国際情報

2004年９月29日

全社的リスク管理における内部監査の役割

内部監査人協会（ＩＩＡ）
訳：川　村　眞　一
（三菱商事株式会社　監査部主席内部監査人　内部監査士）

新たに公表されたトレッドウェイ委員会支援組織委員会（ＣＯＳＯ）『全社的リスク管理の統合的枠組』と関連して、内部監査人協会（ＩＩＡ）は、ＩＩＡイギリス・アイルランド支部（ＩＩＡ UK and Ireland affiliate）と協力して「全社的リスク管理における内部監査の役割」に関する方針書を公表した。

本方針書の目的は最高監査責任者（ＣＡＥs）の当該組織における全社的リスク管理（ＥＲＭ）問題への対応を支援することにある。この方針書は、内部監査人がアシュアランス業務およびコンサルティング・サービスを提供する際に、ＩＩＡの『内部監査の専門職的実施の国際基準（基準）』が要求している客観性および独立性を維持する方法を提案している。

ＥＲＭに関する中心的な内部監査の役割とは、主要なビジネス・リスクが適切に管理され、インターナル・コントロール・システムが有効に稼働していると確信するのを助けるための、組織のＥＲＭ活動の有効性にかかわる客観的アシュアランスを取締役会に提供することである。

◇推奨された役割

内部監査の役割を決定するときにＣＡＥs が考慮に入れるべき主な要素は、活動が内部監査人の独立性および客観性に対する何らかの脅威を引き上げるかどうか、そして組織のリスク管理、コントロール、およびガバナンスのプロセスを改善しそうであるかどうか、ということである。

ＩＩＡの方針書は、内部監査が、ＥＲＭのプロセスの中で、どのような役割を果たすべきか、または果たすべきでないか、を示している。

◇ＥＲＭに関する中心的な内部監査の役割

＊リスク管理プロセスに関するアシュアランスの提供
＊リスクが正しく評価されているというアシュアランスの提供
＊リスク管理プロセスの評価
＊主要なリスクの報告の評価
＊主要なリスクの管理のレビュー

◇予防措置により正当化される内部監査の役割

＊リスクの識別および評価のファシリテート
＊リスク対応における管理者の指導
＊ＥＲＭ活動の調整

＊リスクに関する報告の総括
＊ＥＲＭの枠組の維持および展開
＊ＥＲＭの確立の支援
＊役員会の承認のためのリスク管理戦略の展開

◇内部監査が引き受けるべきでない役割

＊リスク・アペタイトの設定
＊リスク管理プロセスの強制
＊リスクに関する経営的アシュアランス
＊リスク対応に関する決定
＊経営者に代わるリスク対応
＊リスク管理の説明責任

ＩＩＡは、経営者がリスク管理責任を負っていることを組織が十分に理解するべきである、と強調している。内部監査人は、リスク管理を決定するのとは対照的に、助言およびリスクに関する経営者の決定に対する反対または支持を提供するべきである。内部監査の本来的な責任は、監査基本規程に記録され、かつ監査委員会によって承認されるべきである。

最後に、「全社的リスク管理における内部監査の役割」は以下に示すとおりである。

1941年に設立されたＩＩＡは世界中の内部監査、ガバナンス、インターナル・コントロール、ＩＴ監査、教育およびセキュリティにおいて約95,000人のメンバーに役立っている。協会は、認知された権威、主要な教育者、世界中の専門職のための証明、研究、および技術的指導において広く知られた指導者である。

姿勢声明

全社的リスク管理における内部監査の役割

内部監査人協会（ＩＩＡ）

◈序論

ここ数年間にわたってリスク管理のコーポレート・ガバナンス強化への重要性がますます認識されてきている。組織は直面する、財政上および事業上はもちろん、社会的、倫理的および環境上のすべてのビジネス・リスクを識別するように、かつ組織の経営陣が受容可能な水準までビジネス・リスクをどのように管理するのかを説明するように、圧力をかけられている。同時に、組織がそれほど調和がとれていないリスク管理へのアプローチよりも組織の有利な点を認識するにつれ、全社的のリスク管理の枠組の使用は広がった。

内部監査は、アシュアランスおよびコンサルティングの両方の役割において、さまざまな方法でリスクの管理に貢献する。2002年に、イギリス・アイルランドの内部監査人協会（ＩＩＡ）が、許容される役割に関するメンバーに対するガイダンス、および内部監査の独立性および客観性を保護するために必要な予防措置を提供するために、リスク管理における内部監査の役割に関する姿勢声明を発表した。この改訂された新しい姿勢声明は、従来のものに代えてリスク管理および内部監査における分野で世界中の最近の進展を考慮に入れている。

◈全社的リスク管理とは何か

内部監査人は、すべての種類の事象または状況を識別、評価、管理、コントロールする

ために、リスク管理活動を引き受ける。これらの活動は、ただ１つのプロジェクトまたは狭義に定義された形態のリスク、たとえば、市場リスクから、組織全体が直面する脅威および機会まで及ぶ。

本姿勢声明で提示されている原則は、すべての形態のリスク管理における内部監査のかかわり合いの指導に適用できるが、われわれは、組織のガバナンス・プロセスを改善しそうであるという理由で、特に企業全体のリスク管理に興味を持っている。

全社的リスク管理（**Enterprise-wide Risk Management**：**ＥＲＭ**）は、その目的の達成に影響を与える機会および脅威を識別し、評価し、対応および報告を決定するために、組織全体のすべてにわたって構築されている、一貫しかつ連続したプロセスである。

◈ＥＲＭに対する責任

役員会はリスクが管理されていることを確実にする総合的責任を負っている。実際には、役員会はリスク管理の枠組の運用を経営陣に委任するであろうし、経営陣は以下に示す活動を遂行する責任を負うであろう。そこには、これらの活動の調整およびプロジェクト管理を行い、専門的技術および知識を生かす別々の機能があるかも知れない。

組織内の全員が全社的リスク管理の成功を確実にする役割を果たすが、リスクの識別および管理を行う主たる責任は経営者にある。

◈ＥＲＭの利点

ＥＲＭは組織目的の達成に対するリスクの管理を助長することに対して主要な貢献をすることができる。その利点には以下が含まれる。

＊それらの目的を達成するという大きな見込み
＊異種リスクに関する役員会レベルでの総括報告
＊主要なリスクおよびそれらの広範なかかわり合いに関するより深い理解
＊絡み合うビジネス・リスクの識別および共有
＊真に重要な問題に対する経営者による本格的な焦点の絞込み
＊少ない予期せぬ事態または危機
＊正しいことを正しい方法ですることに対する内部的焦点の集中
＊イニシアチブが達成される変化の見込みの増大
＊より大きい見返りでより高いリスクを抱える能力
＊多くの情報に基づくリスクの引受および意志決定

◈ＥＲＭに含まれる活動

＊組織の目的の明確な表現および伝達
＊組織のリスク・アペタイトの決定
＊リスク管理の枠組を含む適切な内部環境の確立
＊目的の達成に対する潜在的な脅威の識別
＊リスク、すなわち脅威発生の衝撃および見込みの評価
＊リスクへの対応の選択および実行
＊コントロールおよび他の対応活動の引受
＊組織内のすべてのレベルにおける一貫した方法によるリスクに関する情報の伝達
＊リスク管理のプロセスおよび結果の中

枢的モニタリングおよび調整
＊リスク管理の有効性に関するアシュアランスの提供

◈ＥＲＭに関するアシュアランスの提供

役員会またはそれに相当する機関の主な要求の１つは、リスク管理プロセスが有効に稼働しており、かつ主要なリスクが合格水準に管理されている、というアシュアランスを獲得することである。

おそらくアシュアランスは異なるソースからもたらされる。それらの中で経営者からのアシュアランスが基本となる。これは客観的アシュアランスの提供によって補完されなければならないが、このアシュアランスにとって内部監査は主要なソースである。その他のソースには外部監査および独立した専門家のレビューが含まれる。内部監査は通常３つの領域でアシュアランスを提供するであろう。

＊デザインおよびどれだけうまく作用しているかの両方のリスク管理プロセス
＊リスクに対するコントロールの有効性および他の対応を含む、「主要なもの」として分類されたリスクの管理
＊リスクの確実かつ適切な評価並びにリスクおよびコントロールの状況に関する報告

◈ＥＲＭにおける内部監査の役割

内部監査は、独立的、客観的なアシュアランスおよびコンサルティングの活動である。ＥＲＭに関する中心的な役割はリスク管理の有効性に関する客観的アシュアランスを役員会に提供することである。

現に、内部監査が組織に対して価値を提供する最も重要な２つの方法は、主要な事業リスクが適切に管理されているという客観的アシュアランス並びにリスク管理およびインターナル・コントロールの枠組が有効に機能しているというアシュアランスを提供することにあると取締役と内部監査人が同意していることを調査が証明した（注１）。

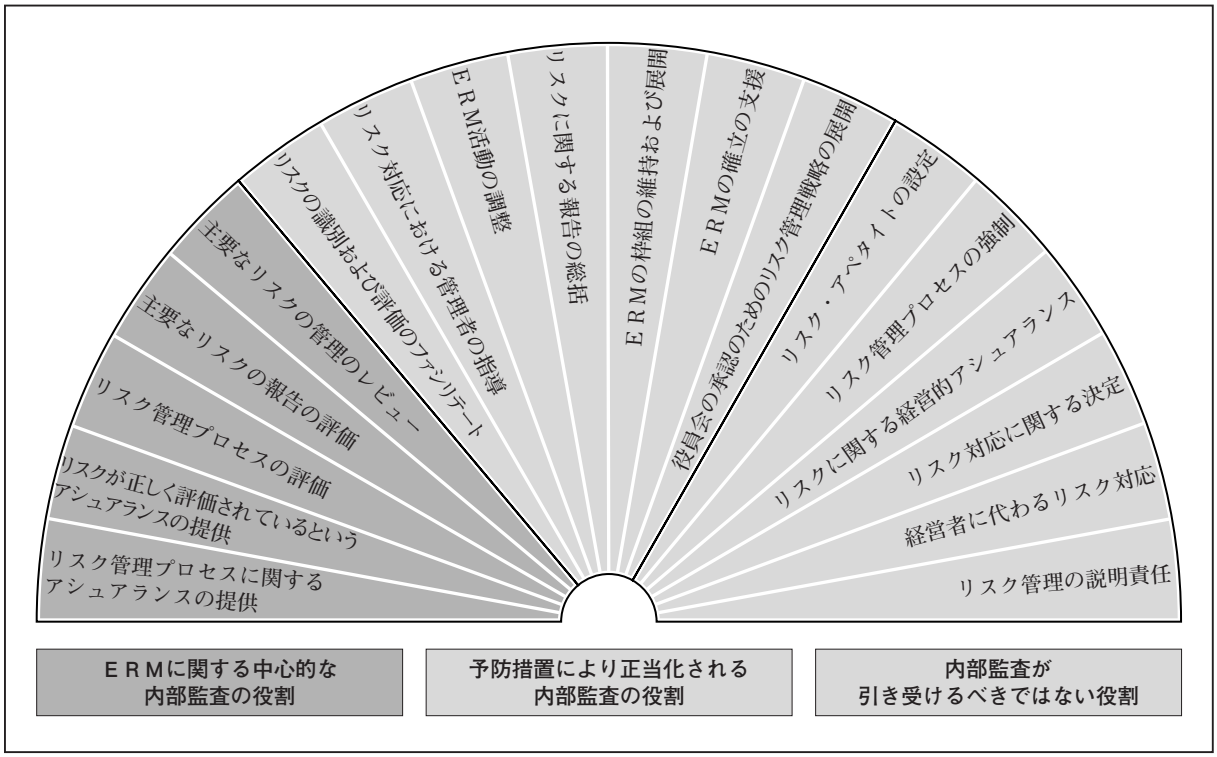
図１は、ＥＲＭ活動の範囲を表示しかつ有効な専門的内部監査の機能が果たすべき役割および同程度重要な引き受けるべきではない役割を示している。内部監査の役割を決定するときに考慮に入れるべき重要な要因は、その活動が内部監査機能の独立性および客観性に対する何らかの脅威も高めるか、そしてそれが組織のリスク管理、コントロール、およびガバナンス・プロセスを改善しそうであるか、である。

図１の左の活動はすべてアシュアランス活動である。それらはリスク管理に関するアシュアランスの提供のより広範囲の目的の一部を形成する。『内部監査の専門職的実施の国際基準』に準拠した内部監査の機能は少なくともこれらの活動のいくつかを実行することができかつ実行するべきである。

内部監査は組織のガバナンス、リスク管理、コントロールのプロセスを改善するコンサルティング・サービスを提供するかも知れない。ＥＲＭにおける内部監査のコンサルティング範囲は役員会が利用可能なその他の内部および外部のリソース並びに時間の経過につれて変質しそうな組織のリスク・マチュリティ（注２）によって決まるであろう。リスクの考慮、リスクとガバナンスの関連の理解および促進における内部監査の専門的技術は、特にその導入の初期の段階で、ＥＲＭの擁護者およびプロジェクト・マネジャーをも務める資格は十分にある。

組織のリスク・マチュリティが増大し、リスク管理が事業活動にしっかりと組み込まれるにつれて、ＥＲＭの擁護における内部監査

＜図１＞ＥＲＭにおける内部監査の役割



の役割は減るかも知れない。同様に、もしも組織がリスク管理の専門家または機能のサービスを使うならば、内部監査は多くのコンサルティング活動を引き受けるよりもアシュアランスの役割に集中することによってもっと多くの価値を提供できるであろう。

しかしながら、内部監査が図１の左のアシュアランス活動によって示されているリスク・ベース・アプローチを未だとっていないのであれば、中枢のコンサルティング活動を引き受ける態勢にはなかろう。

◇コンサルティングの役割

図１の中央部は内部監査がＥＲＭとの関連で引き受けるかも知れないコンサルティングの役割を示している。

一般に、内部監査が指針盤の右に向かえば向かうほど、その独立性および客観性が維持されていることを確実にすることを求められる予防措置がますます重要となる。内部監査が引き受けられるいくつかのコンサルティングの役割は以下のとおりである。

＊リスクおよびコントロールを分析するために内部監査によって使用される管理ツールおよび技術の利用
＊リスク管理およびコントロールにおける専門的技術、および組織に関するその総合的知識を強化することにより、組織へのＥＲＭの導入における擁護者となること
＊研修会を実施し、リスクおよびコントロールに関し組織を指導し、さらに共通語、枠組、および理解が発展するよう促進することによる助言の提供
＊調整、モニタリング、およびリスクに関する報告の中枢としての行動
＊リスクを軽減する最良の方法を識別するために働く管理者の支援

コンサルティング・サービスがアシュアランスの役割と矛盾していないかどうかの決定における重要な要因は、内部監査人が何か経営者の責任を引き受けているかどうかを裁定することである。実際のリスク管理において

いかなる役割も負っていない限り（それは経営者の責任である）、および上級経営者が積極的にＥＲＭを是認して支持する限り、内部監査はコンサルティング・サービスを提供することができる。

われわれは、経営陣がリスク管理のプロセスを設定または向上させることを支援するために内部監査が行動するつど、その業務計画がそれらの活動のための責任を経営陣のメンバーに移すために明確な戦略およびスケジュールを含むべきである、と勧める。

◇予防措置

ある状態が適用されるならば、内部監査は、図１に示されているように、ＥＲＭにおけるその関与を拡張するかも知れない。その条件は以下のとおりである。

＊経営者がリスク管理の責任を負っていることが明確でなければならない
＊内部監査の責任の本質は、監査基本規定に記録され、監査委員会によって承認されなければならない（注３）
＊内部監査は経営者に代わっていかなるリスクも管理してはならない
＊内部監査は、経営者に対して、彼らが自らリスク管理の決定を行うのとは対照的に、忠告、異議の申立、支援を提供するべきである
＊また、内部監査は、責任があるＥＲＭの枠組のいかなる部分であろうとも、客観的アシュアランスを与えることはできない。そのようなアシュアランスは他の相応の適任者によって提供されるべきである（注４）
＊いかなるものであろうとも、アシュアランスを超えた業務はコンサルティング・サービスとして認識されるべきであり、かつそのような業務に関連する実務基準に従うべきである（注５）

◈技能および知識体系

内部監査人およびリスク・マネジャーは何らかの知識、技能、および価値感を共有する。両者は、たとえば、コーポレート・ガバナンスの要求を理解し、プロジェクト管理、分析、およびファシリテーションの技術を持ち、極端なリスクの引受または回避の行動よりも、むしろリスクに関する健全な平衡感覚を持つことを尊重する。

しかしながら、リスク・マネジャー自身は組織の経営だけに務め、独立的、客観的なアシュアランスを監査委員会に提供する必要はない。また、ＥＲＭにおける彼らの役割を拡大しようとする内部監査人は、ほとんどの内部監査人にとって知識体系の外にある（リスクの転嫁、リスクの定量化、およびモデル作りの技法等の）リスク・マネジャーの知識の専門領域を過小評価するべきではない。適切な技能および知識を示すことができない内部監査人は、リスク管理の領域の仕事を引き受けるべきではない。

さらに、内部監査組織の長は、適切な技能および知識が内部監査機能の中で利用可能ではなく、かつ他から得ることもできなければ、この領域でコンサルティング・サービスを提供するべきではない（注６）。

◈結論

リスク管理はコーポレート・ガバナンスの基本的な要素である。経営者は役員会を代表してリスク管理の枠組を確立しかつ運用する責任者である。全社的リスク管理は、一貫したかつ調整されたアプローチを構築した結果として多くの利益をもたらす。

ＥＲＭと関連した内部監査の中心的な役割は、リスク管理の有効性に関するアシュアランスを経営者および役員会に提供することであるべきである。内部監査がこの中心的役割

を超えてその活動を広げている場合は、その業務をコンサルティング・サービスとして取り扱うことを含み、したがって、すべての関連する基準の適用を含んでいる確実な予防措置を活用するべきである。

こうして、内部監査は、その独立性およびアシュアランス・サービスの客観性を保護するであろう。ＥＲＭは、これらの制約の中で、ＥＲＭ自体の評価の高揚および内部監査の有効性の増加を助長することができる。

（注１）The Value Agenda, Institute of Internal Auditors-UK and Ireland and Deloitte & Touche 2003
（注２）The IIA-UK and Ireland Position Statement on Risk Based Internal Auditing 2003
（注３）Attribute Standard 1000.C1
（注４）Attribute Standard 1130
（注５）Perfomance Standards 2010,C1, 2110.C1 & C2, 2120.C1 & C2, 2130.C1, 2201.C1, 2210.C1, 2220.C1, 2240.C1, 2330.C1, 2410.C1, 2440.C1 & C2 and 2500.C1
（注６）Attribute Standard 1210

＜用語集＞

アシュアランス業務（Assurance Services）

リスク管理、コントロール、またはガバナンス・プロセスに関する独立的評価を提供する目的で組織のために行う証拠の客観的調査である。例として、財務、業績、コンプライアンス、システム・セキュリティ、およびデュー・デリジェンス業務に関する業務がある。

役員会（Board）

役員会は、取締役会、監督委員会、政府機関または立法機関の長、非営利団体の理事会または評議会、のような統治組織である。

擁護者（Champion）

人あるいは運動を支持および護る人である。したがって、リスク管理の擁護者は、その利益を促進し、組織の管理者およびスタッフが実行するためにとらなければならない行動において、彼らを教育し、彼らのとる行動を激励し支持するであろう。

コンサルティング・サービス（Consulting Services）

依頼部門と同意した内容および範囲の、しかも、内部監査人が経営の責任を引き受けずに、組織のガバナンス、リスク管理、およびコントロールのプロセスに、価値を付加しかつ改善することを意図した、助言および関連する依頼部門に対するサービスの活動である。たとえば、カウンセリング、助言、ファシリテーション、およびトレーニングを含む。

コントロール（Control）

リスクを管理し、設定した目的および目標が達成されるように実現可能性を高めるために、経営者、役員会、および他の関係者がとるあらゆる行為である。経営者は、目的および目標が達成されるという合理的アシュアランスを提供するために、計画し、組織し、満足のいく行動の実行を指揮する。

事業体（Enterprise）

一連の目的を達成するために設立されたあらゆる組織である。

全社的リスク管理（Enterprise-wide risk management（ＥＲＭ））

事業体目的の達成に影響を及ぼす機会および脅威の識別、評価、対応の決定、および報告を行うために、組織の全体にわたって構築された、着実でかつ連続するプロセスである。

ファシリテート（Facilitating）

グループ（または個人）が、そのグループが会合または活動のために合意した目的の達成を容易にするために、グループ（または個人）とともに働くことである。これは、そのグループおよびメンバーに対する聴取、反論、観測、質問、支持を含む。これは業務の実行あるいは決定を含まない。

リスク（Risk）

目的の達成に影響を与えそうな事象が発生する可能性である。リスクは影響および発生の可能性で測定される。

リスク・アペタイト（Risk Appetite）

役員会または経営者が許容できるリスクのレベルである。これは、異なったグループのリスクに対して、または個々のリスクのレベルにおいて、組織の全体との関連で設定されよう。

リスク管理の枠組（Risk Management Framework）

組織がリスク管理のプロセスを実行するために選択した構造、体系、手続、および定義の総体である。

リスク管理のプロセス（Risk Management Processes）

潜在的事象または状況を識別、評価、管理、コントロールして、組織目的の達成に関して合理的アシュアランスを提供するプロセスである。

リスク・マチュリティ（Risk Maturity）

経営者が組織の目的の達成に影響を及ぼす機会および脅威の識別、評価、対応の決定および報告のために、計画したとおりに、組織の全域で確固たるリスク管理アプローチが採用されかつ適用されている範囲である。

リスク対応（Risk Responses）

組織が個々のリスクを管理するために選定する措置である。その主たる範疇はリスクを許容することであり、リスクの影響または発生の可能性を減少させるように取り扱うことであり、リスクを別の組織に移すまたはリスクを生み出す活動を終了することである。インターナル・コントロールはリスクを取り扱う１つの方法である。

＜参考文献＞

＊Risk Management:Changing the Internal Auditor's Paradigm by Georges Selim and David McNamee, IIA Research Foundation
＊IIA Professional Briefing Note 13:Managing Risk, IIA-UK and Ireland
＊The Complete Guide to Business Risk Management by Kit Sadgrove, Gower
＊Operational Risk and Resilience: Understanding and minimising operational risk to secure shareholder value by PriceWaterhouseCoopers, Butterworth Heinemann
＊Risk Management Guide 2001, White Page
＊It's a Risky Business, CIPFA
＊The Risk Management Standard, IRM, AIRMIC and ALARM
＊ANZ Risk Management Standard, Standards Australia and Standards New Zealand
＊Enterprise Risk Management Framework, COSO
＊Risk Management in the Public Services, CIPFA &ALARM
＊Independence and Objectivity - Professional Issues Bulletin 2003, IIA - UK and Ireland
＊Embedding Risk Management into the Culture of your organisation - Professional Briefing Note 2003, IIA -UK and Ireland
＊Managing business risk - Adam Jolly, IOD, Ernst & Young and Kogan Page

＊The universe of risk - Pamela Shimell, Pearson Education and FT
＊Management of risk - OGC, TSO
＊Enterprise wide risk management - James Deloach, Pearson Education and FT
＊Risk - John Adams, Routledge
＊Risk management for company executives - John Smullen, Pearson Education and Financial Times Prentice Hall
＊Enterprise Risk Management:Trends & Emerging Practices - Miccolis,Hively,and Merkley, IIA Research Foundation
眞田光昭訳『全社的リスクマネジメント―近年の動向と最新実務』日本内部監査協会、2004年７月
＊Enterprise Risk Management:Pulling it All Together - Walker, Shenkir and Barton, IIA Research Foundation
刈屋武昭監訳『戦略的事業リスク経営―ノーリスク・ノーマネジメント』東洋経済新報社、2004年11月

＜ウェブサイト＞
＊The Institute of Internal Auditors, www.theiia.org
＊Institute of Internal Auditors - UK and Ireland, www.iia.org.uk
＊Gee Publishing, www.gee.co.uk
＊Corporate Governance Site, www.corpgov.net
＊The Committee for Sponsoring Organizations（ＣＯＳＯ), www.coso.org
＊The Institute of Risk Management（ＩＲＭ), www.theirm.org
＊The Association of Insurance and Risk Managers（ＡＩＲＭＩＣ), www.airmic.com
＊The National Forum for Risk Management in the Public Sector（ＡＬＡＲＭ), www.alarm-uk.com
＊White Page web-site, www.whitepage.co.uk
＊Standards Australia, www.standards.org.au
＊Standards New Zealand, www.standards.co.nz