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 ～

社団法人 日本内部監査協会
ＣＩＡフォーラム ＥＲＭ研究会 Ａ分科会
２０１０年１月

「ＣＩＡフォーラム」は、ＣＩＡ資格保持者の研鑽および相互交流を目的に活動する、社団法人日本内部監査協会（IIA－JAPAN）の特別研究会である。各研究会は、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る。この研究報告書は、ＣＩＡフォーラム「ＥＲＭ研究会　Ａ分科会」が、その活動成果として取り纏めたものである。報告書に記載された意見やコメントは、研究会の「見解」であり協会の見解を代表するものではなく、協会がこれを保証・賛成・推奨等するものでもない。

目　次

はじめに

１．ＥＲＭ研究会の活動の経緯

２００４年９月にＣＯＳＯ－ＥＲＭ（Enterprise Risk Management＝全社的リスクマネジメント）が公表されて以来、ＥＲＭに対する我が国企業の関心が高まっている。また、内部監査人協会（ＩＩＡ）が制定した「内部監査の専門職的実施の国際基準」では、内部監査部門の重要なミッションの一つがリスクマネジメントの実施状況を評価し、その改善に貢献することと定められている。公認内部監査人有資格者（ＣＩＡ）で構成される当ＥＲＭ研究会は、内部監査人の立場からＣＯＳＯ－ＥＲＭの実施体制の整備・運用に寄与するため、以下のように研究を実施して来た。

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（全社的ﾘｽｸﾏﾈｼﾞﾒﾝﾄ）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 ～（本報告）	ＥＲＭ的な考え方を取り入れた内部監査の価値向上

２．法対応の内部統制からＥＲＭへ

２００６年５月に施行された会社法により大会社に取締役会決議が義務付けられた内部統制システム整備の基本方針、および２００８年４月から適用開始となった金融商品取引法に基づく内部統制報告制度への対応を通して、日本の企業では内部統制への理解が高まったことはもとより、リスクとコントロールおよびそれらを把握し評価するノウハウや手法の習得も深まっている。ＣＯＳＯ－ＥＲＭは、内部統制を包含したものであることから、日本の企業において内部統制に対する理解とノウハウ・手法の習得が進むことにより、ＥＲＭの実施体制の整備・運用が進んでいくと当研究会は考えている。

３．ＥＲＭに対して内部監査部門の果たすべき役割

ＥＲＭに対して内部監査部門が果たすべき役割は以下の３点であると当研究会は考えている。

（１）ＥＲＭに対する監査　（主に保証＝アシュアランス）

ＥＲＭに対する監査とは、ＥＲＭの有効性を独立した立場で評価し、経営者に対してＥＲＭの現行水準を保証するとともに、改善すべき点がある場合には有効な改善提言を行うことによりＥＲＭの水準向上を図ることである。ここで、ＥＲＭの有効性の評価とは、ＥＲＭの８つの構成要素の全てについて、その整備状況および運用状況の有効性を評価することである。

（２）ＥＲＭの整備・運用への助言（コンサルティング）

（３）**ＥＲＭ的な視点を取り入れた内部監査を行うことにより、内部監査の質を高め、企業目標の達成に寄与すること**

４．本報告書の目標について　～従来の内部監査に“ＥＲＭ的な要素”を加味した「良い内部監査」の提唱

日本の企業では、金融機関や総合商社の一部を除き、ＥＲＭを導入している企業はまだ少数であり、内部監査部門が自社のＥＲＭを監査するケース（上記３．（１））は少なく、ＥＲＭに対する監査は研究会のテーマとしては時期尚早であると判断した。また、独立性・客観性を侵さない範囲でのＥＲＭ整備・運用に寄与するコンサルティング活動（３．（２））は、一部の先進的な内部監査部門が実施しているが、これについては別の機会に研究することとなった。

そして最終的に、内部監査人としての本分である**内部監査にＥＲＭ的な視点を取り入れる**ことによって、より**監査の価値を高め、企業目標の達成に寄与**することができるのではないかという思いに至った。つまり、今までの監査に**ＥＲＭ的な要素を加味**する工夫によって、いわゆる**「良い内部監査」**を実現できると考えたわけである。また、そのような内部監査を通して、経営者や被監査部門に対し、ＥＲＭ実施体制の整

備・運用の重要性を認識してもらう副次的効果も期待できると考えた。以上の結果、ＥＲＭに対する内部監査部門の役割の第一ステップとして、上記３．（３）すなわち、「ＥＲＭ的な視点を取り入れた内部監査を行うことにより、内部監査の質を高め、企業目標の達成に寄与すること」を本報告の目標として設定した。

（参考）【良い内部監査】とは？？

（１）被監査部門にとって

・被監査部門の**納得感**のある監査
・監査結果に、心から**共感**を得られる監査
・監査を受けて**良かったと思われる**監査
・**自発的な改善意欲**をもたらす監査

なお、これらを実現するために、内部監査人は以下のようにコミュニケーション上の態度にも留意する必要がある。

・被監査部門に**敬意**を持って接する。
・積極的に**傾聴**する。
・**事実**で物を言う。
・正論で**追い詰めない**。
・信頼できる**カウンセラー**や**コンサルタント**として振舞う。

（２）経営者にとって

経営者にとって内部監査は、自分の目や耳の役割に相当するといわれている。内部監査によって目的と現状とのギャップを浮き彫りにできたり、思わぬ視点からの改善提案を受けた場合には、経営者は内部監査に対する信頼感を深めるであろう。つまり、企業目標を達成するための**適切な組織運営**が実施されているかを**評価**し、かつ必要な場合には適切な**改善提案**を行うことが重要であり、それが【良い内部監査】である。

（３）内部監査部門にとって

【良い内部監査】は、内部監査部門にとっても重要な目標となる。内部監査部門の存在価値は、経営者と被監査部門の評価によって決まる。両者から継続的に高い支持を獲得し続けなければならない。また、両者からの支持があってこそ良い人材や十分な予算がもたらされる。更には、円滑で協力的な監査活動も約束される。そのために内部監査部門は、定まった監査方式に安住することなく、【良い内部監査】を目指して常に革新していく気概が必要である。

日本内部監査協会 ＣＩＡフォーラム ＥＲＭ研究会　Ａ分科会（第５期）会員

	氏　名	所　　属
全体総括	吉野 太郎	東京ガス株式会社 ＩＲ部 リスク管理グループ 主席
座長	大野　勝	コニカミノルタヘルスケア株式会社 常勤監査役
ﾒﾝﾊﾞｰ	金井　智	スターティア株式会社 内部監査室長
ﾒﾝﾊﾞｰ	河岸 満俊	エレマテック株式会社 内部監査室長
ﾒﾝﾊﾞｰ	紀谷 倫有	中外製薬株式会社 監査部課長
ﾒﾝﾊﾞｰ	坂井 香苗	日本電気株式会社 経営監査本部 監査エキスパート
ﾒﾝﾊﾞｰ	竹村 仁一	株式会社ＦＰＧ 内部監査室長
ﾒﾝﾊﾞｰ	常橋 直弓	株式会社ベネッセコーポレーション 経営監査部
ﾒﾝﾊﾞｰ	福井 良一	東洋エンジニアリング株式会社 総務担当部長
ﾒﾝﾊﾞｰ	三神　明	三菱商事株式会社 監査部 関係会社内部監査推進室 次長
ﾒﾝﾊﾞｰ	矢島 博之	キリンホールディングス株式会社 経営監査部 主幹

ﾒﾝﾊﾞｰ氏名は 50 音順

ＥＲＭ的視点を取り入れた内部監査の手法

現在、多くの日本企業において本格的なＥＲＭの導入は未実施の状況であると思われる。しかしながら何らかのリスクマネジメントは実施していると思われるため、本研究会は以下のような企業を想定してこの研究を実施した。以下のような状況においても、内部監査部門としてＥＲＭ的な視点を取り入れれば、「良い内部監査」に近づくことができると考えたのである。

前提とする企業のリスクマネジメント実施状況の想定

- **各部門がリスクを個別的に管理する、従来型のリスクマネジメント（サイロ型リスクマネジメント）を実施しており、全体のリスクを統合的に管理するまでに至っていない。**
- **経営として管理すべき重要なリスクを特定していないか、特定していても社内で共有化されていない。**
- **リスク管理規程がないか、ある場合でも十分に機能していない。**
- **したがって、内部監査部門はＥＲＭの実施状況の評価を行おうとしても、監査としてなじまない状況にある。**
- **ただし、経営者は現状のリスクマネジメントを改善する必要性を感じている。**
- **監査役設置会社である。**

上記前提を踏まえ、これから述べる研究内容は、ＥＲＭの８つの構成要素ごとに以下のような順番で構成している。

- ＥＲＭの構成要素の定義、要約
- **＜ＥＲＭ監査の主なチェックポイント＞**：本格的にＥＲＭ実施体制を評価する場合の主なチェックポイント
- **＜ＥＲＭ的視点を取り入れた内部監査の例＞**：従来の監査にＥＲＭ的な要素を加える工夫をして、良い内部監査を目指した具体例やノウハウ、及び改善提言を行う上での参考になる事項

（注）なお＜ＥＲＭ監査の主なチェックポイント＞と＜ＥＲＭ的視点を取り入れた内部監査の例＞の各項目は、１対１で連動しているわけではない。

１．内部環境

内部環境は、**組織の気風**を組み込み、組織を構成する人々の**リスクに対する意識**に影響を与えるとともに、**ＥＲＭのすべての構成要素の基礎**をなし、**規律**と**構造**を提供するものである。内部環境要因には、企業の**リスクマネジメントの考え方**、**リスク選好**、**取締役会による監視**、企業に属する人々の**誠実性・倫理観・専門能力**および経営者が**権限と責任**を従業員に**割り当て**、彼らを組織しその**能力を開発**する方法が含まれる。

＜ＥＲＭ監査の主なチェックポイント＞

（１）リスクマネジメントの考え方

・経営陣から第一線の社員まで企業に属する者全員が、戦略の策定・実行から日常業務の遂行に至る企業活動のあらゆる場面で、**リスクをどのように考えるのか・考慮するのかについて共通の考え方や姿勢・信念**（以下、「**リスクマネジメントの考え方**」という）を共有しているか。持っている場合にはそれはどのようなものなのか。

・リスクを管理する際、もしくは議論する際に、自社のリスクマネジメントの考え方に基づいて行っているか。

・経営陣からリスクマネジメントの考え方についてどのような**メッセージ**が発信されているか。また、メッセージは社員全員に周知され、理解されているか。

・企業全体として**リスク**に対しどのような**認識**を持っているか。また、社員一人一人がリスクに対してどのような認識を持っているか。

（２）リスク選好[注]

・自社の**リスク選好**は**明確**になっているか。それは**どのようなもの**なのか。また、それは**明文化**されているか。

・戦略策定の際に、**戦略**によって期待されるリターンと想定されるリスクが、自社の**リスク選好**と**整合**するように検討・調整されているか。つまり、**戦略**は**リスク選好**と**整合**しているか。

・戦略において、**リスク選好**が**明確**になっているか、つまり**許容できるリスク**と**許容できないリスク**が**明確**になっているか。

【リスク選好の具体例】

①株主資本利益率１５％を達成するための新しい施策を実施することにより生ずる**リスクを受け入れる**。

②生産拡大のため、多額の資本を投入して、新たな資産、人材等に投資する**リスクを受け入れる**。

③市場シェアの増加と引き換えに売上高利益率が減少する**リスクを受け入れる**。

④製品の品質低下**リスクは受け入れない**。

＊注：リスク選好とは、企業が価値の追求のために、意図的に受け入れたいと考えるリスク総量のことである。「ビジネスモデルとして、どのような（どの程度の）リスクを取るか」という戦略レベルの概念である。

（３）取締役会・経営会議

・取締役会や経営会議に、**社内外の重要な情報**や、**重要なステークホルダーのニーズや期待**が**適時・適切に報告される仕組み**があるか。

・取締役会および経営会議への**付議基準**は明確に定められているか。

・経営者に対する監査機能を果たす独立的な**社外監査役**（あるいは**社外取締役）のサポート体制**は十分であるか。

（４）誠実性と倫理観

・**社員行動基準**や**倫理基準**は制定されているか。

・社員行動基準や倫理基準では、**法令遵守以上の誠実性・倫理性**を求めているか。

・社員行動基準や倫理基準の**遵守**について、常にメッセージが発信され、**周知徹底**されているか。

・社員行動基準や倫理基準が**遵守**されていることをどのように**確認**しているか。

・**コンプライアンス統括（担当）部門**は、適切に**機能**しているか。

・**経営者自ら**が**率先**して社員行動基準や倫理基準を**遵守**し、その重要性を**強調**していることが、社内に十分に**伝達**もしくは**周知**されているか。

（５）専門能力に対するコミットメント

・社員は割り当てられた職務を達成する上で必要な知識、経験、スキルなどの**専門能力**を**有して**いるか。

・特定の職務に**必要な専門能力の水準**は**具体的に定められて**いるか（明文化されているか）。

・必要な知識・スキルを習得するための**教育**や、必要な経験を得るための**育成ローテーション**は計画的に実施されているか。

（６）組織構造

・**権限**と**責任**は明確に**定められて**いるか。

・**報告ライン**は**確立**されているか。
・組織構造は、当該部門・会社の**規模**や**活動の性格**に**合致**したものであるか。
・リスクマネジメントを主管する公式な組織が存在するか。
・期待される水準のリスクマネジメントを実施するために必要なリスク管理体制を有しているか。

（７）権限と責任の付与

・プロセス管理者が**問題への取組み**や**問題の解決**に当たって**イニシアティブ**を**発揮**できるように必要な**権限と責任**が**付与**され、かつそれ（権限と責任の付与）は**必要な範囲**に**制限**されているか。
・権限と責任の付与に当たっては、プロセス管理者に付与された権限はもとより、上位者への**報告責任**と上位者による**承認**が**規約**（職責権限）として**定められて**いるか。
・また、権限と責任の付与に当たっては、**適切な職務遂行**、中心的な人物の**知識や経験**、必要な**経営資源**について記載した**方針文書**が策定されているか。
・社員は、**自分の業務**がいかに組織内で**相互に関係**し、また組織**目標の達成**にいかに**貢献**しいているかを**理解**しているか。
・リスクマネジメントの実施に必要な権限が、プロセス管理者に適切に委譲され、かつプロセス管理者は、リスクマネジメントの実施状況についての説明責任を適切に果たしているか。その結果、権限委譲による業務の効率的な遂行と、説明責任による業務の適切な管理が両立しているか。

（８）人的資源に関する基準

・被監査部門の採用、教育・研修、業績評価、昇進、報酬、懲戒など**人的資源に関する基準**は、自社全体の**誠実性**、**倫理的行動**、および**専門能力**に対する**期待水準**（必要水準）を満たしているか。
・リスクマネジメントを実施するために十分な**人的能力**が存在するか。
・主要な業務におけるリスクマネジメントの実施に必要な**人材の採用・育成**が計画的に行われ、質量ともに必要な人材が確保されているか。
・主要な業務では、急な退職・休職による要員減少に伴う、リスクマネジメントへの悪影響を許容可能な水準に抑制できる最低限の**代替要員**が確保されているか

・専門性が高く特定個人に依存しているため他の者では代替が困難な重要業務については、**業務引継ぎ書**が整備され、また**代替人材**の育成が行われ、当該担当者の急な退職・休職に伴う重要業務におけるリスクマネジメントへの悪影響を許容可能な水準に抑制できる体制が整備されているか。

＜ＥＲＭ的視点を取り入れた内部監査の例＞

（１）リスクマネジメントの考え方

・リスクをどのように認識しているか、どの程度リスクをとって行こうとしているか、どの程度まで許容できるか等のリスクマネジメントの考え方は、経営活動全てに反映される。内部監査部門は、経営陣へのインタビューや経営陣からのメッセージあるいは発信文書をレビューすることにより、**経営陣**の**重要リスク**や**リスクマネジメントについての認識、リスクに対する選好**を確認する。また、社員意識調査等をレビューすることにより、**社員**の**リスクに対する認識**や**考え方**を確認する。経営者と社員のリスク認識の**ギャップが大きい事項**については、リスクマネジメント上の問題点として、内部監査の重点項目とすることを検討する。

（２）リスク選好

・リスク選好は、企業が価値追求のために意図的に受け入れたいと考えるリスクの量であるが、金融機関、総合商社などの業種を除き、明確に認識されていない場合が多い。この場合、内部監査部門は、どのようにしたら良いか？　戦略にはリスク選好が反映されていることが多いため、**戦略からリスク選好を読み取る**ことができる。また、**経営陣**にリスク選好について**インタビュー**することも有効である。

（３）取締役会・経営会議

・必要なリスク情報が取締役会や経営会議に伝達されず、取締役会や経営会議のリスクマネジメントに対する監督機能が働かない場合がある。内部監査部門は、**取締役会や経営会議**の**議題・資料・議事録**を閲覧することにより、議案に取締役会や経営会議が適切な審議・判断を行うために**十分なリスク情報が盛り込まれているか**を確認するとともに、**議案**を上程する際に、**リスク情報を盛り込むことが標準化されているか**を確認する。また、重要な**リスク情報**が、正確かつタイムリーに、取締役会や経営会議に**伝達**されているか確認する。

（４）誠実性と倫理観

・従業員は、善悪について又はリスクおよびコントロールについて経営者が示す態度と同じ態度をとる傾向があるため、内部監査部門はまずは経営者の誠実性や倫理観の現状を念頭に置いておく必要がある。そして、**経営陣へのインタビュー**や**経営者からの発信文書をレビュー**することにより、**経営者の誠実性と倫理観についての期待**を確認する。その後、**社内通知**や**社内規則、関係会議資料をレビュー**することにより、**社員行動基準**の**策定**及び**周知**状況や**統括部門の役割**を確認し、それらが経営者の誠実性と倫理観についての**期待を満たしているか**確認する。

（５）権限と責任の付与

・社員の職務権限の範囲が明確でないことが原因で、それぞれの責任の範囲が不明確となり、不祥事発生の防止に必要な牽制が働かず、結果として不祥事が発生する場合がある。内部監査部門は、**職務権限規程**で**職務権限**が明確に**定められて**いるか、また規程は**定期的に見直し**が行われているかを確認する。

・更に、職務権限規程に準拠して職務が執行されていることと、上位者に適切な結果報告が行われているかを確認する。

（６）監査役と内部監査部門の連係

・経営者の暴走による不祥事発生のリスクを低減するためには、経営者を監督または監視・検証する仕組みが必要である。監査役は、取締役の職務の執行を監査、すなわち監視・検証するための法定機関として会社法上位置付けられている。内部監査はコーポレートガバナンスの重要要素として位置付けられるが、あくまで使用人の立場であり、それ自体として経営者に対する牽制機能を発揮することは困難を伴うため、**監査役と内部監査部門の連係**が重要である。そのためには、監査役と内部監査部門は、**定期的な連絡会**の開催等により、社内外の**リスク情報を共有**することが必要である。

・その結果、監査役は内部監査部門から報告を受領することにより、取締役の業務執行に関する監査の意見形成に資する情報を得ることができる。また、内部監査部門は、監査計画の策定、監査の実施、予算等に関して監査役から支援を受けることにより、その機能と独立性を強化することができる。

２．目的の設定

目的は最初に**戦略目的**が設定され、それに基づいて、**関連目的**、すなわち、**業務目的**、**報告目的**、**コンプライアンス目的**が設定される。そのため、戦略目的は他の３つの目的の基礎となる。目的の設定は、ＣＯＳＯ－ＥＲＭの構成要素である「**事象の認識**」、「**リスクの評価**」、「**リスクへの対応**」を行うための**前提**となる。また、目的は企業のリスク選好とその方向性が合致するように設定される。

参考【関連目的】
（１）業務目的
　業務目標や収益目標および資源の損失に対する防止策などを含んだ、業務の有効性・効率性の向上に直結する目的。事業環境、産業環境、経済環境の特有の要因を反映して設定される。
（２）報告目的
　必要な情報が網羅的かつ正確に伝達できるように設定される目的。報告目的には内部用報告、外部用報告、また財務情報および非財務情報が含まれる。
（３）コンプライアンス目的
　企業が行動する上で最低限の基準となる、関連する法令や規則に準拠するよう設定される目的。

＜ＥＲＭ監査の主なチェックポイント＞

（１）戦略目的の設定

・経営者は企業の**ビジョンやミッションに基づく戦略目的**を設定しているか。
・**戦略目的の設定プロセス**は定められているか。

（２）関連目的の設定

・戦略目的に沿って、企業全体や各部門など**各階層**において**目的**が**設定**されているか、また**各階層間**での目的は**整合**しているか。
・目的は、環境の変化に応じて**定期的に見直され**、常に最新の経営環境に対応したものになっているか。
・従業員は、企業全体や部門の目的を必要な範囲で理解し、**達成すべき目標**レベルとその**測定方法**を**共有**しているか。

（３）目的の達成

・取締役会および経営会議が、**目的の進捗状況**をタイムリーに**確認**できるように**適時・適切な報告**が行われているか。

（４）リスク選好

・前項１．の「内部環境」で述べられている**リスク選好**と**方向性**を合わせた**目的設定**となっているか。また、その際に**許容可能なリスクの範囲**を**設定**しているか。

（５）リスク許容度*

＊注：リスク許容度とは、企業として受け入れることができるリスクの限界レベルのことである。「許容できる、業績指標の変動幅」のような戦術レベルの概念である。

・**リスクの許容水準**（**リスク許容度**）が明確に**定められて**いるか。

【リスク許容度の具体例】

①販売数量、売上高、利益の許容される最低水準

②経営指標（ＲＯＡ、ＲＯＥ等）の許容される最低水準

③支出限度額、取引限度額、信用供与の限度額

④許可される取引や禁止される取引の種類

⑤許容される財務格付の水準

・**リスク許容度**と**リスク選好**の**方向性**は合致しているか。

・設定された**リスク許容度の範囲内**で業務が行われているか。

・リスクを**許容度の範囲内**に**コントロール**する**リスクマネジメントプログラム**を策定しているか。

・策定した**リスクマネジメントプログラム**を計画通りに実行し、リスクを**許容度の範囲内**に**コントロール**しているか。

＜ＥＲＭ的視点を取り入れた内部監査の例＞

（１）戦略目的・関連目的の理解

・**戦略目的**は、企業内のすべての活動を方向付けるものである。戦略目的は、より具体的な経営目的や部門別目的といった**関連目的**にブレイクダウンされ、事業や業務の指針となっていく。監査に当たっては、まず**戦略目的**と**関連目的**を十分に**把握**し**理解**することが必要である。それにより、たとえばリスクアプローチによって被監査部門を特定する場合には、リスクの観点をより明確にすることができる。また問題発見や指摘においても、単に当該部門に起因し単独で解決すべき問題か、上位部門や関連部門の目的達成にも関わる重大な問題かといった見方が可能になる。

・**目的の理解**は準拠性監査の場合でも重要である。業務がルール通りに行われていない場合、内部監査人自身が**ルールの目的**を**部門や企業全体の目的と結びつけて理解**していることで、単にルール違反の指摘にとどまらず、ルール遵守の重要性をより説得力をもって被監査部門に説明することができる。

（２）上位組織・下位組織の目的や関連部門の目的との関係把握

・目的は相互に関連するため、被監査部門単独の目的に限定せず、**上位組織･下部組織の目的**や**関連部門の目的**との**関係**を**把握**することにより、被監査部門の目的に関する理解が深まる。

例１：ある事業本部を監査する場合には、その**下位組織**の事業計画書等を収集し、下位組織の目的を集約してみて事業本部としての目的達成に**つながるか**を確認する。

例２：ある組織を監査する場合には、**上位組織**の事業計画書等を収集し、当該組織の目的が上位組織の目的と**一貫しているか**を確認する。

例３：ある一部門を監査する場合には、**関連部門**の事業計画書等を収集し、当該部門の目的が関連部門の目的と**一貫しているか**を確認する。

（３）目的設定プロセスの確認

・妥当性を欠いていると思われる目的に対して内部監査部門が目的そのものに何らかの問題指摘をするのは難しいが、**目的設定**の**手続**や**プロセス**を**確認**することにより、**目的の妥当性**（合理性）が見えてくる場合がある。たとえば新規事業において、事業承認の決裁書レビューや関係者へのインタビューなどによって**目的**や**達成目標レベル**の**設定根拠**を**確認**していくと、ある部門では市場調査や分

析に基づき売上利益計画を策定しているが、他の部門ではまず黒字化ありきで機械的に目標数字を記載していることが見えてくる場合がある。

（４）目的の共有

・目的の関連性や整合性に疑問がある場合、当該部門内に上位の目的や関連部門の目的が周知されているかを、関係者にインタビューすることで確認してみる。すると、それらの目的が知らされていない、また目標数字だけが与えられ戦略らしきものが見当たらないなど部門間での目的共有の問題点が明らかになる場合がある。

（５）目的達成度の測定方法の確認

・目的は、達成度の評価が行えるように、測定可能なものであることが望ましいが、定性的なものである場合も多い。定性的な目標の妥当性を評価する場合には、関係者へのインタビューによって、**ゴールイメージ**が**客観的**に**想定**されているかを確認する。たとえば達成目標が「サービス品質の向上」としか示されていない場合、どのサービスを指すのか、比較するものはあるか、誰が判断するのか、などを確かめることにより、目標の妥当性を評価することができる。

（６）リスク許容度

・バランスの取れた監査上の判断を下すためには、内部監査部門は、**経営者のリスク許容度**について適切に**理解**していることが重要である。

・企業はその事業環境などから、**ある法律に対して暗黙のうちにリスク許容度が少ない場合**があり、会社の習慣、社是、ルール（行動規範）などから把握しておく必要がある。（以下は例）

①建設、機械製造業における独禁法
②情報・通信、教育産業における個人情報保護法
③製薬業における薬事法
④食品製造、外食産業における食品衛生法
⑤商社、精密機器製造業における外為法（安全保障貿易管理）

・多くの部門では**業務管理指標**（コスト・品質・納期、ミス発生率、顧客クレーム件数など）を定めているが、これらの指標が**リスク**

許容度（「ミス発生率〇%以内」など）を示している場合があるので、監査においてこれらの指標の運用について確認する。

・業務管理指標が、**許容範囲**を示すのか、**達成目標**を示すのか不明確になっている場合には、指標設定の目的を確認する。また、併せて「リスク選好」や「リスク許容度」という考え方を説明する。

・経営陣へのインタビューや取締役会、経営会議等の重要会議の議事録の閲覧により、**経営者がリスクの許容度を設定するために必要なリスク情報**が、正確かつタイムリーに、**経営者**に**提供**される仕組みが整備されているかを確認する。

・他方、社内通知や社内ガイドライン等をレビューすることにより、**経営者が設定したリスク許容度**が、正確かつタイムリーに、**社員**に**伝達**される仕組みが整備されているかを確認する。

３．事象の識別

企業は、その戦略を実行したり、目的を達成したりしようとするときに、戦略の実行や目的の達成に影響を与える潜在的な**事象**を**識別**する。そして、**潜在的にマイナスの影響をもつ事象**が**リスク**であり、**潜在的にプラスの影響をもつ事象**が**事業機会**である。**事象**とは、戦略の実行や目的の達成に影響を与える**内部要因**又は**外部要因**から生じる出来事であり、**事象の識別**とは、どのような**要因**が**リスク**や**事業機会**を**生む**のかを識別することである。

＜ＥＲＭ監査の主なチェックポイント＞

（１）内部要因・外部要因の変化の把握

・自社の事業や業務に大きく影響する**内部環境の変化**や**外部環境の変化**を**把握**しているか。

・**環境変化による影響度**や**環境変化への対応**状況等について**把握**しているか。

（２）事象の特定

・**事象の特定**のために適切な**手法**が定期的、継続的、組織的に用いられているか。

・**過去の事象**に着目するとともに潜在的な**未来事象**も考慮しているか。

・事象の特定は、**現場からの積み上げ**方式で行うとともに、**トップダウン**でも実施しているか。

（３）事象の分類

・**事象**は、事象間の**相関関係**が**理解**でき、リスク管理に関するより高度な**情報**が**収集**できるように、**分類**されているか。

・事象を集約する際に、**水平的**（組織毎、組織間）かつ**垂直的**（職階毎、職階間）に事象を**捉え**ているか。

（４）事象間の相関

・複数の部門にまたがる事象や、事象が相互にどのように影響するのかという事象の**相関関係**を**理解**しているか。

＜ＥＲＭ的視点を取り入れた内部監査の例＞

（１）事象に関する意識の確認

・被監査部門の責任者が、**自分の部門に関連する事象をあらゆる側面に渡って考えてみようとする意識**を持っているのか、あるいは**事象を識別するための何らかの方法**を持っているかを**確認**してみる。

①たとえば、被監査部門に**内部環境に変化を与える事象**（例えば担当者の異動、流出、アウトソーシングの進展等による業務のレベルの変動）や、**外部環境に変化を与える事象**（例えば重要関連法令の発令）があった場合、その部門の責任者がそれらを事業目的達成に影響を与える**事象**として**意識**しているか**確認**してみる。

②**複雑な取引**に対する**理解**が**欠如**していないか、または、複雑な取引をしている部門や人を**聖域視**していないかを確認してみる。

（注）企業経営者が、従業員等が行う**高度に専門性を要するような複雑な取引**について十分に**理解・把握できなかった**ことにより、そのような取引に伴う**リスクを認識できず**、不祥事を訂正できなかったばかりか発生後の損害が拡大（リスクの深刻さが級数的に増大）する場合（例えばサブプライムローン問題）がある。

③**他部門**で起きた問題でも、**自部門でも起こりうる問題**として受け止め、**関心をもって検討しようとする意識**があるのか確認してみる。

（２）事象の識別に対する改善提案

・**事象の識別に対する意識**がない場合、以下のような例を取り上げて、抵抗感を和らげながら**意識改善**を促すことも一つの方法である。

①**過去に起きた事例**を洗い出してみることや、**過去事例**から**想定**される近い将来**起こりうると考える事例**を考慮することを提案してみる。

②**業界・他社**の**事例調査**を行っているか、**他社のリスク発生事例と同様の事象**が発生する恐れはないか、等も事象識別の切り口の一つであろう。

③**ヒヤリハット**（ヒヤリとしたこと、ハットしたことを発表しあって作業の安全性を高める活動）は作業現場などで、一般的に実施されている活動であるが、これはリスクを抽出する前工程と考えられるため、このような**ヒヤリハット**の考え方を**他の業務分野**に**応用**して事象の識別に発展させるよう提案することも有効である。

④会社の歴史（過去の事象）や業務の内容（現在の広範囲な事象）を良く知る良識的な**ベテラン社員にインタビュー**をして事象を

識別するのも一つの方法である。このような方法は、一見原始的に思えるが、リスクマネジメント初期段階では意外に効果的かもしれない。将来的に、より広範囲のインタビューやアンケート、ワークショップなどの手法への発展を促がすようにする。

（３）内部監査部門としての事象の識別

・**複数の部門にまたがる**リスクや**部門と部門の境界線上**にあるリスク、あるいは**事象同士の相関関係**は、サイロ型のリスクマネジメントでは認識できない可能性がある。内部監査部門は、リスクアプローチ実施過程において**会社全体の事象を幅広く認識**しておき、これらの事象に関しては、**特に注意**して**検討**する必要がある。なぜならば、ＥＲＭ未導入の企業では、**会社全体の事象**を**認識**できるのは内部監査部門のみかもしれないからである。

・小さな事象が集まり、大きなリスクにつながることがある。内部監査部門は、事象を断片的にではなく**網羅的にとらえる**必要がある。

（４）内部監査部門としての事象の分類・整理

・内部監査部門が把握した**リスク**を**分類・整理**して**経営者**に**報告**することにより、経営者は**リスクの全体像**を**把握**することができ、**適切な経営判断**の一助となる。

４．リスク評価

経営資源には限りがあるため、想定される全てのリスクに同じようなレベルの対策を実施することは困難である。リスク評価は、リスクが**目的の達成**に与える**影響**の**程度**を**検討**することであり、**発生可能性**と**影響度**の二つの側面から評価を行う。また、通常、**定量的手法**と**定性的手法**とを組み合わせて行う。リスクには**固有リスク**（リスクの発生可能性や影響度を変更させるために経営者がとるであろう行動がとられていない状態において、企業が抱えるリスク）と**残余リスク**（リスク対応後にもなお残存しているリスク）があるが、リスク評価では、この両方のリスクを評価する。

＜ＥＲＭ監査の主なチェックポイント＞

（１）リスク評価**プロセス**の確立

・リスクの発生可能性、影響度の**評価**、および必要な対応策の**策定**を含めた**リスク評価プロセス**を**確立**しているか。

・リスクや対応策の**見直し**は**定期的**に行われているか。また、急激な外部環境の変化等の非常時には、リスクや対応策は必要に応じて**随時見直し**が行われているか。

（２）リスク評価の**目的**の明確化と伝達

・部門長は**リスク評価の目的**を**明確**にし、それを当該部門の従業員に**伝達**しているか。少なくともリスク評価を実施する者は、**リスク評価の目的**について**共通の認識**を持っているか。

（３）評価**基準**および評価**尺度**

・部門長はリスクの**評価基準**および**評価尺度**を明確に**示して**いるか。また、それらは部門長をはじめ、プロセス管理者などのリスク評価を行う者に**共通の理解**を得たものであるか。

【評価基準の例】

①リスクの発生可能性と影響度

②コントロールの有効性

③リスクレベル

④リスク選好

⑤リスク管理能力

（４）評価方法・評価者

・部門長は当該部門員に対し**評価方法**を明確に**示して**いるか。

・**固有リスク**と**残余リスク**の**両方**を**評価**しているか。また、それぞれの定義は明確になっており、周知されているか。

・リスクマップやリスクリストを作成してリスクの**全体像**を**示す**ことにより、リスクを**統一的**に**把握**しているか。

・**定量化できるリスク**のみを評価していないか（**定量化できないリスク**を無視していないか）。**定量化になじまないリスク**もあるため、定性評価と定量評価を組み合わせ、自部門の実情に応じたリスク評価を行っているか。

・各部門はリスク評価を行わず、**リスク管理統括部門**だけがリスク評価を行っていないか。

（５）情報の提供

・リスク評価に必要な**情報**は、当該**リスクを評価（管理）する責任を負う者**に、適時・適切、必要かつ十分に**提供**されているか。

（６）リスク間の相関関係

・**リスク間の相関関係**、またはリスクが**相互に作用**し合うことが**考慮**されているか。**関連する複数のリスク**を**合わせて評価**しているか。単独のリスクの影響度が軽微な場合でも関連する**リスクが組み合わさる**と影響がより重大になることがあり、全く異なる発生可能性や影響度をもたらす場合がある。

・必要に応じて個別の**リスク毎にリスクを評価**しているか。リスクには多様な要因があり、その特性を適切に理解するためにはより詳細な**リスク毎の評価**が必要である。**リスク毎の評価**は個別のリスクを識別するのに役立ち、リスクの重要な属性やその原因、あるいは要因を適切に把握することができる。

＜ＥＲＭ的視点を取り入れた内部監査の例＞

（１）リスク評価手続および全社規程との整合性の確認

・被監査部門において**リスク評価に関する手続・マニュアル**等があるか確認する。ない場合は**リスク評価の手続**を確認し、リスク**評価方法**に関し部門内にどのように**周知**しているか、リスク**評価の結果**について上位の部門や関係部門に**報告**する体制になっているか等について確認する。

・**全社的なリスク管理規程**が制定されている会社については、**部門で設定した手続**が**全社規程**の主旨に**則した**ものになっているかについて確認する。

（２）リスク評価方法の浸透度

・リスクの評価者にリスクの評価方法についてインタビューを行い、リスク評価の目的や評価方法、評価基準等の**リスク評価方法**が部門内に**浸透**しているか確認する。**全社的なリスク管理規程**が制定されている会社については、**全社規程**が社内各部門に**周知**されているかを確認する。

（３）リスク評価のタイミング

・**リスク評価**を行う**タイミング**について確認する。一般的にリスク評価は年度の予算編成や中期計画の策定に併せて行われることが多いが、期中においても**外部環境等が急激に変化**した場合には、重要**リスクの見直し・再評価**と、それに対応した**対応策の見直し・新規設定**を行うことが必要であるが、行われていない場合があるので該当する場合には確認が必要である。

（４）内部監査部門と被監査部門とのリスク評価結果の比較

・内部監査部門は被監査部門とは**別にリスク評価**を行い、双方の**評価結果**を**比較**する。これは被監査部門と内部監査部門では、固有リスクおよび残余リスクに対する**評価が異なる**可能性があるためである。

・特に、被監査部門と内部監査部門で**残余リスクに対する評価**が異なる場合には、両部門間で**コントロールの整備･運用状況に対する評価**が異なっている可能性がある。具体的には、**被監査部門の残余リスクに対する評価**が内部監査部門の評価よりも**高い場合**（被監査部門は**残余リスクをより低減していると評価した**場合）には、被監査部門は自部門での**コントロールの整備･運用状況を**内部監査部門よりも**高く評価**している可能性がある。

・また、内部監査部門が高いと評価したリスクを被監査部門が**高く評価していない**場合には、被監査部門が**恣意的にリスクを高く評価していない可能性**もあるため、その**理由**について**掘り下げ**、内部監査部門との**評価の違い**を明確にした上で監査対象リスクとして選定するかどうかを判断する。

（５）固有リスクと残余リスクの評価結果の比較

・**固有リスク**と**残余リスク**の**評価の差が大きい**リスクについて、**コントロールの構築･運用状況**を掘り下げて確認する。このようなリスクは、コントロールによりリスクが軽減されていると判断されたが、実態は**リスクが軽減されていない**可能性があるため、監査対象リスクとして選定する（ただし過去の監査結果等により、許容範囲内までリスクが軽減されていると内部監査部門が判断した場合は、対象リスクから除外することも可能である）。

（６）リスクの評価者

・被監査部門に対し**リスクの評価者**を確認する。**プロセス管理者**がリスク評価を行わず、**リスク管理統括部門**がリスク評価を行っている場合には、リスク管理統括部門がリスクに対する対応状況等を正しく把握できていないと、リスク評価が適切に行われていない可能性があるからである。

・プロセス管理者はリスクについての広範な知識を持っているため、**リスク評価**は**プロセス管理者**が行うことが望ましい。具体的には、プロセス管理者に集まってもらい、内部監査部門がファシリテーター（進行役）を担当する**討議形式**でリスク評価を行うことも一つの方法として考えられる。評価結果に対してプロセス管理者の納得感や同意が得やすく、書面での評価だけでは吸い上げられない定性的な評価も把握することができる。なお、討議形式のリスク評価を行わない場合は、**部門長がリスク評価の結果について承認**しているか等について確認する。

（７）リスク評価の根拠となる情報

・リスクの評価者になぜそのように評価したのか、**評価の根拠や評価結果が導き出された背景**（どのような情報をもとに評価したか）について確認する。これは、リスク評価者がプロセス管理者の場合、自分のプロセスに関わるリスクとそれ以外のリスクについての評価について、**保有している情報量が異なる**ことにより**評価結果、特に残余リスクの評価結果に差**が生じていないかどうかを確認するためである。

（８）部門をまたがるリスクの評価

＜関連部門のリスクを考慮したリスク評価の実施＞

・被監査部門と事業戦略上、**密接に関連している部門のリスク**評価についても確認する。具体的には、必要に応じて**関連部門**の監査も同時期で実施することや、同一案件で受注からものづくりまでを**関連部門**を横断して一気通貫で確認することにより、**関連部門のリスク**を勘案すると、（被監査部門での）**評価が異なるリスク**がないか、**部門の谷間に落ちて評価の対象となっていないリスク**がないか等の確認を行う。

・特に会社の規模が大きい場合は、一つのプロジェクトや事業に**関わる部門が複数**で**役割分担が明確になっていない**場合があり、本来は評価が必要なリスクを自部門のリスクとして認識せず、結果として**どこの部門もリスク評価をしていないリスク**が存在している場合がある。このような場合は、より上位の部門にもリスクが顕在化した場合の影響について報告し、提言提案を行う。

＜全社共通のリスク評価結果の分析＞

・全社的なリスクマネジメントを実施していない会社であっても、**コンプライアンスに関するリスク**は比較的**全社に共通のリスク**である。内部監査部門は各部門での**コンプライアンスにかかわるリスク評価結果**を分析し、必要に応じて各リスクの主管部門（購買部門、総務部門等）へ改善提案を行う。

５．リスクへの対応

「リスクへの対応」は、リスク評価により把握したリスクのそれぞれに対し、**回避**、**共有**、**低減**、**受容**といったリスク対応の４つのカテゴリーの選択肢の中から、**許容できる水準**にリスクを抑えるリスク対応策を選択するとともに、**費用対効果**の検討･評価を行うプロセスである。複数の選択肢を組み合わせるリスク対応策もある。また、回避以外のリスク対応策では、残余リスクが０になることはないので、どの程度の残余リスク量で受容するかという許容の検討プロセスでもある。

個々のリスク対応策は、残余リスクを望ましい**リスク許容度の範囲内**に収めるように策定される。リスク許容度とは、特定の目的達成に対する差異をどの程度許容できるかというレベルのことである。企業の中の個々の単位（部門等）ではリスク許容度内となっているものの、個々の単位のリスクを合計すると企業全体のリスク選好を超える可能性もある。逆に、企業全体で見ると他のリスクと相殺されることもある。ＥＲＭでは、企業全体からの、あるいはポートフォリオの視点で、リスクを検討することを求めている。

また、リスク対応策は、必ずしも残余リスク量を極限まで減らす必要はなく、**リスク**、**コスト**と**リスク許容度**の**バランス**をとることが重要である。

＜ＥＲＭ監査の主なチェックポイント＞

（１）リスクへの対応策を策定しているか

・把握されたリスクに対してリスク対応策を**策定**しているか。

（２）リスクの発生可能性や影響度に対するリスク対応策の効果を評価しているか。

・採用されているリスク対応策が、**発生可能性**および**影響度**にどの様に**影響**を与えているか**評価**しているか。

（３）リスク対応策により、残余リスクが許容度の範囲内に収まることを確認しているか。

・リスク対応策により、**残余リスク**が**許容度の範囲**内に収まっていることを定期的に**確認**しているか。

（４）リスク対応策の有効性

・リスク対応策は、リスク顕在化の抑制や顕在化した際の**損失の抑制**に有効に**機能**するか。

・リスク対応策が、社内の**部門間**での**リスク移転**となっていないか。

（５）費用対効果

・選択されているリスク対応策に伴う**費用**は、そのリスク対応策がもたらす**効果**と**対比検討**されているか。

・**類似のリスク**が社内の他部門にないか。社内他部門に**類似リスク**がある場合、**重複**して**リスク対策**を行わない等相互に**連携**しているか。

（６）ポートフォリオの視点

・個別事業や部門ごとに作成したリスクマップを一つに集約した全社的な観点から評価したリスクマップ、即ち**リスクポートフォリオ**を作成し、個別事業ごとのリスクや対応策の評価に留まらず、**全社的な視点**からリスクと対応策の費用と効果を**評価**しているか。

＜ＥＲＭ的視点を取り入れた内部監査の例＞

（１）リスク対応策の策定プロセス

・リスク評価により把握されたリスクのそれぞれについて策定された**リスク対応策**を**確認**する。

・リスク対応策の策定に際しての検討過程、例えば検討された他のリスク対応策との比較検討の状況、選択されたリスク対応策実施による発生可能性及び影響度をどのように評価したかを明らかにし、**リスク対応策策定プロセス**を**検証**する。

（２）リスク対応策の実在性

・選択されたリスク対応策の**実施状況**を確認し、リスク対応策は当初の**予定通り**に**実施**されているかを**確認**する。

（３）リスク対応策の有効性

・リスク対応策を実施した結果、リスクの発生可能性及び影響度に対してどのような影響を及ぼしているか、つまりリスク対応策が**有**

効かどうかを**確認**する。例えば、購入部品の品質向上策として仕入先との「品質向上会議」の定期開催が採用されている場合、「品質向上会議」の開催状況、参加者の出席状況、会議の内容等を確認した上、「品質向上会議」開催によるクレーム数への**影響**を**確認**する等が考えられる。

・また、策定したリスク対応策はその後の**状況の変化**に応じて**見直し**されているかを**確認**し、リスク対応策が**継続的**に**有効**に管理されているかを**検証**する。

（４）費用対効果の評価

・リスク対応策の策定プロセスで検討された**費用対効果**の**評価**状況を**確認**する。

・効果の測定は主観的な評価を含むものとなりがちであるが、効果が**目的の達成**に伴う**便益**とのつながりで適切に**評価**されているかを**検証**する。

（５）全社の状況を見ることのできる内部監査の特性を活用する観点

・ＥＲＭ導入前夜にある企業においては、通常、全社横断的にリスク管理を行う部署はない。そのような環境では、**全社の状況**を**横断的**に**検証可能**な**内部監査部門**の**特性**を**活かした観点**から評価することで、被監査部門ごとに立案されるリスク対応策を**企業全体の観点**から**評価**することができる。また、**残余リスク**を**ポートフォリオの視点**から捉えることができる。

・その結果、①**他の部門と共有**すべきリスクを**自部門のみ**で検討、対策を行っているケースや、②他の部門と**重複**してリスク対策を行っているケース、あるいは③対応策の実施が**社内他部門**への**リスク移転**となっているケース等が明らかになる場合がある。

・また、部門単位で保険を付保している場合、全社で**一つの保険にまとめる**ことでコスト削減の可能性がある。

６．統制活動

統制活動は、**リスク対応策**が**実行**されるとの**保証**を与えるのに役立つ**方針および手続**である。統制活動は、企業の**全ての階層**や**全ての部門**で、また**企業全体**にわたり、**通常の業務プロセスの**一環として行われている。統制活動には、承認、権限の付与、検証、照合、業績のレビュー、資産の保全、および職務の分離など、**リスク対応策**の**実行**を**保証**する多岐にわたる多様な活動が含まれている。

＜ＥＲＭ監査の主なチェックポイント＞

（１）リスク対応策の実行保障と業務プロセスへの組込み　（リスク対応策との統合）

・統制活動は、**リスク対応策**が**実行**されることを**保証**するもの（確実にするもの、役に立つもの、一助となるもの）となっているか。同時に、**業務プロセス**の中に**組み込まれて**いるか。

・統制活動は、「低減」以外のリスク対応策（「回避」、「共有」、「受容」）についても、整備・運用されているか。

・リスク対応策が「**受容**」である場合には、**リスクの程度**を**定期的**に**再評価**し、受容可能な水準を超過した場合（固有リスクがリスク許容度を超過した場合）には、リスク対応策を**再検討**する仕組みとなっているか。

（２）統制活動のタイプ

・統制活動は、対象とするとするリスクやリスク対応策、当該業務の特性に**適した方法**で整備・運用されているか。

（３）方針と手続

・**方針**（何を行わなければならないかを示すもの）は、**明確に定められて**いるか。大会社の場合には、それは**文書化**されているか。

・**手続**（方針を実行するための手段）は、**方針に従ったもの**になっているか。

・手続の結果は、**フォローアップ**され、適切な**是正措置**が講じられているか。

・リスクマネジメントの方針や手続が文書で定められているか。また、その方針や手続はプロセスの責任者に正確に伝達され、プロセスの責任者はそれを理解しているか。

（４）情報システムに対する統制手続

・全般統制と業務処理統制は適切か。

（５）自社の特殊性

・統制活動は、組織の規模や複雑性、活動の性質や範囲、歴史、文化、事業環境など**組織固有の要因**を反映した設計になっているか。統制活動を組織固有の要因を考慮せず、一律に設計していないか。

＜ＥＲＭ的視点を取り入れた内部監査の例＞

（１）実質的に機能しているかの確認

・監査対象となる統制活動が**実質的に機能**しているかについて確認する。

例えば、購買取引の不正リスクを軽減する目的で、購入要求部門が直接業者に対し発注を行わず、購買部門に対し購入要求書を提出し、購買部門が業者に対し発注するという統制があったとする。注文書の発行部門が購買部門かどうかを確認するだけではなく、内示発注により購入要求部門が業者に対し注文を行っていないかについても確認し、統制活動が**実質的に機能**しているかどうかについても確認する必要がある。

（２）類似業務を行っている部門との横並び比較

・ある部門の統制活動を評価する際、**類似の事業を行っている部門**の統制活動と**横並びで比較**し、不足している統制がないか、あるいは非効率な統制がないかを確認する。

例えば、あるリスクに対する統制活動を評価する場合、類似業務を行っている部門を横並びで比較してみると、どの部門でも規程・マニュアルは整備されているが、それ以外の統制、例えば規程に則した業務プロセスが整備・運用されていることを確認する統制活動が実施されている部門と、実施されていない部門とがある場合がある。この場合、後者については指摘事項となる。

（３）企業固有のリスクへの対応状況の確認

・**企業固有のリスクに対応した統制活動**が有効に整備・運用されているかを確認する。

例えば、酒類を扱う企業にとって、社員の飲酒運転だけでなく、**二日酔い運転による事故も、企業イメージやブランドに重大なダメージを与える**ため、重要リスクとなる。そのため、飲酒直後の運転禁止の徹底は当然のことであるが、営業担当者による**二日酔い運転のリスクに対応する統制**も重要になる。内部監査部門は、**二日酔い運転防止対策**が徹底されているかを、発信文書や営業マネジャー・営業担当者へのインタビューで確認する。営業車の運転前にアルコール検知器によるチェックが実施されているか、営業車の運行管理表をチェックする。また、アルコール検知器の定期メンテナンスが行われているかについても確認する。

（４）業務実態への適合性の確認

・**業務実態に適合していない統制活動**は形骸化して機能しないため、**統制活動が業務の性質に適合しているか**を確認する。

例えば、本社の統括部門が、現場の実態の把握が不十分なまま、全ての営業所は営業マネジャーが、営業担当者の体調を毎朝の朝礼で確認するというルールを策定したとする。内部監査部門が朝礼への立会、営業マネジャー・営業担当者へのインタビュー等により、ルールの遵守状況を確認したところ、直行直帰の営業担当者が多い営業所では、朝礼への出席率は５０％未満であり、**ルールが業務実態に適合しておらず**形骸化している事例があった。内部監査部門は、朝礼欠席者の自己チェックと報告を行うシステムの整備を提案した。

（５）リスクの大きさやリスク許容度との整合性の確認

・統制活動は対象となる**リスクの大きさ**や**リスク許容度**と**整合性**が取れていることが必要である。

例えば、職務権限規程や決裁権限規程という統制活動の妥当性について監査する場合、リスクが大きいものやリスク許容度が低いものについては、より上位者の決裁が必要なように設計されているかを確認する。

（６）条件付決裁案件での確認

・**条件付で決裁**を取った場合、起案者は最終的に条件が満たされたかを確認していない場合や、条件が満たされたか否かについて決裁者に報告していない場合がある。監査では、**条件付で決裁がなされた案件**を監査する場合、最終的に**条件が満たされたのか**を確認するとともに、条件が満たされたか否かについて決裁者に**報告が行われたか**を確認する。

（７）内容が形式的で実質的に機能していない統制活動

・業務上の**改善を目的として作成された書類**は、所定の記載事項はもれなく記載されており形式は整っているが、肝心の改善策の**内容が形式的**で、**実質的な改善につながらず**、統制活動として機能していない場合がある。

例えば、生産工程の不良の改善を目的として作成された帳票は、受付から原因調査、処置に至るまで定められたフローに従って、それぞれの責任者により適切に記載されていた。しかし、その内容を吟味してみると記載されている改善策の多くは、作業手順の単純な見直しなど**表面的な範囲**にとどまっており、原因まで遡って分析した結果を踏まえた再発防止策など**根本的な改善策**は記載されていなかった。原因は、品質マネジメントシステム（ＩＳＯ９００１）内部監査員の形式的な監査や，被監査部門の品質マネジメントシステムに対する理解不足であった。

（８）方針や手続を担当する部門の権限と責任の明確化

・新しい**方針や手続**を導入する際に、担当部門の**権限と責任を明確化**しておかないと、導入した方針や手続が形骸化する場合がある。

例えば、情報セキュリティ強化の経営方針に基づいて、情報システム部門が担当部門となり、認証機能つきのＵＳＢの使用がルール化されたが、新ルールについての情報システム部門の権限と責任が明確にされていなかった。後日、内部監査で認証機能が付いていないルール違反のＵＳＢが使われている「例外」扱いのパソコンが多数発見された。情報システム部門に理由を確認したところ、ユーザー部門から「認証のために時間がかかって非効率的なので例外を認めてほしい」と部門責任者名で要求されたが、新ルールについての情報システム部門の**権限と責任が明確にされておらず**、新ルールのための環境整備担当に過ぎないと考えられていた同部門としては、そのまま応じざるを得なかったとのことであった。

（９）過大な統制活動の効率化の提言

・内部統制報告制度が適用２年目に入り、多くの企業ではより少ないコストで効率的に制度対応を行うことが大きな課題となっている。同制度への対応を効率化するために内部監査部門は、現在行われている**統制活動がリスクの重要性と比較して不相応に過大**なものとなっていないかを確認し、**過大な統制活動**については**効率化を提言**する。

例えば、①小規模で日中は １ 人体制の事業所でも小口現金の払出について、第三者のチェックを義務付けている場合や、②統制活動としてエラーリストの出力とその内容確認とフォローで十分であるにも関わらず、更にエラーリストに基づいて行ったことの実在

性や網羅性に関するリスクを取り上げて、それに対する統制活動まで義務付けている場合は、**リスクの重要性と比較して不釣合いに過大な統制活動**である。この場合、内部監査部門は**過大な統制活動の効率化を提案**する。

（１０）全社レベルでの統制活動の効率化の提言

・統制活動の一環として業務の標準化、文書化のための業務基準の設定や規定・マニュアル類の整備が進められているが、それらが**職場単位、部門単位で個別に行われる**ため、各職場、各部門で同様の内容の業務基準や規定・マニュアル類がバラバラに設定・作成されており、**全社レベルで見ると効率が悪い**場合がある。内部監査部門は、それら業務基準の設定や規定・マニュアル類の整備状況を**全社レベルで確認**し、**全社レベルで見た場合での統制活動の効率性を高める**ための提言を行う。

（１１）軽微なリスク

・統制活動により、通常は特段の対応を取っていない**軽微なリスク**がどのように発見され、対応されているかを確認することにより、想定する規模のリスクに対する当該統制活動の有効性を推測する。

（１２）訓練

・リスクの顕在化を仮定した**訓練**の実施内容を確認することにより、統制活動の運用の有効性を評価する。

７．情報と伝達

情報と伝達とは、適切な情報が、（組織内の）人々がそれぞれの責任を遂行できるような形式および時間枠で、識別、補足、そして伝達されることである。有効なコミュニケーションは、組織を縦横に（上から下へ、横に、または下から上に）行われるものである。

＜ＥＲＭ監査の主なチェックポイント＞

（１）情報

・内部および外部の情報源より経営に必要な財務･非財務上の情報が**漏れなく収集**されているか。

（２）戦略的・統合システム

・情報システムは、**経営戦略**や**事業戦略**に基づいて、開発または導入されているか。

（３）リスク情報の統合

・情報システムによって、業務や組織のリスク情報が**統合的**に**管理**されるようになっているか。

（４）情報の詳細度・適時性・迅速性

・組織内の人々が多くのデータを利用可能であるなかで、**適切な情報**が**適切な形式**かつ**適切な詳細度**で、**適切な人々**に**適時**に行き渡らせることにより「情報過剰」を防いでいるか。

・**リスク許容度を超える**可能性のある問題が起こった場合の**第一報**は、速報ベースの不確定情報であっても、必要な人に**迅速**に伝えられているか。

（５）内部での伝達

・経営者は、有効なＥＲＭを整備するために必要なメッセージを組織内の人々に**発信**しているか。

・電子メール・イントラネット・会議など、**複数の伝達経路**が用意されているか。

・ホットラインの設置など、**通常の経路が動かないときにも情報伝達ができる経路**があるか。

・**ネガティブな情報**が隠蔽されずに、迅速に**経営トップ**まで**伝達**されるよう体制が整備されているか。

・リスクが発生する可能性が発見された場合の**緊急連絡体制**は整っているか。

・**全社最適化**をする意識を持って、**他部署に有益と思われる情報**を積極的に**提供**しているか

（６）外部との伝達

・顧客、仕入れ業者、規制当局、株主など**外部との有効なコミュニケーション**が行われているか。

＜ＥＲＭ的視点を取り入れた内部監査の例＞

（１）情報

・**経営陣**がリスクを管理したり意思決定したりするために**必要な情報**が**伝達**されているか、経営陣と内部監査部門のミーティング時などを利用して**尋ねてみる**。そこで、経営者がどのような情報を不足と感じているのかが把握できる。

・また、内部監査部門が、**経営陣**に**リスクの発生する場所についての情報**を伝達したり、さらには、プロセス管理者、情報伝達のルート、情報の形式や情報入手のタイミングなどの**あるべき姿**と**現状**を**比較**して提示することも有益である。

（２）内部での伝達

＜上から下への情報伝達＞

・**経営トップ**は、「**伝えたつもり、**従業員は理解しているはず」と思っているが、実際は現場に**浸透していないこと**がある。このような状況が**なぜ生じるのか**を監査テーマとすることは重要である。原因を掘り下げて、情報のパイプ詰まりを解消することに貢献できるかもしれない。

・監査手法としては、どこで情報が滞っているか、また、その原因を解明するため、部門長・中堅社員・社歴が浅い社員の各階層へ**インタビュー**することなどが考えられる。

＜下から上への情報伝達＞

・**不祥事**が**隠蔽**される原因としては、**ネガティブ情報**の報告を受けたときに、**上位者**が感情的になって報告者を**叱る**などの**内部環境上の問題**が考えられる。内部監査部門は、経営者や部門長に対して、「裸の王様」になって失敗した**他社の不祥事の事例**を利用するなど、経営者の不興を買わない工夫をしながら**内部環境**の**改善**を提案する。

・リスクが発生した場合の経営者への報告において、**迅速性**が**損なわれる**要因としては、リスクを発見した人やトラブルを起こした人が、すぐには報告せずに、自ら**問題を解決してから報告**しようとすることがあげられる。これは、トラブルを起こした人が問題を解決してから部門長や経営者に報告した方が体裁が良いと思ってしまうためである。また、解決後に報告を受けた部門長や経営者も、問題が解決済みなので、事後報告をあまり問題視しないかもしれない。

また、報告の迅速性が阻害されるもうひとつの要因としては、「さらに調査を進めないと、それがリスク発生に結びつくのか、判断しかねるため、調査後に報告する」ということがあげられる。しかしながら、リスクへの対応の遅れは、企業に取って致命傷となる可能性がある。このため、内部監査部門は、望ましい**緊急情報の受け取り方**の事例として、「第１報は完璧を求めず**迅速さ**を**重視**、第２報で定型フォーマットに記載」などの具体例を経営者に提案し改善を促すようにしたい。

・仕事上のミスや事故に対して**過度の懲罰的な処遇**を行う人事制度を導入している企業では、従業員が問題点を**隠蔽**する方向に走りやすく、経営者まで問題点が**報告されない**可能性がある。このため、内部監査では、就業規則や賞罰規程などにより、**人事制度**を**確認**し、**過度の懲罰的な制度**がある場合は、「故意ではなく過失によりミスを起こした従業員に対して**挽回の機会**を与えるような制度」を作ることなどを提案する。

また、迅速性を確保するための人事的な処遇として、事故やトラブルを起こしてしまった人の**その後の対応**も含めて**評価**することや、トラブル等を迅速に報告し、適正な処理を行った従業員への**処分**を**軽減**することなどを提案する。

・上記の他に、**緊急時の連絡方法**が**曖昧**なことや、組織変更にあわせて**メンテナンスが実施されていない**などの統制上の不備がある場合がある。内部監査部門は、**緊急連絡体制**を確認するとともに、最新の組織図等と比較して**メンテナンス**が行われているか確認し、不備があれば改善するよう提案する。

＜横への情報伝達＞

・横への連絡は、上下への連絡と比較してルールが整備されていない可能性が高い。このため、ある部門でリスクが発生した場合に、どこの部署に影響が及ぶのかを**事前**に検討し、**報告ルール**を文書化しておくことが望ましい。（製品の欠陥が発見された場合に広報へ報告するなど）

・また、**想定外のリスク**が発生した場合は、前記の文書化した報告ルールだけではカバーできないケースも想定できる。このため、**想定外のリスク**が発生した場合、現場の一人ひとりがそのリスクがどの部署に影響を及ぼすのか**臨機応変**に判断できるようリスクについての**教育**や**意識付け**を行っていくことが重要である。

（３）外部への伝達

・万が一、不祥事や事故が起きた場合のマスコミ対応、消費者への告知、規制当局への報告などの初期対応を間違えると、風評被害等の二次的損失を生み、企業の存続等にも影響を与える可能性がある。そこで内部監査では、不祥事や事故が起きた場合に**適正な公表を行う旨の対応方針**が**策定**され、**共有**されているか確認する。策定されていない場合は、不適切な対応をしてしまった企業の例をあ

げるなどして、会社としての重要度を認識してもらい、**対応方針**を**策定**するよう提案する。

・その際、法令や監督官庁の判断基準以前に、**消費者や社会などが企業に対して求める倫理観**が、判断基準として重視されている社会状況であることも情報として提供する必要がある。

（注）また、近年の不祥事を見ると、組織の中の一部の判断で公表を控えるというよりは、**経営者の判断**によるものがほとんどのように見受けられる。このような内部環境にある企業の場合は、**監査役の協力**を求めることが必要である。

８．モニタリング

モニタリングはＥＲＭの構成要素の一つであるとともに、ＥＲＭの**ＰＤＣＡサイクルを回していくために欠かせない要素**である。即ち、ＥＲＭの各構成要素が、ＥＲＭのフレームワークで示されている４つの経営目標に沿って整備され機能しているかを、**点検・評価**(Ｃｈｅｃｋ)して、**改善活動**(Ａｃｔｉｏｎ)につなげる機能である。

ＥＲＭの各構成要素をどこまで整備し、どこまで機能させるかは**経営判断**であり、改善活動(Ａｃｔｉｏｎ)とは、経営者が目標とするその企業のリスクマネジメントの**あるべき姿**と**現実**との**ギャップを埋める活動**である。従って、モニタリングはＥＲＭの構成要素の一つであるとともに、**ＥＲＭの外側に立ってそのレベルを点検・評価**するという**他の構成要素とは異なる側面**を持っている。

モニタリングは、日常的監視活動と独立的評価に分類される。**日常的監視活動**とは、部門長・プロセス管理者・担当者の業務ラインで行うモニタリングである。また、**独立的評価**とは業務ラインに入っていない第三者が行うモニタリングであり、内部監査はその代表的なものの一つである。

＜ＥＲＭ監査の主なチェックポイント＞

モニタリングにおけるＥＲＭ的視点とは以下のようなものである。

（１）モニタリングの対象

・モニタリングの対象は**リスクマネジメント全般**にわたり、**ＥＲＭの８つの構成要素全体**をカバーしているか。

（２）モニタリングと経営目標との整合性

・モニタリングは、財務報告の信頼性確保だけでなく、①会社のミッションに沿った戦略立案と有効な目標設定・管理、②会社の経営資源の有効かつ効率的な活用、③社内外への報告の信頼性確保、④コンプライアンスの徹底、の観点から、**経営目標を達成する手段**として実施されているか。

（３）期待水準の維持の確認のためのモニタリング

・リスクマネジメントが**期待された水準**を**維持**しているかを**確認**するために、リスクマネジメントの実施状況が定期的にモニタリングされているか。

（４）許容度内での管理の確認、定期的な再評価

・**プロセス管理者**は、部門長が設定した**許容度内**に**リスク**が適切に**管理**されていることを**確認**するために、リスクマネジメントの整備、運用状況を定期的に**評価**しているか。

（５）手法・体制の定期的な棚卸・改善

・現在のリスクマネジメントの**手法**や**体制**が、内部環境および外部環境の変化対応しているかについて、**定期的**に**棚卸**を行い、判明した不備が**改善**されているか。（その結果、リスクマネジメントは、内外の環境変化に対応した**最新**のものとなっているか。）

（６）リスクへの対応および統制活動の定期的な評価・改善

・個々の**リスクへの対応**および**統制活動**は**定期的**に**評価**され、判明した不備は**改善**されているか。（その結果、リスクへの対応および統制活動は**常に適切**なものとなっているか）

（７）日常的監視活動の評価

・業務ラインで行われる**日常的監視活動**について、**独立的評価**を行っているか。

・**自主点検**やＣＳＡを内部監査の補完的機能として有効活用しているか。

（８）内部監査部門、監査役、会計監査人の連係

・独立的評価の主体である**内部監査部門**、**監査役**、**会計監査人**の間の**連係**は有効に行われているか。

＜ＥＲＭ的視点を取り入れた内部監査の例＞

（１）監査フロー各過程にわたるリスクの意識

・監査計画→事前調査→実地監査→結果の取纏めと報告／改善提言→フォローアップという**監査の業務フロー**の全ての過程で、**リスクを意識**することが重要である。

①**監査計画**の段階では、社内外のリスク情報を基に、内部監査部門独自のリスク評価を行い、被監査部門の選定に反映させる。
②個別監査の**事前調査**の段階では、被監査部門の固有リスク・残存リスクを評価し、リスクの高い分野の業務・コントロールに監査の重点を置く。
③**実地監査**では、目標とするリスクコントロールの水準と現状とのギャップを評価する。
④リスクコントロールのギャップを埋める**改善提言**を行う。
⑤改善策が確実に実施されたかを**フォローアップ**することにより、次の監査サイクルに繋げる。

（２）根本原因の追究

・監査業務全般において、問題点の発見は重要であるが、問題点の解決を図るための有効な改善提言を行うには、**根本原因の追究**が欠かせない。根本原因の追究は、あらゆる改善活動において最も重要な要素である。根本原因の追究に当たって、**ＥＲＭの各構成要素**を**意識**して行うことが有効と考えられる。
・例えば、「契約を書面で取り交わしていない」という「リスクへの対応」の問題点が発見された場合、原因を追究していくと**他の構成要素**に問題の**真の原因**が潜んでいるケースも多い。
①漏れのない管理を行うために必要な契約書のリストが作成されていない（統制活動）
②契約書を取り交わさないことによるリスクを認識していない（事象の識別）
③契約書を取り交わすという社内ルールがない、または周知されていない（統制活動）
④契約書の締結権限が曖昧である（内部環境）
⑤上司が部下の業務を点検するという日常的なモニタリングができていない（モニタリング）

＜ＥＲＭ的視点を取り入れた内部監査部門の役割＞

（１）経営と内部監査

・「内部統制の基本的枠組み」にもある通り、企業内における内部統制の独立的評価は本来経営者自らが行うべきものである。とは言っても、企業の規模が大きくなるにつれて、経営者が直接独立的評価を行うことは、実務的に不可能になってくる。従って、経営者は経営者直属の内部監査部門を設置して、独立的評価を実施させる。ＥＲＭは内部統制を包含するリスクマネジメントの枠組であり、

ＥＲＭに対する独立的評価についても、同じことが言える。むしろ、ＥＲＭは経営そのものと言ってもよく、**経営者の内部監査への関与**の度合いは内部統制よりも強い。

・**ＥＲＭ的視点で行うモニタリング**は、**経営の立場**からリスクマネジメントのあるべき姿と現状とのギャップを埋める作業である。ＣＯＳＯ－ＥＲＭで示されたリスクマネジメントの枠組そのものが、当該企業のあるべき姿と合致するとは限らないが、**ＥＲＭ的視点でモニタリングを行う**ことによりＰＤＣＡサイクルを回し、リスクマネジメントの改善活動を実施した結果として、**経営の関与**の下でＥＲＭ的なリスクマネジメント体制が整備されていくことが期待される。

（２）特定の分野の内部統制のモニタリングと内部統制監査の統合

・近年、法律や認証の形で、様々な**特定の分野での内部統制**の仕組みの導入が求められている。これらの内部統制の仕組みは、基本的に**ＰＤＣＡ**の管理サイクルを回す形で組み立てられており、必ず**モニタリング機能**（監査）を**必要**としている。歴史的に内部監査部門は、企業の中でモニタリング機能の中心的な役割を担ってきたため、これら**特定の分野の内部統制**のモニタリングについても内部監査部門が関与している場合も多い。

・内部統制報告制度では、財務報告という特定分野における内部統制の整備･運用状況の有効性を評価するために、監査法人による**定期的なモニタリング**（内部統制監査）が要求されている。（なお、「実施基準」の中に内部監査部門等が果たす役割について明記されたため、内部監査部門の活動に大きな影響を与えている。）

・また、国際規格である**ＩＳＯ１４００１**（**環境**マネジメントシステム）、**ＩＳＯ９００１**（**品質**マネジメントシステム）、**ＩＳＯ２７００１**（**情報セキュリティ**マネジメントシステム）、**ＩＳＯ２２０００**（**食品安全**マネジメントシステム）や、**Ｐマーク**（個人情報保護）も特定の分野での内部統制の枠組であり、そのＰＤＣＡサイクルを回すために、**定期的なモニタリング**（監査）が要求されている。これらの規格は法律ではないものの、取引先や消費者がその企業の製品やサービスを購入する際の、入札条件や目安になることも多いため、企業として導入せざるを得ない場合もある。

・これらの特定分野の内部統制の仕組みは、その目的、文書化やサンプリングの内容・手法において相互に大きな違いがあるとともに、企業内の担当部門も異なり、それぞれ別個のものとして実施されており、企業全体として見た場合多大なコスト負担となっている。効率化のために、複数の**特定分野の内部統制のモニタリング**と**内部監査**を**統合的に行う試み**は、一部で行われてはいるが緒についたばかりである。なお、効率化の一つの試みとしてＩＳＯ９００１の社内審査を行う際に、業務監査のチェック項目も加えて、ＩＳＯ監査人が内部監査を実施している企業もある。

・**これらの特定の分野の各種内部統制のモニタリング**と**内部監査**を、ＥＲＭの観点から**統合**して、**コスト負担を軽減**しながら**有効に実施**していくことは、重要な**経営課題**の一つとなっている。

・なお、本来、内部監査部門はこれらの特定の分野の内部統制の仕組みに当事者として係わるべきではなく、夫々の推進組織が行うモニタリング活動を含めて、その仕組みが有効に機能しているかを社内の第三者として評価すべきと考えられる。

（３）自己点検（自主点検・自己監査・ＣＳＡ）の取りまとめ

・ＥＲＭの概念の中に、「企業の役職員**全員が関与**する」という考え方があり、リスクマネジメントの目標は役職員一人ひとりが**リスクマインド**を以って日々の業務に取り組んでもらうということである。**自己点検**は業務のラインで実施する日常的監視活動の一つとされているが、**内部監査部門**がその**取りまとめ役**として関与し、リスクマネジメントの観点から自己点検を実施するように主導することが、**リスクマインド**の**周知徹底・教育**の面で有効である。当然のことであるが、自己点検の仕組みが有効に機能しているかについては、内部監査部門の定例監査において点検・評価される。

（４）監査役と内部監査部門の連係強化

・会社法が要請する内部統制の監査は**監査役**の役割であるが、その監査対象の一つに「損失の危険の管理に関する規程その他の体制」が明記されており、監査役監査の対象にはリスクマネジメントが含まれると理解される。監査役と内部監査部門はともに、リスクマネジメントの有効性について監査することになるが、特に中小の上場会社の**内部監査部門**は金商法の要請する内部統制評価にかなりの業務量を割いており、リスクマネジメントを対象とした監査には十分な業務量を割けないのが実態である。

・一方、監査役としてもリスクマネジメントを含む内部統制システムの監査を行うためには、現場の状況を正確に把握する必要があるが、監査役専任のスタッフを置いている会社は少なく、内部監査部門の活動に依拠せざるをえない状況である。従って、ＥＲＭの視点に立った**モニタリングの最適化**の観点から、月 １ 回の定例会というような単なる情報交換だけではなく、監査役が内部監査に立ち会うなどの**監査役**と**内部監査部門**との更なる**連係強化**が必要である。

（５）ＥＲＭの運用における内部監査部門の役割

・内部監査部門がイニシアティブを取ってＥＲＭを導入した企業では、内部監査部門にリスク管理推進セクションを設置したが、個々のリスクの把握・評価、および対応策の立案・実施は各部門・関係会社の本来業務であると考えて、リスク管理推進セクションの役

割を支援機能・モニタリング機能および開示機能の３つに限定した。また、ＥＲＭのモニタリングについては、リスク管理推進セクションが年 1 回リスクの見直し・対応策のレビューを行うとともに、それとは別に内部監査部門が原則として３年に１回行う定例監査においてＥＲＭの有効性を点検・評価した。なお、その後、リスク対応策の管理などＥＲＭの機能強化を行うため、リスク管理推進セクションは内部監査部門からコーポレート部門に移管された。

以　上