクについて、「**リスクを判断する階層レベル**」、「**各部門のリスクが統合される過程**」に関して、次の特徴点の理解が必要である。 (a) **リスクを判断する階層レベル**は、次の４つのリスクレベルがある。 ㋐現場レベルで認識している**直接的な最小単位の様々**なリスクレベル ㋑コンプライアンスリスク、オペレーショナルリスクなど、**リスクの性質によりカテゴライズ・統合**されたリスク（リスク**カテゴリー**レベル）

	㋒「財務基盤の強化」、「市場占有率の拡大」など、個々の**経営目標の視点から再統合**されたリスク（リスク**プロファイル**レベル） ㋓「業界のリーダーになる」など、**最終的な経営目的に大きく統合**されたリスク（**ポートフォリオ**レベル） (b)**各部門のリスクが統合されていく過程**は、次の４つの場合がある。 ㋐より高次へのリスク統合で**累積的にリスクが高まる**場合。 例：リスクに正の相関関係がある場合。 ㋑より高次へのリスク統合で**累積的にリスクが減少**する場合。 例：リスクに負の相関関係がある場合。 ㋒リスクに**ナチュラルヘッジ**が見られる場合。 例：豊作であれば価格が下がり、不作であれば価格が上がるので、売り上げが想定以上に大きく振れることが少ないと見込まれる場合。 ㋓リスクカテゴリー間で**正又は負の相関関係**が認められる場合。 例：リコール発生は、コスト上昇のリスクに直結するだけでなく、コンプライアンスリスクにも影響するので、両方の影響を考慮しなければならない。 **【具体例】経営者による高次の視点からのリスクテイク** （上記、「(a)㋓」と「(b)㋑」の組み合わせのケース） ・Ｂ社の技術開発部門は、最新の理論に基づく技術開発に対して、多大な困難を伴うことから躊躇していた。 ・経営者は、同技術開発が成功した場合における、同社の社会的な使命の達成など**高次の経営目的も含めた多方面のプラス面を総合的に評価**し、同技術開発に相応の経営資源を振り向ける意思決定（リスクテイク）を行った。
（３）定量評価も含めてリスクのポートフォリオ分析を行う ・**リスクのポートフォリオの視点からの分析を、定量面も含めた手法で行い**、適切なリスク対応が可能な態勢を構築しているか。	・リスクのポートフォリオの視点からの分析の際に、**定量的な評価を行っていない**と、**適切なタイミングでリスクへの対応が行えず、損失が拡大**する危険がある。 ⇒リスクのポートフォリオの視点からの分析は、定性的な評価と対応策の策定だけに止まらず、**可能な限り定量的な評価と対応策の策定を行う**。 具体的には、リスクのポートフォリオの視点からの分析にあたっては、定性的な分析だけでなく、**定量的な技法による分析**（ストレステスト等も含む）、**モニタリング、対応**が必要となる。

	ここで言う**対応**については、次の４つが考えられる。 ㋐リスクの現状分析による包括的な対応。 例：事前の資本増強。 ㋑リスクプロファイル分析。 例：失業率などのトリガーによる影響を分析し、“アラーム”を特定。 ㋒個別リスクへの事前対応。 例：保険、ヘッジ。 ㋓素早い調整方法・態勢の事前構築。 例：生産量調整機能の強化。 **【具体例】定量的な基準に基づく判断** （上記㋑のケース） ・Ｃ社は、新規事業への進出に当たり、全社的なポートフォリオの重要性に鑑み、当該事業の社内での位置付けを明確化することとし、**市場成長率と市場占有率の観点によるＰＰＭ**（プロジェクト・ポートフォリオ・マネジメント）(注) **の検証**等を行った。 ・その上で、価格、利回り（利益率を含む）、および取引事例などに関する**関連指標のモニタリング部署を設置**し、**月次の分析結果等の経営者への報告**を義務付けた。 （注）ＰＰＭ：ボストンコンサルティンググループが 1970 年代に提唱したもので、市場成長率と相対的市場占有率（トップ企業に対する自社の相対的占有割合）により、次の４つの象限における位置付けから、撤退等も含めた事業戦略を検討するマーケティング手法。 ㋐成長率：高、占有率：高 → 花形（star） ㋑成長率：低、占有率：高 → 金のなる木（cash cow） ㋒成長率：高、占有率：低 → 問題児（question mark） ㋓成長率：低、占有率：低 → 負け犬（dog）

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

質問・確認事項	課題・改善提言
（１）傍流部門を含めた網羅的な事業環境変化のモニタリング ・戦略と事業目標の達成に影響を及ぼす内外の大きな環境変化を傍流部門も含めて網羅的に認識するプロセスを事業活動に組み入れ、継続的に実施しているか。	・内外の環境変化のモニタリングについて、本流業務は事業活動に組み入れているが、傍流は組み入れていないため、傍流の変化の影響が認識できていない。 ⇒戦略と事業目標の達成に影響を及ぼす内外の環境変化について、本流だけでなく傍流もモニタリングする。 **【具体例】ネット通販への需要拡大の把握とそれに対応した投資シフト** ・製紙会社Ａ社は、紙の役割である㋐伝達（印刷用紙等）、㋑拭く、㋒梱包（段ボール等）の観点で、事業本部で受注状況をモニタリングし、管理部門で分析のうえ経営に報告している。 ・印刷物のデジタル化による環境変化をモニタリングする中で、本流㋐（印刷用紙等）は需要が減る一方、傍流㋒（段ボール等）はネット通販により需要が増加しており、十年内に本流㋐と逆転することに気付き、早い段階で傍流㋒の設備投資拡大にシフトした。これにより、他社が苦戦する中、大幅に収益が向上し事業目標を達成している。
（２）外部環境の変化を評価できる人材の確保 ・外部環境の変化が事業に与える影響を評価できる人材を確保しているか。	・外部環境の変化（サイバー攻撃の高度化）が事業に与える影響を評価できる人材がいないため、正しい評価を経営者に伝えられず、適切な経営判断が行えない。 ⇒より高次の次元からリスクテイクの判断を行うために、外部環境の変化を評価できる人材を確保する。 **【具体例】サイバーセキュリティをモニタリングする専門人材の配置** ・暗号資産（仮想通貨）業者Ｂ社は、サイバー攻撃での仮想通貨流出による業務停止を重大なリスクとし、有識者をＣＩＳＯ（Chief Information Security Officer）として任命し、配下にＣＳＩＲＴ（Computer Security Incident Response Team）を設置している。

	・ＣＩＳＯは、サイバーセキュリティに関する情報収集、当局の規制対応状況をモニタリングし、自社への影響や対策について評価のうえ、経営に伝えている。
（３）カルチャーの変化による影響のモニタリング ・カルチャーの変化が事業に与える影響をモニタリングしているか。	・M&Ａで企業を買収した際、カルチャーの変化による買収先企業の社員のモチベーションをモニタリングしていなかったため、退職者が続出し、期待するシナジー効果が得られていない。 ⇒カルチャーの変化が買収先企業の離職率や業績に与える影響をモニタリングする。 **【具体例】カルチャーの変化が買収先企業の定着率に及ぼす影響のモニタリング** ・人を大切にするカルチャーを持つＣ社は、M&Ａの際、カルチャーの親和性を重視している。 ・買収先企業のリストラをせず、高いモチベーションを保って力を発揮できるようにすることが自社の**カルチャー**であることを初期段階から丁寧に説明し、買収後もアンケートや面談によりモニタリングしている。 ・これにより、退職者は少なく、収益が向上し、高いシナジー効果が得られている。

原則１６　リスクとパフォーマンスをレビューする

質問・確認事項	課題・改善提言
（１）パフォーマンスをレビューする際に未達成項目を十分に分析する ・組織は、パフォーマンスをレビューする時に、未達成項目に関する要因分析を十分に行っているか。	・設定されたパフォーマンス目標(注)の遂行状況について、定期的なレビューは実施されているものの、未達成項目に関する要因分析が不十分なため、複数年にわたり同項目の改善が見られない。 （注）例えば、㋐資本効率や健全性、収益性などの財務的指標や、㋑市場シェアなどの成長性指標など。 ⇒パフォーマンスのレビューに際しては、未達成項目について具体的な取組内容の振り返りを実施する。また、外部および内部環境変化に伴うリスク要因の変化の有無や、リスク選好とリスクテイクの実態に乖離がなかったかについても検証する。 **【具体例１】中期経営計画の業績の振り返りと修正** ・Ａ社では３年毎に中期経営計画を策定するとともに、事業環境変化に対応すべく、毎事業年度ごとに業績の振り返りと要因分析、それらを踏まえた中期経営計画の修正を実施している。 **【具体例２】買収事業の成果の振り返りと翌期の事業計画への反映** ・Ｂ社では、事業買収後の定期的な買収成果の振り返りにより、当初想定した事業計画と実際の遂行結果との乖離を検証し、翌期以降の買収対象企業の事業計画策定において検証結果を考慮している。
（２）パフォーマンス目標の修正 ・設定された目標に対するパフォーマンスが、許容できる範囲内に収まっていない場合、必要な対応が講じられているか。	・パフォーマンスのレビューの結果、許容度を超える実績が判明したが、目標設定時には想定していなかったリスクの発生に対して適切な対応が講じられていないため、戦略および事業目標達成に懸念が生じている。 ⇒パフォーマンスが許容度を超える場合、もしくは当初とは異なるリスクプロファイル（リスクとパフォーマンスの関係）が判明した場合には、リスクに見合ったパフォーマンス目標の修正を検討する。

（３）パフォーマンスの継続的モニタリング ・パフォーマンスを継続的にモニタリングすることにより、新たなリスクの認識や、リスクの再評価を行っているか。	・設定された目標に対するパフォーマンスについて、継続的な分析態勢が整備されていないため、新たなリスクの発生の認識や、実際のリスクとリスク評価の乖離に対する再評価が実施されず、事業環境の変化に伴うリスク要因の変化が経営計画策定に考慮されていない。 ⇒パフォーマンスを継続的にモニタリングし、経営に重要な影響を及ぼすリスクの発生や変化を認識し、事業計画やパフォーマン目標に反映する態勢を構築する。 **【具体例１】重要リスクのモニタリング結果のパフォーマンスターゲット設定への活用** ・Ｃ社では、経営に重要な影響を及ぼすリスクについて、毎期「重要なリスク」として各事業部門がモニタリングの上、同リスクをリスク管理部門が特定し、リスク選好およびＫＰＩ（主要業績指標）等のパフォーマンスターゲットの設定を含む経営計画策定の際にこれらが考慮されている。 **【具体例２】財務パフォーマンスの継続的モニタリング** ・Ｄ社では、健全性目標としてリスク量に対する自己資本金額の比率を財務パフォーマンスターゲットとして設定し、当該比率の算出根拠となるリスク量および自己資本金額を月次モニタリングしている。 ・リスク量算出は計測モデルを使用しており、バックテストによってモデルの信頼性維持・向上を図っている。

原則１７　全社的リスクマネジメントの改善を追求する

質問・確認事項	課題と改善提言
（１）経営者による日常的モニタリング活動の結果のレビュー ・経営者が各階層の管理者による日常的モニタリング活動の結果をレビューしているか。	・経営者が各階層での日常的なモニタリング活動の結果をレビューしておらず、統制機能が十分であるか確認していない。 ・そのため業務の効率性・有効性の改善が行われず、パフォーマンスが向上しない。 ⇒経営者が各階層の管理者に日常的なモニタリング活動の結果を報告させ、自らモニタリング活動の状況をレビューし、必要な改善を促す。
（２）中長期的な視点での全社的リスクマネジメントの改善 ・全社的リスクマネジメントの継続的な改善活動は中長期的視点で行われているか。	・全社的リスクマネジメントを評価し改善を行っているが、単年度のパフォーマンスのみに基づいて行っているため、中長期的な改善の方向性を見誤っている。 ⇒全社的リスクマネジメントの評価および改善は、１～2 年程度の視点ではなく、中長期的な視点で行う。

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

質問・確認事項	課題と改善提言
（１）意思決定に有用な情報の収集と活用 ・組織を競争優位に導き、より機動的な意思決定を行うために役立つ情報を収集・活用しているか。	・組織を競争優位に導くために、事業を通じてどのような情報を収集、蓄積し、どのように活用すべきかが十分に検討されていない。 ・そのため、事業の展開や中長期的な戦略の構築に向けた意思決定に向けて、必要な情報を収集できていない、あるいは収集蓄積された情報が意思決定に有効に活用されていない。 ⇒経営者は、「㋐意思決定のどの段階で、㋑どのような結論を導くために、㋒どのような情報を、㋓どのように活用するか」という組織としての情報の活用に対する方針を明確に示す。 **【具体例】情報の有効活用を通じた競争優位の構築** ・小売りチェーンのＡ社では設立後早々に全店にＰＯＳシステムを導入し、日次の販売データを、どのように㋐市場環境の変化、㋑消費者の嗜好の変化等の察知あるいは、㋒将来的な変化の予測等に活用できるかを検討した。 ・日次の販売データおよびその蓄積されたデータを、売り場構成、商品開発、商品仕入れ、および新規事業の開発などの意思決定に活用しており、それにより、他社に対する競争優位の立場（同業他社に比して秀でた営業利益率、顧客リピート率、客単価等）を維持している。
（２）新たなテクノロジーの導入に伴うリスクの検討 ・新たなテクノロジーを開発、導入しようとする際に、新たなテクノロジーの開発・導入により発生する新たなリスク、コストなどの検討がなされているか。	・事業の効果的な運営に情報を有効活用することを目的として、他社に倣って新たな経営情報システムを導入したが、既存のシステムとの連携に不都合が生じ、その調整と再開発に多大な時間と費用が生じている。 ・そのため、業務活動に支障が生じる部分については、新システムが稼働するまでの間、既存のシステムをベースに適宜、エクセルを使用するなど、手作業的な対応をしている。 ⇒新たなテクノロジーを導入する際には、それに伴うリスク、コスト、および自社の既存のテクノロジーの活用を十分に検討する。

	【具体例】リスクの検討を踏まえた効果的なシステムの構築 ・小売りチェーンのＢ社では、設立後早々に全店に導入したＰＯＳシステムのデータを有効活用するために、大手情報機器メーカーと連携して経営情報システムの構築を進め、情報システムの高度化を図ってきている。 ・新たなシステムを追加しようとする際には、その開発・導入に伴い発生する可能性のあるリスクやコスト、既存のシステムとの連携などを十分に検討している。 ・それにより、業界で最高水準の情報システムを構築している。
（３）事業環境の変化に対応した情報システムの変更 ・情報を有効に活用できるように、事業環境の変化、事業構造の変化等に対応して、必要な情報システムの変更を行っているか。	・事業のグローバル化、事業領域の拡大など事業環境の変化が進んでいるが、情報システムは各地域、各社ごとに自律的かつ独立性を尊重され、必要な変更が行われることなく運用されている。 ・そのため、情報の共有・活用は、連結会計に係る情報など一部のものにとどまり、大半の情報についてはグローバルに共有、活用できる体制になっておらず、事業運営の意思決定に有効活用できていない。 ⇒情報をグローバルに共有、活用できるように、事業環境の変化に対応して情報システムに適宜、必要な改善を加える体制を構築する。 **【具体例】事業環境の変化に対応した情報システムの変更** ・Ｃ社では、事業のグローバル化、事業領域の拡大が進む中で、事業に係る情報をグローバルに共有し、活用することを目的に、本社の情報システム管理部門・事業企画部門が中心になり、関係各部署およびグループ各社とも連携を取りながら、情報システムに必要な変更・修正を加えている。

原則１９　リスク情報を伝達する

質問・確認事項	課題・改善提言
（１）リスク情報伝達の責任部門と適切な伝達経路を設定する ①リスクマネジメントに係る情報の社内伝達について、その**職責職権はどの組織が担って**いるか。 （注）監査対象部門により、Who/What/How 質問（どこにやらせていますか。）と Yes/No 質問(あなたの部門ではＸＸを行っていますか。)を使い分ける。 ②責任部門は、リスク情報の社内伝達につき、それぞれの**内容に適した伝達経路**を使っているか。 （注）サンプル調査により**伝達状況を検証**することも考えられる。	①**リスクマネジメント統括部門または統括的規程がなく**、各部門が自部門のリスクについて**自部門の判断で伝達**しているため、同種の情報でも**伝達する部門としない部門**が生じている。 ⇒**統括部門または統括的規程の必要性**についての検討を経営者に具申する。 また、リスクマネジメント統括部門等がある場合には、**統括部門の機能を調査**する。 ②内容と**伝達経路について特段の検討を行っていない**ため、㋐**必要な情報**が**必要な職責職権を持つ職制**に適時に**伝達される**ことが確保されていない、または㋑**不必要な情報**が**適切な職責職権を持たない職制**に**伝達されない**ことが確保されていない。 ⇒経営者に、**伝達経路の有効性の検討**を具申する。 **【具体例】全社リスクマネジメント統括部門への情報伝達管理責任の付与** ・Ａ社は、**全社リスクマネジメントを統括する部門**を持ち、リスクマネジメントに係る**情報の伝達管理については、統括部門が責任を担って**いる。
（２）受け手のリスク対応に役立つ情報を伝達する ・**伝達される**全社的リスクマネジメントに係る**情報は**、㋐位置付け、㋑目指すべき価値、㋒目指すべき企業文化、㋓行動基準、㋔リスク選好、および㋕目指すべき管理レベルなどを含み、かつそれぞれに矛盾がなく、社内の全ての部門や全ての構成員がそれぞれの**司つかさにおけるリスク対応を適切に遂行できる内容**となっているか。 （注）**伝達されている内容の有効性**を分析し評価するが、例えば**目指すべき企業文化の内容自体**や**リスク選好レベル自体**の判断は、内部監査のスコープには通常含まれないことに留意する。	・司つかさに**伝達された情報の内容が、過度に抽象的で具体性が乏しい**、あるいは**矛盾が含まれている**等の結果、**リスク対応を適切に遂行**できるものなっていない。 ⇒情報の発信責任者に対し、以下の２点を提言する。 ㋐**内容**の再検討。 ㋑**発信時の内容検討手順**の見直し。 **【具体例】全社リスクマネジメント統括部門による情報モニタリング** ・Ｂ社の**全社リスクマネジメント統括部門は**、第１線の各事業本部および第２線の各管理本部に対し、㋐**リスクマネジメントに係る全社的方針等を伝達**すると

	共に、㋑各本部が伝達する具体的情報についてモニタリングし、その有効性の評価を各本部にフィードバックしている。
（３）情報が必要な階層に伝達されていることを検証する ・情報の発信責任部門は、必要な階層に情報が伝達されていることを定期的に検証しているか。 （注）上記（１）②のサンプル調査のスコープに含むことも考えられる。	・必要な階層に情報が伝達されているか定期的な検証が行われていないため、一部に情報が伝わっていないことが認識されていない。 ⇒情報の発信責任部門に対し、必要な階層に情報が伝達されていることを定期的に検証することを提言する。 **【具体例】企業理念と行動基準の理解の定期的な検証** ・Ｃ社は、企業理念と行動基準の理解について、年に１度、従業員からオンラインでフィードバックを取り、回答を分析し、その結果を理解を深めるための対策に活用している。
（４）社外に発信する各種情報の整合性を確保する ・各部門が自部門の判断で社外ステークホルダーに発信する業務レベルの各種のリスクマネジメントに係る情報について、その職責職権はどの組織が担っているか。 （注）仕組みの聞取りと、実際の社外発信情報の分析とを並行して行う。	・各部門が発信する情報が、発信部門によって整合しない結果、社外ステークホルダーに誤解を与える可能性がある。 ⇒リスクマネジメント統括部門に対し、各部門が社外に発信する各種のリスクマネジメントに係る情報の整合性を確保するための枠組みの整備を関係部門と調整するよう提言する。 **【具体例】各部門の社外発信情報はリスクマネジメント統括部門と協議** ・Ｄ社では、コンプライアンス統括部門、法務統括部門、財務統括部門、環境統括部門等が、それぞれの担当項目について社外への情報発信の責任を持っている。 ・しかし、リスクマネジメントに係る情報については、各担当部門はリスクマネジメント統括部門と協議したうえで情報発信を行い、社外に発信する情報の整合性を確保している。
（５）経営者の意図に沿わない情報の社外発信を防止する ・各部門が自部門の判断で社外ステークホルダーに発信する経営レベルのリスクマネジメントに係る情報について、その内容が経営	・各部門が発信する情報の内容が、経営者の意図と異なっている。

者の意図を適切に表していることを確保するために、どのような手順を踏んでいるか。	⇒経営者に対し、社外ステークホルダーに経営レベルのリスクマネジメントに係る情報を社外に発信する際の統括部門、および規程または手順の設定を具申する。 **【具体例】経営レベル情報の社外発信時におけるリスクマネジメント統括部門による調整** ・Ｅ社では、全社リスクマネジメント統括部門長が、経営者と直接のレポーティングラインを持ち、経営者の意図を十分に把握した上で、経営レベルのリスクマネジメントに係る発信情報の内容について各部門と調整を行っている。

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

質問・確認事項	課題・改善提言
（１）取締役会への報告を戦略・事業目標・リスク・パフォーマンスに関連付ける ・取締役会への報告内容が、戦略、事業目標、リスク、およびパフォーマンスに関連付けた内容となっているか。	・取締役会において承認決議や個別案件の議論に多くの時間が割かれているため、事業全体の戦略や事業目標に係る議論が十分に行われていない。 ⇒取締役会へ事業全体の戦略および事業目標を達成したときのパフォーマンスやそれらの目標を達成するために生じうる潜在的なリスクの影響度を報告する。
（２）報告の利用者とその役割を認識する ・報告にあたり報告の利用者とその役割を明確に想定しているか。	・報告にあたり具体的な報告利用者を想定していないため、報告がすべての利用者に対して一律の内容で報告が行われている。 ⇒報告の利用者（取締役会、上級経営者、部門のマネージャー、リスクの専門家等）により有用な情報は異なるため、報告の利用者を明確にしたうえで報告を行う。 **【具体例】報告の利用者に応じた情報提供の仕組みの構築** ・Ａ社では、重大リスク問題の発生を受けて、リスク（㋐ストラテジーリスク、㋑カルチャーリスク、㋒プロセスリスク）と、リスクに対応する階層（㋐経営者、㋑事業本部長・事業部長、㋒実務者）との関係を整理し、権限と責任の所在に応じて各階層に必要な情報が提供される仕組みを構築した。
（３）利用者のニーズに合った報告の内容と頻度 ・報告された情報の内容（詳細さや提供形態等）と頻度は報告利用者のニーズに合致しているか。	・報告の内容と頻度が利用者のニーズに合っていないため、報告が活用されていない。 ⇒報告利用者と意思疎通を図り、提供する情報について、その**内容**と**頻度**が利用者のニーズに合ったものとする。

４．参考文献

・トレッドウェイ委員会組織委員会（COSO:Committee of Sponsoring Organizations of 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）

・ポール・ソーベル著　八田進二監訳　堺咲子訳
「**不確実な時代のリスクマネジメント　―ＣＯＳＯ新ＥＲＭフレームワークの活用**」　（2018年8月　日本内部監査協会出版）

・トレッドウェイ委員会組織委員会（COSO:Committee of Sponsoring Organizations of 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）

以　上