日本語訳への序文

国際アクチュアリー会（IAA）の Enterprise and Financial Risk 委員会は保険監督者国際機構（IAIS）の「Standard on Enterprise Risk Management for Capital Adequacy and Solvency Purposes (October 2008)」をベースに、日本語訳のもととなった「Note on Enterprise Risk Management for Capital and Solvency Purposes in the Insurance Industry (31 March 2009)」を発表しました。

IAA の「Note on ERM」はエンタープライズ　リスクマネジメントに関する、これまでの保険業界における経験、関係者が発表したモデルや枠組み等を盛り込んだ「解説書」とでも言えるもので、2009 年 11 月に日本アクチュアリー会も署名に加わった「グローバルな ERM 資格認定に関する協定書」に基づく CERA(Chartered/Certified Enterprise Risk Actuary/Analyst)資格取得のためのシラバスでも主要な参考書の一つとして指定されています。

本会報別冊は、保険会社のＥＲＭについてまとまった記載のある文献の一つとして、ＥＲＭに関心を持つアクチュアリー、その他関係者にとって参考となるものを提供する目的で、ＥＲＭ委員会のメンバーで作成したものです。訳文については、極力原文に忠実なものとなるよう努めましたが、不適切な部分等がありましたら、添付した英文を参照頂くとともに、お気づきの点をご連絡頂けると有難いと思います。

なお、ERM の実践にはゴールや、それを達成するための完璧な教科書というようなものはあり得ず、社会・経済環境に応じて組織の目的達成努力を重ねていくことが必要と思います。実際、IAIS は現在上述の ERM に関する基準等の見直しを進めていますし、そもそも IAA の「Note on ERM」は、作成時期の関係で金融危機前に発表された資料や考え方を参照しているため、そのうちのいくつか（例えば、P4 図にあるようなリターン最適化を究極とするＥＲＭ進化の考え方）は金融危機を踏まえた反省の対象でもあることに注意が必要です。

【今回の翻訳作成メンバー（敬称略、五十音順）】

江戸正寿　黒岩和夫　酒井重人　須江隆太郎　田中周二　田中和宏　内藤和晃　平林宏治　松山直樹　森口康弘（リーダー）　吉田英幸

上記の他、途中段階やレビューでご協力いただいた皆様に感謝申し上げます。

2010 年７月

ERM 委員会 委員長 吉村雅明

※本訳文は教育用教材として IAA 事務局から了解を得て翻訳したものです。

保険業界における
資本とソルベンシーにかかわる
エンタープライズリスクマネジメント (ERM)
に関する報告書

2009 年 3 月 31 日

国際アクチュアリー会

謝辞

本報告書の作成にあたっては、多くの関係者と団体からご協力いただいた。

まず、本報告書作成プロジェクトを推進・支援された国際アクチュアリー会（IAA） の Enterprise and Financial Risk Committee の各委員のご尽力に対し最大の感謝を申し上げたい。当委員会の詳細については、国際アクチュアリー会の HP、 www.actuaries.org の「Committees」欄を参照のこと。

IAG (Insurance Australia Group) は、本報告書の執筆と作成に関して主導的な役割を果たされた。特に、本プロジェクトのスポンサーである IAG の最高リスク管理責任者（Chief Risk Officer）であるトニー・コールマン氏、ならびに本報告書の主要執筆者を務め、同社の Head of Group Risk & Compliance であるピーター・サザーランド氏のご尽力に対し感謝の意を表したい。それ以外にも、多くの IAG 社員からアイデアの提供、事例研究の執筆、ドラフトの検討などの援助をいただいた。

事例資料の作成については、アーンスト・アンド・ヤング、KPMG、PWC の 3 社の協力を仰いだ。これらのコンサルティング会社から提供された国際的な事例に基づき、実務上の課題点が明瞭になっている。

また、スタンダード&プアーズ社からは、業務モデルを異にする複数の企業が自ら公表した ERM の基準や、格付けの対象となっている企業の ERM 活動に関する公開の格付け評価レポートによる検証をベースとして、ERM を導入した際に用いた手法の事例をご提供いただいた。

最後に、保険監督者国際機構（IAIS） に対して感謝の意を申し上げる。国際機構のメンバーは本報告書の作成を強く支持され、2007 年と 2008 年に開催されたソルベンシー小委員会においてドラフトの検討を行っている。

ISBN 978-0-9812787-4-2

Association Actuarielle Internationale
International Actuarial Association
150 Metcalfe Street, Suite 800
Ottawa, Ontario
Canada K2P 1P1

www.actuaries.org
電話:1-613-236-0886　　ファックス:1-613-236-1386

メール:secretariat@actuaries.org

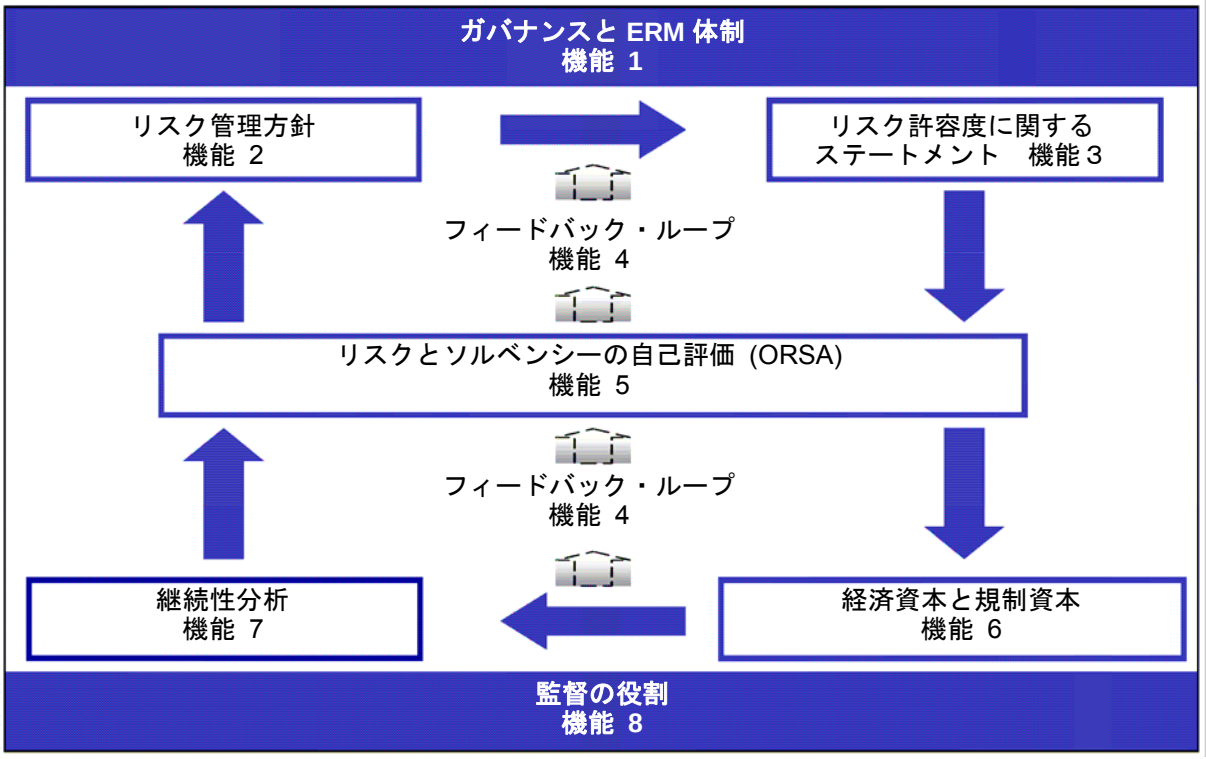
目　　次

1. はじめに

言うまでもなく、保険とリスク管理との間には極めて密接な関連があり、近年、経営方法と業績の改善を求める保険者の間で、エンタープライズリスクマネジメント (ERM) のコンセプトを採用するケースが増加している。市場と経営環境が複雑化し相互依存性を高める中で、ERM はリスク管理のための適切な対策であり、またその解決策であるという認識が高まっている。保険監督者もまた、保険者が適切なリスク管理体制を導入するための基準の設定や保険者への指針の提供を通じて主導的な役割を果たしてきた。

本報告書は、保険監督者国際機構 (IAIS) が監督者のために設定した基準や指針を支援することを目的として、IAA が保険者のために作成したものである。本報告書は、業界における経験、監督者による監督業務の慣行、関係者が発表したモデルや枠組みに基づいており、実務面への配慮を重視したものとなっている。本報告書はまた、リスク管理が高度化する段階ごとに見られる特徴を尺度として、保険者が自社のリスク管理体制の成熟度を評価することを助けることを目的としている。

IAIS 基準には、8 つの重要な機能が述べられており、本報告書は、それぞれの重要機能ごとにその詳細を説明し、保険会社の経営陣が自社の保険業務に ERM 体制を導入する際に直面する戦略面・運用面の課題を解決するための一助となるよう作成されている。本報告書の内容は、ERM を導入する際に考慮すべき事項や他社が採用した解決策に関する情報であり、守るべき処方箋ではない。ただ一つの正しい方法というものはなく、保険者ごとの状況に応じて適切な手法は異なる。添付資料 8 に、本報告書の内容に関する詳細な参考資料のリストを記載した。



1.1 報告書の作成

本報告書の作成にあたっては、Federation of European Risk Management Associations と Standards Australia からそれぞれ発表された総合的な「リスク管理基準」を参照している。また、コンサルティング会社、監督者、学者、業界の専門家から発表された資料もあわせて参照している。内容の理解を深めるために、本報告書全体を通じて豊富な事例とヒントが記載されており、更に、ERM リスク管理体制の導入に役立つ詳細な事例研究、指針および提案を内容とする多くの附属書類が用意されている。

1.2 作業の前提

本報告書は生命保険会社と損害保険会社の両方を対象として作成されている。本報告書で取り上げたコンセプトの適用にあたっては、保険会社ごとに経験と成熟度に大きな差異が存在するが、本報告書では簡明なコンセプトに基づく、段階的に導入可能であり実用的な原則に基づく枠組み、すなわち、保険の専門家が基礎的な ERM から高度の ERM へ移行することを可能にする要素を提供することを目的としている。

紹介された事例と枠組みの多くは、大規模な企業の事例に基づいてはいるが、その内容は中小規模の企業にとっても同様に応用可能なものである。小規模な企業であっても高度の ERM を実施可能だが、この場合は社内ですべての作業を実施せずに一部の作業を外部委託する方法が考えられる。また、小規模な企業であれば包括的な ERM を導入せずに、不可欠な ERM だけを行う選択も可能である。以上の選択は、ERM の基本原則であるリスクとリターンの比較考量に基づくビジネス判断となる。本報告書においては、中小規模の企業に役立つ指針となるコメントも可能な限り記載している。

本報告書は、ERM 業務とその実行に伴う課題に関するアクチュアリーやその他のリスク管理専門家の意識を高め、その理解を求めることによって、国や地域を問わずすべての保険者に適用される IAIS の基準と指針を支持することを目的としている。

1.3 現状の説明

ERM に関してはすでに多くの著述が存在している。それは 21 世紀の企業行動が一層複雑で、不確実で、不明確なものへと変容していることに対する、当然かつ自然な結果である。現在の経営管理はすべてリスク管理と関係している。企業が経営目標を達成するためにはリスクが伴う。一部のリスクは統制が不可能だが、多くのリスクは、直線的な形、すなわちリスクを識別・評価・軽減し、更に必要がある場合には移転することによって管理が可能であり、また管理する必要がある。しかし、現実のリスクは決して直線的なパターンではなく、動的な外部の影響と(予測不可能な)人間の行動との複雑な相互作用を伴う。コンセプトレベルにおいては、ERM は、従来のリスク管理やサイロ型のリスク管理では 21 世紀の保険事業を支えられないという冷静な判断に基づいている。

通常、「リスク」と「リスク管理」という言葉は、「悪い」事態の発生を防ぎ、ダウンサイドを限定することとして理解されている。これはもっともな見方であるが、リスクを価値の維持と創造に結びつけて考える、より高度な考え方も生まれている。こうした見方では、投資機会の活用が正当視され、事実、専門家の間では、市場の投資機会を予測し対応する能力が、事業崩壊の重大な危険への対応能力に劣らず重要であると理解されている。さらに、リスク管理の企業文化が重要であり、効果的な ERM 活動と密接に結びついている。

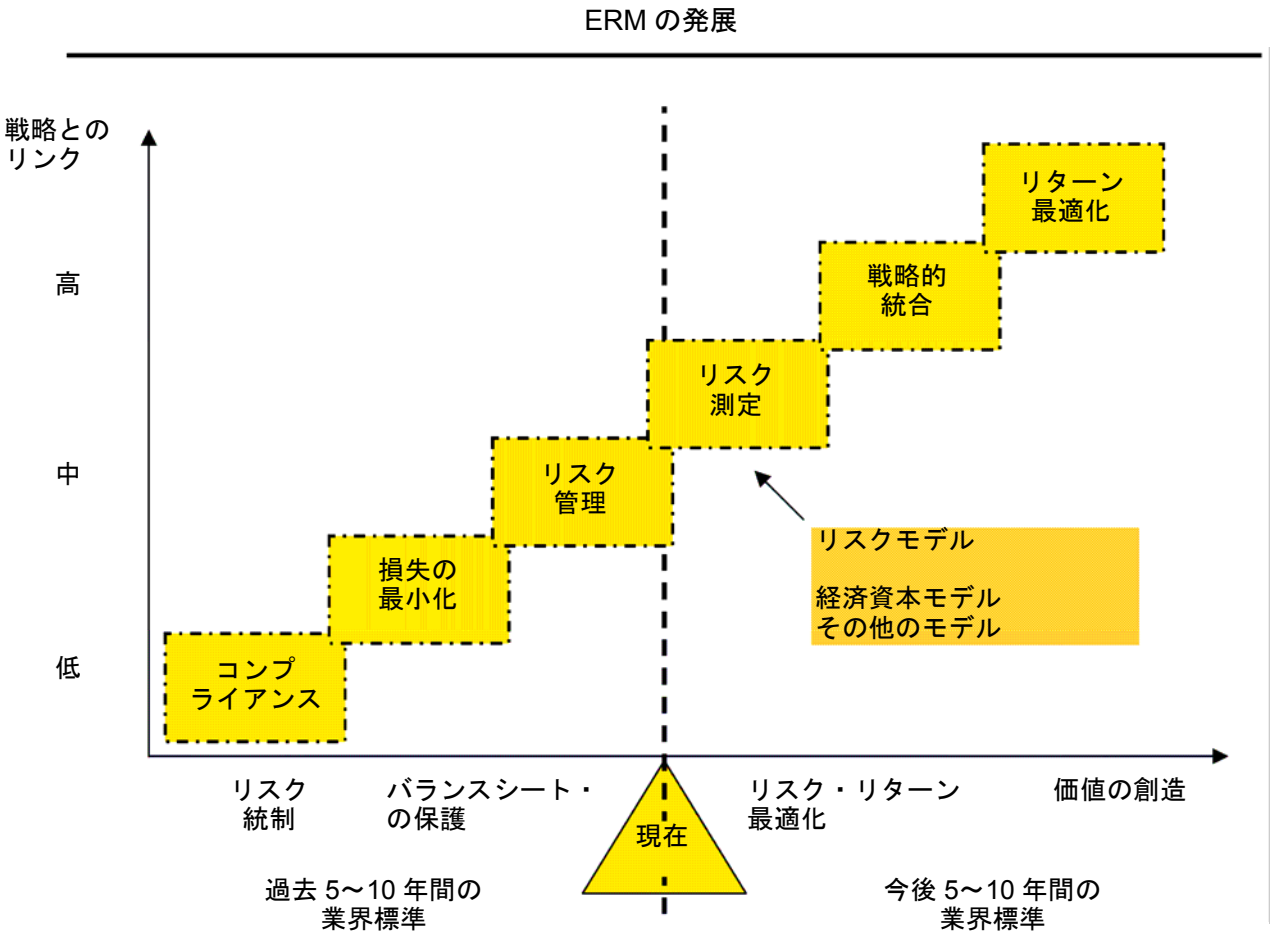
効果的な ERM は事業戦略の策定と不可分の関係にある。ERM と保険者の事業計画サイクルを統合することによって、会社の意思決定（事業ラインの拡大、買収、新商品開発、新規チャネルなど）を、リスク調整後ベースで行い、また ERM 活動による完全なサポートと情報提供を受けることが可能となる。さらに、企業の事業戦略に合致した年間のリスク予算・資本の配分をリスクタイプごとに行うことも可能となる。また、年度末の資本と業績の測定をリスク調整後ベースで行い、価値創造の全サイクルを完結することができる。

有効な全社的リスク管理の導入は容易な作業ではなく、また既存の機能に単に追加すれば済むものでもない。そのためには、モデリングと分析の能力向上のための新たな投資、リスクと資本を異なる角度から把握する方法、リスク管理をあらゆる企業活動に浸透させるための企業文化の変化が必要である[1]。

監督者と格付機関の間で保険者に対し日常の事業管理に ERM の手法の適用を求める声が高まっており、これも ERM の重要性の現れである。

[1] Risk Management Risk Opportunity, The 2006 Tillinghast ERM Survey.

1.4 ERM の歴史



The Role of ERM in Ratings, Mark Puccia, Managing Director, Standard &Poor's (2007 年 3 月 30 日)

1.5 ERM とは

一般に認められている ERM の定義はなく、またそうした定義は ERM のコンセプトからしてありえないかもしれない。その一方で、ERM に関連して頻繁に使われるテーマや用語があることも事実である。現在一般に入手できる ERM の文献に見られるさまざまな定義の中にも一貫して「全体的(holistic)」、「統合的」、「トップダウン」、「戦略的手法」、「価値主導（value driven）」などの用語が使用されている。増え続ける ERM の定義を増やすことが本報告書の目的ではなく、むしろ、本報告書は、さまざまな定義から浮かび上がる共通のテーマと原則を念頭において作成されている。

要約すると、以下の原則が本報告書の基盤である。

- ERM は、保険者が直面するあらゆるリスクをその対象とすること
- ERM は、保険契約者に対する契約の履行を確実とする中で、保険者のオーナーに対する価値の創造を目的とすること

より具体的に言うと以下のようになる。

- ERM は、保険者の事業に影響を及ぼす可能性がある、社内外の一切のリスクの源泉を識別、評価、処理、モニター、報告または伝達するための保険者の社内システム、構造、プロセスの全体を対象とする
- ERM は、保険者の全事業を通じて共有されるリスク管理上の統一的な「言語」を意味する
- ERM は、リスク管理機能を組織的に構成し、その相互の連携を図ることを意味するものである。すなわち、専門家による孤立した「サイロ」型のリスク管理は ERM の基本的な考え方と相容れない
- ERM は、下方リスクだけでなく、上方リスクの管理もその対象とする
- ERM は、あらゆるリスクの定量化を図るが、すべてのリスクの金銭的または財務的な評価は不可能であることを認める
- ERM は、行動 (リスク管理の企業文化)とリスク管理のプロセスの双方を対象とする
- ERM は、過去の出来事(損失など)、現在のパフォーマンス(リスク指標など)および将来の結果（リスクプロファイルやリスク評価）に関係するリスク情報を全体的に考慮する

上記の原則以外にも、保険者の全社員がリスク管理に責任を負い、特定のリスク専門家だけの責任ではないことに留意する必要がある。これは、リスクの引受とその管理が保険事業と一体不可分のものであることの反映である。その他、ERM が定着するためには以下の条件が満たされる必要がある。

- 経営幹部からの明確なサポートが不可欠であること
- ERM と事業戦略ならびに日常業務が密接かつダイレクトに結びついていること

リスク管理業務の各側面に責任が明確に規定され、ラインの事業管理部門の役割とリスク管理部門の役割が区別されている必要がある。自社の事業に関して ERM を正式に定義する場合には、これまでに発表された様々な定義を検討する必要があるが、代表的な定義を添付資料 1 に記載している。

多くの保険者にとって、ERM の導入は簡単な作業ではなく、また短期間に実行できる事業でもない。ERM の導入によってガバナンスと経営のあり方に根本的な変化が生じ、多様な能力開発投資や新しいプロセスの導入や包括的な改革プログラムの実施が必要とされる場合が存在しうる。先端的な制度を採用している数多くの保険者も時間をかけて ERM を段階的に導入したと述べており、ERM の導入を考える際には、こうした考え方が適切であると考えられる。

1.6 戦略的考慮・出発点

ERM の導入の指示・計画・提案は、周到な調査と分析に基づいて行われる必要がある。また、ERM の導入が社内的な要請であるか社外的な要請であるかを問わず、リスク管理者は拙速的な ERM の採用を避ける必要がある。

導入の成否を左右するのは、取締役会の協力と支援であり、そのためには、ERM は、取締役会が ERM について知りたい事項、知らなければならない事項を取締役会に報告する必要がある。

事例:
優先順位の設定に関して取締役会が果たすべき役割

世界的に事業を展開している大規模な多国籍企業が、次のような組織上の諸課題を解決するために、ERM の戦略と枠組みの構築に着手した。

- *各地域からの戦略と資本配分の要請の整合*
- *コミュニケーションの透明性と速度*
- *意思決定の明瞭性と責任*
- *経営、内部統制とプロセスの有効性と効率性を取締役会に保証すること*

内部監査人が取締役会から組織のリスクプロファイルの作成とERM の戦略と体制の立案を命じられた。内部監査と保証責任を重視した包括的なプログラムの導入が提案されたが、プログラムへの時間的な投資が主として監査ニーズに関するもので、最大の関心事である事業の成長や収益性があまり考慮されていないことが分かると、経営幹部の間で不安が広まり、プログラムに投入する時間と取り組みに対する「優先順位を下げる」動きが見られ始めた。プログラムの導入に支障が生じ始め、アプローチを変更する必要が明らかとなった。

そこで、取締役会と経営陣は、ERM への相当額の投資を主要な利害関係者の優先順位と期待に合致させるために作業を再スタートさせた。

- *取締役会は、経営陣ならびにリスクと保証を担当する部門と協力して、各利害関係者のニーズや一切の作業やリスク管理活動のアウトプットと成果の明確化を行った*
- *作業チームは、多様な利害関係者のニーズと事業上の必要性に応じて活動と成果の優先順位を定め、順序付けを行った*
- *取締役会は、すべての利害関係者から実施計画、そのタイムテーブル、投資に関するコミットメントと責任の約束を得た*

ERM の重点分野に関して優先順位を設定し、順序付けることによって、3者すべてがERM 導入のステップ、ならびにいかなる形と時間軸で事業上の価値を実現するのかが明瞭となった。

重要な教訓

1. *ERM は、組織が事業を営む方法を改革する機会を提供し、また事業上の必要性や利害関係者のニーズとの両立が不可能であるかもしれない課題を実現するために「利用可能」な数少ない全社的な事業能力の一つである*

2. *ERM の成果がすべての利害関係者を満足させることができない場合があるため、ニーズと期待を満たし、ERM への投資が最大限の成果をもたらし、かつ、すべてのエージェンシーや利害関係者に対するバイアスを最小限にするためには、取締役会の支持が不可欠である*
3. *取締役会は、ERM への投資を長期的に実施するための戦略的で全体的な視点からの判断を行うことができる*

ERM 導入計画は、大規模なプロジェクトであり、それによって一般的に生じる全社的な影響を避けることは不可能である。「ERM を実行する」任務を負うリスク管理者は、「失敗した」プロジェクト、とりわけ複雑な技術とビジネスプロセスの変更に係わるプロジェクトから多くのことを学ぶことができる。ERM に関して常に該当する重要な教訓は次のとおりである。

- ERM プロジェクトについて期待される成果に関する明確な目標の設定
- 特に、プロジェクトのリーダーと改革管理の役割において、厳正に選抜された経験豊富で適切な能力を備えた人材の配置
- 現実的な作業や時間軸を反映した詳細な計画を事前に策定すること
- ERM の適応範囲、マイルストーンの達成基準およびコストや便益を厳密に管理するプロセスを実行すること
- プロジェクトの全側面にわたる経営トップレベルのオーナーシップと責任の明確化(プロジェクトに関する適切なガバナンス)
- 導入の初期段階を通じて想定される「痛み」と要求されるサポートに関して現実的であること
- 複雑さ、コストおよび時間軸に関して現実的であること
- 徹底したリスク管理やリスク軽減戦略とサポート活動
- プロジェクトに関する客観的で透明性のある報告、ならびに「悪い情報」を上層部に迅速に伝達し（また、それを受け入れ）、問題に迅速かつ低コストで対応することを要求する企業文化

保険者はこれまで戦略的な手法を採用せず、新たな規制や事業の危機に対応する(両者は結びついている場合がある)ために、断片的にあるいは場当たり的にリスク管理体制を構築する傾向があった。内部統制、財務、保険数理業務、コンプライアンスまたは業務リスクの担当者に適切な体制の構築を依頼するケースが少なくなかった。こうした手法によっても通常適切なドキュメンテーションやレビュープロセスは実現可能だが、組織全体からの広範な支援が得られる可能性は乏しく、また多くの場合 ERM がコンプライアンス業務に類似したものであるという見方を強めてしまう。重要なことは、こうした手法には、ERM を保険者の価値観、企業文化、手法と整合させる方法に関する戦略的なとらえ方が欠けていることである。

添付資料 3 に、ERM の導入に関するさまざまな手法とそれに伴う問題点を記載している。

2. ガバナンスと ERM 体制

重要機能 1

保険者は、コーポレートガバナンス体制の一環として、事業とリスクの性質、規模および複雑性に対応した健全な ERM 体制を確立し、社内で運用する必要がある。またこうしたERM 体制と保険者の業務活動を統合し、適切に設定されたリスク管理方針に従って、望まれる事業文化と期待される行動を反映し、かつ合理的に予測可能であり、関連性がある保険者のあらゆる重要なリスクに対応する必要がある。ERM 体制の構築と運用は、保険者の取締役会と経営陣の指導と監督の下に行われる必要がある。

資本管理とソルベンシー目的に関して適切な体制を実現するためには、十分に広範な事態から生じうるリスクを適切な方法によって定量化する規定を設ける必要がある。

リスクの測定は、リスクについての適切に記述された解説および説明を提供する正確な文書化によって裏づけられるべきである。

2.1 はじめに

このセクションでは、ERM に関連するコーポレートガバナンス、経営管理、業務および企業文化などのテーマを扱う。

IAIS は「比例性」というコンセプトを重視している。これは、規制対象である企業の監督は、保険者がさらされているリスクの性質、規模および複雑性に見合ったものでなければならないという監督上の原則である。

この比例性原則は、ERM についても等しく当てはまる。一つの国で事業を営んでいる小規模な自動車保険者の ERM 体制と、生命保険のほかに「ショートテール」や「ロングテール」の損害保険を提供している世界的な規模の保険者が採用する ERM 体制は当然異なる。ここで達成しなければならない課題は、ERM 体制が保険者の性質、規模および複雑性に見合っていることである。

本報告書では、中小・大規模など規模を異にする保険者に参考となる事例研究とその他の事例を取り上げている。その大部分は、大規模な保険者の事例に基づいたものとなっているが、管理すべきリスクの性質、規模および複雑性にかかわりなく、提示された教訓とテーマはすべての保険者に該当するものである。

ただし、大規模な保険者で通常見られる ERM の特徴と小規模な保険者で見られる特徴には違いがある。小規模な保険者では、取締役会と経営陣の協働によるリスク監視体制（共同の監査・リスク・コンプライアンス委員会など）が設立されており、リスクの構成要素に対する経営資源の投入量は少なく、モデリングや測定に関する方法はそれほど洗練されていない傾向がある。これに対し、世界的で大規模な保険者の場合は、共通のリスク管理用語、標準的な分類、詳細な方針や指針およびトレーニング資料、リスク情報の収集に役立つ共通の報告様式とツール、リスク情報の収集、分析および報告のための高度なシステムを内容とする一貫性のある体制が採用される場合が多く見受けられる。

企業規模の大小を問わず、リスク管理の企業文化や行動学的な特徴は、常に個々の企業に固有のものであり、個々の企業の歴史、価値観、スタイルを反映したものとなる。どんなに進歩した ERM 体制であっても、それを支持する企業文化がなければ有効性は失われてしまうことになる。

添付資料 2 にリスク管理の「成熟度」に関するモデルを記載している。資料には保険者の ERM 体制の構成部分と初期、中期および最終段階に分けて一般的に見られる成熟度の特徴が示されており、保険者は、このモデルを基準として自社の ERM の成熟度を評価することができる。保険者が、その規模を問わず、ERM の構成部分ごとに異なった成熟度の達成をめざし、その事業の性質、規模および複雑性の程度に応じて特定の ERM の場面について独自の展開を求めることは極めて当然なことと考えられる。

2.2 リスク管理とコーポレートガバナンス全般

コーポレートガバナンスとは、株主、保険契約者、その他の利害関係者のために企業の業績と規則等への適合状況を改善することを目指すものであり、取締役会、経営者、保険者の株主の行動と 3 者間の関係を重視するものである。またコーポレートガバナンスとは一般に組織の命令、統制、説明責任に関するプロセスであると考えられている。

コーポレートガバナンスとの関連では、リスク管理は命令、統制および説明責任の遂行を可能とし、助けるものであると表現される。実際、コーポレートガバナンスとリスク管理の関係は、取締役委員会や取締役会の規約に基づく責任として表現されている。

ERM と保険者のコーポレートガバナンス体制とを適切に結びつけるためには、取締役会または取締役委員会が責任を負う「リスク」の範囲に、保険者が負うすべてのリスクが含まれている必要がある。

2.3 リスク管理と取締役会の役割

保険者の取締役会のリスク管理に関する役割は、全般的には良く理解されており、保険者のリスク管理体制の最終的な責任を担うことが了解されている。監督者を含めた利害関係者は、この最終的な責任の内容を次のように理解している。

- 保険者の全体的なリスク管理戦略・方針の承認
- 適切な責任者を確保するための人事プロセスの監督
- 保険者のリスク許容度の設定
- 適切なリスク管理と内部統制制度の実施を通じた主要リスクのモニタリング

リスク管理に関連する事項を専門的に扱う特別の委員会を取締役会が設立するのが一般的な慣行となっている。この委員会にはリスク、監査、財務報告、コンプライアンスなどの部門やそれらを兼任する機能を含めることが可能である。

リスク管理に関するリスク委員会の最も重要な課題はおおよそ次のとおりである。

> 取締役会が、保険者の重要なリスクの効果的な管理に関して、相当の注意、デリジェンス、能力を発揮して、責任を履行することを支援し、保険者のリスク管理と内部統制体制が適切であり、有効に機能していることを確認すること

リスク管理に関連する委員会規約では、最低限、以下の事項に関する監督責任が規定されているのが通常である。

- 保険者のリスク管理制度の実効性
- 監督上の要求に対するコンプライアンス
- 適切な独立性を備え、権限を有効に遂行可能な職権、地位および資源を備えたリスク管理部門の構築
- 企業リスクが充分に保険によってカバーされているかどうかのモニタリング

取締役会リスク管理委員会の規程の設定にあたっては、規程上の義務を有効に遂行するために必要な一定のプロセスに留意する必要がある。上記プロセスには、次のようなものが含まれるが、これらに限定されるわけではない。

- 保険者のリスク担当最高責任者と委員会との間に直接的な報告体制を設けること
- 正式な委員会会議の場以外に、委員会の委員長とリスク担当最高責任者との個別会議を定期的に開催すること
- 正式な会議以外に経営幹部が参加しない非公式な会議を行う時間を設定すること
- 委員が外部専門家のコンサルテーションを利用できること
- 取締役会リスク管理委員会および経営陣に対するリスク管理部門からの報告がフィルターにかけられることなく伝達される透明性のある報告体制を確立すること

適切な委員会制度を確立するためには、保険者のリスク管理機能が委員会にとって信頼できるものであることに留意する必要がある。両者には信頼関係が必要である。端的に言えば、委員会の目的は、リスクに関連する重要な問題や悪い情報の上層部への迅速な伝達が奨励される企業文化がある場合の方が達成される可能性が高まるのである。

ERM に関する企業文化や行動学的な側面は、本報告書のセクション 2.8 で詳述する。添付資料 4 にリスク委員会規程の一例を示す。

2.4 取締役会と経営者の責任

取締役会と経営者がそれぞれ担うリスク管理責任の内容には境界があり、また法令上・監督上の要請に従う必要があることは言うまでもない。取締役会（経営委員会）の役割には、保険者のリスクを日常的に積極的に管理することは含まれない。正確に言えば、経営者の役割には保険者のあらゆるリスクを管理し、報告を行う積極的なプロセスが含まれ、そうした経営者の役割を監視し、モニタリングすることが取締役会の役割となる。取締役会が両者の責任範囲を確定し、取締役会や委員会の会議を開催する際には、取締役会、具体的には取締役会リスク委員会が保険者のリスクの管理者であるという経営者の認識を避けることが特に重要となる。同様に、取締役会のリスク管理委員会が、経営者の重要なリスクに関する評価や経営者が重要なリスクの評価に対応するために導入したプロセスについて、質問し検討を行う適切な議論の場を提供するものであることが重要である。

アドバイス：有効なリスク委員会を設立するために注意すべき点

- リスク委員会が、多様な経歴を持ち、探求心、客観性、適切な経験などの適性を備えた委員によって構成されていること。委員を外部から採用し、幅広い経験を備えた委員会を構成すること。組織に関する知識も重要
- リスク委員会が、単に「チェック項目を承認」するアプローチではなく、提出されたレポートの内容や経営者に対して「積極的に質問する」状態を実現すること
- リスク委員会からの指示が、取締役会によってサポートされ、また適切なレベルの経営者によって支持される状態を確保すること
- リスク委員会に対する報告のレベルと件数の適切性を考慮し、委員会に上程され、検討される報告の「品質」を管理し、適切な情報の伝達が確保されていること
- リスク委員会が、先進的な方法や傾向を絶えずフォローし、組織のリスク管理プロセスを常に改善、進化させる責任を負うこと

リスク委員会は具体的で、計測・達成可能で、現実性があり、時間軸が設定された主要業績指標を含んだ適切な自己査定プログラムを採用すべきである。

2.5　経営者のコミットメントとリーダーシップ

保険者の CEO は、取締役会と経営者を結びつける重要なリンクとしての役割を果たす。

CEO が ERM またはリスク管理を重視していることが組織に理解されていないと、取締役会が利害関係者に対して企業文化と取締役会の基本方針や ERM に関して打ち出したコミットメントとの整合性を説得することが困難となる。

ERM に関して CEO と取締役会の優先順位の整合性を実現する最も具体的な方法は、CEO の職務内容とパフォーマンス評価に一定のリスク管理責任を含めることである。例えば、次のような方法が挙げられる。

- 明確で説得力のあるリスクの許容限度を明瞭に表現するリスク管理体制を推進すること
- リスク管理と統制システムの有効性と妥当性に関して取締役会に定期的な保証を提供すること
- 慎重なリスク管理を危険にさらす行動を許容しない環境をサポートすること

それ以外にも、リスク管理が保険者の「コア・コンピタンス」（訳注：他社に真似できない核となる能力）であると CEO と保険者のリーダー層が認めるか、または同様な言葉で評価する声明を発表することも、リスクの適正な管理が保険者の持続性にとって極めて重要であるという見方を一層強化する。

2.6　全社的リスク管理機能の設定と展開

保険者の CEO と取締役会が ERM 制度の導入を決定するためのシナリオを考えよう。更に、ERM 導入に向けたリーダーシップと明瞭なコミットメントを示すために、取締役会は CEO または場合により CFO に対して直接報告を行う最高リスク管理責任者（「CRO」）の採用が最初のステップであると判断した。CRO の主要な役割と責任を汎用的な CRO の職務説明書とともに添付資料 5 に記載している。

新任の CRO が最初に直面する重要な課題は、社内に分散したさまざまなリスク関連機能と専門家を集約して共通の制度と体制を構築することである。

新任の CRO は通常、社内のリスク管理体制がばらばらであることに気がつく。たとえば、

- 事業部門内に置かれた保険数理機能や調査機能
- 内部監査部門
- 事業継続専門家チーム

- 再保険部門や再保険の購入機能
- 財務と信用リスク機能
- 資本管理機能
- 資産運用部門に配置されている市場関連リスク評価スタッフ
- 人事部門に対して報告する労働衛生と安全の専門家
- 詐欺と調査の専門家
- 複数の事業部門内や単一の拠点に集約して設置されたコンプライアンスチーム

上記の事項以外にも、新任の CRO はいくつかのリスク管理委員会が社内のさまざまな組織内で活動していることに気付く場合がある。

こうした状況の中でまず取るべき最も重要なステップは、最低限として以下の事項を明らかにする行動計画を実施することである。

- 保険者のリスク許容度に関して取締役会と経営者の全体を通じて共通の認識があるかどうか
- 経営者に対するインセンティブ制度と慎重なリスク管理との間に整合性があるか
- リスク情報の質、健全性および透明性がどの程度か
- もし能力不足が生じているとすれば、それはどの部分か
- 保険者の事業にリスク調整後ベースで価値を損なっている部分があるか
- リスク管理がどのように資本管理、価格設定、準備金の積み立てと結びついているか
- 保険者の真の財政状態が利害関係者に対して明瞭となっているか
- 重大な問題が発生した場合に、ガバナンス構造は実際に機能するか（リスク管理委員会の範囲、構成およびロケーションと保険者の取締役会ガバナンス構造との関係は適正であるかどうか）
- 経営者の事業運営モデルは適切か（保険者のビジネスモデル、要求されたコンピテンシー、重要なプロセス、スタッフ、インフラストラクチャーに整合性のあるリスク管理が組み込まれているか）

CRO の果たす役割は、性質上必然的に保険者の経営陣に働きかける力を生み出す。通常、保険数理または数学のバックグラウンドを持つ保険者の CRO は、厳密で合理的な経営上の意思決定と冷静なアプローチをもたらしてくれる。商品の資本収益率が許容できる水準なのか、一定の事業分野から撤退すべきかなど、通常批判が許されない事柄が挑戦を受けることもまれではない。そのため、注意深くそして慎重に対応しないと、ERM の導入または構築には当然、緊張を招くことになる。従って、CRO は保険者の業績を決定する要因と社内外の主要な利害関係者を速やかに確定することが大切である。さらに、CRO の戦略と計画に対する取締役会の明瞭な支持が不可欠となる。

保険者の CRO と CFO の関係は極めて重要である。これは利益の予測可能性を高め、利益がマイナスに変動するリスクを軽減する目的を彼らが共有しているためである。両者の関係がうまく管理されれば、株主価値創造と保険契約者の保護の源泉となる。保険契約者の保護は自己資本規制を前提としている一方、株主ニーズは業績・価値創造のベンチマーク設定を前提としている。従って、CFO と CRO 両者の戦略が統合される必要がある。すなわち、両者は充分な投資リターンを生み出し、あらゆる保険契約者を保護できる妥当な資本水準を確保するものでなければならない。

保険者にとって最も重要な ERM に関する判断はリスク許容度の設定であると思われる。新任 CRO の最初の仕事は、次の事項を確認することである。

- 取締役会が承認したリスク許容度が存在するかどうか(それがない場合には、リスク許容度を設定し、維持する）
- リスク許容度が存在する場合、保険引受、投資、再保険の決定に日々従事している社員にそれが理解されているかどうか
- (おそらく最も重要なことであるが、）リスク許容度が保険者の戦略目標に対して適切であるかどうか

CRO は、保険者のリスク許容度に関する経営者と取締役会レベルの対話と議論を促進する理想的な立場にある。CRO が率先して議論をスタートさせ、議論を通じてリーダー役を果たす必要がある。

CRO の存在が注目されるものであり、権限が与えられていることが重要である。執行役員会に近いポジションあるいは執行役員会のメンバーとしてのポジションが推薦される。

最後に、CRO の役割が全社レベルのリスク管理活動・測定のコーディネーターであることを強調しておくべきであろう。これは、保険者における収益部門と区別するためである。最終的なリスクを負担するのは収益部門であり、CRO は、収益部門が ERM 機能によって発見された機会を活かして行動することを支援し、価値を増進するパートナーとなることを目指していく。

就任予定の CRO にとっては、以上の重要事項は決して優先事項として標準化されたものではなく、保険者ごとに状況は異なる。CRO は特に優先すべき課題を早急に確定し、それに関するコンセンサスを得る必要がある。

経営ガバナンス - 考慮すべき事項

ガバナンス体制は以下を考慮したものでなければならない。

- 意思決定プロセスの透明性と重要な決定が行われる場
- 保険者の規模と性質、生命保険会社であるか、損害保険会社であるか、両者の兼営か、また金融コングロマリット企業の一部であるかどうか
- 保険者のリスクミックス

中規模から大規模な保険者の経営ガバナンス構造は通常、グループと事業単位の各レベルに経営委員会を設立し、事業単位の委員会がグループのリスク委員会に対して定期的に報告するプロセスから構成される。別の構成としては、特定のリスクだけを監督する委員会を複数設立する方法がある。例えば、次の事項だけを監督する委員会を複数設立する方法がある。

- 価格設定と保険引受リスク
- バランスシート・市場リスクに対応した投資、流動性、再保険、信用リスクなど
- オペレーショナルリスク

小規模な保険者は通常、一つの委員会にリスク監督機能を集約するか、経営幹部に対する報告とモニタリング活動を統合している。

保険者のリスク管理体制は、経営責任の割当と整合したものでなければならない。例えば、事業単位が独立して経営され、全責任を負う場合には、リスクの集中管理は希望する結果を生まない可能性がある。例えば、事業単位が負担する全責任には保険料収入の拡大目標の達成や成長目標の達成に関連するリスクの管理が含まれる。

リスク管理委員会には、経営陣とリスク管理部門の参加が求められる。

ERM 機能の構造

最高リスク管理責任者（CRO）が率いる管理組織にすべての専門的なリスク管理機能を集約することは実行困難であるか、妥当ではない場合があり得る。重要なことは、リスク管理を機能させ、また調和が取れた形で機能しているように見られるプロセスを設定することである。ライン部門の管理者はさまざまなリスク管理機能を共通のレンズを通して理解するため、事業単位の関与と報告プロセスに一貫性がない場合には、ERM の有効性は希薄化され、弱体化につながる。

大規模な保険者や多国籍企業の場合は、リスクを集中管理し、またはグループ単位で管理し、同時に各事業単位や地域にリスク管理機能を置くことが通常である。こうした場合、リスク管理がばらばらとなり、情報の流れと重要な問題の上層部への報告が妨げられる危険性がある。こうした状況が発生する理由としてさまざまな要因が考えられるが、分散したリスク管理体制とそれぞれの部門の役割および責任を明確にするマトリックス型の報告制度を組み合わせると、リスクに関連する問題のより効率的な管理の実現に役立つ。

保険者のリスク管理部門には ERM の目的の達成をサポートできる能力とスキルを備えた人材を適切に組み合わせて配置する必要がある。例えば、リスク管理部門は ERM を実行できる能力を備えていなければならない。専門的知識だけでは十分ではないことがある。プロジェクトやリスクの管理技術だけでなく、幅広いリレーションシップマネジメント技術を活用することを考える必要がある。

サマリー

保険者のリスク管理構造の形それ自体が､ERM 制度の有効性を決定する決め手となるわけではない。適切な管理体制が、事業単位の関与を一貫して求めるプロセス、リスク管理用語の統一、標準的なリスク管理プロセス、合意された行動、適切な報賞制度、明瞭な報告とモニタリングによってサポートされることによって、持続可能な ERM 制度の実現が促進される。

2.7 リスクに関する社内用語の統一

企業が使用しているリスク管理用語、ツール、テンプレート、評価システム、報告制度に違いがあることは珍しくない。また、系統だったリスク管理プロセスの実行を希望する保険者のために監督者から詳細なガイダンスが提供されている場合もある。例えば、リスクが発生する可能性とその影響[2] をプロットする従来からのリスクマトリックスにもさまざまな表現方法がある。また、内部監査人と外部監査人(および監督者)がリスクに関連する問題を評価する方法が同じであるとは限らない。第三者（プロジェクトを援助させるために保険者が雇ったコンサルタントなど）が持ち込む方法も影響を与える。

競合するリスク管理用語が過剰に存在すると､ERM の有効性が多くの点で損なわれることがある。

- ERM の方法の開発・維持に直接関与していない社員に混乱が生じる傾向があり、経営者の支持や ERM の定着の障害となる
- サイロ的なアプローチが強まる。サイロの発生は、事業単位の内部であることも、複数のリスク管理機能にまたがることもある
- 実質よりも形式が重視される。その結果、「本当」のリスクが看過されることがある
- プロセスの非効率化と模倣が蔓延する

それ以外にも、リスクの計測に不統一が生じ、カテゴリー別のリスクを集計することが特に困難となる。共通のリスク管理用語の内容には次のようなものが含まれる。

- 全員に理解されているトップダウンのリスク評価システム、例えば、高い（「レッド」）リスクと低い（「イエロー」）リスクを定義する財務的および非財務的な指標
- リスク格付けと当該リスクの軽減措置を講じる責任を負う管理レベルを関連づけるリスク格付け制度
- 社内全体で使用される標準的なテンプレートと共通のリスクカテゴリー
- 報告と上層部への伝達に関する基準。例えば、いかなるリスクに関連する問題をいつ、誰に対して報告する必要があるのかに関するガイダンスや規則

[2] これに関連して、「発生の可能性」と「影響」の意味で「頻度」と「重大性」という表現が誤って使用されたことがあることに注意。38 頁の脚注を参照。

事例：
「競合他社よりも多くのリスクを認識していたのに...」

多くの海外支店を持つ保険者が先進的な規制基準に基づいて認定を申請した。だが、これまで同社は事業を営む多くの国でリスク分類（信用リスク、オペレーショナルリスク、市場リスク、不正リスクなど）に関して異なった定義を使用してきた。

共通言語がないためにオペレーションにも監督面でも問題が発生していた。定義に一貫性がなく、曖昧であったため、単一のリスクとして処理できたリスクが多重に識別され、管理や資本配分の対象となっていた。重要なリスクの一部がリスク管理プロセスの対象から外れ、経営管理体制が非効率になっていた。さらに、共通言語がないために、認定の申請の処理はこの問題が解決されるまで棚上げとなり、企業に余計な費用負担が生じ、業績にも影響が生じた。

同社は、リスクの定義は正確で、組織の事業目的に対する「本当」のリスクを正しく認定し、分類でき、社内のリスク管理制度による経済的価値の拡大に結びつくものでなければならないことを身にしみて理解することになった。さらに、リスク管理用語は首尾一貫性のある形で使用され、全組織に対して効果的に伝達され、あらゆるリスクが定義され、一貫性のある形で分類、評価されていることを組織が理解し、リスク管理を全社的に捉えることを可能とするものでなければならない。また、企業の規模にかかわらず、共通のリスク管理用語はグローバル化が進展する規制上の要求を満たすためにも不可欠となる。

2.8 リスク管理の企業文化

簡単に言えば、企業文化とは組織内の人々の行動が結びついて生じるもので、「当社のやり方はこうです」という形で表現されることが多い。どの組織にも独自のリスク管理の企業文化が存在している。企業文化については、それが適切な目標、活動および結果をサポートし、希望された結果が達成されないリスクの軽減に役立つかどうかだけが問題となる。従って、ERM の推進を考慮する際には、「リスク管理に関して社員にいかなる行動を期待するか」という点を明確にする必要がある。適切なリスク管理行動は、組織、業界、国内外で事業活動が行われている場所、それに伴う法制上の要求などによって異なる。だが、リスクへの対応に関する責任を不明確とし、恐怖や報復の企業文化を奨励し、「悪い情報を伝えた人を責める」ことを許し、「悪い情報の伝達を遅らせる」ことを奨励する行動は、良いリスク管理を促進することにはならない場合が多い。

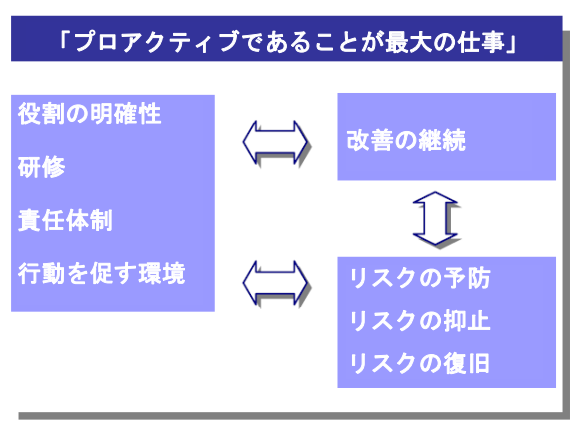
だが、期待される行動を決めるだけでは、適切なリスク管理に関する適切な企業文化を生みだすことも、強化することもできない。リスク管理体制とプロセスが効果的に実行されなければならない。また、社員が適切に行動する意欲を持ち、行動可能でなければ、リスク関連の活動はサポートされない。こうした行動がやがて望まれる企業文化の創造に繋がる。従って、人々の行動と能力が有効な ERM の成否の決め手であると言える。

経験によれば、望まれる行動を最も効果的に導入する方法は、それをグッド・ビジネス・プラクティス（good business practice）の一部として実行することであり、「華々しいスタート」は社員にただの一時的なものにすぎないと受け取られかねない危険性がある。こうした行動を通常の業務として位置づければ、社員全員が実行チームの一員となり、組織全体にコンセプトを順守させることに役立つ。だが実際には、そのために多くの時間と労力が必要となる。通常、導入した新しい行動が定着し始めるのに少なくとも 3 年、企業文化に完全に組み込まれるためにはさらに長い時間がかかる。

事例：
プロアクティブ（先を見越した）なリスク管理の企業文化（リスクカルチャー）促進

アジア太平洋地域を本拠地とする国際的な損害保険会社が、社員に一層プロアクティブな姿勢を奨励し、経営リスクを改善できると考えた。こうした形でERMの企業文化面に働きかけることによって何点かの潜在的な恩恵が期待された。プロアクティブであれば、リスクを早期に防止することも、リスクがまだ小さいうちに、少ない費用で短期間に解決できる段階で発見することもできる。プロアクティブであり、「異常」な事態を指摘することが奨励されれば、問題点がすみやかに発見される。改善策についてアイデアを提案させることによって、企業成長に欠かせない革新が促されるプラス面もある。

だが、これまで企業文化の変更には長い年月がかかると認識されていた。そこで、プロアクティブなリスク管理行動を導入する計画が立案された。最初のステップとして、以下のモデルに示すように、リスクカルチャーの構成要素が定義された。次に、このモデルに関連する行動が年次ベースの社員調査の内容に採用された。質問に基づきリスクカルチャー指数が作成され、進捗状況のトラッキングが可能になり、またオペレーショナル・パフォーマンスとの相関性が示された。



「プロアクティブであることが最大の仕事」というキャッチフレーズを軸として、プロアクティブな行動の促進計画が立案され、実施された。

- *リスク管理戦略、グループ全体の方針と実践にプロアクティブな原則を導入*
- *リスクカルチャー指数の改善に基づく経営幹部のための全社的リスク目標*
- *プロアクティブな行動を職務内容、パフォーマンス管理、引き継ぎ・能力開発過程に組み込む*
- *管理者とスタッフを対象とした、対面式、オンライン、または両者を組み合わせた方式による研修プログラムの開発、ならびにプロアクティブな原則をその他の研修に導入*
- *事故報告窓口を含め、情報を社内イントラネットに掲載*

数年を要して大幅な進歩が見られたが、プログラムを常に活性化し、プロアクティブな状態の維持を社員に意識させておくことが課題となっている。

以下のセクションでは、適切なリスク管理行動モデルの開発と測定、ならびに効果的な実行計画の立案という関連する 2 つの課題について詳述する。

2.9　リスクに関する行動モデルの開発

リスク管理に関する行動の検討にあたっては、3 つの側面を考慮する必要がある。まず、リスク管理がリスクを排除することではないということである。リスクの排除は成長と変化を阻害する。組織がいかなるリスクを進んで引き受けるのかを判断し、引き受けたリスクを首尾良く管理することがリスク管理である。従って、リスクの予防、発見および復旧というコアの行動と継続的な改善に関するさまざまなリスク基準（オーストラリアのリスク管理基準 AS4360 など）の記述を採用することが有益となる。

これを裏付けているのが、通常、リスク管理に関連してはっきり発言するには自信を持つことが必要という第 2 のコア・コンセプトである。この点は、例えばコールセンターにおけるマイナーなプロセス上の問題であるか、企業買収の可能性に関するリスクであるかにかかわらず、リスクの検討にあたっては徹底的かつ率直な検討が必要となるというようなことである。また、事態に異常が生じた場合、社員は報復を恐れることなく悪い情報を迅速に伝えることができるという自信を持てることを意味する。そのため、管理者はあらゆるレベルにおいて支援体制を提供する必要がある。

上記の 2 つの側面を裏づける第 3 の側面は、リスク状況を管理するために必要な技術、能力および権限（役割の明瞭性と責任を負う)を社員に与えることである。興味深いことに、これらの 3 つの側面はイノベーション、従って事業の成長と密接な関係がある。このようなリスク管理行動の側面は下方リスクに対応すると同時に上方リスクの管理をサポートする（以下のセクション 2.11 を併せて参照)。

2.10　導入計画の設定

組織内の誰もが利用できる形で行動を記述する共通の用語を開発することによって、適切なリスク管理行動を「実行可能な状態に」することが重要である。こうした記述内容をコア・コンピタンス、能力、能力評価・開発、あらゆるリスク・コンプライアンス研修の内容に取り入れるべきである。経営幹部と保険者の取締役会はこうした活動を強力にサポートし、事業全域にわたる進歩に強く関心を抱いていることを示す必要がある。

会社は以上の要素を毎年測定し、リスク管理の企業文化が強みのある部分と改善が求められる部分を理解する必要がある。まったく新しい手段を考え、事業に時間的な負担を掛けるよりも、最初のステップとして利用可能な既存の手段があるかどうかを確認すべきである。こうした手段には、既存の社員調査、業績データおよび監査報告書などが含まれる。既存の手段を強化して、リスク管理の企業文化の強さを評価するために用いることも検討の対象となる。追加手段を用いることは好成績を達成するための駆け引きを評価から遮断する利点がある。特に、ボーナスが業績によって決まる場合はそうである。モデルと測定アプローチともにシンプルであることがキーワードとなる。

つまり、社員、行動、その結果である企業文化は、効果的で持続可能な ERM を発展させるための基本的な構成単位となる。ERM の企業文化面における実行では次の点を考慮する必要がある。

- 保険者の会社全体の企業文化と事業環境にあったリスク管理行動モデルの検討と開発。モデルは測定可能で客観的な表現によって正確に行動を表現し、研修、報告、ボーナス・業績管理システムに導入可能なものでなければならない
- 上級経営者のサポートの確保とリスク意識の向上。経営幹部の研修、フォーカスグループ、教育、ブリーフィング、ならびにこれまでのリスク管理方法、その改善策などの検討がこの達成に役立つ。「非常時の体験談」が理解と関心を高める
- 適切な行動が制度とプロセスのデザインに組み込まれ、ERM 体制内部で整合性を持ち、機会があれば常にその強化を図る必要がある
- 現実的な時間枠内での実行計画立案と適正な予算の確保
- 多様な働きかけのチャンネルを通じた行動の強化
- 実行計画の開始前に行動に関するベンチマークを設定し、進捗度合を最低年に一回測定する。必要性がある場合、とりわけ外部要因の発生によって必要が認められる場合は、設計と改革プログラムを修正する
- 測定値を客観的な事業業績とリンクさせ、希望するリスク管理の企業文化が付加価値をもたらすことを証明する

リスクカルチャー改革プログラムの実行に関するアドバイス

レバレッジ - 一から新しいプログラムを始めるよりは既存の全社的プログラムを利用し、管理者とスタッフ双方の負担を軽減させ、できるだけ速やかに通常事業としての組み込みを図る。

用語 - 曖昧で漠然としていると感じられる企業文化ではなく、社員が変えることできると実感できる行動に焦点を当てる。

変化を実現するスキル - 変化を実現するための管理、学習、人的資源、プロジェクト管理など、リスク管理部門を支援できる専門家を雇うか、またはその関与を求める。

基本原則の組み込み - 新しい企業文化の基本原則を促進する改革イニシアチブを人々が関与するプロセスに組み込み、プログラムを絶えず強化し、継続する。

測定と結果 -企業文化にベンチマークを設定し、進捗度合を測定し、取締役会やリスク委員会にプログラムをサポートさせ、改善状況を理解させる。ボーナスの支給などを「てこ」として、適切な行動を強化し、不適切な行動を修正する。

2.11　上方リスクの管理

リスク管理には潜在的な悪影響の管理だけでなく、潜在的なチャンスの実現も対象に含まれることは広く理解されている。悪影響の管理を目的とする活動は良く理解され、確立された方法に従って実施されているが、チャンスの実現についてはそうなっていない。これは保険者の経営者がチャンスを見過ごしているということではなく、チャンス（上方リスク）の管理に関して一貫性のあるリスク管理プロセスが実行されている場合が比較的少ないことを意味する。

リスクに関する管理報告書に通常含まれている情報に、両者間のギャップが明瞭に現れている。報告書には通常、主なリスク、事件、問題点、リスク指標の推移などが取り上げられている。だが、報告書に重要なチャンスの分析が含まれていることは稀であり、リスク全体を対象としているとは言えない。もちろん、保険者は通常、CEO や事業部長への報告を通じてチャンスについても報告を行っている。だが、こうしたチャンスの評価は保険者のリスクの評価と常に切り離されている。効果的な ERM は悪影響とチャンスを統合的に評価することを内容とする。

従って、ERM 体制の開発に際しては、上方と下方のリスクがうまく統合される状況を作りだすことが保険者の最大の課題となる。統合に役立つ方法には次のようなものがある。

- リスク管理部門を戦略計画に結びつける
- リスク管理部門(および内部監査部門)が作成する報告書の対象にリスクとチャンスの両方を含ませる。チャンスの具体例は次のとおり
    - 過剰または非効率な統制を除去することによるコスト削減
    - 他の事業目標を達成する方法としてリスク管理を活用する（例えば、自宅勤務を事業継続（BCP）リスクの統制だけでなく、スタッフの採用や雇用維持のために柔軟な労働条件として利用）
- 計算されたリスクテークを奨励する報賞システム
- 新たな、業界全体にかかわり、垣根を越えた長期的なリスクの報告

リスク管理プロセス(セクション 6.2)は、リスクとチャンスの評価に対して同様に適用できる。リスクとチャンスの両方を同じ評価方法によって定量化することが要請される。

効果的な上方リスクの管理は、あらゆるリスクをチャンスとして捉える考え方が前提となる。

- 認定されたリスクを軽減または移転する戦略を実行するチャンス
- 危機シミュレーションを実行することなどによって、発生する可能性は低いが、影響が大きいシナリオに対して積極的に対応する計画を策定するチャンス
- 将来の収益力に影響を与える可能性のある長期的なリスクの管理能力の開発に投資するチャンス

リスク管理部門が上方リスクの管理を行うことによって、積極的に戦略的な活動に参加し、保険者に対して付加価値をもたらすチャンスが生まれる。

セクション 2.8 で述べたように、保険者の企業文化が上方リスクの効果的な管理にとって極めて大きな重要性をもつ。

2.12 パフォーマンス管理と報賞システム

企業文化に関する以上の議論は、パフォーマンス管理やインセンティブ制度においてリスク管理の要素を認識し、または取り入れる必要性を裏づけている。例えば、明確なリスク管理上の成果にインセンティブを与えずに、広範な ERM を実行すると失敗の可能性が極めて高くなる。

リスク管理方法の改善やそれに基づく価値創造を目的に含むインセンティブ制度の開発に際しては注意が必要である。考慮すべき主要な事項には次のようなものが含まれる。

- 両者間の適正なバランスの実現。例えば、リスク管理の改善に関するインセンティブが、対象となる個人やグループを現実に動機づけるものであること
- 対象とする個人とグループの決定。リスク管理目標が上級経営者に対する報賞システムの対象に含まれていない場合には、保険者の ERM 体制の発展に困難が生じる
- 測定対象と測定に用いる指標を明瞭にする。アクティビティベースの測定（マイルストーンの達成など）、財務的測定（(バリューアットリスク)の変化など）、監査結果や業績および社員調査への考慮が必要
- リスク管理の実績、能力管理、能力開発プロセスを関連づける。例えば、リーダーとしての可能性が、リスクのプロアクティブな管理を促進する環境を形成できる個人の能力を一つの尺度として評価されることとして理解されていれば、保険者の取締役会は経営者が積極的に ERM を支持しようとすることを確認できる
- インセンティブ・プログラムが適切なレベルの社員をターゲットとし、意図しない結果の発生を招かないものとする。例えば、社員のインセンティブを社員調査やフィードバックの結果とリンクさせることは、調査結果をゆがめる

事例：
「間違った」行動の奨励

大規模な金融サービス企業が自己売買部門の活動に関する巨額の損失を発表した。巨額の損失が発生していたにも関わらず利益の報告を続けていた理由は、社員がさまざまな隠ぺい手段を用いたことであった。利益目標を達成し、ボーナスの支給を受けることが動機の一部であったようであった。

調査の結果、インセンティブとの関連が確認された。同社の企業文化に関して次のような事実が観察された。

- *プロセス、ドキュメンテーション、手続きのマニュアルが重視され、問題の本質の理解や責任の所在の明確化、問題の解決が軽視された*
- *リスクの測定と報告は信頼されず、またリスク・エクスポージャーを正確に反映するものとはみなされず、無視されていた*
- *おごりによって危険信号が無視された*
- *取締役会や委員会に対して諸問題は報告されず、悪い情報は隠ぺいされた*

正式なリスク管理プロセス、体制およびシステムは強い警戒信号を発していたが、損失の発生を招き、隠匿し、発覚を回避する機会を促す企業文化が支配的であった。社員は正直に行動せず、リスク管理プロセスが機能していなかった。

巨額の金銭的損害が発生したため、何名かの上級経営者が辞職した。会社の信用が大きく失われ、株価が大幅に下落し、監督当局による監視が強化され、それに伴い経営コストが増加し、またトレーダーが刑事訴追を受け、有罪となった。

重要な教訓

1. *危険信号に注意し、その上で行動せよ*
2. *判明した統制の欠陥の是正を優先する*
3. *インセンティブ制度が意図せざる結果を招くことに留意する*
4. *リスク管理のギャップを縮小するためにリスク管理のエレメントすべての協働が必要*
5. *最善のシステムと統制であっても、貧弱な企業文化と整合性を欠くインセンティブ制度によって効果が失われることがある*

2.13 報告とモニタリング

優れたリスク管理情報が優れた決定を生み出すため､ERM の効果はリスク管理情報の質に大きく依存する。保険者のリスク管理部門は、経営幹部と取締役会に対して正しい情報が提供されているか否かを判断する必要がある。通常、保険者は保険、市場・投資および信用リスクに関する詳細な情報を持っている。だが、オペレーショナルリスクや総合的なリスクポートフォリオ、すなわち、全社的リスク報告については必ずしもそうとは言えない。理想的なリスク報告は、次のような質問に対する答えを提供する必要がある。

- 現在および将来の主要な事業リスク、環境リスク、ならびに経時的変化（保険者のリスクプロファイル）
- リスク指標（リスクの発生可能性・影響度）の変化
- リスクを識別し、管理する能力

以下の表にリスクのカテゴリー別に、全社的リスク報告書に記載される情報の代表例を示す。

リスクのカテゴリー	情報
全社的・全リスクカテゴリー	• 全社的リスクプロファイル(リスクプロファイルのサンプルについてはセクション 6.2 を参照) • 自己資本比率 • 重要な通常業務 • 重大な損失、事故 • ERM 体制の改善 • 主要リスク管理指標 (KRI) の変化
保険引受リスク（再保険を含む）	• 地域別、危険の種類別、チャネル別のリスクの集計（保険金額） • 準備金の積み増しまたは取り崩し
市場リスク	• VaR • ストレステストやシナリオテストの結果
信用リスク	• カウンターパーティの信用状態、資産・負債の多様性 - 信用格付けの分析
流動性リスク	• 総資産に対する流動資産の比率
オペレーショナルリスク	• 重要なリスク（オペレーショナルリスク・プロファイル)の分析 • 主要リスク管理指標 (KRI) の変化 • 内部監査結果
その他	• 業界における新たなリスクのベンチマーキング • ビジネスサイクル、保険サイクルのデータ

ダッシュボード型の報告書のサンプルを次に示す。

事例：
「報告事項は?」

多くの利害関係者が高品質のリスク情報に依存している。

- *監査委員会 - 重要な財務リスクのモニタリングと軽減*
- *経営者 - 盲点を避けるためのリスク情報の検討*
- *管理者 - 盲点を避けるためのリスク情報の検討、リスクプロファイル・リスク統制の有効性の変化の検討*
- *リスクオーナー - 必要に応じたリスク情報の更新と発生可能性、影響度、統制の有効性の変化を上層部に報告*
- *コントロールオーナー - 責任範囲である統制の処理状況の更新*
- *内部監査 - 内部統制手段の有効性の検討*
- *外部の利害関係者 - 監督機関による調査*

ダッシュボード型の報告書は、簡潔で情報の一覧性があり、最も効果的である。詳細が必要な場合には、補足情報を添付できる。ダッシュボード型報告書に記載される主要カテゴリーには次のようなものが含まれている。

- *残存リスクトップ10*
- *主要リスク管理指標*
- *リスクの程度と統制の有効性を示す採点表*
- *すべての重大な固有・残存リスクのヒートマップ*
- *補足コメント欄*
- *プロジェクトの重要な進展*

2.14　内部監査の役割

社内の内部監査部門が保険者のリスク管理体制を開発することが少なくない。これは、ERM の実行に求められるスキルと内部監査人のスキルが合致しているという見方に基づいている。

こうした方法は短期的には保証面で利点が期待でき、また取締役会は作業が順調に進捗していると安心できるが、中長期的に真に実効性があり確立した ERM 制度が実現される可能性は乏しい。さらに、内部監査部門がプロセスを開発してしまうことは、事後のチェックと利益相反が生じ、本来要求される独立性が失われる可能性がある。一層問題なのは、ERM が合意されたリスク選好の範囲内で価値を最大化することに最終的な狙いを置いたプロセスではなく、本質的に保証ないしコンプライアンス問題であるというメッセージを組織全体に送ってしまうことである。多くの国の監督機関がこうした方法に伴う問題を理解しており、リスク管理に関する内部監査部門の役割を定義する基準を導入している[3]。

この点に関して有力となっているベストプラクティスは、内部監査の機能と、保険者の ERM 体制を開発し維持する機能とを明確に区別することである。こうすることによって、内部監査の独立性は損なわれず、取締役会に対し、取締役会の監査委員会を通じて保険者の ERM 体制の有効性に関する保証を提供する機能が果たされる。

[3] 具体例については、APRA Prudential Standard GPS510、ガバナンス、パラグラフ 46 と 47 を参照。

2.15　変化への対応

保険者が新たな活動を始める場合には、ERM 体制はこうした活動もカバーする必要がある。新たな活動に伴って新しいリスクが必ず発生し、保険者のリスクプロファイルに大きな影響が生じる可能性があるからである。新たな活動には次のようなものが含まれる。

- 商品の変更や新商品の導入
- 会社の組織や管理構造の変化
- コンピューターシステムやネットワークの構築や改良を内容とする大規模なプロジェクトの発注
- デュー・デリジェンス、企業買収、企業分割、資金調達などの企業行動
- アウトソーシングやオフショア（域外移転）戦略

保険者のリスク管理部門は、変更の全範囲または「進行中」の活動を常時把握している必要がある。また、保険者のリスク管理部門と新たな活動や戦略の実行を担当する部門の間に密接な協力関係があれば、「リスクに関する声」に対する適切な対応が図られる可能性が高まる。これはリスク管理部門が新たな活動の計画段階から関与し、当該活動に関するリスク管理部門の役割と責任の詳細について合意することによって実現される。

従って、保険者のリスク管理部門は、戦略、財務、商品開発、IT、法務、人事などの担当部門と密接で、透明性があり、計画的な関係を築く必要がある。

保険者のリスク管理部門が新たな活動に関与する方法にはさまざまなやり方がある。例えば、

- デュー・デリジェンス作業に参加し、アクチュアリーやその他のリスク管理の専門家の能力を活用してリスクの識別と評価を助け、バリュエーションとモデル化の側面を支援すること
- 戦略チームと協力して、選択された戦略に伴うリスクの適正な評価を戦略に取り入れること
- 大規模なプロジェクトや新商品発売に関するリスク評価を実行・促進すること
- 新たな活動の実行に関して監督者との関係を管理し、調整すること
- 買収した新規事業と協力して、保険者のリスク管理制度への適応とその実行を支援すること

保険者のリスク管理部門がこうした活動に参画することによって、密接な関係が養成され、より良い経営意思決定が生まれ、リスク管理機能とその目的である価値の維持と創造との整合性が高まる。このようにして、ERM による規律とそのプロセスが変化を実行する活動の中に組み込まれることになる。

3. リスク管理方針

重要機能 2

保険者は、戦略上および運営上、関連する重要な各リスクの分類をどう管理するのかを概説するリスク管理方針を設けるべきである。当該方針では、保険者の許容限度、規制上の資本要件、経済資本、ならびに、リスク・モニタリングのプロセスおよび方法との関連性を説明すべきである。

保険者のリスク管理方針は、保険者がそのリスクポートフォリオの管理に関する基本的な考え方と最小限の必要事項を明らかにし、伝達する手段を提供する。リスク管理方針は保険者の取締役会によって設定される必要がある。また、多くの国では取締役会によるリスク方針の承認が規制によって義務づけられている。リスク管理方針に通常記載される事項のリストとその構成に関する提案を添付資料 6 に記載した。

リスク管理方針を開発し、設定するプロセスには、多くの利害関係者を関与させ、時間をかけ、また方針の実行と順守の担当責任者と共にテストを実施する必要がある。現行の方針は定期的に、少なくとも年に一度は見直す必要がある。

保険者がリスク管理方針を作成する際には、少なくとも以下の点に留意する必要がある。

- リスク管理に関する明確な基本方針 - リスク管理がなぜ重要なのか、また価値の創造との関連性など
- リスク管理と保険者の事業目的・ミッション、価値、戦略的な目的との関係
- リスク管理が、資本管理、価格設定、準備金の設定、パフォーマンス管理のプロセスなどの関連するプロセスにどのように組み込まれているか
- 方針が適用される活動の範囲。例えば、方針は多様な所有形態（完全所有、過半数の株式所有、合弁など）に対応できる柔軟性を備えている必要がある
- 監督上の要件に対する適切な対応と配慮
- 新規事業の買収に関連する要件。例えば新規事業を ERM 体制に組み込むための時間枠
- リスクのカテゴリー、リスクの定義、ならびにこれらの国際的に受け入れられているカテゴリー・定義への分類
- リスクのカテゴリー以外に、方針にはリスク、リスク管理、リスク管理体制などのリスクに関する専門用語を定義する必要がある

- 最も重要なことは、リスク許容度の議論を促進するために、保険者のリスク選好を方針（セクション 4 を参照 ）に記載することである。
- ガバナンスと監視
    - 取締役会、取締役委員会の構造と責任
    - 運営体制、役割、責任
    - 全社単位および事業単位のリスク管理部門の役割および責任
    - 内部監査と外部監査の役割
    - コンプライアンス問題、方針違反に対する対処
- スタッフ全員の行動に関する期待
- 保険者の全オペレーションについて一律に適用される最小限度のプロセス上の要求。すなわちリスク管理研修、リスクのプロファイリング、ビジネスプロセスの文書化、リスク報告と上層部への報告、リスクのモニタリングと確からしさ等
- 保険者のリスクとソルベンシーの自己評価に関する要件（セクション 6 を参照）
- 必要に応じ、定義されたリスクカテゴリーに関する特別要件
- 方針の見直しと更新に関するプロセス

上記の「作業リスト」は、方針を記載した文書がかなりの長文になるという印象を与えたかもしれない。だが、必ずしもそうではない。一部の組織にしか読まれない、または理解されないような長い文書の作成は避ける必要がある。従って、方針の作成者や管理者は、ERM に関する取締役会の期待を適切に伝達するための戦略を立案するために幅広い層と協議すべきである。そのためには、根幹となる基本原則が内容に含まれ、また保険者内の異なる読者を対象とした複数の文書を作成することが考えられる。

新しい方針の策定または既存の方針の更新は、組織内部におけるリスク管理に対する姿勢や理解を評価する絶好の機会となる。ERM 方針の実行がトップダウンの形で行われ、事業部門の関与が限定的である場合には、ERM に必要な事項の日常業務への統合と組み込みが適正に行われない可能性が高くなる。

4. リスク許容度に関するステートメント

重要機能 3

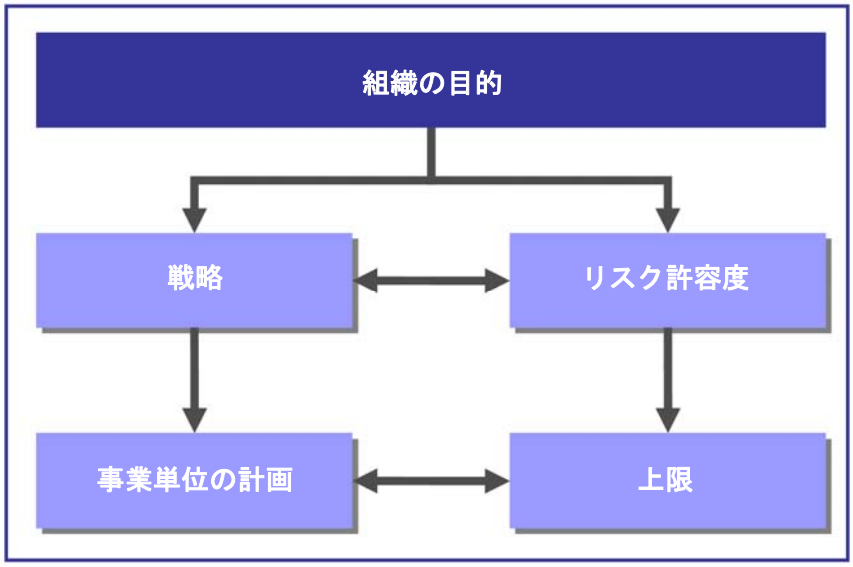
保険者はリスク許容度に関するステートメントを作成し、定量的、定性的に全体的なリスク許容度を明らかにするとともに、リスクカテゴリー相互の関係を考慮し、関連性のある重要なリスクカテゴリーごとにリスクの許容限度を定義する必要がある。

リスク許容度は保険者の戦略と適合したものであり、ERM 体制とリスク管理方針に従って積極的に活用されるべきである。リスク管理方針および手順を通じて、設定されたリスク許容限度を保険者の継続的な業務に組み込むべきである。

本セクションでは、リスク許容度のコンセプト、リスク許容度と保険者の戦略との関係を検討し、リスク許容度の設定と更新に関する実務面に関するガイダンスを提供する。

保険者のリスク許容度の設定は、戦略の選択と関係する。そのプロセスは戦略と長期的な方針の設定と結びついていなければならない。トップレベルの経営者は所与の戦略に適合した適切なリスク許容度の検討に積極的に関与する。だが、そのリスク許容度と戦略を決定しなければならないのは取締役会である。CRO も関与すべきであるが、リスク許容度の設定に責任は負わない。

保険者のリスク許容度はその戦略および事業計画に対応して設定される。リスク許容度は企業戦略と同じタイムスパン、すなわち通常 3 年から 5 年の期間を前提として設定され、年次ベースの予算・事業計画等によって左右されるべきではない。言い換えれば、保険者のリスク許容度が毎年変更されることはほとんどあり得ない。リスク許容度と戦略との関係を以下の図で説明する。



保険者のリスク許容度は、保険者が受け入れ可能なリスクの限界を示すものである。上限は、プランの達成にリスクが生じていることを警告する基準としての性格が強い。

- リスク許容度は取締役会が容認できると考えるリスク水準全般に関する基本的な宣言である。
- 上限はより具体的で、保険者の年次計画や予算にかかわる目標の変動について許容可能な水準を設定する。上限は、日々の事業に即して利用可能な表現でリスク許容度を表現したものである

保険者では通常、以下の項目に基づいて財務面、非財務面に関するリスク許容度が設定される。

- 保険者が受け入れ可能または不可能な保険種目
- 利益の変動性
- 不測の事態に備えるための準備金などを含めた規制上の要件
- 望まれる資本水準。通常、信用ある格付機関が定義した格付け基準をもとに設定
- 保険契約者に対する義務が特定の確率で履行できる、また「破産リスク」の 目標再現期間(target return period)を満たす水準の経済価値ベースの資本の維持
- 規制上の最低必要資本を上回るバッファー資本の維持
- 負担可能な総リスクの上限
- 株主配当支払能力(上場会社の場合)
- 万一大災害が発生した場合に対応可能な年間の最大損失額（損害保険者）
- 承認可能な最低限の価格設定原則
- 保険者の効率的な運営の持続を不可能にし、容認不可能なオペレーショナルリスクの記述
- 買収、事業分割、資金調達、保険者のグループ内部の多数の事業単位や企業にまたがるプロジェクトなどの全社的取引および戦略プロジェクトの承認・不承認

一方、「上限」は対象範囲が限定されており、リスクカテゴリーのレベルで機能する。リスクが上限以下であれば、保険者の全体的なリスク許容度が守られていることになる。

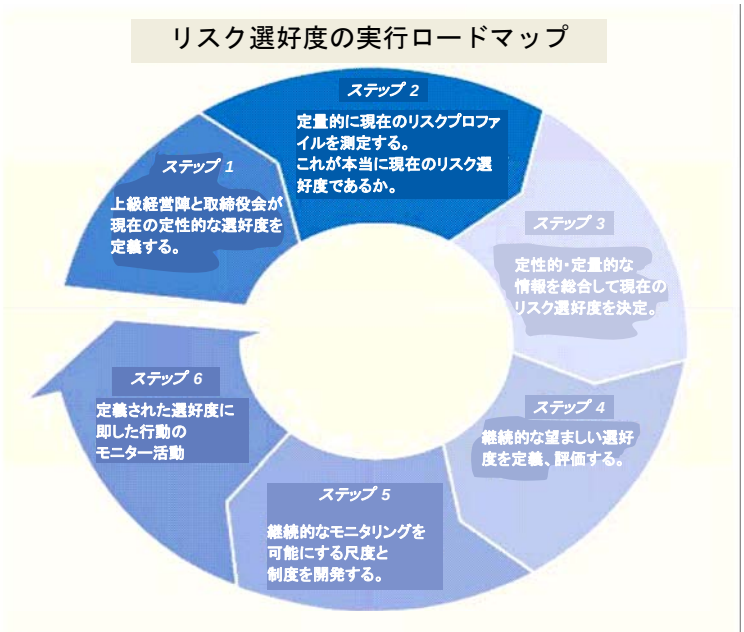
リスクの上限の具体例には以下のようなものが含まれる。

- 投資と再保険のカウンターパーティに要求される最低限度の信用状態の設定
- 通常信用格付けを基準とした、再保険購入プログラムの信用状況に関する全体的なターゲットの設定
- 保険種目・商品、地域、カウンターパーティの集中に関する制限の設定

- 保険の引き受けと価格設定に関する原則と制限の遵守
- 明確に確率的に定量化された必要額をターゲットとする保険準備金の設定
- 流動性が高い資産への投資額を基準とした流動性のベンチマークの設定
- 保険契約者勘定と株主勘定の資金の投資対象を市場のある投資商品に限定する投資範囲
- 金融派生商品の利用に関する制限
- アウトソーシングの範囲、事業中断、不正、労働衛生と安全、プロジェクトの遂行などに関する制限を内容とするオペレーショナルリスクに関する方針の設定

上記の内容から分かるように、ビジネスマネジャーは制限をより明確に意識している。また、制限違反が発生する可能性や重要な基準値に接近していることを明らかにするために、ビジネスマネジャーが重要リスク指標（KRI）を利用することが一般的になっている。従って、保険者がリスク管理部門を通じてリスク許容度と上限との間の関係を明確にすることが重要となる。それによって、ガバナンスに関するメリット（リスク方針が適切にオペレーショナルな状態となっていることが取締役会によって保証される）とパフォーマンス管理に関するメリット（サプライズ発生の減少と利益の変動幅の縮小）が得られる。さらに、目標とする信用格付けを基準としてリスク許容度を調整する際には、保険者は、格付機関や他の第三者から提供を受けた外部データを参考にして独自の評価分析を適切に行うべきである。

各保険者がそれぞれの状況に即して適切なリスク許容度に関するステートメントを作成することが重要である。保険者によっては、リスク許容度に関する基本的な宣言の作成を選択する場合も、リスクカテゴリーのレベルやそれ以下のレベルでリスク許容度を定義する場合もありうる。下記の図は、リスク許容度を確立するステップの典型的なロードマップを示したものである。



出所: Bennet C: Cusick, K. (Trowbridge Deloitte Limited)
Risk Appetite:
Practical Issues for the Global Financial Services Industry 2007
URL: http://www.actuaries.asn.au/IAA/upload/public/4.a_Conv07_Paper_Bennet%20Cusick_Risk%20Appetite.pdf

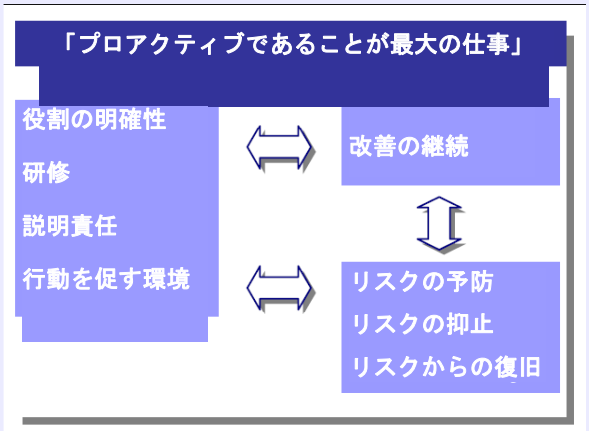
このプロセスに関する詳細な情報については、添付資料 8 の参考資料をご覧いただきたい。特に、上記の図表で言及した出所が有益である。

方法を問わず、保険者のリスク許容度の設定にあたっては、常に以下の事項を考慮する必要がある。

- リスク許容度の設定は経営戦略の達成に役立つものでなければならない
- 適切な財務その他の方針によって、リスク許容度に関する基本的な宣言は業務レベルの制限に置き換えられなければならない。

事例：
リスク許容度を設定する方法

次の図に示すように、リスク許容度とはどれだけの量のリスクを引き受けるのかではなくて、いかなるリスクをなぜ引き受けるのかに関するものである。



1. *リスクプロファイル:*
   事業が直面する現在および将来のリスク
2. *リスク負担能力:*
   リスク・エクスポージャーに耐え、管理可能な事業の財務、評判、業務能力または優位な競争力
3. *リスク許容度:*
   リスクプロファイルがリスク負担能力、戦略、市場ポジション、事業の強みに関して合致しているかどうか

リスク許容度を設定する場合に、検討すべき事項

- *戦略的なオプションもしくは選択との関連において、また自社のリスクプロファイル（現在および将来）、リスク負担能力（現在および将来）を考慮して、リスク・エクスポージャーを継続的に受け入れることに問題はないか。*
- *不安を生じさせるリスクの集積や集中がないか*
- *リスク・エクスポージャーと比較して、期待されるリターンの水準（必要な資本）は満足できるものか*
- *将来のいくつかの想定シナリオのもとで、仮に異なる選択肢・判断もしくは決定を選択した場合に後悔する程度*

5. リスクへの即応能力とフィードバック・ループ

重要機能 4

保険者の ERM 体制は変化に迅速に対応できるものである必要がある。

ERM 制度は、適切な高い品質の情報、管理プロセス、客観的な評価に基づくフィードバック・ループを備え、保険者がリスクプロファイルの変化に対応して時宜を得た必要な措置を講じることが可能なものである必要がある。

5.1 フィードバック・ループの性質

保険者の ERM 体制の実効性を判断する決め手は変化に対する対応力である。通常の業務(BAU:Business As Usual)活動だけを対象とした制度では、市場の変化、規制の変更、顧客の選好の変化、世界的な流れなどに組織が対応できない可能性がある。

保険者のリスクプロファイルは以下のものによって影響を受ける。

- BAU 活動、新しい取り組みや戦略、環境の変化を考慮した全社レベルおよび事業単位レベルの定期的なリスク評価の結果（将来）
- 重要なリスク指標の動き（現在）
- 予期しない損失の発生、重要な統制の欠陥あるいは事故（過去）

以上の 3 要素を総合すると、保険者の内部統制環境の有効性に関して貴重な生情報が得られる。従って、保険者の ERM 体制には上記の 3 つのソース（過去、現在、未来）からの情報を検討する系統的なプロセスを正式に設ける必要がある。

事故と問題からは特別なフィードバックが得られる。顧客からの苦情、監査結果、プロジェクトの失敗またはシステムの故障、危機の発生、監督機関の行為などからこうした情報が得られる。保険者の ERM 体制には、原因の分析と報告を含めて、一定の基準を超える事故や問題を正式に調査するプロセスを導入する必要がある。それによって、失敗から学び、継続的な改善を図るカルチャーが生まれる。効果的なフィードバック・ループの基盤は次のとおり。

- 重要な問題を報告するための基準（閾値）の設定（セクション 2.13 を参照）
- 問題点をさまざまなレベル、経営者、必要があれば、監督者へ報告するための手順
- 制限 (場合によりリスク許容度)を超過した可能性がある場合を示す、リスク集計値の報告

5.2　新興リスク

新興リスクとは、発展中または既に判明しているリスクで、不確実で曖昧であるために、従来からのリスク評価方法では定量化が難しいものをいう。

アドバイス：　なぜ保険者は、新興リスクに関心を持つのか

保険者は次のような理由から新興リスクに関心を持つ。

- 組織の戦略への影響
- 予想外の（潜在的な）保険金請求・保険金請求の頻度・保険金請求のコストなど、保険引受ポートフォリオへの影響
- 組織のオペレーショナルリスクへの影響
- 新しいタイプの保険商品を提供するチャンスの発生

こうした問題に対する回答が、保険契約約款、保険金請求、準備金戦略、再保険契約、保険者自身のオペレーショナルリスク戦略に直接的な影響を与える。

新興リスクに関して組織の状況および戦略とリンクさせた明確な目的を設定することがまず重要となる。状況設定の具体例には次のようなものがある。

- 事業の地理的範囲 - 地方・国・地域・グローバル
- 測定期間 - ロングテールの保険には長い測定期間、短期の保険には短い測定期間
- 影響の種類 - 器物の物理的損壊、責任保険、健康問題、複合タイプ

添付資料 8 に新興リスクに関する有用なウェブサイトを掲載する。

目的と範囲が確立されれば、新興リスクの特定を進めるための一定の方向性が得られる。リスクの特定には、新聞報道、業界紙、ワークショップ、外部エキスパートの意見など、さまざまな方法を利用できる。

新興リスクは、損失が発生する可能性の高い保険金請求につながる可能性があるが、同時に「先行者利益」に類似した新しい事業チャンスを提示する可能性がある。こうしたリスクやチャンスの特定が早ければ早いほど、行動の余地が広がる。成熟した ERM 制度は新興リスクに対応し、その新興リスクへの対応戦略に関してビジネス部門とリスク管理部門との間の対話を可能とする環境を作り出す。

新興リスクの共通の特徴は次のとおり。

- 利用可能な情報が乏しいため、不確実性が高く、また頻度と損害規模[4] の評価が難しい
- リスクが定かでなく定量化が難しい、またリスク移転に疑問がある。
- 保険者が市場シェアを失うことを恐れて最初に動くことを躊躇するため、業界全体としてのポジションが生まれない
- 実体のないリスクに対応することになる危険があり、リスクのコミュニケーションが困難
- 監督機関の関与が多くの場合必要

2005 年には、最高リスク管理責任者(CRO)フォーラムが、保険業界に関係する新興リスクに対する意識とコミュニケーションの向上を目的として、Emerging Risks Initiative (ERI) を設立している。ERI は、保険業界に関係する新興リスクの特定、優先順位づけ、伝達に焦点を当てている。CRO フォーラム新興リスク計画 (http://www.croforum.org/emergingrisc.ecp) は、これまでのところ「パンデミック」、「テロリズム」および「気候変動と熱帯低気圧」の 3 つのポジションペーパーを発表している。

ERM を実行する保険者は、以下のセクション 6.2 に示すリスク・プロセスを通じて、自社の事業に関連する新興リスクに対応するプロセスを設定する必要がある。さらに、新興リスクに対応する制度に関する以下の情報がアプローチの決定にあたって参考となる。

5.3 シナリオ・プランニング

シナリオ・プランニングは、発生する可能性は低いが、影響が大きい事象を評価する方法の一つであり、それによって統計モデルが強化される。また、企業が特定の出来事に対し、準備を整えることを助ける。シナリオ・プランニングには、ワークショップ、危機シミュレーション、シンクタンクなどの形態がある。また、業界全体に関する問題について協働するチャンスも生み出される。

シナリオ・プランニングは、組織が社内外のショックに対してどの程度の抵抗力を持っているのかを経営者が評価する強力なツールである。リスクの本質に関する想定や、統制とコンティンジェンシープランの機能がテストされ、しばしば変更が実施される。

多くの保険者が予期しない事態への対応力を強化する投資をすでに実施している。特に、事業継続管理（BCM）の採用が近年急速に進んでいる。BCM チームは通常、一連のシナリオに基づいた危機シミュレーションを実行する。シミュレーションに参加した多くの管理者はシミュレーションを経験したことによって現実のリスクに対してよりうまく対応できると報告することとなるだろう。シミュレーションが多数の事業単位に影響を与え、経営陣の参加を必要とする場合には、こうした効果が強まる(詳細については、セクション 8.3 を参照)。

[4] 「頻度と損害規模」は両者ともに確率分布であり、リスクマトリクスの「可能性と影響」とは異なる。

6. リスクとソルベンシーの自己評価 (ORSA)

重要機能 5

保険者は定期的にリスクとソルベンシーの自己評価(ORSA)を行い、取締役会と経営陣および経営会議に対して自社のリスク管理と現在および将来のソルベンシーの状態を報告する必要がある。ORSA は、少なくとも、保険引受リスク、信用リスク、市場リスク、オペレーショナルリスク、流動性リスクを含め、合理的に予測可能な重大なリスクをすべて対象とする必要がある。評価にあたっては、リスク管理と必要とされる財務的なリソースの水準と質との関係を明らかにする必要がある。

6.1 はじめに

ORSA では、定量的・定性的技術を組み合わせ、リスクの識別、評価、管理が行われる。その一環として、定期的にアクチュアリアルなコントロールサイクルが実施され、過去に行った決定とそれに基づいた行動の結果を検討し、こうした結果が将来の決定と行動にフィードバックされる。このセクションでは、リスク管理プロセスの基本的な構成要素を検討し、また異なった種類のリスクの評価に適した方法を提案する。

6.2 リスク管理のプロセス - リスク・プロファイリング

リスク管理の骨格となるプロセスは、適切に状況を考慮して、リスクを系統的に識別し、分析し、評価し、処理することである。通常、「(リスク管理の) 状況」はビジネスプロセス、プロジェクト、または幅広く保険事業そのものの目的を軸として、構成される。さらに、リスク管理の状況の重要な要素として、リスク許容度（上記セクション 4 を参照）の設定が含まれる。リスク管理プロセスからのアウトプットは通常、リスクプロファイル、リスクレジスター、ヒートマップ、リスク管理自己評価と呼ばれるものである（以下、「リスクプロファイル」と言う）。

リスク・プロファイリング、関連するガバナンス・制度面の活動を資本モデリング（下記セクション 7 を参照）と混同してはならない。資本モデリングは、統計的でアクチュアリアルな方法であるが、リスク・プロファイリングは、オペレーショナルなプロセスとしての性格が強く、事業計画やプロジェクト管理のような活動と類似した特徴を持つ。リスク・プロファイリングのプロセスは、保険者の全社的なレベル、事業単位、重要なビジネスプロセスのレベル（保険引受や保険金請求）で適用することも、プロジェクト管理で適用することもできる。リスク・プロファイリングには、固有リスクと残存リスクの双方のレベルの評価が含まれる。固有リスクと残存リスクの定義を以下の表[5] に示す。

[5] Enterprise Risk Management-Integrated Framework, The Committee of Sponsoring Organisations, (2004 年 9 月)

固有リスク	残存リスク
経営者がリスクの可能性と影響を変更するために何らの措置を講じない場合の企業リスク	経営者がリスクの可能性と影響を変更するために措置を講じた後に残存する企業リスク

リスク管理プロセスのこの側面は、例えば、保険の引受マネジャーにとっては退屈で直感的な理解が難しいと感じられる可能性がある。保険の引受マネジャーは、あらかじめ定められたコントロールのレンズを通して引受プロセスを理解しているかもしれない。だが、固有リスクと残存リスクの双方を評価することによって、他の方法では簡単に明らかとならない重要な管理情報が明らかになる。

- リスク管理が、重要な統制の継続的で効果的な運用に強く依存するリスク（高い固有リスク・低い残存リスク）
- 統制の実施後もその性質があまり変わらないリスク。これは、一部の統制が有効性を欠き、資源を他の分野で使用した方が良い場合があること、統制の変更が必要であることを示す（高い固有リスク・高い残存リスク）
- 統制が過剰である可能性のあるリスク（低い固有リスク・低い残存リスク）

より広く言えば、リスク・プロファイリングの価値はそれによって社員がリスクとその管理を検討する機会が生じることである。新しい発見が得られ、リスクの性質に関する意識が向上する。そのプロセスが重要なのは、以下の点が推進され、強化されるためである。

- 最も重要なリスクに関する理解を共有し、検討することによる一貫性と理解。このプロセスによって、経営陣はそれぞれのリスクを対比させて評価することになる
- 取締役会に対する透明性と重要なリスクに関する経営陣の正式な評価を検証する機会が得られる
- 経営努力やリスク軽減が、最大のリスクがあると評価された分野で優先的に実施され、組織の効率が高まる
- リスクプロファイルを変化させ、理想的には削減させる措置を講じることを通じた学習と改善の継続
- 革新と持続性をサポートする、プロアクティブなリスク管理の企業文化

リスクプロファイルの開発に関係する、ワークフローあるいはタスク水準の機械的なステップを検討することは本報告書の目的ではない。だが、リスクプロファイルには通常次のような情報が含まれる。

- それぞれのリスクを区分して理解可能な充分に詳細なリスクの記述
- 所与のリスクが実際に発生または具体化する原因または基本的な条件

- リスクによって発生する結果。結果は通常、顧客離れ、監督機関による制裁、コスト超過など、財務的および非財務的な表現で示される
- 各リスクの適切な分類。保険者に多数の事業単位があり、全社レベルでリスクを統合する必要がある場合には、このことが特に重要となる
- リスクが発生する可能性・頻度と影響を考慮した、固有リスクの評価。リスク評価に関する明確な評価基準の設定、すなわち、高、中、低レベルのリスクを判断する財務的又は非財務的な指標の設定
- 統制やリスク軽減戦略の有効性の評価。本評価に統制の設計および機能の検討と統制のオーナーシップの記載が必要
- 統制の有効性を反映した残存リスクの評価
- 容認できない残存リスクを適切な限度内に収めるための行動の記述

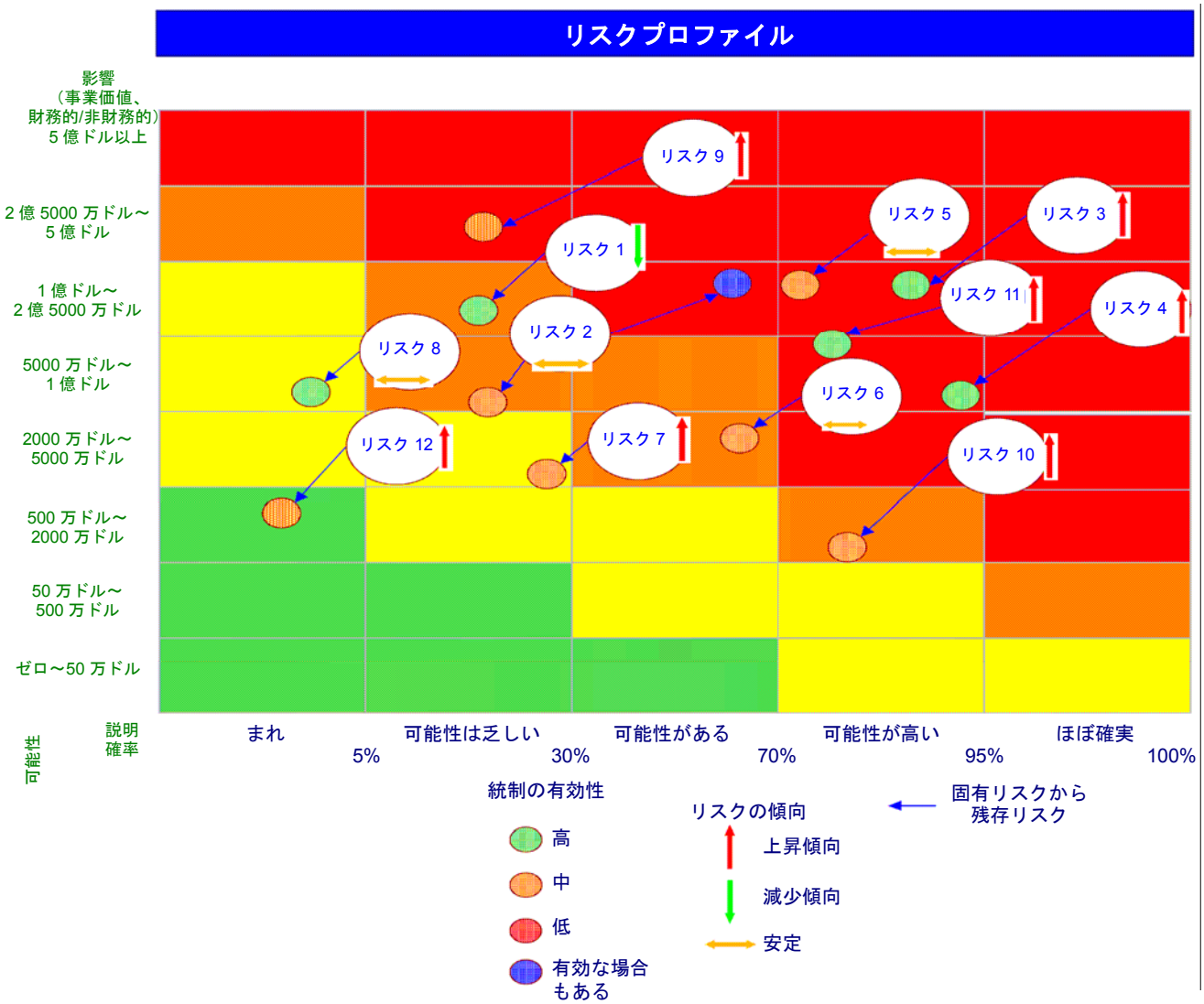
リスクプロファイルに関する文書には、担当管理職の承認が通常必要である。保険者の全社的リスクプロファイルの場合には CEO、事業単位のリスクプロファイルの場合には事業単位の部長が署名を担当する。

保険者の経営陣は、リスクの評価および定量化を進んで行う傾向がある。つまるところ、それは彼らにとって中心的な業務である。だが、経営陣は非保険リスクを財務的に定量化しようとする傾向が発生する。多くのリスク、特に戦略またはオペレーションに関係するリスクは、確率的な動きを示さない可能性があり、また統計的な分析やアクチュアリアルな分析の対象にはなりにくい。そのような場合、より単純な基準もしくは定性的な基準によってリスクを定量化する方が良いのではないかと考えられる[6]。

リスク担当者は、リスク・プロファイリングが形骸化することや、それ自体が目的であると見られる事態を避けるよう注意する必要がある。作業の大半はリスクプロファイルの作成に費やされ、その維持のための作業は少ない。事業が急速に変化している場合や拡大している場合を除き、通常、リスクプロファイルに大きな変化が短期的に生じることはない。従って、リスク担当者はこのことを念頭に、リスクプロファイルが経営意思決定にとって常に適切なものであるようにしておく必要がある。

リスクプロファイルの報告書には、重要な（「トップ 10」）リスク管理情報（固有リスクの評価、統制の有効性、残存リスク、リスクの傾向）の寸評を記載する必要がある。次のグラフは 1 ページで情報を伝える方法を示したものである。

[6] 具体例については、Australian Risk Management Standards or Committee of Sponsoring Organizations of the Treadway Commission (COSO)などを参照。


リスクプロファイル
影響
（事業価値、
財務的/非財務的）
5 億ドル以上
2 億 5000 万ドル～
5 億ドル
1 億ドル～
2 億 5000 万ドル
5000 万ドル～
1 億ドル
2000 万ドル～
5000 万ドル
500 万ドル～
2000 万ドル
50 万ドル～
500 万ドル
ゼロ～50 万ドル
可能性
説明
確率
まれ
5%
可能性は乏しい
30%
可能性がある
70%
可能性が高い
95%
ほぼ確実
100%
リスク 9
リスク 1
リスク 5
リスク 3
リスク 11
リスク 4
リスク 2
リスク 8
リスク 6
リスク 12
リスク 7
リスク 10
統制の有効性
高
中
低
有効な場合
もある
リスクの傾向
上昇傾向
減少傾向
安定
固有リスクから
残存リスク

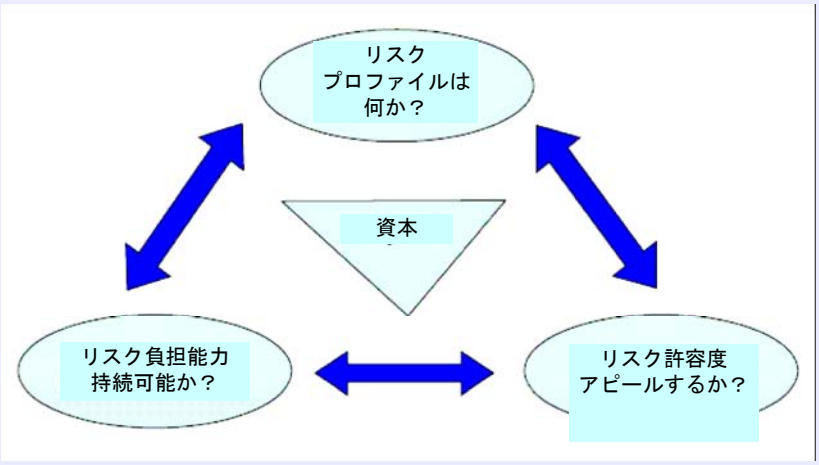
事例：
「リスク・プロファイリングのプロセスとは」

リスク・プロファイリングは主に3 つのプロセスから構成される。

1. 準備作業 *- リスク・プロファイリングの目的は、系統的なアプローチに基づくリスクの記録と評価を企業にもたらすことである。それによってリスクの理解が共有され、明確になる。従って、リスク・プロファイリングの作業の前に既存の資料を準備することがリスクの識別と統制の評価に役立つ。*

2. リスク・プロファイリングの作業 *- リスク・プロファイリングの作業を進めるために、リスク管理を推進するリーダーを定め、そのリーダーガイダンスを行い、プロセスの一貫性を確保する必要がある。実務担当者の関与がリスク・プロファイリングの成功のカギとなる。これはそれによってリスクの正確な把握が可能となるためである。リスクプロファイルの完成には時間的な初期投資が必要であり、またそれを維持するためには継続的な関与が要求される。要求される時間の量は、リスク・プロファイリングの作業の完成のために採用したアプローチ（ワークショップか一対一のミーティングかなど）によって異なる。*

3. レビュー *- プロファイリング作業の終了後に、リーダーが検証を行い、ミーティングの結果が正確に記録され、経営者の承認を得ていることを確認する。*



このアプローチの主要な効果は次のとおり。

- *組織全体にわたって一貫性のあるリスク･プロファイリングを推進する系統的なプロセスが実現される*
- *リスク・プロファイリング作業の事前にリスクに関連した資料を検討することにより、参加者はリスク・プロファイリング作業の絶好の出発点に立つことができる*
- *リスクに関する専門知識とビジネスに関する知識の双方がリスクプロファイルに活用される*
- *リスク・プロファイリングの透明性の向上*
- *リスク・プロファイリングの時間的効率*
- *リスクと統制の間の明瞭な関係性*

だが、以下の点に注意する必要がある。

- *既存の資料の提供によって、参加者が今後の問題点よりも、既に判明しているリスクに注意を向ける可能性がある。常に潜在的なリスクを考慮することが必要*
- *「年に一度」作業を行うアプローチが採用されることがあるが、それではワークショップ以外の場所でリスクプロファイルが更新されることが阻まれる場合がある。リスクプロファイルを絶えず更新し、事業の効果的な運営に役立てることが必要*

6.3　リスク・モデリング技術

リスク・プロファイリングのプロセスとは別に、保険者は保険リスクを定量化するために、さまざまな統計的手法やその他のモデル化技術を一般的に使用している。下表に保険リスクの定量化に適切であると考えられる一連のモデル化技術と統計的手法を記載する。これらの技術の詳細については、添付資料 8 の参考資料を参照のこと。

リスクカテゴリー	モデル化技術
全社的 ・ 全リスクカテゴリー	• 動的財務分析（Dynamic Financial Analysis）
保険引受リスク（再保険を含む）	• 財政状態報告書（FCR）や保険引受に関するモデル化または検証
市場リスク	• バリューアットリスク（VaR）やテールバリューアットリスク（TVaR） • 金利モデル • シナリオテスト
信用リスク	• 信用リスク・モデル
流動性リスク	• 資産・負債モデリング
オペレーショナルリスク	• 内部ロスデータ • 外部ロスデータ • シナリオ分析、シミュレーション

コメント:
「ブラックスワン」ジレンマ - ERM で充分か

ナシーム・タレブ（Nassim Taleb）[1] は、影響が甚大で、予測困難であり、通常の予想範囲を超える稀な出来事を表現するために、「ブラックスワン」という言葉を作り出した。この例えは、多くの人々は白鳥が白いものと思っている（少なくとも黒い白鳥がオーストラリアで 17 世紀に発見されるまでは）ので、黒い白鳥の出現は不測の出来事であり、あり得ないことが起きていると認識されることを意味している。

ブラックスワンは歴史上頻繁に現れている。最近では、9/11 のアメリカ同時多発テロやアメリカのサブプライム問題が記憶に新しい。こうした事件は実際に予見され、また予見可能であったと主張する人々がいるかもしれないが、現実に事件が起きると人々は驚く。とりわけ、金融サービスセクターの奥深くまで及んだ影響の大きさには驚かされた。

だが、ここにジレンマが発生する。ブラックスワンが一度現れると、既に経験されたことになり、不測の出来事であるブラックスワンは二度起こることはあり得ないことになる。こうした出来事が繰り返して発生することを防止する計画を立てることは良いアイデアであるが、不測の出来事の発生を防ぐことはできない。こうした出来事を詳細に理解しても、ブラックスワンの再現の防止にはほとんど効果がない。

新興リスクを登録していけば、不測の出来事の防止に役立つという意見もある。新興リスクに関する最近の話題の 1 例はナノテクノロジーである。前もって分かっていれば、不測の出来事にはならないとしても、費用対効果の問題が生じる。とりわけ、その正確な規模がはっきりしていない場合に、発生の可能性がある出来事を防止するためにどこまで資金を使うことが正当であるのか。

リスク管理に関するグッドプラクティスが唯一の予防策であるが、不測の出来事は常に発生する。適切な ERM 体制を通じて、不測の出来事の発生を適切に管理し、影響を軽減することが可能となる。

ERM は、あらゆるリスクによる影響、特に不測の出来事を防止するために十分でないかもしれないが、まったく予防する制度がない場合よりもはるかに良い結果が得られる。

1 Learning to Expect the Unexpected by Nassim Taleb, The New York Times, 2004 年 4 月 8 日

7. 経済資本と規制資本

重要機能 6

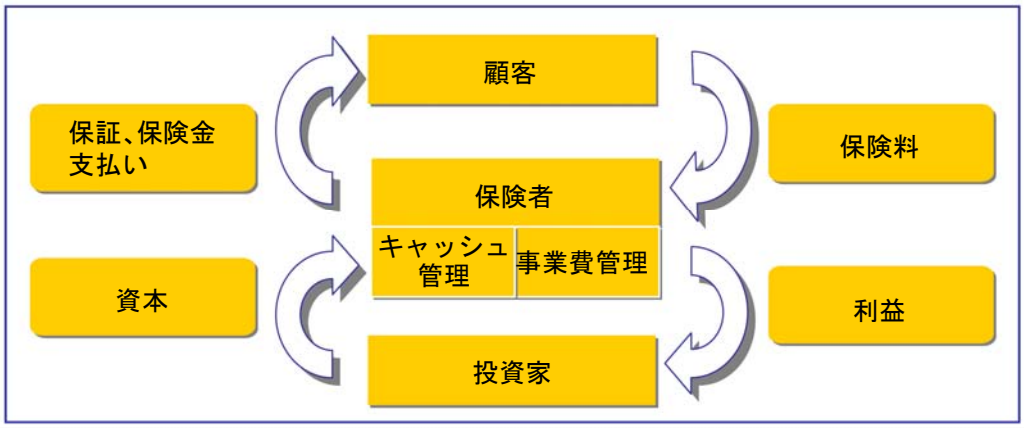
保険者は ORSA の一環として、自社のリスク許容度と事業計画を踏まえたうえで事業を経営するために必要な財源、また、監督上の要件が充足されていることを立証するために必要な財源の全体を決定する必要がある。保険者のリスク管理対策は自社の経済資本、監督資本の要件、および財源を基礎としたものでなければならない。

7.1 はじめに

資本主義の背後にある基本原則の一つは、最も生産的な活動と組織に対して、市場が資本を配分するというものである。その生産性は供与された資本に基づいてリターンを提供する能力を基準として測定される。企業はこの原則に基づいて、資本を必要とする新規事業を提案し、その資本に対して提供するリターンを提示する。資本所有者はそうした提案を評価したうえで、個々の提案の潜在的リスクを考慮しながら、限られた資本を最も自分に適合した提案に提供する。時間の経過につれ、国や業界や企業の実績が確立され、資本の継続的な提供や期待リターンが精緻化される。

保険分野について見れば、保険金支払という約束を履行し、経費やキャッシュフローを効率的に管理するために適正な保険料を徴収することが、保険者にとって必然となる。保険者は、そうした保険事業の運営に際して、資本提供者への支払いに充当できる利益を減少させる可能性のある多くのリスクにさらされる。したがって、そうしたリスクの管理は保険事業運営の重要な一部をなす。主要なリスクは、ライフサイクルの段階（新設とランオフなど）、相対的な規模、引き受けた契約の性質などの要因により保険者ごとに異なる。

以下の図表 1 は保険分野における以上のような関係を図示したものである。



以上のようなリスクの管理における重要な構成要素は、保険者が事業を行う環境のシミュレーションを企図したモデルを確立することである。そのようなモデルを使えば、多くのさまざまに異なる前提の下でどのような利益が獲得されるかについて示唆が得られるうえ、保険者の経営者にとっては、特定の意思決定が将来利益の予想水準や予想ボラティリティにどのように影響するかに関する指針を入手できる。また、モデルから保険者の破綻リスクに関する示唆を得ることもできる。このようなモデルは経済資本(Economic Capital)モデルと呼ばれることが多い。このモデルは資本提供者、監督者および企業によって使用される。

資本提供者と監督者は個別企業に適用するより一般的なモデルを使用し、個別企業の特性を考慮に入れるために若干の調整を行う。企業の経営者は一般に、社内で開発され、従って比較的正確なモデルを使用する。そうした社内開発による経済資本モデルからは通常、資本の必要性に関するより正確な評価のほか、経営管理上の主要な意思決定へのインプットに関するより優れた洞察が得られる。

内部的な経済資本モデルの「ベストプラクティス」は、企業の全体的な資本とリターンをより細かな部分に分解することができ、その細かな部分について個別の意思決定を下せるようなものである。その重要な事例として、企業の販売する各種商品が異なるリスクプロファイルと利益特性をもつような場合がある。必要資本に照らしてどの商品が会社の全体的利益を高めるか、あるいは希薄化するかを知ることによって、究極的に企業の全体的な資本収益率を改善するうえで必要な是正措置が可能となる。

事例：
評点

価格設定が果たす役割の一つは保険料の競争力を強化し、適正な資本収益率が達成されるようにすることである。

保険者の会社全体の必要資本は通常、その保険者のリスク選好、市場や規制当局からの期待、自社の経済資本モデル（ECM）などによって決定される。保険者はまた、その資本に基づく全体的な予想収益を設定することもある。

しかしながら、保険者は価格設定の機能に依拠して全体的な成果を実現するが、これは通常、さまざまなリスククラスに関する詳細レベルでの多くの意思決定が基礎となる。価格設定機能がそうした役割を効果的に果たすためには、保険者全体の必要資本要量を基本的なリスククラスに配分することのできる堅固で正確なECM が必要となる。各リスククラスの資本収益率のパフォーマンスを理解し、価格設定やリスククラスの特徴や契約量を調節することによって、保険契約者にとっての全体的な資本収益率の結果の舵取りを行うために、そうしたECM を使用するのである。

例えば、下表の列(A)には、ECM によってそのリスククラスに割り当てられた資本について、望ましい資本収益率（RoC）を達成するために必要な価格設定基準（例えば保険商品のプロフィットマージンなど）が示されている。「局所化」された意思決定が可能となる下位の詳細レベルにまで資本を割り当てられるのがECM の優れた特長であり、価格設定機能の成功にはこれが不可欠である。

リスククラス	X%の RoC を達成するための価格設定基準	実際の価格設定基準	評点	実際の取引量
	(A)	(B)	(B/A)	
X	10%	11%	1.10	100
Y	5%	4%	0.80	200
Z	7%	7%	1.00	70
合計			0.92	370

上例の詳細レベルをさらに引き下げるという点に関してこの事例を使うなら、ECM を用いてリスククラス Y に関してより下位の詳細レベル（すなわち、Y1 と Y2）で必要資本要件を定めることが可能な場合、リスククラス Y のアンダーパフォーマンスの原因を把握して、より効果的な経営決定を下せる公算が大きい。例えば、リスククラス Y2 の価格設定を改訂したり契約量を制限することにより、より的を射た措置が可能となるであろう。

リスククラス	X%の RoC を達成するための価格設定基準	実際の価格設定基準	評点	実際の取引量
	(A)	(B)	(B/A)	
X	10%	11%	1.10	100
Y1	5%	6%	1.20	67
Y2	5%	3%	0.60	133
Z	7%	7%	1.00	70
合計			0.92	370

7.2 経済資本モデル（ECM）

経済資本モデル（ECM）の目的は、組織内の主要なリスク要因に関する全体的な評価を提供し、そのリスクに対処するリスク管理技法を考案することにある。

ECM は一般的に資産・負債の統合モデルによって構成され、将来の期間にわたる資産および負債のキャッシュフローをシミュレートするものである。ECM からは通常、予想される将来のバランスシート、損益計算書、キャッシュフロー計算書、予想される利益分布のほか、資本および資本収益率が得られる。これらはモデルを何回も繰り返し実行することによって得られる。分布は、主要指標が許容水準を外れる確率（リスク許容度に関する可能な定義の一つ）についての見解を経営者が形成することを可能とするものであり、したがって、必要資本の決定に対する不可欠なインプットである。このようなモデルは時には「内部モデル」と呼ばれることもあるが、この用語は、保険者の業績やリスクの一部の、それほど全体的でないモデル化についても使用することも可能である。リスク・資本管理を目的とした保険者による内部モデルの使用については IAIS ガイダンス・ペーパー（2007 年 10 月）も参照されたい。

ECM の資産モデル部分は、十分に調査された金融市場モデルを基礎とする必要がある。インプットとなるのは経済および金融にかかわるパラメーターであり、モデルは各種資産クラスのリターン間の相関や時系列的なリターンの相関に対応することが可能である。多国籍の保険者については為替変動に対応できることが望ましい。

負債モデルは保険料と保険金請求との関係およびその変動性を分析するものである。考慮すべき変動原因の例としては一般経済条件、将来的な保険金請求状況の悪化（あるいは改善）、市場シェアの変化、引受サイクルの影響などがある。再保険やクラス間の相関も考慮の対象とする必要がある。

一部の経済変数（インフレ、金利など）を通じた資産モデルと負債モデルの関連性についても検証が必要である。ダイナミック・モデルの用途および利点として以下のものが挙げられる。

- 保険者の現行戦略から生じるバランスシートのダイナミックスに関する理解の深化
- 異なる資産戦略と負債戦略（および再保険戦略）の実行に関する効果の検討
- 各種の資本調達源（例えば、再保険、将来利益、留保利益、資本市場、準備金など）による相対的影響の分析
- 買収や投資撤退の意思決定にかかわるデュー・デリジェンスの支援
- 地域ごと、商品ごとの資本配分
- さまざまな事業部門のリスク調整後パフォーマンスの評価
- 最適な資産構成の決定
- 財務状況の報告
- 保険者の財務状況に対して想定される極端な事象の影響の把握

モデルは単なる手段であり、インプットの完全性に大きく依拠していることに注意する必要がある。加えて、何らかの主観性が混じることは不可避である。モデルの結果それ自体が主要なメリットではなく、むしろ、モデル化の過程によって得られる、事業上のリスクや牽引要因に関する理解の深化の方が有益である場合が多い。

ダイナミック・モデルでは、資産からのキャッシュフローと負債のキャッシュフローのマッチング（あるいはミスマッチ）を企業が選択する度合いを考慮し、それに対処できるようにする必要がある。また、保険者の具体的な流動性要件も考慮に入れなければならない。ECM には通常、投資と再投資に関する企業の方針に関連する規程や、保険者を取り巻く流動的な金融状況に応じた投資ポートフォリオの組み替えとリバランスを定めた規程が反映される。

また、ダイナミック・モデルは、経営者が収益の不安定性を引き起こす要因を体系的に理解する手段にもなると同時に、収益の不安定性を低減させる、目標を定めたリスク管理戦略の開発に対して健全な基礎ともなる。

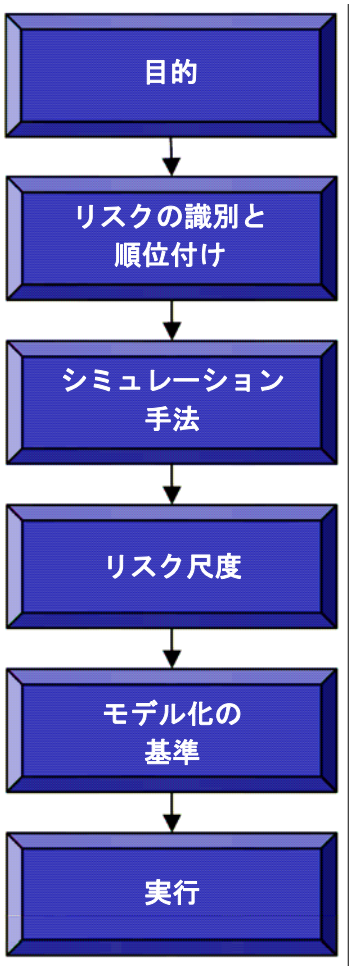
ECM の形式と用途に影響する重要な意思決定は、ECM をどの程度企業の日常業務に統合するかということである。この点に関するさまざまな選択肢として以下のものが挙げられる。

- 事業の（実際または潜在的な）変更事項に関する ECM のリアルタイムの実行

- ECM の成果を企業が日常ベースで活用することのできる「経験則」に置き換える
- ECM の統制を集中管理的にするために使用されるプロセス。通常、個々のビジネス単位はそれぞれ詳細なモデルをもち、それらは中央集権モデルによって取り込まれ、保険者の全活動を通じて一貫した基礎に基づく、より集約されたアウトプットをグループレベルで生み出すことが可能となる。

7.3 経済資本モデルの実行プロセス

ECM の実行プロセスには多くのステップを伴う。以下のフローチャートは段階的な要約を示したものである。



ECM の実行プロセスの各ステップについては以下のセクションで説明する。

a) 目的

ECM を使用する目的は監督上の必要資本要件なのか、それとも保険者自身のソルベンシー評価なのか。監督資本に関連する目的で ECM を使用する場合には、内部モデルに関する IAIS のソルベンシー要件[7]を遵守しなければならない。本報告書は保険者自身によるソルベンシー

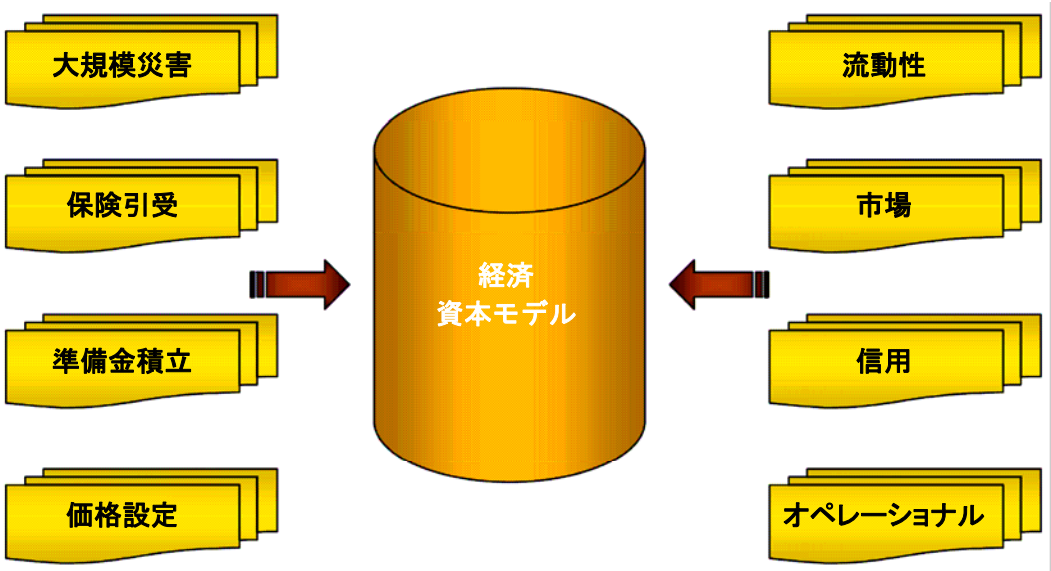
[7] リスク管理および資本管理を目的とした保険者による内部モデルの使用に関する IAIS ガイダンス・ペーパー（2007 年 10 月）

評価や資本管理を目的とした ECM の使用をサポートしている。ECM は以下の点に重要な影響を及ぼすため、その目的を明確にしておくことが重要である。

- 誰が ECM の責任者になるべきか
- ECM に関連してどのような水準の統制やプロセスを組み入れる必要があるか
- ECM はどの程度柔軟でダイナミックなものである必要があるか
- ECM についてどの程度の詳細性と正確性が必要となるか
- どの程度のリソースが必要となるか

b) リスクの識別とランク付け

個々の保険者の特定の要件に従って評価とランク付けを行う必要のあるリスクを以下に示す。主要なリスクは保険者によって異なるであろう。



モデルの精緻化にあたってはリスクのヒエラルキー（階層）が反映されることになる。すなわち、主なリスクにはより詳細なモデル化や分析が必要となる。

リスク間（およびリスク内）に認められる分散効果は一般にモデルに組み入れられる。組み入れは、例えば相関行列、コピュラなどの手法を通じて実行される。

オペレーショナルリスクの範囲を勘案するなら、国内の保険業界と海外の保険業界との一貫性を確保するために、明確に定義されたガイドラインが必要である。ここではその例として、銀行のオペレーショナルリスクに関するバーゼルⅡの定義を挙げておく[8]。

[8] 「自己資本の測定と基準に関する国際的統一化 - 改訂された枠組」、バーゼル銀行監督委員会、2004 年 6 月

> オペレーショナルリスクは、内部プロセス・人・システムが不適切であることもしくは機能しないこと、または外的要因に起因する損失にかかわるリスクと定義される。この定義には法務リスクが含まれるが、戦略リスクや風評リスクは除外される。

バーゼルⅡはオペレーショナルリスクの計算のために 3 つの方法を説明している。それらの方法について洗練度の低い順に以下で述べる。

(i) 基礎的指標手法

- オペレーショナルリスク資本は、過去 3 年にわたるプラスの年間粗利益の平均に固定比率（15%）を乗じた値である。

(ii) 標準的手法

- オペレーショナルリスク資本は、8 種類の具体的な事業別の年間粗利益に固定比率（12%、15%、または 18%）を乗じた値である。直前の 3 年間について、全事業のプラス値の合計を平均する。

(iii) 先進的計測手法

- オペレーショナルリスク資本は公認内部モデルを用いて計算される。

欧州保険・年金監督者委員会（CEIOPS）は直近の定量的影響度調査結果（2007 年春の QIS3）においてオペレーショナルリスクにかかわる資本負担の計算方法を説明している。オペレーショナルリスク資本は次の 2 つの値のうち低い方とされる。

- 基本所要ソルベンシー資本（Basic Solvency Capital Requirement）の固定比率（30%）
- 収入営業保険料の固定比率（損害保険は 2%、生命保険は 3%）と技術的準備金の固定比率（損害保険は 2%、生命保険は 0.3%）のうち高い方

どの方法を採用するかの選択は企業構造（モノライン保険会社、マルチライン保険会社、保険と保険外事業のコングロマリット）、組織内の資本モデル化の成熟度、リソース、費用などによって決められる。

国際的な保険業界にとっての課題はオペレーショナル損失を独立に記録するプロセスの確立である。オペレーショナルリスクに関する過去のデータは限られており、現在、そのためオペレーショナルリスクの確率論的モデルの高度化や信頼できる適用が十分でない状況となっている。

c) シミュレーション手法

保険者がモデル構築のために使用できるリスク計量化の技法としては数種類のものがある。大まかに言って、その中には基本的な決定論的シナリオから複雑な確率論的モデルまで多様なものが含まれている。決定論的シナリオでは通常、所定の確率をもつ事象を反映したストレステストやシナリオテストを用いた、保険者の資本水準に対する一定の事象（株価の下落など）による影響のモデル化が行われる。この技法では基礎をなす前提は固定されている。一方、確率論的モデリング（モンテカルロ法など）では、保険者の必要資本の確率分布を反映させるために、異なる確率を持つ複数のシナリオを用いることが多い。
選択は費用、時間、メリットなどによって決まる。

決定論的なテストは主要なリスクを浮き彫りにするものであり、より先進的なシミュレーション手法に対する適切なチェックの役目を果たす。特に重要なのは、リスク間の相互関係を理解し、そうした相互関係がストレスのかかったシナリオでどのように変化するかを把握することである（例えば、以前は無関係だった影響要因が厳しいストレスの下で相互に関係するようになることがある）。苦境時に保険者の経営者が検討すると思われる定性的、主観的な意思決定（例えば、資産構成や再保険の水準の変更）は ECM のインプットとして重要なものである。

d) リスク指標

ECM に関連する伝統的なリスク指標には次のものがある。

- VaR と TVaR
- 計測期間
- 信頼水準

これらは保険者の戦略やリスク許容度によって決まる。

e) モデル化の基準

モデル化の基準例としては次のものがある。

- 絶対的破産によって測定される出口価値
- 監督者の介入によって測定される継続企業の基準
- 一定の投資格付の達成

保険者は自社の各事業セグメントに複数の基準を適用することを追求する必要がある。

f) 実行

- ECM の開発に対して主に 2 つの手法を用いることができる。
- 業務全体の相互関係を考慮に入れる完全統合モデル
- 個別的な部門を別々に考慮した単独モデル(Univariate Model)を使用し、何らかの結合方法（コピュラなど）を用いてすべての構成要素を統合する

完全統合モデルは直ちにモノライン保険会社に適用できるのに対して、単独モデルは、保険事業と非保険事業に関わるマルチライン会社に適している。

使用するモデルの種類は、保険者の事業の性質、規模、複雑度に適合したものでなければならない。

7.4 資本管理との関係

監督資本の要件は必要資本要件に対するインプットの一つにすぎない。前述のように、以下のものを含め、他にも多くのインプットがあり得る。

- 格付機関による望ましい格付
- 望ましい、収益のボラティリティ
- 望ましい、株主のリターン - 配当や自己資本の増加
- リスクの蓄積
- 市場の期待値

ECM を用いた場合、一般に、監督資本規制の方法を適用するよりも事業に関する正確で完全な見通しが得られる。

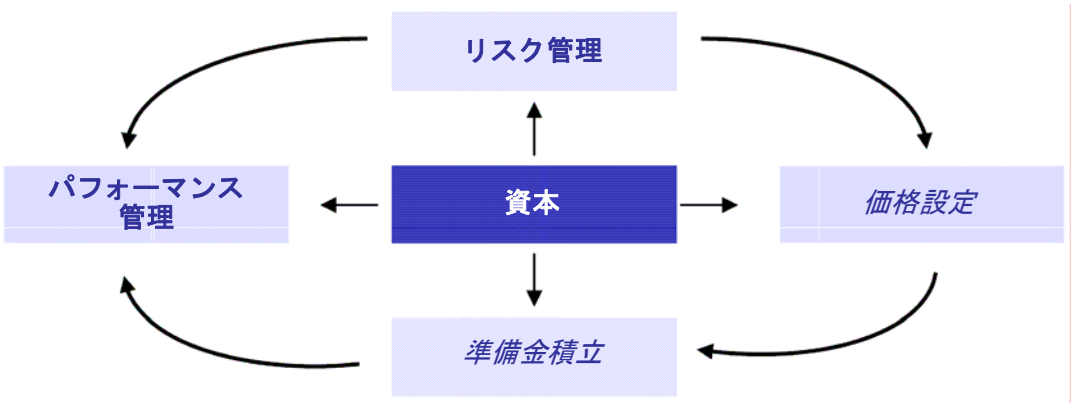
監督規制の方法と ECM との間に想定される主な差異としては、多くの場合以下のものが挙げられる。

- さまざまな事業クラスのボラティリティに関する見解の差異（絶対的なもの、および他のクラスと比較した相対的なもの）
- リスクタイプ間およびリスクタイプ内の分散効果の反映度合（相関行列によって算定されるが、コピュラによる場合もある）の差異
- 資本に影響する焦点の差異（目的の差異など）
- 対象とするリスクタイプの差異（例えば、オペレーショナルリスクは、監督規制の方法では対象外であったり、対象であっても暗示的に計算されるが、ECM では明示的に計算されるなど）
- 各種資産が資本として扱えるか否かに関して表明される見解の差異（例えば、税制上の優遇措置やのれんなど）

ECM を用いる場合でも、監督規制の方法による資本の計算や予測が必要となる公算が大きい。これは、関係する監督者がその相対比較を把握したいと望むためである。

効果的な資本管理ではリスクを株主価値に変えることが焦点となる。業務の観点からすれば、このことは、「適切な」量の資本を適切なリスクに帰属させれば、適切な情報に基づいた意思決定が可能となることを意味する。

以下の図式は、資本と資本管理の中核的要素との関係を明確に表そうとしたものである。



リスクを価値に変えるサイクルの中で資本は中心的な役割を果たす。資本は成長、設備投資、事業計画に向けた資金となる。また、保険業務活動、投資パフォーマンス、支援活動などによる望ましくない結果に直面した場合、支援の役割を果たす。

市場の観点からすれば、価格設定の役割の一つは保険料の競争力を確保し、十分な資本収益率を達成できるようにすることである。業務の観点からすれば、価格設定プロセスの目標は、予想される保険金請求のほか営業費や一般管理費を充足できるようにすることである。言うまでもなく、価格設定には、固定費を負担する必要性の考慮や必要に応じた監督上の要件の充足といった他の側面も含まれている。

準備金積立プロセスでは、未払保険金の予想中央値を定め、不確実性を補填するマージン（リスク・マージン）を提供し、将来の出来事に関する経験と予測を勘案したうえで保険負債に対して十分に対処できるようにし、さらには、予想される保険料率の不足を補填できるようにする。

リスクに応じた事業単位や保険種目への資本の配分はパフォーマンス管理プロセスの基礎を成し、予測を基にした結果やリターンの測定を可能にする。効果的なパフォーマンス管理には、リスク管理、準備金積立および価格設定のプロセスを調節して結果の向上につなげられるようにするための早期警告の仕組みが組み入れられる。

資本管理の観点からすれば、リスク管理は、全体的なリスク許容度の策定、リスクの識別と評価、およびリスクの継続的統制という三重の役割を果たす。リスク許容度の策定プロセスはどのリスクをとり、どのリスクを回避するかに関する系統だった決定に依拠している。先に述べたように、リスク許容度の明確な規定は、最終的には目標とする財務力（受け入れ可能な「破産リスク」）の形で表示できるが、その一方で、目標とする信用格付や受け入れ可能な収益のボラティリティといった戦略的な構成要素をそこに含めることができる。

8. 継続性分析

重要機能 7

保険者は ORSA の一環として、自社の事業継続能力のほか、規制必要資本要件の決定に通常用いられる計測期間よりも長期にわたって事業を継続するのに必要なリスク管理や財源を分析する必要がある。

そのような継続性分析に際しては、保険者の中長期的な事業戦略における定量的要素と定性的要素を組み合わせて取り扱い、保険者の将来の財務状態の予測および将来の規制資本要件を満たすための能力分析を含む必要がある。

8.1 はじめに

ECM を使用する主な利点は、規制上定められるもの以外のシナリオの分析が可能となることにある。例えば、規制必要資本の要件は継続ベースではなくランオフベースで実行される場合が多い。同様に、ECM の下では、保険者は規制上定められた大半の方法が基礎としている期間よりもさらに将来の期間に目を向けることが可能となる。そのためには（とりわけ）以下の事項について明確な決定を下すことが必要となる。

- モデル化においてどの程度の期間を用いるべきか
- 保険者の財政状態の評価は将来の一時点で行うべきか、それともすべての関連負債のランオフをモデル化したうえで行うべきか(訳者注：一期間で見るべきか、多期間で見るべきかということ)
- 最悪の結果が見込まれる場合、どのような経営行動が想定されるか
- どのような資本減少（配当など）や資本注入の方針が想定できるか
- 保険者の長期予測はどの程度信頼できるか、またその予測は ECM の基礎を十分に形成し得るものか

モデル化の手法とその諸前提は基本的に、リスクがモデル化される計測期間に依存している。計測期間が 1 年であれば保険者の経営行動は無視することができる。しかし、長期にわたるモデル化の場合には、保険者の行動がより重要になる。

計測期間が長期のモデルでは、保険者の行動を想定しない静的な事業・資産構成に基づく前提に立った場合、計測と予測の実効性が低下する。しかしながら、保険者の戦略や経営行動などの前提を考慮したモデルでは、そうした前提がかなり主観的であることから、モデルの結果を読み解く必要性が大きくなり、モデルの制約を明確に表示することが必要となる。

長期的なモデル化では、短期の計測期間において用いられるものとは別のモデルの開発が必要となることがある。例えば、長期の計測期間において金融市場のリスクをモデル化するためには、関連するリスクファクターを一貫して予測するモデルが必要となる。そのためには、純粋にヒストリカルなデータに大きく依拠したモデルよりもより説明的な（指標間の因果関係が明瞭な）モ

デルを使用すべきである。

1 年より長期の計測期間にわたって予測を行うモデルでは、経営者の行動と戦略のモデル化が重要な部分を占める。これには以下のものが含まれることになる。

- 保険料の設定：損失が発生したり利益が不十分だったりした場合、企業はどのような戦略をとるか。価格が低水準の場合、企業は市場シェアの維持や拡大を試みるか。保険サイクルにおける企業の戦略はどのようなものか。
- 資産配分：財務上のストレスが発生した場合、企業はどのように対応するか。
- 保険契約者への裁量的給付：とりわけ、(a)当該企業のみが財務的苦境に陥っているとき、および(b)市場全体が財務的苦境に陥っているとき、保険者は保険契約者への裁量的給付についてどのような戦略をとるか。
- 配当方針：とりわけ企業に損失が発生したときの配当方針はどのようなものか。
- リスク軽減戦略：再保険戦略、ALM 戦略、証券化など市場へのリスク移転手段など。

8.2 定量分析 - 資本計画

保険者の内部において真の統合的 ECM が幅広い目的で使用される。例えば、以下の事項に関係する分析を行うために使用することができる。

- 経済資本の要件
  ECM は組織のリスクプロファイルに基づいて必要資本要件を計測する主要な手段である。そのアウトプットは保険会社の資本管理プロセスと緊密に統合される必要がある。

  しかしながら、このモデルは資本をより緊密に事業運営の方法に連動させる目的でも活用することができる。組織のリスク選好の明確化や定義の一助として活用できるのである。例えば、このモデルは破産リスクや「規制上の破産」のリスクの計測を検討できるし、また、収益のボラティリティ尺度にもなり得る。
- 破綻に備えた計画
  ECM はまた財務的苦境の影響を分析する目的でも活用できる。その場合、保険会社が事業展開する管轄区域の法律上・監督上の要件に関する詳細な分析を含めることが必要となる。また、この分析において、資本調達の可能性に対する潜在的な制限も考慮する必要がある。分析終了後の結果は、資本管理戦略を変更し、必要に応じて、例えば緊急時資本ソリューションを通じて潜在的な資本移転の問題を緩和する手段を実行するために利用することができる。
- 投資戦略
  投資戦略に対する組織のアプローチでは保険者のリスク許容度や目標など数多くの要素を検討する。その算定に際しては、当該組織の将来的な資本の必要性も関連してくる。投資戦略は事業に将来必要となる資本量に応じて変わってくる。

- 合併、買収、企業分割
  ECM は企業が合併や買収、撤退の影響を理解する一助として活用することができる。つまり、リスクの分散化が必要資本要件に及ぼす影響のモデル化や、合併や企業分割の活動が原因で必要（あるいは不要）となる追加資本の実際金額の定量化の目的で利用できる。また、経済資本は買収（あるいは分割）した企業の評価を補足するためのメカニズムとしても利用できる。

- 資本配分
  資本配分は事業単位のパフォーマンスの計測に用いられる主要方法の一つである。資本を各事業に配分する方法は一つにとどまらないが、この手法はリスクを基礎とするものであり、企業が自社のリスク（資本に対する要求）を効果的に管理するためのインセンティブのほか、配分した資本に基づく妥当なリターンを稼得することを確実にするための方策を提供する。

  資本配分に際して用いるべき手法は組織の目的、例えば「最適ポートフォリオ」（リスクの分散という点で）の構築を目指すか否かということによって変わる。この場合、リスクの尺度は、単純な成長目標によって示唆されるような結果の分布の中央値よりも、クラスごとの周辺分布から導き出されるであろう。資本配分に際して克服すべき問題点としては、支援（すなわち、収益を生み出さない事業単位に対する支援）の取り扱いや、トップダウンの配分かボトムアップの配分か（あるいはその併用）という使用すべき手法などがある。

- 再保険プログラム
  ECM は組織のリスクプロファイルに基づいて必要となる資本を評価する目的で活用することができる。企業の財務諸表上のリスクが大きければ、それだけ多くの資本を留保することが必要になる。再保険は、保険者がリスクの一部を第三者に移転し、それにより保有が必要な資本量を削減するために利用できる主なメカニズムの一つである。したがって、この場合、再保険の価値は資本の代替機能として導き出される。

  組織は資本保有の費用と再保険の費用を比較検討することにより、より豊富な情報に基づく意思決定が可能になる。

- 最適な事業構成
  最適な事業構成の策定は当該事業への効果的な資本配分に関係している。事業毎のリスクを基にして資本配分が行われるなら、リスク調整後パフォーマンスの計測が可能となる。リスク調整後パフォーマンスの管理を活用することにより、商品構成や事業構成の最適化が可能となり、また、組織の戦略に沿った経営者の意思決定が促進される。考慮すべきファクターは資本だけではないものの、相対パフォーマンスを評価する適切な尺度が資本から得られる。

- 準備金積立のボラティリティ
  この場合、ECM は、保険金と保険料の準備金におけるリスク・マージンを「保険契約者資本」（バランスシート上の資産と負債の差額によって指定される「株主資本」との対比）として効果的に取り扱うために機能する。
- 資本の流出・流入に関する方針
  これは経済資本のモデル化の一部と考えられるものの、リスク許容度を特定の仕方で捉える（すなわち、企業にとっての資本充実度の「範囲」を分析する）ため、別立てで取り扱うことが重要となる。

ソルベンシーⅡに基づく資本コストのリスク・マージン（スイスのソルベンシーテストに由来する）では、実際に既契約の必要資本量を予測することが必要となる。そのために、組織は事業の長期的影響を評価する必要に迫られる。最低限のリスク管理として、負債の存続期間全体にわたる保険事業の必要資本を定量化することが可能でなければならない。

OSFI（金融機関監督官局）（カナダの規制当局）はすでに DCAT（動的資本充分性検証）の要件（10 年内に生じ得る望ましくないシナリオの予測）を通じてこれまで以上に長期の予測を要求している（2002 年 4 月、North American Actuarial Journal 掲載、Allan Brender（アラン・ブレンダー）による「The use of internal models for determining liabilities and capital requirements（内部モデルを用いた負債および必要資本要件の決定）」も参照されたい）。

一部の監督者は、しばしば財政状態報告書（FCR）と呼ばれる、財務的実行可能性に関するより正式な評価を保険者に対して要求している。FCR は通常、保険者が直面する広範囲のリスクを対象とするが、取締役会と監督者のために保険者に関する全体的な見解を提供する場合に最も有益なものとなる。FCR は通常、明確な数値で示される保険者の財政状態（財務諸表のほか上記の ECM の結果を含む）を対象とするだけでなく、多くの場合、オペレーショナルリスクや風評・ブランド関連のリスクなど保険者が直面する定量化困難な一連のリスクも取り扱う。FCR には通常、保険者のリスク管理体制の実効性に関する評価が記載されている。

8.3 定性分析 - 事業継続計画

事業継続計画はオペレーショナルリスク管理の不可欠な構成要素である。企業は事業継続計画により事業中断リスクの予測、識別および評価が可能となる。適切な文書化と検証が行われた事業継続計画（BCP）により、主要な事業プロセスに対する中断の影響が緩和され、さらに、最も重要なこととして評判が保護される。また、堅固な BCP により、企業は生じ得る事業中断に関連するリスクが管理可能であることを利害関係者と業界の監督者に説明することも可能となる。

8.4 危機管理とコンティンジェンシープラン

危機管理計画により、あらかじめ定められた対応手続きに支えられた明確かつ組織化された対策が確立され、重大な事故が発生した場合に企業が受ける悪影響と損失が最小化される。危機管理計画は、例えば危機管理グループ（CMG）が、事故の最中にその性質と重大性を評価し、その事故が危機水準の対応を必要とするかどうかを決定し、そして、経営者と社員による適切な行動を発動させるために実行すべき基本的行動を定めるものである。

結果に対する一つの対処方法は、偶発事象に備えた計画と準備に着手して、保険者が予想外の利得を有利に生かしたり、損失を限定したり、混乱を防止・抑制したりするために迅速な行動をとれるようにすることである。そのためには、計画が適切なリスク管理の原則にしっかりと基づいて策定され、検証済みかつ最新のものであることが必要となる。ある事象が発生した場合、組織の経営者は、収益フロー、商品の品質、会社の評判、顧客満足といった事業目標の達成に対する当該事象の悪影響を緩和するために迅速に対応する必要に迫られることがある。ほとんどの場合、そうした悪影響は通常の管理プロセスの一環として管理できるであろう。しかしながら、事象の規模が経営者の通常の対処能力を超える場合には、危機事象管理に対する系統だったアプローチが必要となる。

危機事象管理の中核を成すのは事業継続管理（BCM）である。組織はこの計画により、重大な事業混乱の可能性に直面しても持続可能な形態で事業を継続する規律ある業務能力を備えることが可能となる。適切に導入された BCM は、混乱リスクへのエクスポージャーに対して費用効率よくかつ時宜を得た仕方で対処するための堅固な枠組みを提供できる。また、組織が、経済的環境や業界環境、安全環境の混乱増大に直面した際に、適切なコーポレートガバナンスを維持し、顧客基盤と市場シェアを堅持し、利害関係者の信頼をつなぎ止め、自社の評判を維持するための主要な構成要素を提供する。最低限の対応として、BCM が効果的であれば危機が根強く継続し、拡大するのを阻止できる。

事例：
再び水没！

「クイーンズランド州では全土が洪水に見舞われ数億ドルの損害に直面している。道路は寸断され、炭鉱は水浸しになり、貯蔵された農産物は打撃を受け、人々は家に住めなくなった。活況に沸いていた同州の石炭業界はボーエン盆地の石炭生産に数千万ドルの損失が出ると予想している。この洪水により、一部の農家では大量の貯蔵農産物が被害に遭い、また灌漑のインフラも破壊され、作物にも損害が出ている」（news.com.au、2008 年 1 月 22 日）

保険業界にとって気候変動が大きな問題となっており、極端な気象事象の発生の増加は地球環境の変化の兆候であると考えられる。オーストラリアでは極端な気象事象が主要な財産損傷の原因の大部分を占めており、そのため、損害保険会社にとって強い関心の的となっている。クイーンズランド州の洪水は、ごく最近オーストラリアの保険業界が対応を迫られた天候関連の災害の一例にすぎなかった。この災害では遠く離れた数多くの場所が被害を受けた。

事業継続の観点に立った場合、顧客サービスを重視する保険者にとってどのような対応が適切なのか。また、自社の建物やデータセンターが被害を受けた場合、どのように対処すべきであろうか。

2008 年に、規制要件に従い、実証済み・テスト済みの回復戦略や、十分に検証を繰り返した継続計画、明確な危機管理手続き、不可欠なサービスを継続して実施する必要性を自覚したカルチャーを備えた「堅実な」保険者があった。広い地域にわたって顧客基盤を抱えるこの保険者はまた、保険金請求の処理を業務機能回復の最優先事項とする堅実なサービスモデルを導入していた。この業務モデルに従い、処理業務がどれか一つの建物、場所、データセンターに依存することがないような体制がとられていた。同社のインフラは一部が損傷を受けても、他の部分が短期間のうちにその分の作業を引き継ぐことができ、被害地域の機能はすぐさま別の施設で作動できるよう回復された。

この保険者は、顧客のニーズに対する重要な初期対応として、機動性のある査定担当者を被災地に派遣した。査定担当者は保険金請求の受理と処理、請求に基づく支払い、緊急の貸し付けの承認、および保険契約の範囲内にある他の特別な支援要求への対応などを行うために必要な技術と権限を備えていた。この保険者は予備の携帯電話インフラを用意しており、担当者全員が常に連絡をとれるように、それを速やかに配備できるようにしている。また、自社の担当者が責任ある方法で被災地に立ち入ることができるようにするため、また危険に遭わないようにするため、災害救援・緊急医療サービスの担当者と密接に協力して作業を進めた。

大規模な異常災害事象は非常にまれにしか発生しないとしても、保険業界に大きな難題を突き付け、個々の保険者では対処できないこともあり得る。このような状況で、責任ある保険者は、前もって準備され検証された大災害時協力協定に基づいて全国的な業界統括組織と連携して活動する。州・連邦の政府機関、保険業界組織、保険オンブズマン・サービス組織、ブローカー・損害査定人の団体などで構成される作業部隊を組織することによって、以上のような課題に対応するための広範囲な共同責任体制が構築される。

9. リスク管理における監督の役割

重要機能 8

監督者は保険者のリスク管理プロセスと財務状況のレビューを行う必要がある。また、その権限を行使して、必要に応じてソルベンシー評価や資本管理プロセスを含めたリスク管理の強化を保険者に要求しなければならない。

9.1 はじめに

このセクションの目的は、保険者が監督者と建設的で透明でプロアクティブな関係を構築するのを支援することにある。

9.2 監督者の役割

プルーデントな監督[9]は、金融機関に対する規制の不可欠な構成要素として世界中で受け入れられている。監督者の役割を支える基本的な前提は、監督対象となる金融機関の財務健全性や慎重なリスク管理に関する第一義的な責任が取締役会と経営陣にあるということである。これに関連して、監督にあたっての主な重点は、問題発生の責任者の処罰ではなく問題の回避に置かれる。

保険との関連で言えば、プルーデントな監督では以下の要素から成るシステムを構築することが含まれる。

- 財務状況の監督
- 許認可権
- プルーデントな基準など事業継続要件
- 許認可の条件や事業継続要件の遵守をモニタリングするための手続きとプロセス
- 必要な場合、遵守していない保険者に遵守させるか、あるいは業務を停止させるための強制措置の発動

[9] 銀行、保険者、住宅金融組合、共済組合などの金融機関の監督・規制に関して用いられる用語。当該金融機関によって維持される預金者や保険契約者の保護が財務上健全であることを監督当局が求めることをいう。

監督者は監督手法としてリスク・ベースの手法を採用する。実際このことは、より大きなリスクに直面している金融機関は監督者からより入念な注視を受けるということを意味する。したがって、監督者は、監督を効果的に行うために、リスクについて、また個々の監督対象金融機関におけるリスク管理の実効性について、自らの見解を形成する必要がある。

また、監督者は、監督行政においてリスク管理実務を全体的に捉えるという点で、特定のマーケットにおいて独自の地位にあるということに留意する必要がある。監督者は最悪のプラクティスからベストプラクティスまでのあらゆる範囲を取り扱うことになる。したがって、自社のリスク管理実務の改善を追求する保険者は、リスク管理の改善を目的として監督者と交流する機会を見逃してはならない。

9.3 リスク・ベースの監督

監督者は保険者を理解するため、通常、保険者の事業の性質、ガバナンスの取り決め、戦略計画・事業計画、財務報告書、リスク管理の戦略とプロセスなどの検討から始める。許認可や事業継続に関する監督活動には通常、それらの領域に関係する文書のレビューが含まれている。

保険者は、監督者が会社に関する上記の主要側面を理解し検証するのを手助けするように、監督者に対しプロアクティブな対応活動を行うべきである。監督者は、保険者のリスク管理体制の戦略的側面や高度な側面について安心感をもてない場合には、より厳しい監督手法を採用する公算が大きくなる。したがって、保険者は監督者との間で戦略や体制の問題について継続的で率直な対話を促進するよう心がける必要がある。そうすることで、中長期的により開放的で生産的な関係が醸成されることになるであろう。

9.4 監督者との関係構築

関係構築の原則

保険者は監督者への対応活動の指針となる一連の基本原則の採用を検討する必要がある。保険者は一連の適切な原則を策定するにあたり、以下のことに配慮する必要がある。

- 監督目標との整合性
- 企業評価の維持と向上
- プロアクティブかつ早期の対応活動
- コミュニケーションにおける透明性
- 責任と協調の関係構築

戦略的アプローチ

監督者は保険者にとって主要な利害関係者の一人であるので、保険者は監督者の目標とプロセスを全体的に把握することが必要になる。監督者との関係構築のための戦略的アプローチの一つとして、とりわけ主要な監督者のプロファイルの維持管理がある。そのプロファイルの中には、監督者と保険者内部の主要連絡担当者、将来的な監督上の優先事項や目標、弱点、具体的な重点的リスク領域、関係分析、関係強化計画、対応活動の機会などが含まれている。

監督者との交流の特質

保険者は通常、自社が業務展開するさまざまな管轄区域の規制を行う監督者との間で一連の多様なやりとりや意思疎通を行う。その包括的な区分は次のとおりである。

- 業務・手続関連
    - 標準化された定期的な収益データや統計データの提出
    - 標準業務に関係する日常的問い合わせへの回答（保険金請求に関わる業務遂行のベンチマークなど）

- 非標準的・非定期的
    - 顧客の苦情に起因する問題に関する監督者への回答
    - 業界の問題とそれに対する会社のエクスポージャー（リスク負担状況）に関する監督者への回答。例えば、ハリケーンやサイクロンまたは台風などに対するエクスポージャー（リスク負担状況）に関する調査への回答
    - 調査や強制措置の開始を知らせる監督者からの通知
    - 監督者の実査結果に関する、監督者から経営陣への報告
    - 重大な事故および違反の監督者への報告
    - 現在の法律または提案中の法律にかかわる救済措置や免除措置の要請
    - 罰金の通知または「説明」要求
    - 業界レベルや企業レベルの強制措置に対応するための戦略や戦術の策定
    - 非標準的な通知への対応（強制的約束など）
    - 保険者が懲罰措置の対象となるか、不利な結果を被る可能性のある特別な調査

- 戦略的
    - 現在の法律や方針または提案中の法律や方針に関する提案
    - 監督者の方針上のスタンスの変更の働きかけ
    - 保険者の見解や方針上のスタンスに関連する社会（マスコミや政府など）向け声明
    - 戦略的取り組み（買収、企業取引など）に関連する監督者との協議

以上のような広範なやりとりを背景として、多くの保険者（および大半の大手保険グループ）は「適材者」が適切に監督者に対応できるようにするための責任体制と手順を策定している。その一例として、買収提案に関係する監督者への対応については保険者の最上位の経営者が当たるという場合がある。

保険者によく見られるアプローチは、監督者との関係に関する全責任を一人の役員、通常は最高リスク管理責任者（CRO）や最高財務責任者（CFO）に担当させるというものである。こうすることによって、監督者への対応を効果的に計画したり調節したりすることが可能となる。このアプローチによれば、すべての非標準的対応や戦略的対応に対して最終的に関係する責任者の目が届くようになる。

監督方針の策定

保険者にとって、方針策定の分野において監督者と交流することが極めて重要となる。その理由は、保険者が、提案中の監督上の変更による実務的な影響について評価する最良の位置に立っているからである。監督者は自らの提案に関する建設的なフィードバックを求めており、保険者が新提案の堅固性と相応性を検証することを望んでいる。

監督者は新提案に関する意見提出について期限を設定するのが一般的である。保険者は意見提出への対応に関して戦略的・積極的なスタンスをとる必要がある。最終期限日に回答書面を届けるというだけの提出プロセスでは、わずかな成果しか得られないことが多い。むしろ、保険者は、監督者と会って提案の影響や変更の根拠を理解する機会として方針策定プロセスを利用すべきであろう。

今日の状況にあって、監督者はプリンシプルベースの監督に向かう方向へと動いている。したがって、保険者はやむを得ない理由がない限り、自社が独自であるとする主張を避けなければならない。むしろ、業界団体を通じ、提案された新政策に関する見解を調整する必要があろう。

監督者による実査

監督者は実査によって保険者の業務やリスク管理プロセスの特定の側面について深く掘り下げる機会を得る。保険者はまず第一に、監督者に協力し、通常は年度毎の監督計画全体の策定を支援する必要がある。

計画全体について合意がなされた上で、保険者は、日程表の作成、文書の提出、実査全体の実行など、実査の調整を監督者と行う必要がある。このプロセスは業務レベルで監督者との関係を強化する絶好の機会となる。

監督者の実査でなされた要求や提言は前向きに、かつ、真剣に受け止める必要がある。保険者が監督者の要請や要求に対して不当な異義を唱えようとした場合、監督者は根底にある企業文化に問題がある兆候として受け止める恐れがあり、その場合、一段と徹底的な監督につながる可能性がある。したがって、保険者は現場視察の間、あらゆる機会を捉えて積極的に率直な姿勢をとって自由に意見交換を行うのがよい。

事故や違反の報告

監督者との関係の実効性に関する重要なテストの一つは、保険者が要件を満たす違反の管理と報告の扱い方である。多くの場合、違反の原因は規則の明確な無視というよりは、不注意による人為的ミスやプロセスの誤りにある。

監督者は違反の報告義務に関する要件を定めているのが普通である。そうした要件では、法令違反事項が監督者に報告されるため、重要性に関する基準が定められる。そのため、保険者は、監督者の法令違反報告要件に基づき、社内報告と重要事項の上申および監督者への報告に関する明確な責任を定めたプロセスを策定することが必要となる。

違反の発見、管理および報告はプロセス改善の機会と捉える必要がある。違反が全く発生しないことも逆にあり得ないだろう。皮肉なことに、長期にわたり監督者に違反の報告が全くなされていない場合、実効性の乏しいリスク管理や企業文化活動の兆候として受け止められる可能性がありうる。

国際的グループの考慮事項

複数の管轄区域で事業を行う保険者は複数の監督者とのリレーションシップマネジメントを行うという点で複雑性が増す。このような状況でも上記の諸原則が同様に適用される。一国・現地レベルと会社全体またはグループレベルでリレーションシップマネジメントに関する明確な責任を定める必要性は一層大きくなる。監督者自身が国境を越えた適切な情報共有に関する手順を定めるであろうこと、したがって、国際的な保険グループに関連してそうした動的な関係を反映した、合意による透明なプロセスを策定するであろうことを保険者は想定しておく必要がある。

ガバナンスの諸側面 - 監督者への対応活動の透明性

取締役会は監督者への対応活動の方針を設定するうえで重要な役割を果たす。取締役会は、保険者と監督者間の重要な対応活動を監視しなければならない。特に、戦略的対応と非標準的対応は取締役会または適切な権限を付与された委員会にとって、透明性の高いものでなければならない。例えば、取締役会または取締役会の下の関係委員会は、戦略的対応と非標準的対応に関する詳細について定期的に報告を受ける必要がある。それによって、取締役会は監督者とのリレーションシップマネジメントに関する期待が継続的に満たされているという保証を得ることができる。

アドバイス：現地国および世界全体で監督者にどのように対応すべきか

KPMG は“Bringing regulation into the boardroom - A global survey of the supervisory function in the communications sector”（規制を取締役会議室に持ち込む - 通信セクターにおける監督機能の世界的調査）（2007 年 12 月）において、「規制がますます重要視される中、企業は伝統的市場において監督者の方針に対して働きかける能力と、それに対応する能力を共に備える必要があり、新興国市場でもその必要性はますます高まっている」と指摘している。

世界中で規制上の要求と監督者の要求がますます強まる状況にあって、保険者は規制を日常業務の一部として組み入れなければならない。規制を企業の「DNA」の一部とする必要がある。しかし、問題は「どのようにすればそれが可能か」ということであり、どのようにすれば監督者に「対処」できるかということである。

アドバイス：

1) 組織のあらゆるレベルで監督の全体的枠組みの原則とその指示・基準を受け入れて理解し、取締役会またはガバナンス委員会がコンプライアンス戦略の実行を推進する。そのためには、監督対応戦略を会社全体の戦略と連携させる必要がある。

2) 透明性の高い包括的な監督対応戦略を導入し、その戦略を監督機関と社内全体に通知する。監督者が組織による監督対応戦略の達成度の証拠を入手できるようにしなければならず、また、組織は、監督対応戦略が監督者によって指示された基準の遵守にどのようにつながるかを立証できなければならない。

3) 監督者が提示した監督上の変更案に関して、具体例に加えて財務や市場への影響を取り入れるなど、実際的なフィードバックを行って自社の見解を裏付ける。また、決定的に重要な問題を中心的に取り上げながら、常に公平な論拠を提示する。監督者の討議資料に含まれるすべての側面にコメントしなければならないというプレッシャーを感じる必要はない。

4) 指示を受ける前にベストプラクティスを採用する。取締役会またはガバナンス委員会と経営陣は、規制が遵守されるようにするために「先取り思考のアプローチ」を採用する必要がある。

5) プロアクティブに行動する。監督の変更を予測し、会社や業界にとって最も有利な状況を生み出すために業界団体と連携して監督者に働きかける。その中には、監督者との協議や監督者の調査に積極的に応じる姿勢を示すことが含まれる。

6) 監督者との率直な定期的コミュニケーションを行う。そのため、監督者の監督担当窓口との間に良好な仕事上の関係を構築することが重要になる。このことはリスク管理関連の問題のみならず、あらゆる種類のコミュニケーションについて言える。

7) 監督者の責任遂行につながる適切な情報をプロアクティブに提供する。その例として、リスク管理における一定の定性分析や定量分析の進捗状況や結果に関する最新情報を常に監督者に提供することなどがある（結果だけを期限日に提供するということがないようにする）。言い換えれば、潜在的な問題や会社が予定する問題点の是正方法について率直に知らせる。しかしながら、監督者は必ずしも関係があるとは言えない膨大な情報の提供を望まないはずであるから、あらかじめ希望を確認しておくことが重要である。

8) 社内における監督者に関する認識を管理する。監督者との関係が対決的、否定的に捉えられている場合、対応活動が行動の正当化に努めるような防衛的な対処になりがちである。そうではなく、監督者を会社のパートナー兼重要な利害関係者として扱い、率直なコミュニケーションによって対処する。

9) 監督者が次の課題が浮上しつつあると認識している事項については、業界への予想される悪影響を最小限にとどめるために、監督者と連携し協力関係を築く。

以上を要約すれば、保険者の ERM の枠組みは、保険者が監督者との関係の効果的な構築を重要な構成要素として組み入れない限り完全なものにはならない。したがって、保険者は、ERM の全体的枠組みの継続的な発展の一部としてそうした側面に注力することが望ましい。

添付資料 1

公表されている ERM の定義

エンタープライズリスクマネジメント（ERM）とは、企業の目的達成に関して合理的な保証を提供することを目的として、企業に影響する可能性のある潜在的事象を識別するため、また、企業がリスク選好の範囲内にとどまるようにリスクを管理するために設計され、当該企業の取締役会、経営陣その他の構成員により遂行され、戦略策定時および企業全体に対して適用されるプロセスをいう。

COSO：Enterprise Risk Management - Integrated Framework Executive Summary（エンタープライズリスクマネジメント - 統合的枠組み、要旨）（2004 年 9 月）

ERM とは、業界を問わず、ある組織が、利害関係者にとっての当該組織の短期的・長期的な価値を増大させる目的で、あらゆる源泉に由来するリスクの評価、統制、活用、資金調達および監視を行うための規律をいう。

米国損保アクチュアリー会 ERM リサーチ委員会：Overview of Enterprise Risk Management（エンタープライズリスクマネジメントの概要）（2002 年）

ここで説明する ERM とは、あらゆる種類の組織におけるあらゆるレベルのあらゆる構成員に適用される全体的な管理プロセスを指す。ERM は一部のセクターで用いられる、より限定的な「リスク管理」とは異なる。例えば、一部の分野では、「リスク管理」あるいは「リスク統制」という用語は識別されたリスクを処理する方法を指すために使用される。これについては、我々は「リスク処理」という用語を用いる。本文書で使用される他の用語も異なる用法で用いられる。例えば、リスク管理に関する文献では「リスク分析」、「リスク査定」、「リスク評価」などの用語がさまざまな使われ方をしている。それらの用語の定義が重なり合ったり、交換可能だったりする場合も少なからずあり、また、時にはリスク識別のステップが含まれていることもある。

ERM とは、企業が価値創出に際して直面する不確実性を評価し管理する目的で、戦略、プロセス、人材、技術、および知財を整合させる、構造化された規律ある取り組みをいう。

KPMG：Enterprise Risk Management - An emerging model for building shareholder value（エンタープライズリスクマネジメント - 株主価値を構築するための新しいモデル）（2001 年 11 月）

ERM とは、組織の資本および収益に対するリスクの影響を最小化するために組織の活動を計画し、組織し、指揮し、統制するプロセスをいう。

KPMG: Viewpoint for Consumer Markets（消費者市場に対する観点）（2005 年 8 月）

ERM とは、当該企業の取締役会、経営陣その他の構成員により遂行され、戦略策定時および企業全体に対して適用されるプロセスとして定義され、企業の目的達成に関して合理的な保証を提供することを目的として、企業に影響する可能性のある潜在的事象を識別し、企業がリスク選好の範囲内にとどまるようにリスクを管理するために設計される。

内部監査人協会：What is ERM and what role in it does internal auditing play? （ERM とは何か、また、内部監査は ERM の中でどのような役割を果たすか）（2004 年 9 月）

添付資料 2

ERM の成熟段階

枠組みの洗練度	この添付資料で用いられる定義
初期的レベル	リスク管理と内部統制の活動は部分的にしか存在せず、その適用は一貫しておらず、経営者および限定された事業分野の関係社員は内容を十分に理解していない。大幅な強化の必要性が存在する。
中間的レベル	リスク管理と内部統制の活動は確立されているが、その適用が一貫していないか、あるいは、経営者および重要な業務・事業分野の関係社員が内容を完全には理解していない。ある程度強化の必要性がある。
先進的レベル	リスク管理と内部統制の活動が確立されており、その適用は一貫しており、経営者および組織全体の関係社員が内容を十分に理解している。組織全体にわたって活動を整合させ、調整するという強化の必要性がある。

	初期的レベル	中間的レベル	先進的レベル
取締役会の役割	取締役会がリスク管理に密接に関与していない。	取締役会がリスク管理の環境と構造の創出に責任を負う。	取締役会の下に専任のリスク管理小委員会が存在し、それらの小委員会の役割と責任は一般に公開されている。
	リスク管理責任に関するステートメント	取締役会がリスク管理方針を承認する。	取締役会が方針をレビューし、ベストプラクティスの目標を設定している。
	リスク許容度が未定義	取締役会がリスク許容度を設定している。	組織のリスク許容度に対する変更には取締役会の事前承認が必要
			取締役会または関係委員会は、リスク管理制度が組織のリスクプロファイルに応じ適切な資源の支援を得るように図っている。
			取締役会と委員会が組織におけるリスク管理の重要性に関し適切な「経営陣からの基本方針」を設定している。

	初期的レベル	中間的レベル	先進的レベル
リスク選好	リスク許容度は企業プランから推測されるが、明瞭な形で適用されていない。	組織がどれだけのリスクを受け入れる用意があるかについて、リスク許容度とリスク限度の両方によって限界が規定されている。	組織の戦略および長期（3 年超）戦略計画を考慮のうえリスク許容度を決定している。
	リスク選好は明確でないが、意思決定プロセスにおいて取締役会および経営陣により理解されている。	リスク選好は取締役会により設定され、組織の大部分に対して十分明確に示されている。しかし、戦略上・業務上の意思決定プロセスに完全には組み込まれていない。	リスク選好は取締役会により設定され、組織の大部分に対して十分明確に示されている。内部の利害関係者に対して効果的に通知され、戦略上・業務上の意思決定プロセスを支える役目を果たしている。
			戦略的意思決定はリスク選好に照らして独立してレビューされる。弱点分野が是正される。
リスク管理方針	正式な方針により内部統制の責任が定められるが、定期的にはなされない。	リスク管理方針にリスク管理の要件の概要が記載されている。 方針は手順、基準およびガイドラインによって支えられている。	ERM プログラムのすべての主要要素がリスク管理方針で取り扱われている。
	内部統制は他のコーポレートガバナンス（戦略など）と正式に関連付けされていない。	リスク管理方針によって組織の目的が直接に支えられ、リスク管理にかかわる役割と責任が特定されている。	戦略目標とリスク管理が明白に整合される。 外部環境の改善に関する補助的活動が行われる。 新規買収はリスク管理方針の下に統合される。
	現地国の法律および監督要件を遵守 方針は必要になった時点で策定	リスク管理がコンプライアンスやオペレーショナルリスクと関連している。 会社全体のリスク担当部門が定期的にリスク管理方針をレビュー	リスク管理が事業目標と連動する。 方針の枠組みが存在し、12 カ月ごとにレビューされる。
経営の説明責任	内部統制のための責任のステートメントは作成されているが、CEO または役員チームの所管になっていない。	経営幹部がリスク管理方針を導入	経営委員会がリスク管理方針を監督
	コンプライアンス活動の事業上の価値が理解されていない。	リスク管理は事業を行うにあたり不可欠なものである。	リスク管理プログラムの結果は測定可能であり、価値創造を行うものである。
	上級職（内部監査人など）がリスク管理に責任を負う。	事業単位は、リスク管理方針に含まれる要件を充足するための適切な構造とプロセスを備えている。	事業単位のリスク担当部門は事業単位の管理者および会社全体のリスク担当部門の双方に対し報告を行う。
	リスク管理にかかわる非正式の手続きが存在する。	各事業単位には実状に合わせたリスク計画・コンプライアンス計画の策定に当たるリスク担当部門がある。	リスク担当部門は自己評価の統制を行い、行動計画を策定する。
経営者のコミットメントとリーダーシップ	リスク管理は専門分野（内部監査など）の責任とみなされている。	あらゆるレベルの管理者が通常のプロセスと手続きにリスク管理方針を使用する責任を負う。	管理者はリスク管理を競争優位性の源泉と捉えており、そのことが社員（の活用）に反映されている。

	初期的レベル	中間的レベル	先進的レベル
	内部統制の責任は通常、職務定義書および人事考課に含まれていない。	リスクの識別と管理は全社員の責任 各社員の役割が正式に規定されている。	プロアクティブなリスク管理行動の支援と促進 社員に対して問題点や事故の報告を奨励している。
企業のリスク担当部門	内部統制は内部監査に任されている。	CRO（最高リスク管理責任者）はリスク管理方針の責任を負う。	全社的なリスク担当部門がリスク管理方針を策定し維持管理している。
	資源は専門のリスク分野に提供されている。	経営幹部は、十分な資源を備え、諸活動を支える事業単位のリスク担当部門の確立に責任を負う。	リスク関連の資源確保の効率性と有効性が定期的にレビューされる。
リスク管理用語	リスク管理用語は共通に使用されていない。	リスク管理用語が共通に理解されている。	一貫したリスク管理用語・用語集、国際的に認められたリスクカテゴリー、格付け、報告などを使用
	定められた定義はリスクの識別と管理にそれほど役立っていない。識別され管理されているリスクの一部は重大なリスクではなく、リスクの原因や結果である。	定められた定義により、重大なリスクの識別と管理が十分に可能である。 かなりのリスクが誤って区分されている。	定義は明瞭かつ簡明で、あらゆるリスクの識別と適切な区分が行われ、そのリスクの効率的な管理が可能になっている。
リスク管理の企業文化	企業計画は価値に言及している。	組織は以下の確実な実施を目指している。 役割の明確化 研修 責任	プロアクティブにリスクを管理する望ましい企業文化を支え、推進するための行動モデルが策定されている。 役員がリスク管理の企業文化を推進し、強化している。 機会リスクの識別、評価、評定、および活用を行うプロセスが存在する。
	行動規範が存在し、新入社員のオリエンテーションの中に研修が含まれている。	役職員がプロアクティブな行動の活用方法を理解するのを支援する研修	毎年、リスク管理の企業文化を計測している。
	社員は内部統制を個人的責任と認識していない。	リスク管理方針が社員と経営者の研修に反映されている。	社員は業務に役立てるためにプロアクティブなリスク管理をすることに責任を負う。
パフォーマンス管理と報賞システム	社員のパフォーマンスについてインセンティブが存在している。	経営者のインセンティブの一部は、プロアクティブにリスク管理する企業文化の推進が目的	毎年、特別賞与制度の一部としてリスク目標が設定される。
自己リスクとソルベンシー評価	反応を基にしたその場かぎりの分析	経済資本モデルにより、主要なリスク要因の評価およびそうしたリスクに取り組むためのリスク管理技法が提供される。	経済資本モデルには将来のバランスシート、損益計算書、予想利益分配のほか資本および資本収益率に関する予測が含まれている。 リスクに応じた事業単位や保険種目への資本の配分がパフォーマンス管理プロセスの基礎を成し、その予測に対する結果やリターンの測定が可能になっている。

	初期的レベル	中間的レベル	先進的レベル
リスク管理プロセス	統制とリスクのつながりが明確でない。	該当するリスクの種類すべてが明確に識別される。	事故またはリスクの問題の報告に関する重大性の限定について、経営幹部が少なくとも年に１回のベースで承認する。
	統制は一般に探偵的な特性を備える。	リスク管理プロセスが適用される。	リスク管理プロセスが適用され、リスク評価にはオペレーショナルリスクの定量化が含まれる。
	リスクに関して取るべき行動を含む正式なリスク管理計画が定期的に策定される。	リスクプロファイルが事業単位レベルと組織レベルで定期的に行われる。	新興リスク（すなわち、不確実性の増大につながり定量化が困難な、発生中の事項）を識別し評価するプロセス。
	財務およびコンプライアンス上の目標がリスク評価プロセスで考慮される。	リスク分析と対応プロセスによって「固有リスク」と「残存リスク」、そして統制の実効性に対する評価と定量化が可能である。	シナリオ分析を遂行することで確率は低いが大きな影響をもたらす事象の評価を行うことができる。
	損失事象が中心的機能（例：内部監査）によってモニターされる。	損失事象とリスクプロファイルへの対応が行われる。	重要なリスク指標（先行指標と遅行指標）やリスクプロファイルを損失事象と統合することが可能となる。
	統制では財務報告とコンプライアンスが重視される。	統制はすべてリスクを基準とし、定期的に検討される。	統制活動はすべてのリスクを対象とし、各事業単位内で行われる。ビジネスプロセスは文書化され、方針と手続きが盛り込まれる。
報告およびモニタリング	統制上の重要な欠点に関する報告が切迫感を伴うことなく特定の当事者（例：内部監査）に伝えられる。	これらの要件に対する違反はすべて全社的なリスク担当部門に報告される。	統制リスクの自己評価を通じて、経営幹部、監査委員会、取締役会に保証が与えられる。 統制リスクの自己評価に対する回答が内部監査チームによって検討され、検討結果が取締役会に報告される。
	取得された情報によってライン管理者がリスクを効率的に識別し対処できる場合がある。	内部リスク報告にはリスク管理方針の主要な側面が網羅される。 事業単位が策定したリスクおよびコンプライアンス計画によって外部報告の要件、タイミング、義務が特定される。	全社的なリスク担当部門が以下を執り行う。 会社レベルでのリスク関連データの本部での回収、照合、分析 報告の共通基準、ツールおよびリスク管理情報システムの策定 リスク管理報告書の作成
	中間管理者の行動や組織の活動に対する監督またはモニタリング。	事業単位は統制活動のモニタリングに対する責任を負う。	重要リスクの一致指標が組織全体に適用され、集約が可能になる。

	初期的レベル	中間的レベル	先進的レベル
	社員は不適切な行動に関わる問題を経営陣に提起することが奨励される。	不適切な行動を指摘するための正式な内部チャネルが存在する。	不適切な行動を指摘するための独立した正式なチャネルが存在し、使用される。
	内部監査が統制の実効性の検討に不可欠な役割を果たす。	経営陣はリスク管理システムの定期的な検討の全体的責任を負う。	リスク管理が経営陣と社員によって継続的にモニターされ、評価される。
内部監査	内部監査では役員または監査委員会へのアクセスが制限される。	リスク管理の効果的な実行と遵守が内部監査機能と当該組織の外部監査人によってモニターされる。	内部監査機能と全社的なリスク担当部門がリスク管理方針の年次監査を行う。
新規活動	主要プロジェクトに対してはリスクを考慮した費用対効果分析が行われる。	主要プロジェクトにはリスクと統制が存在する。	新規のプログラム、プロジェクト、進行中のタスク変更、戦略的な進展（例：買収）に対するリスク、統制および保証。
継続性分析	情報システムアプリケーションには災害復旧計画が盛り込まれている。	適切に文書化され検証されたビジネス継続性計画。	保険者が 1 年以上事業を継続する能力に関わるリスクおよび財務状況の評価。
			重大な事故発生時に事業への影響と損失を最小限に食い止めるための危機管理計画。

添付資料 3

ERM 導入の事例研究

ERM の導入－資本モデルの組み入れ

某大手保険者は組織全体にわたり ERM 戦略の導入を目指していたが、戦略に欠くことのできない側面となっていたのが資本モデルの構築であった。保険会社が資本モデルを構築するにあたっては幾つかの促進要因があった。その時点で監督者や格付機関は、資本モデルを ERM の枠組みに組み入れることが経営の良好な保険会社にとって極めて重要であると考えるようになっていた。資本モデルは必要資本要件の低減につながるだけでなく、社員が事業におけるリスクに対する理解を深め、リスクをより効率的に管理する上でのツールを提供する。

プロジェクトの開始に先立ち、保険者は資本モデル策定について企業内のサポートを得ることが重要であると認識していた。企業全体にとって有用な資本モデルを策定するには組織全体からのインプットが必要となるため、おそらくこれは最も重要なステップであろう。このため、欧州資本モデル策定プロジェクトの代表責任者にはチーフアクチュアリー（役員会のメンバー）が、グループの資本モデル策定の代表責任者にはグループの最高経営責任者が就任した。このように地位の高い人物がプロジェクトの代表責任者となったことで ERM 戦略を実行する上で明確なビジョンがもたらされた。また、これによってプロジェクトへの参加に対する企業意欲が高まり、プロジェクト期間を通じてプロジェクトチームが障害を乗り越えることが可能になった。

次に、モデル策定の進捗状況をモニターするために運営委員会が設置された。委員会は重要な問題の解決に役立つ様々なビジネススキルを持つメンバーでうまく構成されていた。例えば、欧州資本モデル運営委員会は以下のメンバーで構成された。

- チーフアクチュアリー（委員長）
- 最高経営責任者
- 最高財務責任者
- 最高保険引受責任者
- オペレーション・ディレクター2 名
- 上級アンダーライター2 名

練り上げられたプロジェクトの計画と共にそのプロジェクトに理解のある人を活用することで、進捗状況の効率的なトラッキングと運営委員会への時宜を得た包括的な報告が確保された。

導入段階では、重要な社内利害関係者への対応が運営委員会を通じて行われ、可能な限り広範な周知を図るために協調的な努力が払われた。社外利害関係者も早期段階で関与するところとなった。保険者は、プロジェクトの最終段階で、報告書を検討するために必要な資源を持ち合わせていない社外利害関係者に対して大量の報告書を手渡すよりも、資本モデル策定の過程で彼らを取り込む方が遥かに簡単だということを理解していた。欧州モデルに関して、保険者は英国の２つの監督機関（ロイズ・オブ・ロンドンおよび金融庁）と何度も会合を重ねた。会合は、全般的なアプローチは健全であるというコンセンサスが得られたという点で有益であった。資本モデル策定チームは策定段階で企業内の保険引受チームの大半と 1 時間にわたる会議を開いた。

広い意味での ERM 導入の一環として、以下を含む重要なリスクをすべて資本モデルに組み込むことが求められた。

- 保険引受リスク ー 社員は現在保険を引き受けている事業が直面しているリスクに精通しており、保険引受人は保険を引き受けようとしている事業を取り巻く不確実性を考慮することに詳しいということが分かった。
- 信用リスク ー 信用リスクの最も一般的な源泉は外部の再保険会社だった。再保険会社が一般に巨額の債務を計上しているためである。保険者は自社のバランスシートに計上されている各再保険会社の信用力を考慮することにより再保険の信用状況を組み入れた。
- 資産（市場）リスク ー 過大な投資リスクを避けるため、保険者は優良社債に投資していた。しかし、優良社債はたとえ安全であっても、時価が市場のイールドカーブに左右されるため、社債の時価は確率論に基づいてモデル化された。
- 流動性リスク ー 流動性リスクは損害保険会社にとってどちらかといえば重要ではないリスクだが、自然災害が起こった場合には流動性に危機が生じる可能性がある。流動性の問題に対処するため、資本モデルでは短期キャッシュフローが考慮の対象となった。
- オペレーショナルリスクー資本モデルではオペレーショナルリスク評価として、リスクレジスターとともに厳密なオペレーショナルリスク・シナリオ分析が盛り込まれた。

資本モデルの各部の評価が終わると、当該分野の専門家による検討が行われた。

- アンダーライターおよび保険引受リスクを算定するアクチュアリー（保険引受リスク）
- 再保険部門および証券委員会（信用リスク）
- 投資部門（市場リスク）
- リスク管理部門（オペレーショナルリスクおよびグループリスク）
- 経営陣および取締役会（資本モデル全体の妥当性）

広い意味での ERM 戦略の一環としての資本モデルが包括的であったため、ERM 導入プロセスでは当保険会社の取締役会の間で高い信頼性が得られた。しかし、組織全体レベルでのリスク管理を一段と重視し、実際の問題に効果的に対応するため、ERM 戦略の継続的な検討が必要であることも認識された。

ERM の導入 ー 教訓的な事例

某大手保険者は組織全体にわたる ERM プロセスの設計および導入プロジェクトに着手した。内部監査部はリスク識別の責任部門であるとみなされていたため、プロジェクトの管理と責任が同部門に割り当てられた。内部監査部門はすぐさま各事業単位のリスクの識別とリスクプロファイルの草案の作成に乗り出した。しかし、このリスクプロファイルは、内部監査部が理解しモニターする分野のみを対象としていたため限定的なものだった。このリスクプロファイルは事業の実情を反映したものとして経営幹部に承認されなかったばかりか、幾つかの「重要なリスク」が完全に欠落していた。こうした中断の結果、ERM 導入プロセスは大幅にスローダウンした。

ERM 導入で経験した問題を受けて、取締役会は ERM プロジェクトの責任を各事業単位に割り当て直すことにした。各事業単位はプロジェクトに対する適切な判断力を持ったメンバーから成る

プロジェクトチームを共同で立ち上げた。しかし、各メンバーは引き続き日常の職務を担当していたためプロジェクトの専任者とはならなかったことから、プロジェクトに再び遅れが生じた。

各事業で新たなリスク管理のリーダーが特定された。彼らはリスク関連の作業に関わっておらず、既に専任の仕事を抱えたマネジャーであった。予算と時間の制約からこれらの新たなリーダーに対する訓練はなされなかった。彼らは有能なマネジャーですぐに作業に取り掛かることができるとみなされた。その頃までには取締役会は ERM の導入が保険業界の「リーディング・プラクティス」であると結論づけていた。このため、プロジェクトチームと新たなリスク管理のリーダーに対するプレッシャーが高まった。彼らは成功のために一段と高い基準の達成に向けて懸命に努力したが、ERM の導入は数カ月後に完了した。

プロジェクトおよび ERM の枠組みの有効性に関する見解を評価するため、ビジネスマネージャーに対する導入後の調査が行われた。フィードバックは極めて批判的であった。ERM のプロセスはある事業分野では「過度に設計されて」おり、他の事業分野では不完全だとみなされた。また、事業単位のリスクチームまたはリスク管理のリーダーに対する訓練やサポートが十分でなく、グループの体制を構築する前にリスク管理ツールのソリューションが決定されたとの指摘もあった。さらに、詳細な導入計画が策定されていれば実行に役立ったであろうとの意見もあった。これによってフラストレーションが引き起こされ、実際、リスク認識の後退につながった。目標が何であるか、望ましいインプットとは何か、どのようなアウトプットとメリットがもたらされたかを把握することは困難であることが分かった。プロセスは非常に使い勝手の悪いものとなった。

その後、取締役会は既存の ERM を「簡素化する」ための新たなプロジェクトに乗り出し、将来的に問題を回避するため以下の教訓を指摘した。

- 取締役会および経営陣が ERM プロセスを「引き受ける」こと、すなわち、明確なビジョンを持って達成可能な結果に同意することがスタートの時点から必要である。
- ERM の設計および導入の計画責任者は組織内の一部門であってはならず、常にスタートの時点から組織全体にわたる責任を含めなければならない。
- プロジェクトの計画、プロジェクトの規律、専任の人材を活用する。日常業務の他に、残業をしてプロジェクトを策定するよう要請してはならない。
- 実行に先立って、組織の下位レベルでのリスク管理のリーダーを関与させることが極めて重要であり、関連する訓練を必ず受けさせるようにする。
- グループ体制の実行のための時間と人材を過小評価してはならない。
- 新技術の導入は一般に予想よりも困難であるため、ベストシナリオではなくワーストシナリオに備える。
- ERM の導入には時間のかかる企業文化の変化を伴うため、これらの予想をプロジェクト計画の中に組み込む。
- プロセスの設計が過剰であってはならない。簡単かつシンプルにする。

ERM の導入：成功が定義できたら ERM は成功だ

世界的な某大手保険者が ERM 導入プログラムに着手した。同社は一般的な基準、指針、専門資料を使って、監督者、投資家、顧客、保険契約者、経営陣のニーズをすべて一つのプログラムで満たすべく、全体的で戦略的、そして統合的なリスク管理の策定に乗り出した。

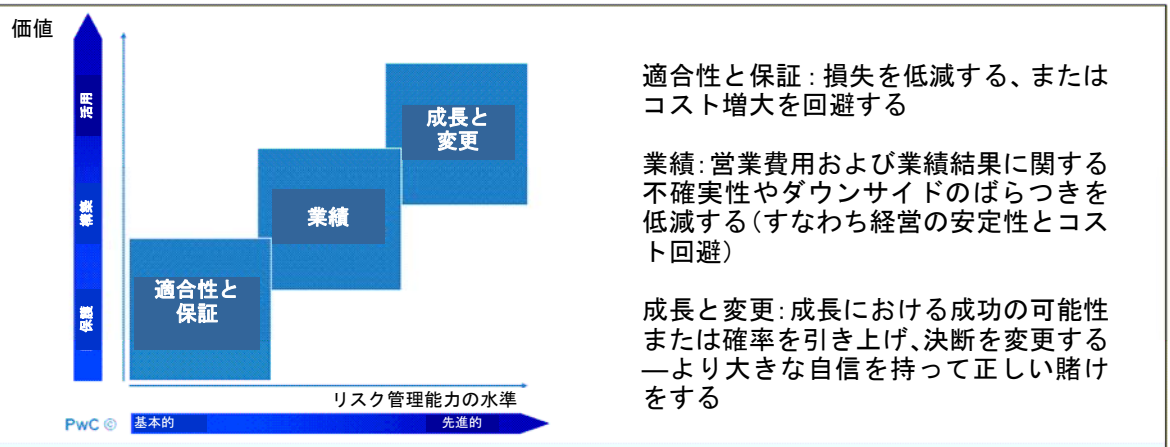
その ERM プログラムではプロジェクト活動、プロジェクトのマイルストーンの達成、セミナーの数、アウトプットの報告の頻度と量、ツールや技術の高度化という視点から見た成功の尺度、多くのプロセスまたは活動という点から見た成功の尺度が定義されていた。しかし、結果は不成功に終わり、大半の仕事が後退し投資評価損が計上されたばかりでなく、リスク管理部門のスタッフの多くは仕事を失うところとなった。

では、何がうまくいかなかったのだろうか。基本的に ERM プログラムは事業の目標や結果に対して明確な影響を与えなかったのである。すなわち、

- 組織のリスクプロファイルやリスク管理能力は大きく変化しなかった。
- 事業の目標や結果に沿い、十分な関わりを持った、ERM の事業の明確な結果がなかった。
- マネジメントに投入されたコスト、仕事量、時間は増大したが、他のマネジメントの慣行や能力を通じて既に得られていた事業に対する洞察よりも優れた洞察は得られなかった。
- 既存の分析、プロセス、報告が重複し、わずかな経済効果しか得られなかった。

では、どのようにすべきだったのだろうか。ERM にとっての成功とは、ビジネスの成果と事業に対する価値の寄与という観点から判断される必要がある。

1. ERM 活動の範囲と重点を非常に明確にする。例えば、下の図には ERM が影響を与えるべき分野に関する見解が示してある。



ERM の実行にとって事業の第 1 の重点はどの分野にあるのか。

2. ERM の成功および ERM が事業に与える影響に対する定性的、定量的、経済的な尺度が必要である。

3. 利害関係者は成功の尺度について同意・支援しなければならず、ERM の代表責任者は成功に導く責任がある。
4. ERM への投資が事業の結果にとって引き続き重要であることを保証するため、現状の継続的な評価と挑戦が必要である。

添付資料 4

リスク委員会規約例

リスク委員会規約には何を盛り込むべきか。

- リスク委員会の目的。例：重要なリスクおよびそれに関連するリスク管理活動に関して、監督の集中化、方針の設定、情報収集、経営陣や取締役会とのコミュニケーションを実行する
- リスク委員会の責任の概要。例：企業の戦略目標や経営目標の達成に対する重要な既存のリスクと新たに発生するリスクを識別・モニターし、適正な方針、モニタリングおよび報告体制を策定する
- 委員または委員会構成についての最低限の前提条件。例：経営陣による指名、委員会のメンバーの 3 分の 1 は外部者とする
- リスク委員会の会議開催頻度。例：取締役会議の 1 か月前に開催
- リスク委員会の年次評価に使われる重要業績評価指標（KPI）の概要：リスク委員会が 1 年間に検討した方針の数、1 年間に取締役会に提言して採用された方針の数、1 年間に開催された会議の数、取締役会に承認され実行に成功した方針の数
- リスク委員会が直接アクセスしオープンなコミュニケーションを図る人材の概要。例：経営陣、内部監査担当者、内部法務担当者、財務担当者、および組織内外の他のアドバイザー

規約例

1. 目的

リスク委員会の主要な目的は、重要なリスクおよびそれに関連するリスク管理活動に関して、監督の集中化、方針の設定、情報収集、経営陣や取締役会とのコミュニケーションを実行することである。これに加えて、当委員会は取締役会が当社のリスク評価およびリスク管理プロセスに関わる監督責任を果たすことを支援するものとする。

2. 責任

- *リスク委員会は以下の活動に対する責任を負うものとする。*
- *当社の戦略目標および運営目標の達成に対する重要な既存のリスクと新たな発生するリスクを識別しモニターする。*
- *重要なリスクに対する効果的な管理を支援するため、適切な方針、モニタリングおよび報告体制を策定する。*

- *係るリスクに対応するための管理プロセスおよび行動計画の有効性を検討・評価する。*
- *当委員会がリスクの効果的な管理に必要とみなす重要な行動や構想を経営陣に助言・提言する。*
- *社内の個々のリスク管理規律を適切に調整しながら実施する。*
- *当社の重要なリスクおよび関連するリスク管理プロセスの現状を取締役会に報告する。*

3. 委員および会議

最高経営責任者および取締役会は、取締役会の代表者からなるリスク委員会を設置することをここに決定する。リスク委員会は取締役会および最高経営責任者によって指名された委員長を有する。委員長は委員会活動の統率と委員会の議題決定の責任を負う。

リスク委員会は隔月ごとまたは四半期ごとに会議を開くほか、必要に応じて会議を開く。

業績および規約

リスク委員会は年に 1 回、重要業績評価指標（KPI）に対する自己評価、委員会の委員の検討および委員の変更に関わる提言を行うものとする。
さらに、委員会は毎年規約を見直し、修正の推奨を行う。

人材および委員会の権限

当委員会は意思決定とモニタリングを支援するため、経営陣とのオープンなコミュニケーション、内部監査・内部法務・財務部門、他のアドバイザーからの連絡や支援に対して直接アクセスできるものとする。また、必要に応じて外部のアドバイザーにもアクセスできるものとする。

委員会のパフォーマンス評価のための重要業績評価指標（KPI）

例：
- *委員会が 1 年間に承認した方針の数*
- *委員会が 1 年間に検討した方針の数*
- *委員会の 1 年間に開催した会議の数*
- *各委員会の平均出席者数*

添付資料 5

最高リスク管理責任者—主要な役割と責任

最高リスク管理責任者

最高リスク管理責任者（CRO）は組織全体を通じて市場リスク、資産・負債管理リスク、信用リスク、投資リスク、オペレーショナルリスクおよび監督リスク、保険数理上の問題を監視し、リスク委員会およびその小委員会に役務を提供する。

組織の運営方針に従って、最高リスク管理責任者は以下の役割を果たす。

- 指針を示し、組織全体にわたるリスク管理活動の実施のための最低基準を設定する
- 組織全体にわたるリスク管理活動を監督し、リスクの集計データのモニタリングを含め最低基準が確実に守られているようにする
- リスク委員会を統率し、規約遵守を確保する
- 組織全体にわたるリスク管理活動に関与する組織の専門家チームを機能的に統率し、リスク管理の専門要員が組織全体にわたり高い基準で活動するようにする
- 先進的な実施技法の動向をモニターし、ERM プログラムの継続的な発展を確保する
- 調査力を高め、組織が自己の利益のために最新の進展を常に把握し、係る進展を活用するようにする
- リスク管理措置の実効性と効率性に関する独自の見解を確保する
- 格付機関と連絡を取り合い、関係する情報を必要に応じて提供する
- 組織によって必要とみなされた、もしくは自己の役割と矛盾しない各事業単位の要請に応じて、追加的な役務を提供する
- 最高リスク管理責任者は適宜、主要なリスク分野に関わる決定に対して問題提起を行い、各事業単位で解決できない問題をその事業単位の経営責任者または最高経営責任者に上申する。非常に希なケースとして、重要な事業リスク事項がその事業単位の経営責任者の下で解決できない場合には、最高経営責任者に上申する。

これに加えて、その事業単位の経営責任者または最高経営責任者は組織の方針を含む、もしくは付託権限内の事項に関わる、すべての問題に関して最高リスク管理責任者との適切な協議が行われるようにする。

次の事例では、職務説明書に記載され得る責任の内容を示す。

事例：
一般的な職務説明

報告先：保険会社グループ最高経営責任者
主要な役割と責任
最高リスク管理責任者は、グループのリスク管理、内部監査、衛生、安全、福利厚生、環境に対するライン管理責任を含む、グループ全体にわたるリスク管理の適用に関わる統率、指示、調整の責任を負い、リスク管理の原則と要件がグループ全体を通じ一貫して採用されるようにし、グループの事業目的の実現と継続的な発展を支援するためリスク管理体制を構築し適切な人材を育成する。

主要な責任：

方針と戦略

a) *グループ全体のリスク管理戦略を策定・監督し、すべてのリスク管理とそれに関連する内部統制活動を整合させることによって保険会社グループの株主価値の実現を支援する。*

b) *保険会社グループのリスク管理方針を提示して検討させ、保険会社グループのリスク管理委員会または取締役会の承認を仰ぐ。*

c) *グループ全体にわたるリスク管理の継続的な進展に関する経営陣の見解を詳しく調査し、保険会社グループのリスク管理戦略を支援するための組織体制が常に適切であるかどうかを検討する。*

d) *保険会社グループと直接子会社にとって重要な意味を持つ可能性のある、リスク管理のトレンドや進展を継続的に把握する。*

e) *グループのすべての保険契約、ブローカー契約、引受者契約の獲得を監督し、必要に応じて保険会社グループ全体にわたるリスク管理のベストプラクティスの実現を支援する専門アドバイザーを認定する。*

f) *投資決定におけるリスク管理の検討を含め、保険会社グループのすべての事業戦略と活動に、リスク管理の方針と戦略を組み込むことを支援する。*

g) *会長および最高経営責任者と連携して、リスクと内部統制に関わる適正な情報が株主を含む投資市場に提供されるようにする。*

h) *既存の規制、新たな規制、将来の規制に関して監督者と連絡を取り合う。これには、枠組みや原則に関わるフィードバックの監督者への提供、ならびに監督者の質問や要請への対応に対する関与が含まれる。*

リスクの識別と評価

a) *保険会社グループのリスクへのエクスポージャーの総合的なレベルをモニターし、保険会社グループのリスク管理委員会に報告する。*

b) *独立性を維持し、保険会社グループのリスクと保証を担当する部門管理者を通じて、リスクと保証に関する個々の課題に挑む。*

c) *保険会社グループと直接子会社全体にわたって行われるリスクの識別と評価作業の検討、必要に応じた問題提起、最上層への上申手続きの適切な整備が確実に行われるようにする。*

管理と報告体制

a) *グループのリスクマネジメント（(団体保険を含む）内部監査、衛生、安全、福利厚生、環境（企業の社会的責任を含む)）の管理と調整の責任を負う。*

b) *保険会社グループと直接子会社全体にわたり、グループのリスクに見合ったリスクの適切な管理と報告体制が整備されているようにする。*

c) *保険会社グループのリスク管理パフォーマンス年次報告書を INSURER の最高経営責任者に提出する。*

報告と利害関係者への取り組み

a) *グループレベルでの全体的なリスク管理パフォーマンスをモニターし、グループの直接子会社内とグループレベルでリスク管理情報の効果的かつ時宜を得た報告が行われるようにする。*

b) *保険会社グループのリスク管理委員会に出席し、委員会が保険会社グループ全体にわたるリスク管理のベストプラクティスの策定に携わるようにする。*

c) *戦略的リスク検討の要旨報告書を提示して議論や問題提起を行い、主要なリスクとそれに関わる内部統制手続きを保険会社グループのリスク管理委員会に報告する。*

d) *社内外のフォーラムで保険会社グループのリスク管理の状況、戦略、経験を発表し、グループに対する高い評価を維持する。*

e) *保険会社グループの利害関係者と適切な関与プロセスを策定・維持し、INSURER グループの直接子会社で一貫した同等なリスク管理プロセスが実行されるようにする。*

f) *ストラテジー&コミュニケーションズや適宜他の部署と連携して、特に「社会的に責任ある投資」に関連したリスク管理パフォーマンスに関して、投資業界や信用格付機関に助言を行う。*

ラインの支援と知識の共有

a) *外部の指標やベンチマークを適宜参照して、グループ全体にわたりリスク管理の知識とベストプラクティスの共有を促す。*

b) *保険会社グループのリスク管理コーディネーター・フォーラムで議長を務め、専門知識と支援を提供し、保険会社グループのリスク管理委員会で取り上げられたリスクとそれに関連する内部統制手続きについて伝えると共に、フォーラムとリスク管理委員会との情報の橋渡し役を務める。*

c) *リスク管理の進展のあらゆる面で経営陣をサポートし、主要な経営陣に対する研修を含む主要なリスク管理研修への取り組みを監督し、リスク管理を社員への導入プログラムに組み込む。*

添付資料 6

典型的なリスク管理方針の記載事項と構成

1　前文

1.1　リスクと全社的管理の定義

1.2　エンタープライズリスクマネジメント（ERM）の目的

2　リスク管理方針

2.1　リスク管理方針の目的

2.2　リスクの種類と定義

保険者のためのリスク例：

- *オペレーショナルリスク*
- *企業および戦略に関わるリスク*
- *保険引受および価格設定に関わるリスク*
- *準備金積立に関わるリスク*
- *流動性リスク*
- *信用リスク*
- *市場リスク*
- *法務およびコンプライアンスに関わるリスク*
- *財務リスク*

2.3　ERM の潜在的な利点

2.4　成功の基準

3　リスク管理体制

（組織図と各役職の役割の詳細を含む）

3.1　リスク管理の組織構造

3.1.1　リスク委員会の役割
例：監督の集中化、方針の設定、情報収集、経営幹部ならびに取締役会とのコミュニケーション

3.1.2　CEO の役割

3.1.3　CRO の役割

3.1.4　経営幹部の役割

3.1.5　リスク代表責任者の役割
例：企業の主要な各事業単位を代表し、部門を支援する。委員会の目標が実行されるように所与のリスクがリスク代表責任者に「割り当てられる」

3.1.6　リスク責任者の役割
例：特定のリスクを管理する責任を負う

3.1.7　リスク管理者の役割

3.1.8　モニタリング担当者の役割

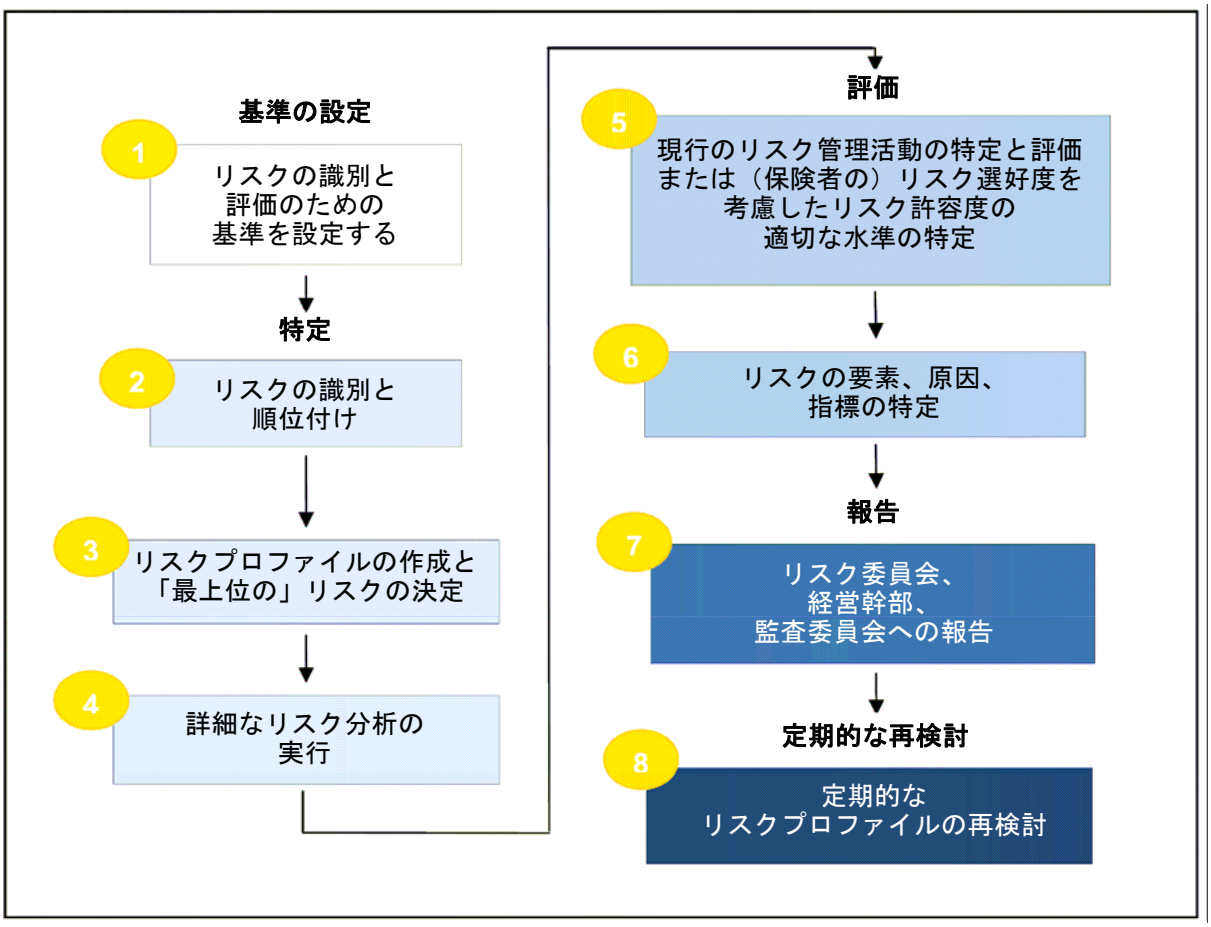
例：企業のリスク統制のプロセスがリスク責任者とリスク委員会レベル、およびリスク統制を担当する部門（例：内部監査、コンプライアンス、法務）によってモニターされる

4　リスクの識別と評価プロセス

（企業によるリスクの識別と評価のプロセスを定義する）

4.1　リスク評価プロセスの概要

全体的なリスク評価プロセスを以下の表に示し、各ステップの詳細を説明する。



4.2　ステップ 1—基準の設定

4.2.1　リスクの順位付けの基準

4.2.2　現行のリスク管理活動の有効性スコア

4.2.3　リスク選好度

4.2.4　リスク許容度

例：

報告先	報告の頻度	報告の書式
リスク委員会	*四半期ごと*	
経営幹部	*四半期ごと*	
監査委員会	*最上位のリスクは四半期ごと*	

添付資料

添付資料 L：　リスク内容報告書

用語集

例：

- リスク委員会：リスク評価、リスク管理、偶発債務、重大な意味を持つ可能性のあるリスクに関する企業の方針を検討する
- エンタープライズリスクマネジメント（ERM）：企業が価値を創出する時に直面するリスクの管理・評価を目的として、戦略、プロセス、人材、技術、知財を整合させた、構造的で規律ある取り組み
- モニタリング：企業のリスク統制のプロセスがリスク責任者とリスク委員会レベル、およびリスク統制部門によってモニターされる
- リスク：発生した場合には企業の価値に悪影響を及ぼす可能性のある事象、行動、機会喪失の恐れ
- リスク選好度：企業が目標達成のために受容する意思のあるリスクの全体的な水準を表すのに使用される表現
- リスク委員会：監督の集中化、方針の設定、情報収集、経営幹部と取締役会とのコミュニケーションを実行する
- リスク責任者：特定のリスクを管理する責任を負う個人
- リスク代表責任者：企業の主要な各事業単位を代表し、部門を支援する。委員会の目標が実行されるように所与のリスクがリスク代表責任者に「割り当てられる」
- リスク許容度：企業の重要な各リスクに関して受容する意思のあるリスク水準を定量的に定義したもの

添付資料 7

新興リスクに関するリンク集

CRO Forum home page: http://www.croforum.org/

CRO Forum Emerging Risks Initiative page: http://www.croforum.org/emergingrisc.ecp

CRO Forum Emerging Risks Initiative - “Position paper - Climate change & tropical cyclones”: http://www.croforum.org/emergingrisc.ecp

CRO Forum Emerging Risks Initiative “Position paper - Pandemic”: http://www.croforum.org/publications/20080201_1_resource/File.ecr?fd=true&dn=cro_pandemie_final

CRO Forum Emerging Risks Initiative “Position paper - Terrorism”: http://www.croforum.org/publications/20072711_resource/File.ecr?fd=true&dn=terrorismpositionpaper_nov07

Swiss Re emerging risk initiate: http://www.swissre.com/pws/media%20centre/online%20magazine/market%20trends/the%20cro%20emerging%20risk%20initiative.html

Ernst & Young report - “Strategic Business Risk 2008 - the Top 10 Risks for Business with Oceania Perspectives”: http://www.ey.com/Global/assets.nsf/Australia/AABS_Strategic_Business_Risk/$file/SBR.pdf

Ernst & Young report - “Property/Casualty Insurance Industry 2007 Outlook”: http://www.ey.com/Global/assets.nsf/International/Industry_Insurance_US_Property_Casualty_Insurance_Industry_Outlook_2007/$file/EY_USProperty_Casualty_Insurance2007Outlook.pdf

Ernst & Young report - “Strategic Business Risk - Insurance 2008”: http://www.ey.com/Global/assets.nsf/International/Industry_Insurance_StrategicBusinessRisk_2008/$file/Industry_Insurance_StrategicBusinessRisk_2008.pdf

World Economic Forum report “Global Risks 2008 - A Global Risk Network Report”: http://www.weforum.org/pdf/globalrisk/report2008.pdf

OECD Report - “Emerging Risks in the 21st Century - An OECD International Futures Project”: http://www.oecd.org/dataoecd/23/56/19134071.pdf

Economist Intelligence Unit Report – “Risk 2018. Planning for an unpredictable decade”: http://www.btglobalservices.com/business/global/en/docs/other/risk_2018_planning_for_an_unpredictable_decade.pdf

Deloitte report – “2008 Industry Outlook. Insurance overview. A look around the corner”: http://www.deloitte.com/dtt/cda/doc/content/us_2008CrossIndustryOutlook_insurance.pdf

添付資料 8

参考資料

Note: All websites accessed on 1 July 2008.

Acharyya, M. 2007. *Proposing a conceptual framework to measure the performance of Enterprise Risk Management from an empirical study of four major European insurers.*
http://www.egrie2007.de/EGRIE%20Papers/EGRIE_2007_Acharyya.pdf

A.M. Best. 2006. *A.M. Best Comments on Enterprise Risk Management and Capital Models.*
http://www.ambest.com/ratings/methodology/enterpriserisk.pdf

American Academy of Actuaries. 2001. *Risk Management in the Insurance Industry.*
http://www.actuary.org/pdf/finreport/risk_09dec01.pdf

Bennet C.; Cusick, K. (Trowbridge Deloitte Limited) 2007. *Risk Appetite: Practical Issues for the Global Financial Services Industry.*
http://www.actuaries.asn.au/IAA/upload/public/4.a_Conv07_Paper_Bennet%20Cusick_Risk%20Appetite.pdf

Bohn, C.; Kemp, B. 2006. *Enterprise Risk Management Quantification – An Opportunity.*
http://www.soa.org/library/monographs/other-monographs/2006/july/Bohn-abstract.pdf

Casualty Actuarial Society. May 2003. *Overview of Enterprise Risk Management.*
http://www.ucop.edu/riskmgt/erm/documents/overview.pdf

Committee of Sponsoring Organizations of the Treadway Commission. 2004
Enterprise Risk Management – Integrated Framework: Executive Summary.
http://www.coso.org/publications/ERM/COSO_ERM_ExecutiveSummary.pdf

Continuity Central. 2007. *Emerging Governance Practices in Enterprise Risk Management.*
http://www.continuitycentral.com/feature0439.htm

D' Arcy, S. 2006. *Enterprise Risk Management in the Insurance Industry.*
http://www.business.uiuc.edu/~s-darcy/present/ERM%20Symposium%20-%202006%20-%20Workshop% 202%20(D'Arcy%203-31-06)%20with%20Template.ppt#258,2,Overview

Deloitte. 2006. *The Risk Intelligent Enterprise: ERM Done Right.*
http://www.deloitte.com/dtt/cda/doc/content/us_risk_RIPOV.pdf

Ernst & Young. 2006. *Insurance Risk Leadership Roundtable: Setting Risk Appetite, Tolerance and Limits.*
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Insurance_Risk_Leadership_Roundtable_Corporate_Risk/$file/AABS_RAS_Insurance_Risk_Leadership_Roundtable_Corporate Risk.pdf

Ernst & Young. 2006. *Insurance Risk Leadership Roundtable: Preparing for the new ERM Environment.*
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Insurance_Risk_Leadership_Roundtable/$file/AABS_RAS_Insurance_Risk_Leadership_Roundtable.pdf

Ernst & Young. 2005. *Managing Risk across the Enterprise: Connecting New Challenges With Opportunities.*
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Managing_Risk_Across_Enterprise/$file/AABS_RAS_Managing_Risk_Across_Enterprise.pdf

Ernst & Young. 2006. *Managing Risk Across the Enterprise: The Value of Enterprise Risk Management* .
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Value_ERM/$file/RAS_Value_ERM.pdf

Ernst & Young. 2007. *Managing Risk Across the Enterprise: Building a Comprehensive Approach to Risk.*
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Manag_Risk_Enterprise/$file/AABS_RAS_Manag_Risk_Enterprise.pdf

Financial Services Authority. 2006. *Insurance Sector Briefing: Risk Management in Insurers.*
http://www.fsa.gov.uk/pubs/other/isb_risk.pdf

Financial Services Authority (McDonnell, William). 2002. *Managing Risk: Practical Lessons from Recent "Failures" of EU insurers.*
http://www.fsa.gov.uk/pubs/occpapers/OP20.pdf

Gates, Stephen. 2006. *Incorporating Strategic Risk into Enterprise Risk Management XVème Conférence Internationale de Management Stratégique, Annecy / Genève 2006.*
http://www.strategie-aims.com/aims06/www.irege.univ-savoie.fr/aims/Programme/pdf/SP26%20GATES .pdf

Hoyt, R.E; Liebenberg, A.P. 2008. *The Value of Enterprise Risk Management: Evidence from the U.S. Insurance Industry.* http://www.ermsymposium.org/pdf/papers/Hoyt.pdf
Ingram, D. 2003. Life Insurance Industry Risk Management.
http://www.iafe.org/upload/Ingram_Talk.pdf

Institute of Internal Auditors. 2004. *The Role of Internal Audit in Enterprise-wide Risk Management.* http://www.ucop.edu/riskmgt/erm/documents/erm1.pdf

International Association of Insurance Supervisors. 2007. *Guidance Paper On Enterprise Risk Management For Capital Adequacy And Solvency Purposes.* http://www.iaisweb.org/__temp/2_2_6_Guidance_paper_on_enterprise_risk_management_for_capital_adequacy_and_solvency_purposes.pdf

International Association of Insurance Supervisors.2007. *Guidance Paper On The Use Of Internal Models For Risk And Capital Management Purposes By Insurers.* http://www.iaisweb.org/__temp/15__Guidance_paper_No__2_2_6_on_the_use_of_internal_models_for_risk_and_capital_management_by_insurers.pdf

International Electrotechnical Commission (IEC). *Draft IEC 31010 Risk Management - Risk Assessment Techniques.* http://www.rmia.org.au/LinkClick.aspx?fileticket=uXc91tcaLVU%3d&tabid=85&mid=634

International Organisation for Standardization (ISO). 2008. *Draft International Standard ISO/DIS 31000: Risk management - Principles and guidelines on implementation.* http://rmia.org.au/LinkClick.aspx?fileticket=AWkZuS%2bB6Wc%3d&tabid=85&mid=634

KPMG. 2001. *Enterprise Risk Management: An Emerging Model for Building Shareholder Value.* http://www.kpmg.com.au/aci/docs/ent-risk-mgt.pdf

KPMG. 2006. Risk and Capital Management for Insurers. http://www.kpmg.cz/czech/images/but/Risk_Capital_Management_for_Insurers_2006.pdf

Lam, J. 2000. *Enterprise-wide risk management and the role of the chief risk officer.* http://www.erisk.com/Learning/Research/011_lamriskoff.pdf

Matthews, A.; Wang, S.; Cassidy, P.; Faber, R.; Newton, T. 2007. *Enterprise Risk Management and Exploring Best Practice in Commercial Insurance Pricing and Underwriting.* http://www.actuaries.asn.au/IAA/upload/public/2.c_Conv07_Paper_Matthews_putting%20enterprise%20risk%20mgt%20into%20best%20practice.pdf

McConnell, Patrick. 2004. *A 'Standards Based' approach to Operational Risk Management under Basel II.* http://www.m-bryonic.co.uk/library/ORStandards.pdf

PWC. 2004. *Enterprise-wide Risk Management for the Insurance Industry - Global Study.* http://www.pwc.com/extweb/pwcpublications.nsf/docid/57b887e9d239274785256e470020a3a5

Rech, J. E. 2005. Enterprise *Risk Management for Insurers: Theory in Practice.* http://www.contingencies.org/novdec05/enterprise_1105.asp

Schmidt Bies, S. 2006. *A Bank Supervisor's Perspective on Enterprise Risk Management*, BIS Review, publication 34/2006. http://www.bis.org/review/r060502d.pdf

Shamieh, C. 2007. *Implementing EC - Recent experience.* http://riskisopportunity.com/files/pdf/2007-chicago-shamieh.pdf

Society of Actuaries, 2006. *Enterprise Risk Management Specialty Guide.* http://soa.org/library/professional-actuarial-specialty-guides/enterprise-risk-management/2005/august/spg 0605erm.pdf

Standard and Poor's. 2005. *Enterprise Risk Management For Financial Institutions: Rating Criteria And Best Practices.* http://www.mgt.ncsu.edu/erm/documents/sp_erm_busdevbk.pdf

Standard and Poor's. 2007. *Enterprise Risk Management Can Help U.S. Commercial Lines Insurers Ward Off Irrational Pricing.* http://www.rims.org/resources/ERM/Documents/ERMReportCard4-30-07.pdf

Standard and Poor's. 2006. *Insurance Criteria: Refining The Focus of Insurer Enterprise Risk Management Criteria.* http://www.actuaries.org.hk/doc/ET060808_Ref4.pdf

Teuten, P. 2005. *Enterprise Risk Management: Its Evolution And Where It Stands Today.* http://www.keanebrms.com/portals/0/JLR-Fall%202005.pdf

Tillinghast - Towers Perrin. 2000. *Enterprise Risk Management: An Analytic Approach.* http://www.towersperrin.com/tillinghast/publications/reports/Enterprise_Risk_Management_An_Analytic_Approach/erm2000.pdf

Tillinghast - Towers Perrin. 2001. *Creating Value Through Enterprise Risk Management - A Practical Approach for the Insurance Industry.* http://www.towersperrin.com/tillinghast/publications/reports/Creating_Value_through_Ent_Risk_Mgmt/2002051306.pdf

Treasury Board of Canada. 2004. Integrated Risk Management - Implementation Guide http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/guide01_e.asp

Tripp, M.H; Chan, C; Haria, S; Hilary, N; Morgan, K; Orros, G.C; Perry, G.R; Tahir-Thomson, K. 2008. *Enterprise risk management from the General Insurance perspective.* http://www.actuaries.org.uk/__data/assets/pdf_file/0017/132038/sm20080428.pdf

UK Cabinet Office. Government Strategy Unit Report. 2008. *Risk: Improving Government Ability to Handle Uncertainty.* http://www.cabinetoffice.gov.uk/strategy/work_areas/risk.aspx

Wang, S; Faber, R. 2006. *Enterprise Risk Management for Property-Casualty Insurance Companies.* http://www.ermii.org/Research/downloads/erm_paper080106.pdf

Warrier, S.R; Chandrashekhar, P. 2006. *Enterprise Risk Management: From the boardroom to shop floor.* http://www.infosys.com/industries/insurance/white-papers/enterprise-risk-management-paper.pdf

Wason, S. 2007. *Repositioning ERM.* http://www.actuaries.asn.au/IAA/upload/public/1.a_Conv07_Paper_Wason_repositioning%20ERM.pdf

Yow, S; Sherris, M. 2007. *Enterprise Risk Management, Insurer Pricing, and Capital Allocation.* http://wwwdocs.fce.unsw.edu.au/actuarial/research/papers/2007/iisyowsherrisfinal.pdf

Note on Enterprise Risk Management for Capital and Solvency Purposes in the Insurance Industry

Published 31 March 2009

International Actuarial Association **Association Actuarielle Internationale**

Acknowledgements

Many people and organisations have been involved with the development of this Note.

First and foremost the members of the IAA Enterprise and Financial Risk Committee are thanked for their efforts in promoting and supporting the development of the Note. For more information about the committee, please visit www.actuaries.org and click on committees.

IAG (Insurance Australia Group) played a pivotal role facilitating the writing and development of the material included in the Note. Particular recognition needs to be given to Tony Coleman, Chief Risk Officer who sponsored this project in IAG and Peter Sutherland, Head of Group Risk & Compliance who was principal author. A number of other IAG people also contributed thoughts, wrote case material and reviewed drafts.

Three companies were involved in the development of the case material. These companies were Ernst and Young, KPMG and PWC. As consulting companies they were able to draw on international material to provide rich illustrations of the practice points being presented.

In addition, Standard and Poor's provided examples about approaches companies had used to implement Enterprise Risk Management in the context of their different organisation operating models from their published ERM criteria and from public rating report discussions of rated firms' ERM processes.

Finally, thanks go to the International Association of Insurance Supervisors. Members took a keen interest in the development of this Note and dedicated time to review drafts at their Solvency and Actuarial Issues Subcommittee meetings in 2007 and 2008.

ISBN 978-0-9812787-4-2

Association Actuarielle Internationale
International Actuarial Association

150 Metcalfe Street, Suite 800
Ottawa, Ontario
Canada K2P 1P1

www.actuaries.org
Tel: 1-613-236-0886 Fax: 1-613-236-1386

Email: secretariat@actuaries.org

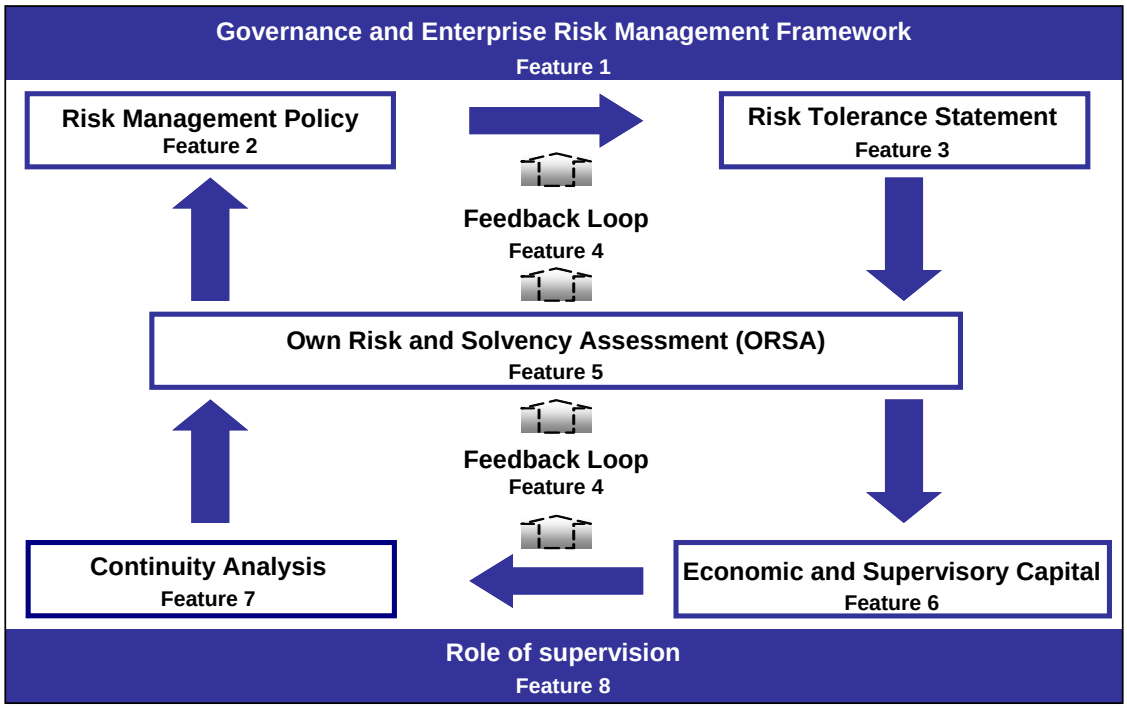
Table of Contents

1. Introduction

It is self-evident that insurance and risk management are very closely linked. In recent years the concept of Enterprise Risk Management (ERM) has been embraced by an increasing number of insurers seeking to improve their management practices and the operating performance of their businesses. Today, ERM is increasingly regarded as an appropriate response or indeed a solution to managing risk in today's more complex and interdependent markets and operating environments. Insurance supervisors have also played a leading role in setting standards and providing guidance to insurers on implementing appropriate frameworks for the management of risks faced by insurance companies.

This Note has been developed by the IAA for insurers to support the Standards and Guidance materials developed by the International Association of Insurance Supervisors (IAIS) for supervisors. It draws on industry experience, supervisors' supervisory practices, models and frameworks published by others and emphasizes practical considerations. The Note also seeks to help insurers assess risk framework maturity by reference to characteristics associated with different stages of development of risk management sophistication.

The IAIS Standard describes eight Key Features. The Note "unpacks" each of the Key Features by explaining them in more detail, thereby assisting insurance executives address strategic and operational issues associated with implementing an ERM framework in their insurance business. The material is presented as issues to consider and information about solutions others have used rather than a prescription to follow when implementing ERM. There is no one right way; rather the appropriate approach will depend on the insurer's particular circumstances. Appendix 8 lists Useful References that provide more information about the topics covered here.



1.1 Development of the Note

In developing this Note, use has been made of standards issued by the Federation of European Risk Management Associations and Standards Australia, both of which have issued comprehensive Risk Management Standards. Additionally, extensive use has been made of material from consulting firms, supervisors, academics and industry professionals. A number of examples and tips have been included throughout the Note to illustrate the points being discussed. In addition, a number of appendices have been compiled to provide more detailed case studies, guidance and suggestions for the implementation of an ERM risk management framework.

1.2 Working Assumptions

This Note has been developed for both life and non-life (general) insurance businesses. The breadth of experience and maturity in insurance businesses varies greatly in applying many of the concepts dealt within the Note. However, the Note attempts to provide a framework that is conceptually straightforward, based on practical principles that can be implemented in manageable steps – a series of building blocks to enable an insurance professional to move from basic to advanced ERM.

Many of the examples and frameworks provided are based on experiences in larger organisations. Nevertheless the information can equally apply to medium or small organisations. Smaller organisations can still be advanced in ERM but may outsource some of the activities instead of completing all activities in house. Alternatively, smaller organisations may choose to undertake the essential activities for their organisation context rather than a full ERM implementation. This would be a business decision about balancing risk and return, a fundamental principle of ERM. Where possible, comments have been included to provide guidance to small and medium organisations.

This Note is intended to support IAIS Standards and Guidance Notes for insurers in all jurisdictions by raising of awareness and building understanding among actuaries and other risk management professionals about ERM practices and the challenges associated with implementation.

1.3 Setting the Scene

Much has been written on the topic of ERM. This represents a logical and evolutionary response to growing complexity, uncertainty and ambiguity associated with 21st century corporate life. Now all management is risk management. In a corporate context we encounter risk when we pursue our goals. Some risks are beyond our control but many may and should be managed – in a linear sense this means identifying, assessing, mitigating and, if necessary, transferring risk. In reality however the pattern of risk is anything but linear, involving a complex interplay of dynamic external influences and (unpredictable) human behaviour. At a conceptual level, the development of ERM is a rational acknowledgement that traditional or silo risk management is not enough to sustain a 21st century insurance business.

The terms “risk” and “risk management” are commonly viewed through a lens of avoiding “bad” things happening and limiting the downside. Whilst understandable, the more enlightened view emerging is one of connecting risk to value maintenance and creation. This includes, for example, the empowerment of people to exploit opportunities. Indeed, market watchers view the ability to anticipate and react to a market opportunity to be as important as readiness for a potentially significant business disruption. Moreover, the importance of the risk management culture is naturally being linked with effective ERM practices.

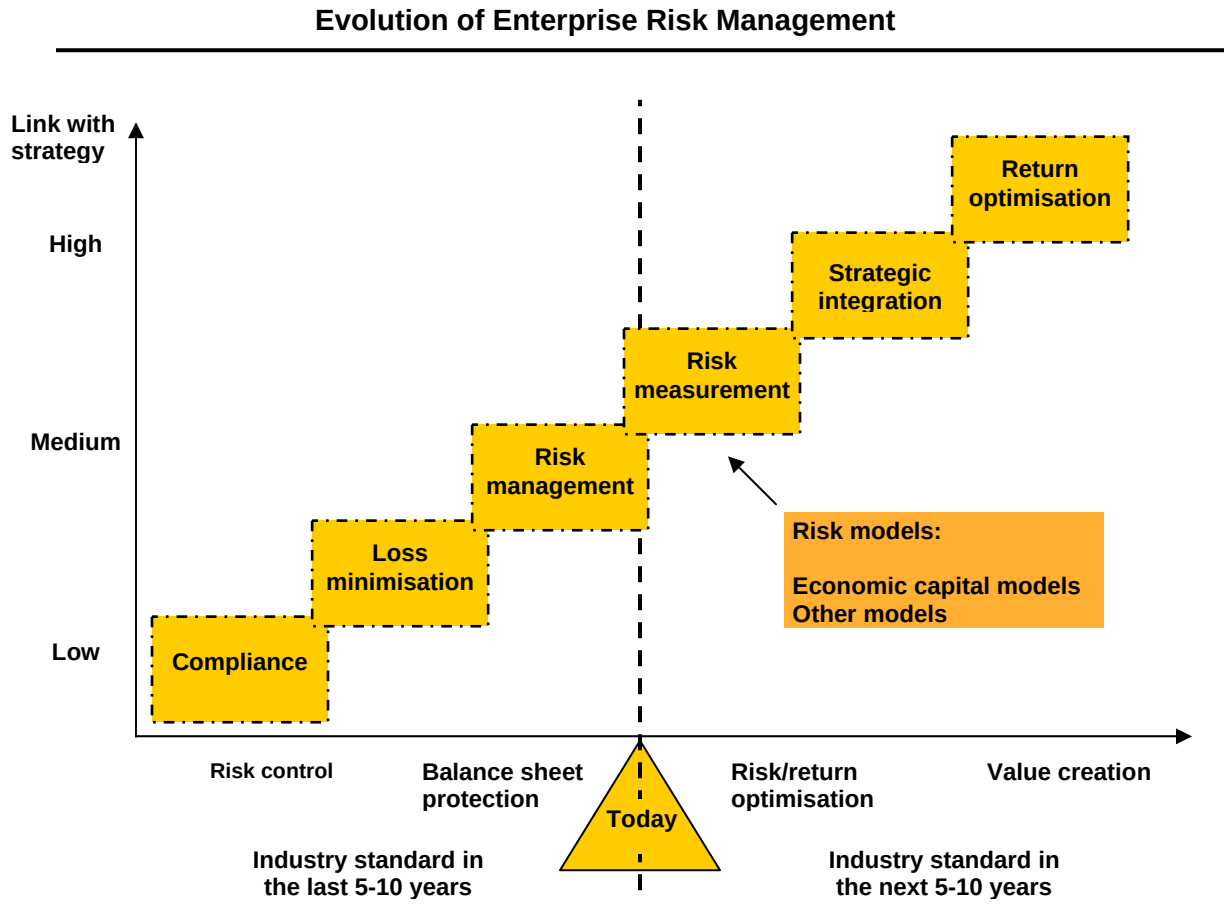
Effective ERM is inextricably linked with strategic planning for a business. When ERM is integrated in the business planning cycle of the insurer decisions of the company (e.g., growth of business lines, acquisitions, new product development, new channels) are made on a risk-adjusted basis and fully supported/informed by the ERM process. And, in turn, the annual risk budget/capital allocation by risk-type should be set in accordance with the business strategy of the enterprise. Finally, end-of-year capital measurement and performance measurement is conducted on a risk-adjusted basis, to complete the full circle of value creation.

Developing an effective enterprise-wide approach to risk management is not a straightforward exercise or one that can be neatly added on to the responsibilities of an existing function. It requires new investments in modeling and analytical capabilities, a different way of looking at risk and capital, and cultural changes that would embed risk management in all activities of a corporation.[1]

ERM’s importance is also reflected in the way supervisors and rating agencies increasingly expect insurers to apply its techniques for managing their business on a day-to-day basis.

[1] Risk Management Risk Opportunity, The 2006 Tillinghast ERM Survey.

1.4 Enterprise risk management history



The Role of ERM in Ratings, Mark Puccia, Managing Director, Standard & Poor's (March 30, 2007)

1.5 What is Enterprise Risk Management?

There is no universally accepted definition of ERM and the very nature of the concept suggests that there may never be one. However, a number of recurring themes/terms appear in an ERM context. Terms like "holistic", "integrated", "top-down", "strategic approach" and "value-driven" consistently appear in the various definitions found in ERM literature widely available today. It is not the intent of this Note to add to the growing list of ERM definitions. Rather, the Note has been developed having regard to the common themes and principles that emerge from the various definitions.

In summary, the Note is underpinned by the following principles:

- ERM is concerned with all risks faced by insurers
- ERM is concerned with creating value for the owners of an insurance enterprise whilst ensuring that promises made to policyholders are met.

More specifically,

- ERM is concerned with the totality of systems, structures and processes within an insurer that identify, assess, treat, monitor, report and/or communicate all internal and external sources of risk that could impact on the insurer's operations
- ERM implies a common risk management "language" across the operations of the insurer
- ERM involves systematic organisation of and coordination between risk functions, i.e., specialist risk "silos" operating in isolation from each other are inconsistent with ERM principles
- ERM includes both the management of downside as well as upside risks
- ERM seeks to quantify all risks but acknowledges that not all risks can be measured in currency/financial terms
- ERM is concerned with both behaviours (the risk management culture) and risk control processes
- ERM involves holistic consideration of risk information relating to past events (e.g., losses), current performance (e.g., risk indicators) and future outcomes (e.g., the risk profile or risk assessment).

Having framed the above principles it must be remembered that risk management remains the responsibility of all personnel in the insurer, and not just designated risk professionals. This reflects the fact that risk acceptance and management is integral to insurance. Moreover a series of enabling conditions must exist for ERM to take hold, namely:

- Demonstrable executive management support is critical
- Strong and direct linkages must be made between ERM and the insurer's business strategy and its day-to-day operations

The insurer must establish clear accountabilities for the various aspects of risk management, distinguishing between those in line management roles and those in risk management roles. Insurers wishing to develop a formal definition of ERM for their business should review the various definitions that have been published. A list of a representative number of these can be found in Appendix 1 to this Note.

For many insurers, implementation of ERM will not be straightforward nor a short term undertaking. For some, ERM will bring fundamental changes to governance and management structures, investing in different capabilities, implementing new processes and embarking on comprehensive change programs. Many of the insurers who have developed advanced practices describe ERM as a journey implemented in waves and this is perhaps the more appropriate way to think about ERM when deciding on a course of action.

1.6 Strategic Considerations/Where does one Begin?

It goes without saying that any directive, plan or recommendation to pursue an ERM implementation should emerge from careful research and analysis. Moreover, risk managers should avoid a quick fix approach to ERM, irrespective of whether the driver is internal or external to the insurer.

Key to implementation is buy in and support from the board. For this to occur, ERM needs to inform the board about issues they want and need to know about.

EXAMPLE:
THE BOARD'S ROLE IN SETTING PRIORITIES

A large multinational, with operations in all continents around the world, set about developing an enterprise wide risk management strategy and framework to meet a number of needs for the organisation:

- *Alignment of strategies and capital allocation demands from each of the regions*
- *Transparency and speed of communication*
- *Clarity and accountability for decision making*
- *Assurance to the Board on the effectiveness and efficiency of management practices, internal controls and processes.*

The internal audit manager was charged by the Board to develop the risk profile for the organisation and the enterprise risk management strategy and framework. With an eye to internal audit and assurance responsibilities, they proposed to roll out a comprehensive program for implementation. Executive management became uneasy as they realised their investment of time in this program would focus mainly on audit needs with little attention to the growth or profitability of the business, their prime objectives. Therefore management began 'de-prioritising' time and involvement to this program. Implementation began to falter. Clearly a different approach was needed.

The Board initiated a re-engagement process with management to ensure that the significant ERM investment would meet the priorities and expectations of key stakeholders.

- *The Board workshopped with management and the risk and assurance function to clarify each of the stakeholder needs, outputs and outcomes from any process/risk management activity*
- *The team prioritised and sequenced the activity and outcomes to reflect multiple stakeholder needs and business imperatives*
- *The Board gained commitment and accountability for the implementation plan and timetable and investment form all stakeholders.*

Prioritisation and sequencing of the ERM focus areas enabled all three parties to gain clarity on the implementation path and how the business would realise the value and over what time frame.

Key Lessons

1. *ERM is one of the few truly enterprise wide business capabilities that both provides an opportunity to change the way an organisation does business, but also can be 'used' to drive certain agendas that may not be aligned to the business imperatives, and stakeholder needs.*
2. *The output of ERM may not suit all stakeholders, so Board buy-in with management is critical to ensure needs and expectations are met and the ERM investment delivers maximum return and minimises any agency/stakeholder bias.*
3. *The Board is well placed to take a strategic and holistic perspective to ensure long term sustainability of the ERM investment.*

ERM implementation programs are not immune from the problems typically encountered by large-scale projects impacting the whole of an insurer. Risk managers tasked with the job of "implementing ERM" would benefit from studying lessons learned from "failed" projects, particularly those projects involving complexity in both technology and business process change. Invariably, key lessons from an ERM context relate to:

- Setting clear objectives for the delivery of expected outcomes associated with the ERM project
- Assigning experienced and suitably skilled resources using a rigorous selection process, in particular with respect to project leadership and change management roles
- Sufficient detailed planning upfront to reflect realistic effort / timeframes
- Implementing rigorous processes to tightly manage scope, gated criteria for milestones and cost / benefits
- Clear executive-level ownership and accountability for delivery of all project aspects (appropriate project governance)
- Realism about the expected "pain" through early stages of implementation and support required
- Realism around complexity, cost and timeframes
- Thorough risk management / mitigation strategies and support processes
- An organisational culture that demands objective and transparent project reporting and rapid escalation (and welcoming) of "bad news" so that problems get addressed earlier and at less cost.

Rather than adopting a strategic approach, insurers have often tended in the past to develop their risk management frameworks in a piecemeal or ad hoc manner, usually in response to either new supervisory requirements or a business crisis (and sometimes these drivers are connected!). A not uncommon scenario involves the identification of a manager working in the disciplines of internal audit, finance, actuarial, compliance and/or operational risk and tasking them to build the appropriate framework. Such an approach, whilst generally resulting in the production of appropriate documentation and review processes, is unlikely to garner broad-based support across the organisation and will more likely reinforce a view that ERM is something more akin to a compliance exercise. More importantly, it does not take a strategic view about how ERM aligns with the insurer's values, culture and approach.

Appendix 3 contains case studies to illustrate different approaches and issues involved in implementing ERM.

2. Governance and an Enterprise Risk Management Framework

Key Feature 1

As part of its overall governance structure, an insurer should establish, and operate within, a sound ERM framework which is appropriate to the nature, scale and complexity of its business and risks. The ERM framework should be integrated with the insurer's business operations, reflecting desired business culture and behavioural expectations and addressing all reasonably foreseeable and relevant material risks faced by the insurer in accordance with a properly constructed risk management policy. The establishment and operation of the ERM framework should be led and overseen by the insurer's board and senior management.

For it to be adequate for capital management and solvency purposes, the framework should include provision for the quantification of risk for a sufficiently wide range of outcomes using appropriate techniques.

2.1 Introduction

This section of the Note addresses a range of corporate governance, management, operational and cultural considerations relating to ERM.

One of the core IAIS principles relates to the concept of "proportionality". This principle of supervisory supervision establishes that supervision of regulated entities should be proportionate to the nature, scale and complexity of the risks to which the insurer is exposed to.

The proportionality principle can be equally applied in an ERM context. The ERM framework for a small motor insurer operating in one country will necessarily be different to the ERM framework adopted for a global insurer offering "short tail" and "long tail" non-life classes, as well as life insurance. The objective is for ERM frameworks to be proportionate to the nature, scale and complexity of the insurer.

This Note provides case study and other examples relevant to small, medium and large insurers. Whilst the majority of these draw on the experiences of larger insurers, the lessons and themes can be applied to all insurers, irrespective of the nature, scale and complexity of the risks they manage.

Nevertheless, there are certain aspects of ERM typically observed in small insurers and certain aspects observed in large insurers. Smaller insurers will tend to have consolidated board and management structures for risk oversight (e.g., combined audit/risk/compliance committee), less resources applied to component risk disciplines and less sophisticated modelling and measurement methods. On the other hand, large global insurers are more likely to promote consistent frameworks that incorporate common risk language, standardised categories, extensive policy/guidance and training materials, common reporting templates and tools to facilitate aggregation of risk information, and sophisticated systems for collecting, analysing and reporting risk information.

Cultural and behavioural characteristics of risk management will invariably be unique to an individual insurer, whether they be small, medium or large, reflecting the history, values and style of the insurer. An absence of a supportive culture will undermine the most sophisticated of ERM frameworks.

Appendix 2 to this Note describes a risk management "maturity" model. It lists components of an insurer's ERM framework and describes typical characteristics of early, intermediate and advanced stages of maturity. Insurers can use this model to benchmark their ERM maturity. It is very likely that insurers, irrespective of their size, will aim for different levels of maturity for different components, seeking to differentiate themselves on particular aspects of ERM appropriate to the nature, scale and complexity of their business.

2.2 Risk Management and Corporate Governance Generally

Corporate governance is concerned with improving the performance and conformance of companies for the benefit of shareholders, policyholders, other stakeholders and the wider economy. It focuses on the conduct of, and relationship between, the board of directors, managers and the insurer's owners. Corporate governance generally refers to the processes by which organisations are directed, controlled and held to account.

In a corporate governance context risk management is best described as an enabling process in the sense that it enables and facilitates the exercise of direction, control and accountability. In practice, the link between corporate governance and risk management is manifested in the form of a board committee and/or board charter responsibilities.

To ensure that there is a proper joining of ERM with an insurer's corporate governance structure, it is self-evident that the scope of the board's and/or board committee's "risk" responsibilities include all types of risk to which insurer is exposed.

2.3 Risk Management and the Role of the Board

The role of an insurer board with respect to risk management is broadly well understood and reflects an ultimate responsibility for the insurer's risk management framework. Stakeholders, including supervisors, interpret this ultimate responsibility to mean, amongst other things:

- Approving the insurer's overall risk management strategy and/or policy
- Overseeing the process of ensuring the insurer's responsible persons are fit and proper
- Setting the risk appetite of the insurer
- Monitoring key risks by ensuring the implementation of a suitable risk management and internal controls framework.

It is established practice for boards to form a dedicated committee to focus on matters relating to risk management. This committee may include risk, audit, financial reporting and compliance disciplines, or some combination of these.

The overarching objective of a risk committee with respect to risk management is generally described along the following lines:

> To assist the Board of Directors to discharge its responsibility to exercise due care, diligence and skill in relation to the effective management of major risks to which the insurer is exposed and verify that the insurer's risk management and internal control systems are adequate and functioning effectively.

Typical committee charter responsibilities relating to risk management include oversight responsibilities associated with at least:

- Effectiveness of the Insurer's Risk Management Framework
- Compliance with supervisory requirements
- Establishment of a suitably independent risk function with the authority, standing and resources to effectively execute its mandate
- Monitoring the adequacy of corporate insurance covers.

In developing an appropriate charter for a board risk management committee regard should be given to certain processes that enable effective discharge of charter obligations. These include, but may not necessarily be limited to:

- Establishing a direct reporting line between the committee and the most senior risk executive in the insurer
- Scheduling regular one-on-one meetings between the chair of the committee and the most senior risk executive outside of formal committee meetings
- Setting aside time in formal meetings for private meetings without executive management being present
- Consultation of external experts by committee members
- Transparency of reporting by the insurer's risk function such that reports to the board risk management committee and to management are not subject to any form of filtering.

In developing appropriate committee processes one must also bear in mind the essential reliance the committee places on the insurer's risk function. The relationship can be characterised as one of trust. Put simply, charter objectives are more likely to be met if they are

accompanied by an organisational culture that fosters rapid escalation of significant risk issues and/or bad news. Cultural and behavioural aspects of ERM are discussed further in section 3.8 of this Note. An example of a Risk Committee Charter is provided in Appendix 4.

2.4 Board versus Management Accountabilities

It goes without saying that the respective risk management responsibilities of the board and management should reflect natural boundaries and various legal and supervisory requirements in different jurisdictions. The (supervisory) board's role does not involve active day to day management of the risks faced by the insurer. Rather, it oversees and monitors management's role which should involve an active process for managing and reporting on all the insurer's risks. Of particular importance for boards when articulating respective responsibilities and conducting board and/or committee meetings is for them to avoid a perception amongst management that the board, or more particularly the board risk committee, is managing the insurer's risks. Equally, a risk management committee of the board provides an appropriate forum for the committee to question and challenge management's assessment of key risks as well as the process put in place by management to settle its assessment of key risks.

TIPS: WHAT SHOULD WE WATCH OUT FOR IN ORDER TO HAVE AN EFFECTIVE RISK COMMITTEE?

- Check that the Risk Committee comprises of members of a diverse background with the appropriate qualities such as inquisitive / questioning minds, objectivity and relevant experience. Consider the inclusion of external committee members to create a broader band of experience on the committee. Knowledge of the organisation is also important.
- Ensure the Risk Committee "ask questions" of the reports submitted and of management rather than apply the "tick the box" approach.
- Ensure the Risk Committee directives have the support of the Board and the appropriate level of management "buy in".
- Consider the appropriateness of the level and volume of reporting to the Risk Committee and keep the "quality" of the reports tabled and discussed under review to ensure the right information is being communicated.
- Risks Committees should also be responsible for keeping track of leading practices, trends and aiming to continually evolve and improve the organisations risk management processes.

Risk Committees should have an appropriate self-assessment program which includes Key Performance Indicators which are Specific, Measurable, Achievable, Realistic and Time bound.

2.5 Management Commitment and Leadership

The critical link between the Board and management is the insurer's CEO.

If ERM or risk management generally is not seen by the wider organisation as important to the CEO, the Board will have a hard task convincing stakeholders that the culture of the company is aligned with the Board's philosophy and/or some stated commitment to ERM.

Perhaps the most tangible means of ensuring alignment of CEO and board priorities with respect to ERM is to include certain risk management responsibilities in the job description and performance evaluation of the CEO, for example:

- promoting a risk management and control framework that articulates clear and powerful risk tolerance boundaries
- providing periodic assurance to the Board about the effectiveness and adequacy of risk management and control systems
- supporting an environment that does not tolerate behaviour that might compromise prudent risk management practices.

Moreover, public statements by the CEO and the leaders of the insurer that describe risk management as an insurer's "core competency" or in similar terms further reinforce the view that proper management of risk is seen as critical to the insurer's sustainability.

2.6 Establishing and Developing an Enterprise Risk Function

Consider a scenario whereby the insurer's CEO and board have decided to implement an ERM framework. Furthermore, as a sign of leadership and demonstrable commitment to ERM, the board has agreed that its first act in this journey will be to source and recruit a Chief Risk Officer (hereafter referred to as "CRO") who will report directly to the CEO, or possibly the CFO. The key roles and responsibilities together with an example of a generic CRO role description are in Appendix 5.

The first major challenge for the newly appointed CRO is likely to be a bringing together of the various risk-related functions and specialists within the insurer under a common framework and structure.

A newly appointed CRO will typically encounter a fragmented series of risk structures within an insurer, for example:

- Actuarial and/or research functions in some business units
- An internal audit function
- A specialist business continuity team

- A reinsurance department or reinsurance buying function
- Treasury and credit risk functions
- A capital management function
- Market risk assessment staff within asset management operations
- Health and safety experts reporting to the HR function
- Fraud and investigations experts
- Compliance teams in business units or in a central location.

In addition to the above, the newly appointed CRO might observe some risk-related committees operating within various structures within the insurer.

Perhaps the most important steps to take early in such a situation involve undertaking a program of action which will address at least the following questions:

- Is there a clear, shared understanding throughout the Board and management of the insurer's risk tolerance
- Are the incentive arrangements for management aligned with prudent management of risk
- What is the quality, health and transparency of risk information flows
- Where are the capability gaps, if any
- Are there elements of the insurer's business that are destroying value on a risk adjusted basis
- How is risk management connected with capital management and/or pricing and/or reserving
- Is the true financial condition of the insurer transparent to stakeholders
- Do the governance structures really work when there are stressful issues to deal with? (i.e., is the scope, composition and location of risk management committees and their relationship with the insurer's board governance structures adequate?)
- Is the management operating model appropriate? (i.e., is risk management embedded in and aligned with the insurer's business model, required competencies, key processes, people and infrastructure?)

The nature of the CRO role inevitably introduces a new dynamic to an insurer's senior executive team. The typical insurer CRO has an actuarial or mathematical background, brings rigour, method and a typically dispassionate approach to management decision-making. It is not uncommon for sacred cows to be challenged – are products delivering an acceptable return on capital? should the insurer exit certain lines of business? and so on. In this context, unless carefully and sensitively managed, the introduction or development of ERM can create natural tensions. It will therefore be important for the CRO to quickly establish the insurer's performance drivers and key internal and external stakeholders. Moreover the board's demonstrable support for the CRO's strategy and plans will be critical.

The relationship between the insurer's CRO and CFO is a very important one as, amongst other things, the CRO and CFO share the objectives of improving earnings predictability and limiting exposure to adverse variations in earnings. Managed well, the relationship can be a source of value creation for shareholders and security for policyholders. Policyholder security underpins capital requirements whilst shareholder needs underpin the setting of performance/value creation benchmarks. CFO and CRO strategies therefore need to be integrated, i.e., they need to generate adequate returns AND provide for an appropriate level of capital to protect all classes of policyholder.

Arguably the most important ERM decision for an insurer relates to the setting of its risk tolerance. One of the first tasks for a new CRO is to establish whether:

- a board-approved risk tolerance exists (and, if not, move to create and maintain one)
- if so, whether it is understood by people making day-to-day underwriting, investment, reinsurance decisions, and
- (perhaps most importantly), is it appropriate having regard to the insurer's strategic objectives?

The CRO is ideally placed to facilitate a dialogue and debate at management and board level about the insurer's risk tolerance. The CRO should lead the debate, both initially and over time.

Visibility and authority of the CRO are essential. A close position to the executive board or even a position in the executive board may be recommended.

Finally, it should be emphasised that the CRO role is one of coordinator of risk activities/ measurement at the company level. This is to be distinguished from the role of the income-producing units in the insurer. These units are the ultimate risk takers. In this context the CRO seeks to be a value-adding partner by helping them act on opportunities identified by the ERM function.

The above key considerations are by no means the standard priority issues for an incoming CRO. Each insurer presents a unique set of circumstances. However, the CRO should establish, and gain consensus around, the particular priority issues as soon as practicable.

Management Governance – Considerations

Oversight structures will need to have regard to:

- Transparency of decision making processes and the forums used to make key decisions
- The size and nature of the insurer and whether it is involved in life or general insurance, or both, or is part of a financial conglomerate
- The mix of risks faced by the insurer.

A typical management governance structure for a medium to large insurer will include the establishment of management committees at the group and business unit level with processes to ensure periodic reporting by business unit committees to the group risk committee. Another

structuring option relates to forming oversight committees with a dedicated focus on particular risks. For example, a natural delineation might be to establish oversight committees for:

- Pricing and underwriting risk
- Balance sheet/market risk addressing investments, liquidity, reinsurance, credit risk matters, etc.
- Operational risk.

Smaller insurers typically combine risk oversight activities under one committee or integrate the process with executive management reporting and monitoring activities.

The risk management structure of the insurer should align with the distribution of management accountability. For example, if business units are run in a standalone manner with end-to-end accountability, the centralisation of risk functions will potentially conflict with the desired accountability outcomes. For example end-to-end accountability means accountability for meeting premium growth targets and managing risks associated with pursuing growth targets.

Risk management committees should comprise senior management from business and risk management functions.

Structure of the ERM Function

It may prove impractical or inappropriate for an insurer to combine all specialist risk functions within a management structure headed by a Chief Risk Officer. What is important however is that processes are established to ensure that risk functions act and are seen to be acting in a coordinated fashion. From a line management perspective, the various risk functions will be viewed through a common lens and therefore inconsistent business unit engagement and reporting processes will invariably dilute and undermine the effectiveness of ERM.

In the case of large and/or multinational insurers the structure will typically involve a central or group risk function plus risk functions in each of the business units or regions. In such cases there is always the possibility of risk functions operating in isolation from each other, inhibiting information flows and escalation of key issues. Whilst there may be a range of reasons for this to happen, a decentralised risk management structure supported by matrix reporting clarifying respective roles and responsibilities serves to help create a more effective management of risk issues.

An insurer's risk function should also comprise an appropriate mix of capabilities and skills to support the delivery of ERM objectives. This means for example ensuring the function has the capability to implement ERM. Technical expertise may not be sufficient. The function will need to consider utilising project and change management skills as well as broader relationship management skills.

Summary

The form of the insurer's risk management structure will not of itself be the key determinant of the effectiveness of the ERM framework. An appropriate structure supported by consistently applied business unit engagement processes, a common risk language and standard risk management processes, agreed behaviours, appropriate reward systems, and clearly understand reporting and monitoring will help drive a sustainable ERM framework.

2.7 Importance of a Common Risk Language in the Insurer

It is not uncommon in businesses for there to exist a range of risk management terminology, tools, templates, rating systems and reporting protocols. Moreover, a number of supervisors have produced detailed guidance for insurers seeking to implement more structured risk management processes. For example, the traditional risk matrix plotting risk likelihood and impact[2] can be presented in many different ways. In addition, internal auditors and external auditors (and supervisors) may not necessarily use the same methodology for rating risk issues. Another dynamic relates to introduced methods by third parties, typically consultants engaged by the insurer to assist with projects.

A plethora of competing risk language can undermine the effectiveness of ERM in a number of ways:

- It inhibits business management buy-in and the task of embedding ERM by tending to confuse people not directly involved in developing and maintaining the methodology
- A silo approach is reinforced. Silos may exist in business units and across risk management functions
- A focus on form over substance. This could result in "real" risks not being identified
- A proliferation of process inefficiencies and duplication.

In addition to the above, aggregation of risk across categories is made particularly difficult because of inconsistent measurement of risks. Attributes and practices associated with a common risk management language include:

- A universally understood top-down risk rating system e.g., a set of both financial and non-financial parameters that define high (or "red") risks versus low (or "yellow") risks
- A rating system that relates risk rating to the level of management responsible for taking action to mitigate the risk
- Standard templates for use across the insurer and common risk categories
- Reporting and escalation thresholds e.g., guidance and/or rules governing what risk issues need to be reported to who, and when.

[2] Important to note that *Likelihood* and *Impact* are sometimes inappropriately characterized in this context as *Frequency* and *Severity* – see footnote on page 38.

EXAMPLE:
"BUT WE IDENTIFIED MORE RISKS THAN OUR COMPETITORS …"

An international insurer with a number of overseas branches was seeking accreditation under an advanced supervisory regime. However over time the insurer had developed different definitions of the risk classifications (such as Credit, Operational, Market, Fraud, etc) across many of the various jurisdictions that it operated in.

The lack of a common language created both operational and supervisory problems. The inconsistent and vague definitions created multiple risk identification, management and capital allocations of what could have been single risks. Some key risks were omitted from the risk management process which in turn, resulted in an inefficient business management structure. In addition, the lack of a common language meant that applications for accreditation could not be progressed until this could be resolved creating extra cost for the business and impacting on performance outcomes.

The company learnt to its cost that risk definitions should be precise enough to allow for the correct identification and classification of the 'real risks' to the organisation's business objectives, enabling economic value drivers within an organisation's risk management framework. In addition, risk language needs be consistently applied and communicated effectively across the organisation, enabling the organisation to take an enterprise-wide view of risk management, aware that all risks have been defined, classified and assessed consistently. Moreover a common risk language is essential to meet increasingly global supervisory requirements, no matter what size your company.

2.8 Risk Management Culture

Simply put, culture is the combination of the behaviours of people in the organisation – often described as "the way we do things around here". All organisations have a risk management culture. The only issue is whether it is supporting the appropriate goals, activities and outcomes and mitigating the risks of not achieving desired outcomes. Therefore a question to ask when considering promotion of ERM is: "What are the behaviours you want people to use in relation to management of risk?" Appropriate risk management behaviours may vary according to the organisation, the industry context, the location of operations both within and across national boundaries together with the resultant jurisdictional requirements. However behaviours that allow responsibility for dealing with risk to be unclear, that inspire a culture of fear or retribution, that allow "shooting the messenger" or that help "bad news to travel slowly" are not likely to be conducive to good risk management.

However deciding on behaviours is not sufficient to create or reinforce an appropriate risk management culture. There needs to be effective implementation of risk frameworks and processes. Furthermore, people need to be willing and able to use the appropriate behaviours to support risk related activities. It is these behaviours that over time will create the desired risk management culture. Therefore it can be said that human behaviour and capability are key to effective ERM.

Experience has shown that the most effective way to introduce these behaviours is as part of good business practice rather than a "big launch" which can be perceived as a fad by employees. Positioning these behaviours as business as usual also serves to bind the whole organisation to the concept because everyone is on the implementation team. In reality this takes significant time and effort. Typically adoption of new behaviours requires at least three years to start to take hold and longer to embed into the corporate culture.

EXAMPLE:
PROMOTING A PROACTIVE RISK MANAGEMENT CULTURE

An international general insurer based in Asia Pacific saw an opportunity to improve management risk by encouraging people to be more proactive. There were several potential benefits for working on the cultural side of ERM in this way. Being proactive meant that risks could be prevented or detected earlier, when smaller and were therefore typically quicker and less costly to remediate. Being proactive and encouraging speaking up about things 'not right' could enable speedier detection of issues. On the upside, hearing about ideas for improvements could support innovation, a key to business growth.

However it was recognised that changing the culture would take a number of years. So a program to embed proactive risk management behaviours was developed. The first step was to define the elements of a proactive risk culture, shown in the model below. Then behaviours associated with this model were incorporated into the annual staff survey. These questions form a risk culture index that not only enabled tracking of progress but also correlated with operational performance.

Initiatives to promote proactive behaviours were designed and implemented, all framed around the tag line of ***It's all about being proactive.***

- *Inclusion of proactive principles in the Risk Management Strategy and Group policies and practices*
- *A corporate risk goal for senior managers based in improving the risk culture index*
- *Proactive behaviours included in role definition, performance management and succession/talent development processes*
- *Training programs developed for managers and staff in face to face and online/blended formats and inclusion of the proactive principles in other training*
- *Information placed on the company intranet including incident reporting portals.*

Several years on, measurable progress is being made however the challenge is to continually invigorate the program to ensure being proactive stays at the top of people's minds.

The following sections expand on two of these challenges: the development and measurement of an appropriate risk management behavioural model and designing an effective implementation plan.

2.9 Developing a Risk Behaviour Model

There are arguably three aspects to consider in addressing the behavioural aspects of risk management. The first is a proposition that risk management is not about eliminating risk, as this would inhibit growth and change. Rather, it is choosing the risks the organisation is willing to take and then managing them well. Therefore it is useful to adopt the description from various risk standards (e.g., the Australian Risk Management Standard AS4360) about the core risk behaviours of prevention, detection and recovery combined with continuous improvement.

Supporting this is a second core concept that people need to feel confident to speak up about in this risk management context. This may involve full and frank discussion of the risks being considered, whether they are minor process issues in a call centre or risks associated with a potential acquisition. It also means people feeling confident to communicate bad news promptly when things go wrong without fear of retaliation. This requires managers to provide an encouraging environment at all levels.

Underpinning both of these is a third aspect involving people having the skills, capability and empowerment (role clarity and accountability) to undertake the behaviours necessary to manage risk situations. Interestingly, these three aspects also link strongly to supporting innovation and therefore growth of the business. In this way the behavioural aspects of risk management can be positioned as addressing the downside and supporting the upside of risk management (refer also to Section 3.11 below).

2.10 Developing an Implementation Plan

It is important to "operationalise" appropriate risk management behaviours by developing a common language to describe them in a way that everyone in the organisation can use. These descriptions should be incorporated into descriptions of core competencies and/or capabilities, talent assessment and development and all risk and compliance training. These activities should be supported strongly by executive management and the insurer's board who need to demonstrate a keen interest in progress across the business.

The organisation should measure the above elements each year to observe areas where the risk management culture is strong and where there is opportunity for improvement. Rather than creating an entirely new measure and an extra burden on the business in time, the first step should be to identify if there are measures already available to use. These could include existing employee surveys, performance data and audit reports. Consideration could be given to augmenting existing measures identified so they can be used to assess the strength of the risk management culture. Using additional measures also has the benefit of shielding the measurement from gaming to achieve a good result, especially if bonuses are dependent on results. The key word is simplicity, both for the model and the measurement approach.

In summary, people, behaviours and resultant cultures are a fundamental building block for the development of effective and sustainable ERM. Implementation of a culture component of ERM should address the following aspects:

- Consideration and development of a risk management behavioural model that suits the insurer's broader culture and operating environment. The model should be precise in describing behaviours in measurable and observable terms that can be incorporated into training, reporting, bonus and performance management systems
- Securing support of senior management and development of their risk awareness. This could be facilitated by training, focus groups, education and briefing of executive management and by examining how risks have been managed in the past together with better approaches. "War stories" help understanding and engagement
- Ensuring that the right behaviours are embedded in the design of frameworks and processes so they have integrity within the ERM framework and also are reinforced at every available opportunity
- Design of an implementation plan over a realistic time frame, appropriately resourced
- Reinforce behaviours through multiple influencing channels
- Benchmark behaviours before starting the implementation program and measure at least annually to assess progress. Be ready to make adjustment to the design and change program if required, particularly if external events indicate the need
- Link the measures to measurable business outcomes to prove the value add of the desired risk management culture.

TIPS FOR IMPLEMENTING RISK CULTURE CHANGE PROGRAMS

Leverage – Use existing organisation-wide programs rather than starting new ones to both lessen the load of managers and staff and facilitate embedding as business as usual as soon as possible.

Language – Focus on behaviours which people feel they can change rather than culture which can be considered amorphous and intangible.

Change skills – Hire or engage people with skills to assist the risk function such as people skilled in change management, learning, human resources, project management etc.

Embed Principles – Ensure the change initiatives to promote the new cultural principles are embedded into the people processes so the program is continually reinforced and maintained.

Measures and Consequences – Benchmark the culture then measure progress and ensure the Board/Risk Committees are supportive of the program and aware of improvement. Reinforce good behaviours and reorient inappropriate behaviours through use of levers such as bonus payments.

2.11 Upside Risk Management

It is commonly accept ed that risk manageme nt involves both the management of potential adverse effects and, conversely, the realisat ion of poten tial opportu nities. Whilst pract ices associated with managi ng adverse effects are well understood and follow establish ed patterns, the same c annot be said for the re alisation of opportunities. This of course is not to say that insurance managers miss opportunities. Rather, it reflects a relative lack of consisten tly applied risk management processes for the management of opportunities (or upside risk).

Perhaps the best way to illustrate t his relative gap is to reflect on the information generally presented i n management reports dealing with risk. These will typically highlight key risks, incidents, issues and trend in risk indicators, etc. Howe ver these reports rarely include an analysis of key opportunities and t herefore are arguably incomplete in addressing the full spectrum of risk. Of course insurers do report on opportunitie s, typically via CEO and business head report ing. However the assessment of the value of these op portunities is invariably disconnected from the assessment of the value of the insurer's risks. Eff ective ERM implies an integrated assessment of adverse effects and opportunities.

The real challenge then for insurers is to create an environment around the development of their ERM frame work that facilitate s bett er integratio n of the ma nagement o f upside an d downside risks. Some of the practices that will support integration include:

- Ensuring the risk function is involved in strategic planning
- Including both risks and opportunitie s in reports prepared by risk functio ns (and internal audit functions). Some examples of opportunities can be:
    - Reduce costs by removing excessive or ineffective controls
    - Leveraging risk management controls to achieve other business goals (such as utilising work from home solutions not just as a BCP risk control but also to achieve a human resourcing goal to establish more flexible working con ditions to attract / retain staff)
- Reward systems that encourage calculated risk taking
- Reporting on emerging, industry-wide, cross-border, and longer term risks.

The risk management process (Section 7.2) ca n be equally applied to t he assessm ent of risks and opportu nities. The discipline of the process require s people to quantify bo th risks and opportunities using consistent rating methods.

Effective upside risk management is u nderpinned by a mindset t hat views all risks as opportunities:

- Opportunities to implement mitigation or risk transfer strategies for identified risks
- Opportunities to develop plans to proactively prepare for low likelihoo d – high impact scenarios e.g., by running crisis simulations
- Opportunities to invest in new ca pabilities to manage longer term risks po tentially impacting future profitability.

Involvement of the risk function in upside risk management provides a real opportunity for the function to actively participate in strategic activities and add value to the insurer.

As described in Section 3.8 above, the insurer's organisational culture is critical to the effective management of upside risks.

2.12 Performance Management and Reward Systems

The discussion above about organisation culture reinforces that performance management and/or incentive systems should include a recognition or inclusion of a risk management component. For example, a broad scope ERM implementation that is not accompanied by management incentives tied to clearly defined risk management outcomes will, most likely, fail.

Care should be taken when constructing incentive programs that include a component aimed at improving risk management practices or extracting value through better risk management. Key considerations include:

- Getting the balance right and, for example, ensuring that the relative size of the incentive for improving risk management does in fact motivate targeted individuals and/or groups
- Deciding which individuals or groups to include. If senior management reward systems are not inclusive of a risk management goal then the insurer will struggle to evolve its ERM framework
- Establishing clarity about what to measure and what are appropriate measurement proxies. Consideration should be given to activity-based measures (e.g., milestone completions), financial measures (e.g., value at risk over time), audit results/performance and staff surveys
- Making linkages between risk management performance and talent management and capability development processes. For example, if it is understood that leadership potential is in part measured by an individual's capacity to create an environment that fosters proactive management of risk, then the insurer's board can gain comfort that managers will actively support ERM
- Ensuring that incentive programs are targeted at the appropriate level of staff and that they do not have unintended consequences. For example, linking staff incentives to results of staff surveys/feedback is likely to skew the results of the surveys.

EXAMPLE:
ENCOURAGING THE "WRONG" BEHAVIOUR

A large financial services organisation announced significant losses relating to the activity of their proprietary trading division. It seemed that people had used various methods of concealment so they could continue reporting profits despite the significant losses being incurred. One of the motivations appeared to have been the desire to achieve budgeted profits and receive bonus payments.

Investigations confirmed this link to incentives. The following observations were made regarding the culture:

- *There was an excessive focus on process, documentation and procedure manuals rather than on understanding the substance of issues, taking responsibility and resolving matters.*
- *Risk measures and reporting were not relied upon or believed to characterise the risk exposure correctly and therefore were ignored*
- *There was arrogance in dealing with warning signs*
- *Issues were not escalated to the Board and its Committees and bad news was suppressed.*

The prevailing culture fostered an environment that provided the opportunity to incur losses, conceal them and escape detection despite ample warning signs from the formal risk management processes, structures and systems. The employees did not behave honestly and the risk management processes failed.

As a result of these significant financial losses, several senior managers resigned, there was considerable damage to the organisation's reputation; significant fall in share price; heightened supervisory supervision with associated increased management time and cost; and criminal proceedings and convictions of the traders.

Key lessons

1. *Listen to the warning signs and ACT*
2. *Prioritise the correction of known control breakdowns*
3. *Consider the unintended consequences of incentive plans*
4. *Risk management needs all its elements to work together to reduce gaps*
5. *A poor culture and misaligned incentive plan can override the best of formal systems and controls.*

2.13 Reporting and Monitoring

Effective ERM relies heavily on quality risk management information because better risk management information means better decisions. The insurer's risk management function should form a view as to whether executive management and the board are receiving the right information. Typically, insurers produce detailed information about insurance, market/investment and credit risk. However this is not always the case with operational risk and the overall portfolio of risk – the enterprise-wide risk report. At the highest level risk reporting should seek to answer the following kinds of questions, such as:

- Current and emerging key risks in the business and within the wider environment, and changes over time (the risk profile of the insurer)
- Changes in risk indicators (measures influencing risk likelihood and/or impact)
- Capability for identifying and managing risks.

The table below provides, by risk category, an indicative list of the sort of information typically associated with enterprise risk reporting:

Risk Category	Information
Enterprise/all risk categories	• Enterprise risk profile (refer also section 7.2 for sample risk profile layout) • Capital adequacy ratios • Significant regular engagement • Significant losses, incidents • ERM framework improvements • Changes in key risk indicators (KRIs)
Underwriting (including reinsurance)	• Risk aggregations (sum insured) by region, peril, distribution channel • Reserve strengthening/release
Market	• Value at risk (VAR) • Stress and scenario test results
Credit	• Counterparty credit quality and diversity for assets and liabilities – credit rating analysis
Liquidity	• Proportion of liquid assets to total assets
Operational	• Analysis of key risks (operational risk profile) • Change in key risk indicators • Internal audit results
Other	• Benchmarking of emerging industry risks • Business, insurance cycle data

The following is an example of dashboard reporting:

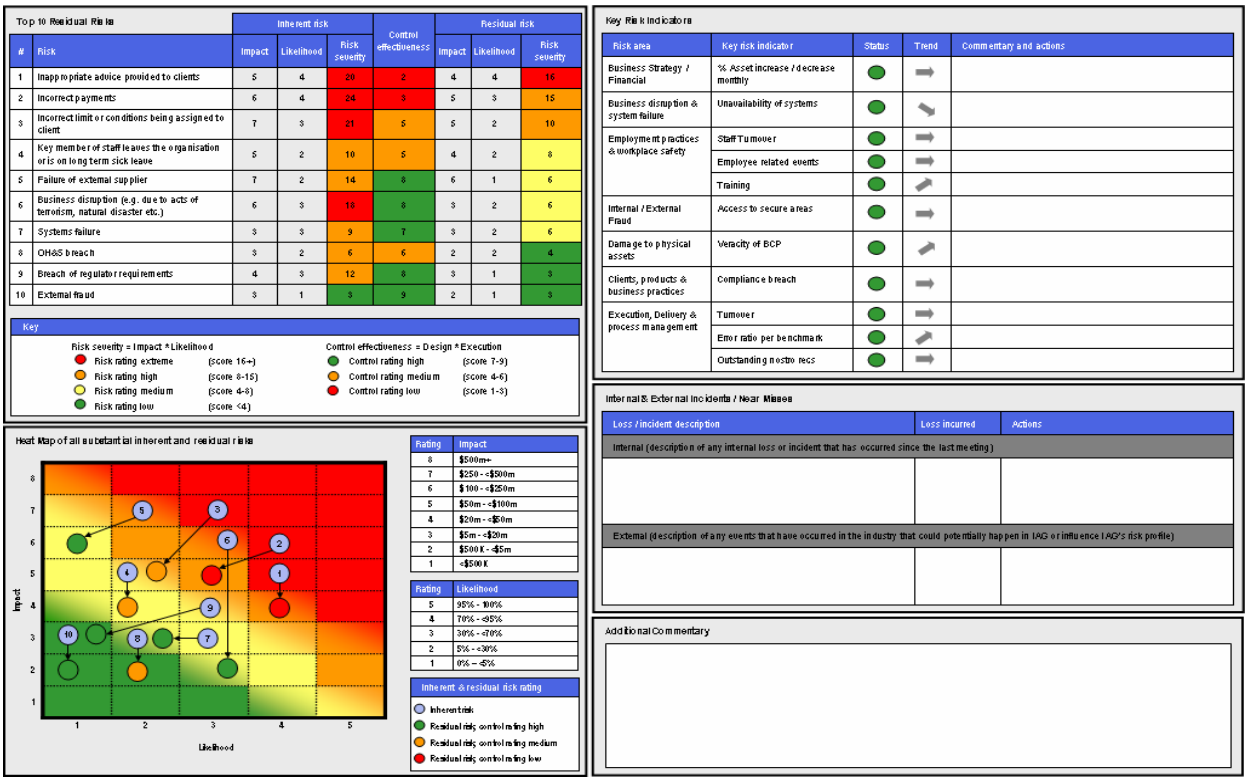
EXAMPLE:
"ANYTHING TO REPORT?"

Many stakeholders rely on quality risk information:

- *Audit Committees – Monitoring material financial risks and mitigation of those*
- *Executives – Reviewing risk information for completeness*
- *Managers – Reviewing risk inf ormation for co mpleteness and chang es in risk profile or control effectiveness*
- *Risk Owners – Updatin g risk information and escalating changes in likelihood, impact or control effectiveness as required*
- *Control Owners – Updating statu s of treatments for co ntrols that they are responsible for*
- *Internal Audit – Reviewing the effectiveness of internal control measures*
- *External Stakeholders – Reviews by supervisory bodies.*

A succin ct dashboard is the m ost effective way to report so the infor mation can be assessed at a glance. Supporting inform ation can be attached for those who require more detail. Some of the key categories of a dashboard may include:

- *Top 10 residual risks*
- *Key risk indicators*
- *Scoring chart for risk severity and control effectiveness*
- *Heatmap of all substantial inherent and residual risks*
- *An additional commentary section*
- *Significant project progress.*



2.14 Role of Internal Audit

It is not uncommon practice for the role of developing an insurer's risk framework to be allocated to an insurer's internal audit function. This reflects a view that there is a good match of the desired skill sets for ERM implementation and those of internal auditors.

This practice may deliver short term assurance benefits and give insurer boards a sense that progress is being made but is unlikely in the medium to longer term to deliver a truly effective or embedded ERM framework. Moreover, the practice can potentially undermine the necessary independence of the internal audit function by putting it in the position of creating processes that it is consequently conflicted from checking. Perhaps more importantly, it sends a message to the wider organisation that ERM is essentially an assurance or compliance exercise rather than a process that is ultimately intended to optimise value created within an agreed risk appetite. A number of national supervisors have recognised this inherent conflict by introducing standards that define the role of an insurer's internal audit function with respect to risk management.3

Emerging best practice in this area is to clearly delineate the roles of internal audit and the function tasked with developing and maintaining an insurer's ERM framework. In this way, the independence of internal audit is not compromised but rather is preserved and directed at providing assurance to the board, and typically via the board audit committee, about the effectiveness of the insurer's ERM framework over time.

[3] For an example refer APRA Prudential Standard GPS510, Governance, paragraphs 46 and 47.

2.15 Dealing with New Activities

An insurer's ERM framework needs to extend to new activities as these are invariably sources of new risks that can significantly affect an insurer's risk profile. New activities could include:

- Product changes and introduction of new products
- Changes in corporate and management structures
- Commissioning of major projects to build and/or upgrade computer systems and networks
- Due diligence, acquisitions, divestments and other corporate transactions e.g., capital raisings
- Outsourcing and off-shoring strategies.

It is important for the insurer's risk function to be familiar with the range of change or "pipeline" activity under way at any given time. Moreover, strong working relationships between the insurer's risk function and functions driving the pursuit of new activities or strategies increase the likelihood that the "risk voice" will be appropriately heard and considered. In practice this means involvement of the risk function at the planning stage of new activities and agreeing details of the role and responsibilities of the risk function with respect to such activities.

The insurer's risk function should therefore develop close, transparent and systematic relationships with functions such as strategy, finance, product development, IT, legal and human resources, amongst others.

There are a number of ways that the insurer's risk function can become involved in new activities, including:

- Involvement in due diligence work where the skills of the actuary and other risk management professionals can be utilised to help identify and assess risks and to assist with valuation and modelling aspects
- Working with the insurer's strategy team to ensure the strategy incorporates an appropriate assessment of risks attaching to the chosen strategic direction
- Preparing and/or facilitating risk assessments for major projects or new product launches
- Managing and coordinating engagement with relevant supervisors with respect to pursuit of new activities
- Working with newly acquired businesses to help them adapt to and implement the insurer's risk management framework.

Engagement by the insurer's risk function in these kinds of activities fosters strong relationships, facilitates better management decisions and aligns the risk function with the objectives of sustaining and creating value. In this way ERM disciplines and processes become naturally embedded in change activities.

3. Risk Management Policy

Key Feature 2

An insurer should have a risk management policy which outlines the way in which the insurer manages each relevant and material category of risk, both strategically and operationally. The policy should describe the linkage with the insurer's tolerance limits, supervisory capital requirements, economic capital and

The insurer's risk management policy provides an important opportunity for the insurer to establish and communicate philosophy and minimum requirements for the management of the portfolio of risks to which the insurer is exposed. Risk management policy should be set by the insurer's board. In a number of jurisdictions it is also a supervisory requirement for risk policy to be approved by the board. A list of the typically topics included in a risk management policy together with a suggested structure is provided in Appendix 7.

The process of developing and setting risk management policy should involve many stakeholders, take some time and be tested with those responsible for implementing and complying with the policy. An in-use policy should be regularly reviewed, at least on an annual basis.

In formulating risk management policy the insurer should address at least the following aspects:

- A clear risk management philosophy – for example outlining why risk management is important and the linkages with value creation
- The relationship between risk management and the insurer's purpose or mission, values and strategic objectives
- How risk management is embedded in the related processes of capital management, pricing, reserving and performance management
- Scope of activities to which the policy applies. For example, the policy should be sufficiently flexible to cater for multiple ownership structures (e.g., wholly-owned, majority-owned, joint venture etc.)
- Appropriate supervisory requirements and considerations
- Requirements with respect to acquisition of new businesses e.g., time frame for integration with the insurer's ERM framework
- Categories of risk and risk definitions and how these map to internationally accepted categories/definitions
- In addition to risk categories, the policy should define risk terminology used e.g., risk, risk management, risk management framework

- Most importantly, the insurer's risk appetite should be set forth in the policy (refer Section 6 below) for further discussion on risk tolerance
- Governance and oversight aspects
    - Board, board committee structures, responsibilities
    - Management structures, roles, responsibilities
    - Roles and responsibilities of the various corporate and business unit risk functions
    - Role of internal and external audit
    - Compliance aspects, including consequences associated with policy breach
- Behavioural expectations of all staff
- Minimum process-level requirements that apply universally across the operations of the insurer e.g., risk management training, risk profiling, business process documentation, risk reporting and escalation, risk monitoring and assurance
- Requirements for the conduct of the insurer's Own Risk and Solvency Assessment (refer Section 7 below)
- As appropriate, specific requirements attaching to defined risk categories
- The process for reviewing and updating the policy.

The above "shopping list" may be suggestive of a policy document of some considerable length. This should not necessarily be the case. Care should be taken to avoid writing a long policy document that is not read or understood by the wider organisation. Therefore, the writer or policy custodian should consult widely to formulate an appropriate strategy for communicating the board's expectations with respect to ERM. This may involve the development of a suite of documents, including a high level set of policy principles, tailored to different audiences within the insurer.

Development of new policy or renewal of existing policy provides an excellent opportunity to assess attitudes to and understanding of risk management in the organisation. If ERM policy implementation is carried out in a top-down fashion with limited engagement of business functions, then it is unlikely that ERM requirements will be properly integrated with and embedded into the day-to-day operations of the insurer.

4. Risk Tolerance Statement

Key Feature 3

An insurer should establish and maintain a risk tolerance statement which sets out its overall quantitative and qualitative tolerance levels and defines tolerance limits for each relevant and material category of risk, taking into account the relationships between these risk categories.

The risk for bearance le vels sh ould be based on the insu rer's strateg y and be actively applied within its ERM fra mework and risk management policy. The defined risk tolerance limits should be embedded in the insurer's ongoing operations via its

This section discusses the concept of risk tolerance, the relationship between risk tolerance and the insurer's strategy and provides guidance for insurers on some of the practical aspects of setting and updating risk tolerance.

Establishing an insurer's risk tolerance involves making strategic choices. The process must be connected with setting strategy and longer term direction. Whilst top-level management may be heavily involved in debating the appropriate risk tolerance to match a given strategic direction, it is the board who must decide on risk tolerance and the insurer's strategy. The CRO should be involved in but not responsible for defining the insurer's risk tolerance.

The insurer's risk tolerance is framed having regard to the insurer's strategy and business plan. The risk tolerance shares the same time horizon as corporate strategy, typically three to five years, and therefore should not respond to, for example, annual budget targets/business plans. Put another way, it would be highly unusual for an insurer's risk tolerance to change every year. The relationship between risk tolerance and strategy is illustrated in the diagram below:

The insurer's risk tolera nce articulates boundaries for how much risk th e insurer is prepared to accept. Limits are more in the nature of thresholds that warn insurers that achievement of plans may be at risk:

- Risk toleran ce is a high er-level statement that considers br oadly the levels of exposure to risks that the Board deems acceptable
- Limits are narrower and set the acceptable level of variation aro und objectives associated with an insurer's annu al busine ss plan and budget. In particular, Limits translate the risk toleran ce into lang uage that can be used by the business on a da y to day basis.

For an insu rer, the following parameters are typi cally used to articu late risk tole rance across financial and non-financial risks:

- Lines of business that the insurer will/will not accept
- Earnings volatility
- Requirements to meet supervisory criteria including allowance for unexpected events
- Desired capital strength, usually by reference to a defined rating level o f a recognised credit rating agency
- Maintaining levels of economic capital by reference to a specified chance of meeting policyholder obligations or target return periods for "risk of ruin"
- Maintaining a buffer level of capital in excess of the minimum supervisory capital
- Maximum exposure to aggregation of risk
- Dividend paying capacity (for listed company insurers)
- The maximum net loss the insurer is prepared to accept in a ny given year in the event of a catastrophic loss (general insurers)
- Minimum acceptable pricing principles
- Descriptions of unacce ptable operational risk scenarios typically disruptive of the continued and efficient operation of the insurer
- Setting go/no-go criteria for corporate transactions a nd strategic projects e.g., acquisitions, divestments, cap ital r aisings, pro jects spanning multiple busine ss units and/or entities within an insurance group etc.

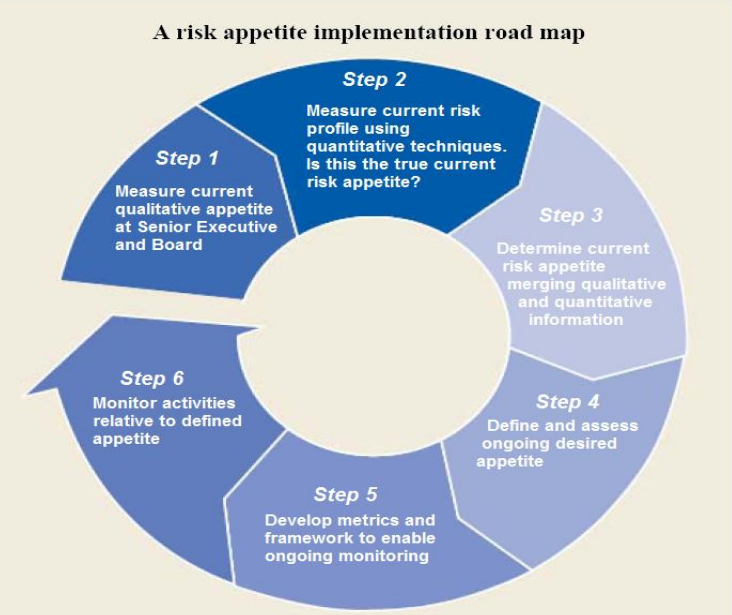
On the othe r hand, limits, being nar rower in scope, tend to operate at the risk cat egory level. Staying within limits should mean that an insurer w ill st ay within its overall risk tolerance. Example of risk limits include:

- Establishing counterparty credit limits for investments and reinsurers
- Setting an overall target for credit quality for a reinsurance buying program, usually b y reference to credit rating
- Establishing concentrat ion limits f or lines of business/p roducts, ge ographies and counterparties

- Maintenance of underwriting and pricing principles and limits
- Setting insurance reserves to target an explicitly quantified probability of adequacy
- Setting liquidity benchmarks by reference to the amount of investment assets to be held in highly liquid assets
- Investment mandates setting limits for the investment of policyholder and shareholder funds in traded instruments
- Limits on the use of financial derivatives
- Establishing operational risk policies that include limits for outsourcing, business interruption, fraud, health & safety and project delivery, amongst others.

As can be seen from the above, limits are more transparent to business managers. Moreover it is becoming increasingly common for business managers to utilise Key Risk Indicators (KRIs) to highlight how and when limits may be exceeded or are reaching key thresholds. It is therefore important that the insurer, usually via its risk function, establishes clear linkages between risk tolerances and limits. This delivers governance benefits (board assurance that risk policy is appropriately operationalised) and performance management benefits (fewer surprises and reduced earnings volatility). In addition, it is important to consider when calibrating risk tolerance by reference to target credit ratings, that insurers should also undertake their own appropriate rating analysis to triangulate external data supplied by ratings agencies, and other third parties.

It is important that each insurer develop a statement of risk tolerance appropriate to its own circumstances. Some insurers may choose to develop high level statements of risk tolerance whereas others may define risk tolerance at the risk category level, and even within the risk category level. The diagram below shows a typical roadmap of the steps to establish a risk tolerance.



SOURCE:
Bennet C; Cusick, K. (Trowbridge Deloitte Limited)
Risk Appetite: Practical Issues for the Global Financial Services Industry
2007
URL: http://www.actuaries.asn.au/IAA/upload/public/4.a_Conv07_Paper_Bennet%20Cusick_Risk%20Appetite.pdf

More details about this process can be found in the Useful References in Appendix 8 particularly the source referenced in the diagram.

Whatever path is chosen, the following should be borne in mind when settling an insurer's risk tolerance:

- It must support the achievement of business strategy
- It must be supported by appropriate financial and other policies that translate higher level statements of risk tolerance into operational limits.

EXAMPLE:
HOW TO DEVELOP A RISK TOLERANCE

As shown in the following graphic, risk tolerance is about which risks to take and why, not just how much risk to take.

1. ***Risk Profile:*** *The current and emerging risks facing the business*
2. ***Risk Capacity****: The financial, reputational and operating capacity or comparative advantage of the business to withstand or manage the risk exposures*
3. ***Risk Tolerance****: Whether the risk profile is appealing within the context of our risk capacity, strategy, market positioning and business competencies*

When developing a position on risk tolerance the questions to ask are:

- *How comfortable are we in the continuing exposure to an individual or basket of risks given our Risk Profile (current and future), our Risk Capacity (current and future) and within the context of our strategic options or choices?*
- *Is there a build up or concentration of risk that makes us uncomfortable?*
- *In light of the risk exposure, are we satisfied with the level of return (and capital requirements) expected from the decision?*
- *What would be the level of regret if we took an alternative option/decision or bet under different future scenarios?*

5. Risk Responsiveness and Feedback Loop

Key Feature 4

The insurer's ERM framework should be responsive to change.

The ERM framework should incorporate a feedback loop, based on appropriate and good quality information, management processes and objective assessment, which enables the insurer to take the necessary action in a timely manner in response to changes in its risk profile.

5.1 Nature of Feedback Loops

A key test of the effectiveness of an insurer's ERM framework is the extent to which it caters for change. A framework geared only towards business as usual (BAU) activity may fail to prepare the organisation for shifts in market dynamics, supervisory change, changing customer preferences, global trends and so on.

The insurer's risk profile over time will be influenced by:

- Outputs from periodic risk assessments at the enterprise and business unit levels that have regard to BAU activities, new initiatives/strategies and external events (looking forward)
- Movements in key risk indicators (the present)
- Unexpected losses, and significant control failures or incidents (looking back).

Taken together these three influences provide valuable ongoing information about the effectiveness of the insurer's internal control environment. The insurer's ERM framework should therefore include formal and systematic processes to collate information from the above three sources (past, present, future).

A particular source of relevant feedback is incidents and issues. These could be generated by customer complaints, audit findings, project or system failures, crisis events and supervisory action. The insurers ERM framework should incorporate processes for the formal review of incidents/issues above certain thresholds, including the analysis and reporting of root causes. This practice supports a culture of learning from mistakes and continuous improvement.
An effective feedback loop is underpinned by:

- Establishment of thresholds for reporting significant issues (see also Section 2.13)
- Protocols for escalation of issues to various levels and management and, if necessary, supervisors
- Reporting of risk aggregations to identify where limits (and potentially risk tolerance) may have been exceeded.

5.2 Emerging Risks

Emerging risks are developing or already known risks which are subject to uncertainty and ambiguity and are therefore difficult to quantify using traditional risk assessment techniques.

TIP: WHY INSURERS WANT TO KNOW ABOUT EMERGING RISKS

Insurers are interested in emerging risks for a number of reasons including, whether emerging risks will:

- Influence the organisations strategy
- Impact the performance of the underwriting portfolios – unexpected (latent) claims / claims frequency / claims costs
- Impact on the operational risks facing the organisation
- Present opportunities for new types of insurance products?

The answers to these question may have a direct impact on policy wording, claims reserving strategies, reinsurance arrangements and the insurer's own operational risk strategies.

Having a clear set of emerging risk objectives linked to the organisation's context and strategy is critical before starting this step. Some examples of the context setting characteristics to consider include:

- Geographical scope - local / country / regional / global
- Time Horizon – long time horizon for long tail classes of insurance, or, short time horizon
- What types of impacts – physical damage to property; liability exposures; health issues; or multiple types of impacts.

Appendix 8 provides some useful emerging risks websites.

Once the objectives and scope are established this will provide some direction to help identify emerging risks. The identification can be done using a variety of methods ranging from reviewing the press and trade publications, workshops, the opinions of external experts, etc.

Emerging risks may lead to claims with a high loss potential but may also represent a new business opportunity akin to "first mover advantage". The earlier these sorts of risks and/or opportunities are identified, the greater the room for action. A mature ERM framework will be addressing emerging risks and creating the conditions for dialogue between business functions and risk functions about strategies for dealing with them.

The common characteristics of emerging risks are:

- High uncertainty as there is little information available and the frequency and severity[4] is difficult to assess
- Difficulty in quantification as risk is uncertain and the risk transfer may be questionable
- No industry position as no single insurer wants to make the first move for fear of losing market share
- Difficulties for risk communication as there is the danger of reacting to phantom risks
- Supervisory involvement often being necessary.

In 2005, the Chief Risk Officers (CRO) Forum founded the Emerging Risks Initiative (ERI) with the aim of raising awareness of and communication about emerging risks that are relevant to the insurance industry. The ERI focuses on identifying, prioritising and communicating information on emerging risks relevant to the insurance industry. The CRO Forum Emerging Risk Initiative (http://www.croforum.org/emergingrisc.ecp) has so far published three positions papers: pandemic; terrorism; climate change & tropical cyclones.

An insurer implementing ERM needs to establish a process for dealing with emerging risks relevant to its own business, working through the risk processes identified in Section 7.2 below. In addition the following information about emerging risks frameworks may assist in formulating an approach.

5.3 Scenario Planning

One way to evaluate high impact/low probability events is through scenario planning, which can augment statistical models and help companies prepare for specific events. Scenario planning can take the form of facilitated workshops, crisis simulations and think tanks. It can also provide opportunities for collaboration on industry issues.

Scenario planning is a powerful tool that helps executives assess the resilience of the organisation to internal and external shocks. Assumptions about the real nature of the risks and operation of controls and contingency plans are tested and often result in changes being made.

A number of insurers have invested in capabilities to help them cope better with the unexpected. In particular, the practice of Business Continuity Management, or BCM, has evolved rapidly in recent years. BCM teams typically run a schedule of crisis simulations under a range of scenarios and managers who participate in simulations typically will report that they feel better prepared for a real crisis having experienced a simulated one. This is particularly the case when simulations affect multiple business units and require participation of senior executives. (Refer Section 8.3 for further details).

[4] *Frequency* and *Severity* are both probability distributions as opposed to *Likelihood* and *Impact* which are dimensions of a matrix.

6. Own Risk and Solvency Assessment (ORSA)

Key Feature 5

An insurer should regularly perform its own risk and solvency assessment (ORSA) to provide the board and senior management with an assessment of the adequacy of its risk management and current, and likely future, solvency position. The ORSA should encompass all reasonably foreseeable and relevant material risks including, as a minimum, underwriting, credit, market, operational and liquidity risks. The assessment should identify the relationship between risk management and the level and quality of financial resources needed and available.

6.1 Introduction

ORSA involves carrying out a combination of quantitative and qualitative techniques to identify, assess and manage risk. It is important that this involves the regular actuarial control cycle that essentially examines experience from decisions and actions taken and provides the feedback from this experience into future decisions and actions. This section discusses the basic building blocks of the risk management process and also suggests appropriate methods for assessing different kinds of risk.

6.2 The Risk Management Process - Risk Profiling

The core process of risk management involves a systematic identification, analysis, evaluation and treatment of risks having regard to an appropriate context. Typically, the context is framed around objectives of a business process or project or indeed the broader insurance enterprise. In addition, a critical aspect of context involves the setting of the risk tolerance (Section 4, above). The output of the risk management process is usually described as a risk profile, risk register, heat map and/or risk control self assessment (hereafter described as a risk profile).

Risk profiling and related governance and/or framework activities should not be confused with capital modelling (refer Section 7, below). The latter process is primarily concerned with statistical and actuarial methods and processes whereas risk profiling is more in the nature of an operational process, sharing similar characteristics with activities like business planning and project management. The process of risk profiling can be applied at the insurance enterprise level, business unit, key business process level (e.g., underwriting, claims) or be applied in the management of projects. Risk profiling involves an assessment of risk at both the levels of inherent risk and residual risk. A working definition of these terms is shown in the table below[5].

[5] Enterprise Risk Management-Integrated Framework, The Committee of Sponsoring Organisations, September 2004

Inherent Risk	Residual Risk
The risk to an entity in the absence of any actions management might take to alter the risk's likelihood or impact	The remaining risk after management has taken action to alter the risk's likelihood and impact

This aspect of the risk management process can be tedious and counter-intuitive in the hands of, say, an underwriting manager who may view the underwriting process through the lens of controls built-in. Nevertheless, assessing both inherent risk and residual risk highlights important management information not otherwise readily apparent:

- Those risks whose management rely heavily on the continued and effective operation of key controls (high inherent risk/low residual risk)
- Those risks whose nature does not significantly alter following the application of controls. This highlights that certain controls may be ineffective and that resources might be utilised better elsewhere, or that different controls are needed (high inherent risk/ high residual risk)
- Those risks that may be over-controlled (low inherent risk/low residual risk).

More broadly, the value in risk profiling revolves around bringing people together to debate risk and its management. New insights are gleaned and awareness of the nature of risks is raised. The process is important because it promotes and reinforces:

- Consistency and understanding, by collating and presenting a shared view of the most significant risks from time to time. The process also forces management to assess risks relative to each other
- Transparency to the board and an opportunity for the board to review management's formal assessment of significant risks
- Organisational efficiency by ensuring that management effort/risk mitigation is prioritised to the areas of greatest assessed risk
- Learning and continuous improvement through taking action to alter and ideally reduce the risk profile
- A culture of proactive risk management that supports innovation and sustainability.

It is not the purpose of this Note to discuss the mechanical, workflow and or task-level steps associated with developing a risk profile. However, a risk profile will typically include the following information:

- A description of risks in enough detail for each risk to be understood in isolation
- The cause(s) or underlying conditions giving rise to a given risk actually occurring or crystallising

- The consequence(s) of the risk. These are typically expressed in both financial and non-financial terms e.g., loss of customers, supervisory sanction, cost over-runs etc
- An appropriate categorisation of each risk. This is particularly important where an insurer comprises multiple business units and there is a requirement to perform some form of risk aggregation at the enterprise level
- An inherent risk assessment that considers likelihood/frequency of risk occurrence and impact of the risk. It is best to establish clear rating criteria for the risk assessment e.g., establishment of financial and/or non-financial proxies for , say, high, medium, or low risks
- An assessment of the effectiveness of controls and/or risk mitigation strategies. This assessment should consider both design and performance aspects of controls and note control ownership
- A residual risk assessment after taking into account the effectiveness of controls
- A description of the action(s) to be taken to bring unacceptable residual risk within appropriate limits.

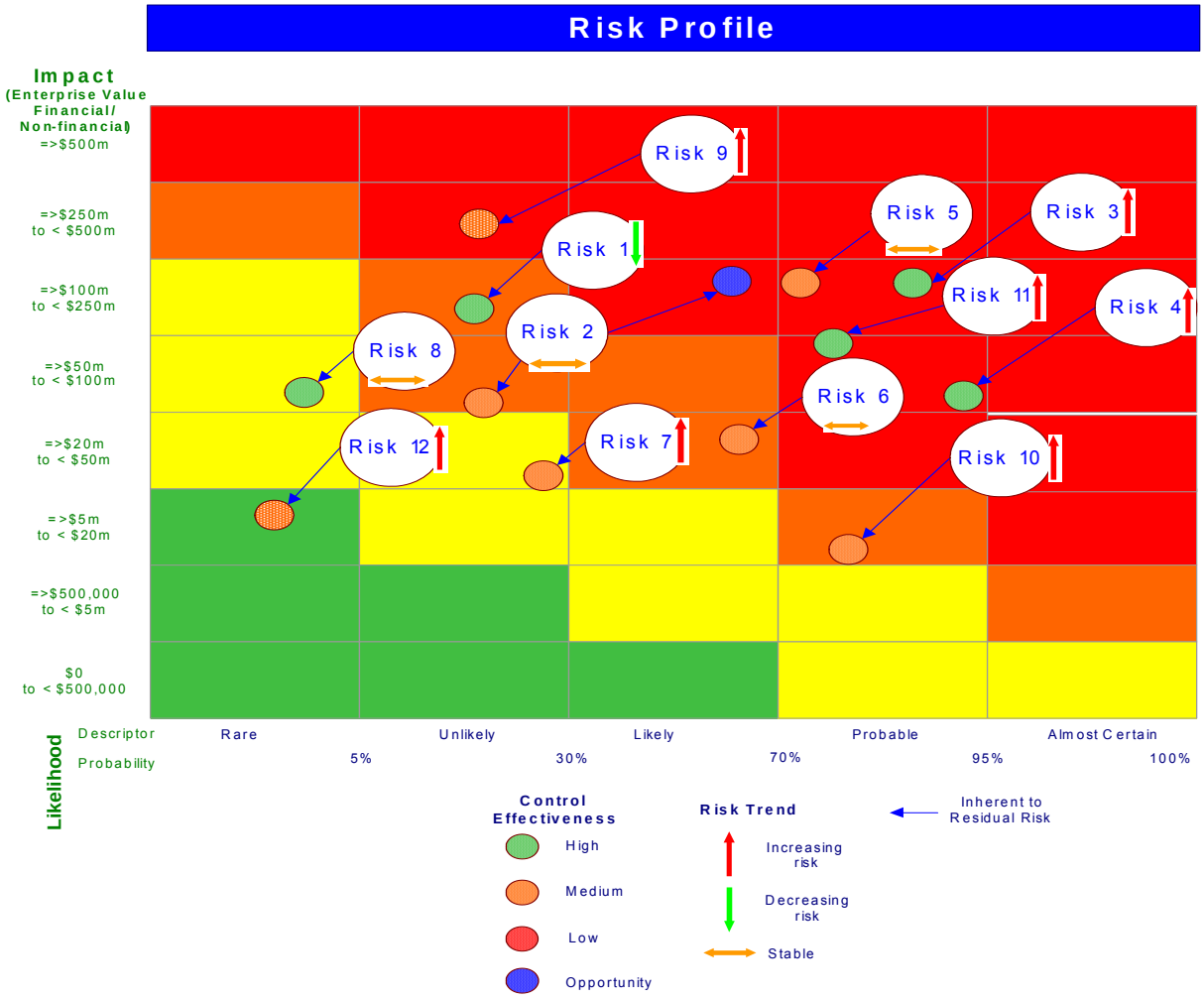
Risk profile documents are typically signed off by the responsible executive. This could be the insurer's CEO in the case of the enterprise risk profile or business unit head in the case of a business unit risk profile.

Insurance company managers tend to be very comfortable with the assessment and quantification of risk. After all, it should be core business for them. However this can also result in a tendency amongst insurance managers to seek to quantify non-insurance risks in financial terms. Many risks, in particular those of a strategic or operational nature may not behave stochastically nor readily lend themselves to statistical or actuarial analysis. In such cases it is perhaps better to opt for more simple or qualitative criteria to quantify the risks.[6]

Risk practitioners should also be careful to ensure that the risk profiling process does not become stale or be seen as an end in and of itself. Much of the work is done in creating the risk profile and less work is required to maintain it. Typically the risk profile does not change significantly over the short term unless the business is rapidly changing or growing. Therefore, risk practitioners need to be mindful of this and look for opportunities to ensure the risk profile remains relevant to management decision-making over time.

A risk profile report should provide snapshot management information about significant ("top 10") risks – an assessment of the inherent risk, effectiveness of controls, residual risk and the risk trend. The graphic below provides an example of how this information could be presented on one page.

[6] See Australian Risk Management Standards or Committee of Sponsoring Organizations of the Treadway Commission (COSO), etc., for examples.


Risk Profile
Impact
(Enterprise Value
Financial/
Non-financial)
=>$500m
=>$250m
to < $500m
=>$100m
to < $250m
=>$50m
to < $100m
=>$20m
to < $50m
=>$5m
to < $20m
=>$500,000
to < $5m
$0
to < $500,000
Risk 9
Risk 1
Risk 5
Risk 3
Risk 11
Risk 4
Risk 2
Risk 8
Risk 6
Risk 12
Risk 7
Risk 10
Descriptor
Rare
Unlikely
Likely
Probable
Almost Certain
Probability
5%
30%
70%
95%
100%
Likelihood
Control
Effectiveness
High
Medium
Low
Opportunity
Risk Trend
Increasing
risk
Decreasing
risk
Stable
Inherent to
Residual Risk

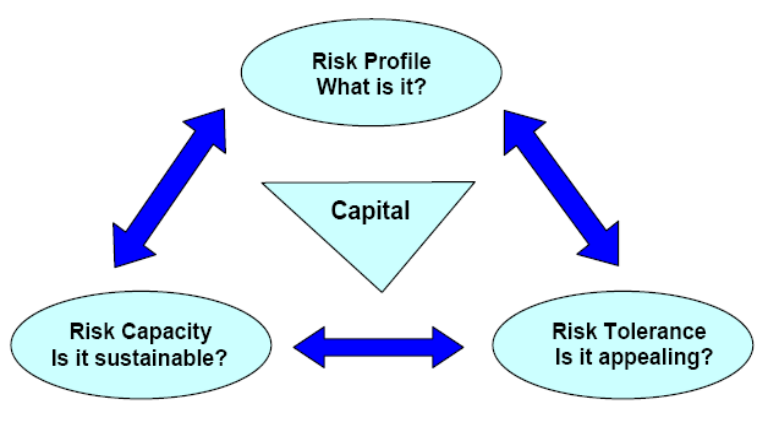
EXAMPLE:
"WHAT IS THE RISK PROFILING PROCESS?"

The risk profiling process is comprised of three main phases:

1. Preparation *- The objective of risk profiling is to provide the business with a structured approach to recording and assessing risk. This facilitates the common understanding and articulation of risk. Therefore, it is useful to prepare any existing material prior to the risk profiling exercise to assist the process of identifying and assessing risk and controls.*

2. Risk Profiling Exercise *- The risk profiling exercise should be facilitated by a risk champion from the business to provide guidance and help drive consistency of the process. Business involvement is key to the successful completion of the risk profile as it effectively ensures an accurate capture of risks. There will need to be an initial investment of time to complete the risk profile and an ongoing commitment to maintain it. The amount of time required will vary dependent on the approach used to complete the risk profiling exercise (e.g. workshops vs. one-on-one meetings).*

3. Review *- Following the risk profiling exercise, a review should be undertaken by the risk champion to ensure the outputs of the meeting have been recorded accurately and agreed by management.*



Key benefits of this approach are:

- *A structured process that promotes consistency for risk profiling across the organisation*
- *Collation of risk related material before the risk profile exercise provides participants with a good starting position for risk profiling*
- *Both risk expertise and business knowledge being used to risk profile*
- *Promoting transparency of risk profiling*
- *Time efficiency for risk profiling*
- *Clear linkage between risks and controls.*

However watch out:

- *Providing existing material may cause participants to focus on known issues, rather than future issues – always ensure they also consider potential risks*
- *Sometimes used as a 'once a year' approach which could discourage updating of the risk profile outside of the workshop – promote the risk profile as a living document and ensure it is relevant for the effective running of the business.*

6.3 Risk Modelling Techniques

Apart from the process of risk profiling, a range of statistical and other modelling techniques are commonly used by insurers to quantify insurance risks. The table below lists a range of modelling and statistical techniques considered appropriate for the quantification of insurance risks. Refer to Appendix 8 – Useful References for more details on these techniques.

Risk Category	Modelling Technique(s)
Enterprise /all risk categories	• Dynamic Financial Analysis
Underwriting (including reinsurance)	• Financial Condition Report (FCR) and/or underwriting modelling or reviews
Market	• Value at risk (VAR) or Tail VAR • Interest rate models • Scenario tests
Credit	• Credit risk models
Liquidity	• Asset/Liability modelling
Operational	• Internal loss data • External loss data • Scenario analysis, simulations

COMMENT:
THE "BLACK SWAN" DILEMMA – IS ERM ENOUGH?

Nassim Taleb[1] coined the phrase "black swan" to describe something that is a large-impact, hard-to-predict, and rare event beyond the realm of normal expectations. The metaphor here is that most people would expect a swan to be white (at least until black swans were discovered in the 17th Century in Australia) and therefore a black swan is a surprise or something perceived as impossible actually occurring.

Black swan events have occurred throughout history. More recently the events of 9/11 and the sub prime meltdown in the USA spring to mind. While some may argue that people did and could have predicted these events people were still surprised when they occurred, particularly the magnitude of the impacts that reached far into the financial services sector.

But here is the dilemma. Since black swan event are surprises they cannot happen twice because once they have occurred they are within know experience. Planning to avoid repeated events of this nature is a good idea but cannot prevent further surprises. Even a forensic understanding of such events will do little to prevent the next black swan.

Some argue that developing an emerging risks register will prevent surprises. One topical example of an emerging risk is nanotechnology. However, apart from the fact that if we know about them they are not surprises, the question of cost benefit comes into play. To what extent is it worth spending money to prevent something that might happen, particularly if we are not sure of its exact manifestation?

Good risk practices are our only real preventative measure – and honesty that surprises will happen. Through an appropriate ERM framework we can be well placed to manage surprising situations appropriately and decrease the impact.

So ERM is probably not enough to prevent all manner of risks impacting, especially surprises, however it is a lot better than not having any preventative framework at all.

[1] Learning to Expect the Unexpected by Nassim Taleb, The New York Times, April 8, 2004

7. Economic and Supervisory Capital

Key Feature 6

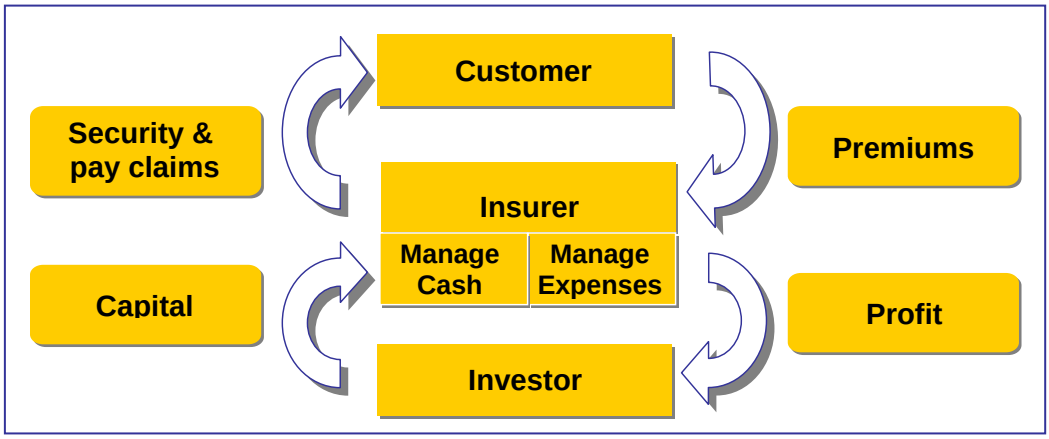
As part of its ORSA an insurer sho uld determ ine the overall financial resources it needs to manage its bu siness given its own risk tolerance a nd business plans, an d to dem onstrate that supervisor y requirem ents are met. The in surer's risk management actions sh ould be based on consideration o f its econo mic capital, supervisory capital requirements and financial resources.

7.1 Introduction

One of the basic principles behind capitalism is that the ma rket will allocate capital to the most productive activities and organisations as measured by their ability to provide a return on that capital. Based on this p rinciple, enterprises will propose bu siness ventures that re quire capital and indicate the return they will provide in this capital. The owners of capital will a ssess these proposals a nd provide their limited capital to the best available prop osals, allow ing for the potential r isks of each proposal. Over time the track r ecords of countries, industries an d companies are established and the continued provision of capital and the return expected i s refined.

In the Insurance context, the Insurer essentially needs to charge the correct premium for the promises it makes to pay claims and to manage expenses and cash flows efficie ntly. In the running of this insurance business the insurer is exposed to many risks that may reduce the profit it can pay to the capital pro viders, and hence the management of these risks i s an important part of runni ng the insu rance busin ess. The dominant risks will vary by insurer according to such factor s as their stage in life- cycle (e.g., st art-up versus run-off), r elative size and nature of business written.

Figure 1 below illustrates this relationship in the Insurance context.



A key component to managing these risks is to have a model that attempts to simulate the environment in which the insurer is operating. Such a model can provide indications of what profit will emerge under many different assumptions and provide a guide to management of the insurer of how specific decisions may impact the expected level and volatility of future profit. The models can also provide indications of the risk of failure of the insurer. These models are often referred to as Economic Capital Models. They are used by capital providers, supervisors and companies.

The capital providers and supervisors will have more generic models that they apply to individual companies with some refining to attempt to allow for the individual company characteristics. The management of companies will generally have a model that is developed internally and therefore should be more accurate. This internal economic capital model is usually able to provide more accurate assessments of the need for capital and provide better insights for input into key management decisions.

The "best practice" internal economic capital models are able to break up the overall capital and return of the company into smaller parts for which individual decisions can be made. A key example of this is where different products sold within the company have different risk and profit profiles. By knowing which products are enhancing or diluting the company's overall profit relative to capital required enables corrective action to be taken so as to ultimately improve the company's overall return on capital.

EXAMPLE:
RATING STRENGTH

One of the roles of pricing is to ensure premiums are competitive and that an adequate return on capital is achieved.

For the insurer overall, the capital required will usually be determined using the insurers risk appetite, market or regulator expectations and their Economic Capital Model (ECM). The insurer will also set an overall planned return on this capital.

However, the insurer will be relying on the pricing function to deliver these overall results, usually based on many decisions at lower levels of detail for various risk classes. For the pricing function to fulfil this role effectively it will need a robust and accurate Economic Capital Model (ECM) that can allocate the capital requirements of the overall insurer down to the underlying risk classes for it to understand the return on capital performance of each risk class, and to adjust pricing, risk class features or business volumes in order to steer the outcome for the overall return on capital for the insurer.

For example, column (A) in the table below shows the pricing measure, for example insurance profit margin, that is required to achieve at a desired return on capital based on the capital allocated to that risk class using the ECM. ***It is the ability of the ECM to allocate the capital down to the level of detail where 'localised' decisions can be made that is crucial to the success of the pricing function.*** *Based on this example in*

Risk Class	Pricing Measure to Achieve X% RoC	Actual Pricing Measure	Rating Strength	Actual Business Volumes
	(A)	(B)	(B / A)	
X	10%	11%	1.10	100
Y	5%	4%	0.80	200
Z	7%	7%	1.00	70
Total			0.92	370

Taking the example above to a lower level of detail, if the ECM can provide capital requirements at for Risk Class Y at a lower level of detail, i.e. Y1 and Y2, then more effective management decisions are likely to be made by understanding the source of the underperformance of risk class Y. For example the more focused action is likely to be made to correct the pricing or limiting volumes of risk class Y2.

Risk Class	Pricing Measure to Achieve X% RoC	Actual Pricing Measure	Rating Strength	Actual Business Volumes
	(A)	(B)	(B / A)	
X	10%	11%	1.10	100
Y1	5%	6%	1.20	67
Y2	5%	3%	0.60	133
Z	7%	7%	1.00	70
Total			0.92	370

7.2 Economic Capital Model

The purpose of an Economic Capital Model (ECM) is to provide a holistic assessment of the key risk drivers within an organisation and to devise risk management techniques to address these risks.

An ECM generally comprises integrated asset and liability models and simulates the out-turn of asset and liability cash flow experience over future periods. Typical output from an economic capital model comprises forecast future balance sheet, profit and loss accounts cash flow statements, and projected distributions of profit; capital and return on capital. This is based on running many iterations of the model. The distributions enable management to take a view on the probability of key indicators falling outside an acceptable level (one possible definition of risk tolerance) and hence are a critical input to the determination of capital needs. Such models are sometimes also referred to as "internal models", but that term can also apply to less holistic modelling of part of an insurer's business performance and risks. Reference should also be made to the IAIS Guidance paper on the use of internal models for risk and capital management purposes by insurers (Oct 2007).

The asset model component of an ECM should be based on well researched financial market models. Inputs incorporate both economic and financial parameters and the model allows for correlations in returns from different asset classes and correlations in returns over time. For multinational insurers, an allowance for potential exchange rate fluctuations is advantageous.

The liability model examines the relationship between premiums and claims and their variability. Examples of causes of variability to be taken into account would include general economic conditions, future claims deterioration (or improvement), changes to market share and the effects of the underwriting cycle. Reinsurance and correlations between classes should also be considered.

A link between asset and liability models through some economic variables (inflation, interest rate etc.) has to be established. The uses and benefits of a dynamic model include:

- Improved understanding of the dynamics in the balance sheet arising out of the insurer's current strategy
- Consideration of the effects of implementing different asset and liability (and reinsurance) strategies
- Examining relative impacts of different sources of capital (e.g., reinsurance; future profits; retained earnings; capital markets; reserves etc)
- Due diligence support for acquisition and divestment decisions
- Capital allocation by region and product
- Assessment of risk adjusted performance of different business units
- Determining the optimal asset mix
- Financial condition reporting
- Understanding the possible impact of extreme events on the financial position of the insurer.

It should be noted that the model is only a tool and is heavily reliant on the integrity of inputs. In addition, some subjectivity is unavoidable. It is often not the modelling results themselves which are of key benefit; rather it is the deeper understanding of the risks and drivers of the business that has resulted from going through the modelling process.

A dynamic model will need to consider and allow for the extent to which a company chooses to match (or mismatch) the cash flows from its assets and those required to meet its liabilities. The model will need to take into account any specified liquidity requirements of the insurer. An ECM will typically also include rules in relation to the investment and reinvestment policy of a company and rules specifying the switching and rebalancing of the investment portfolio to changing financial circumstances of the insurer.

A dynamic model also enables management to systematically understand the factors driving volatility of earnings and provides a sound basis for the development of targeted risk management strategies to reduce earnings volatility.

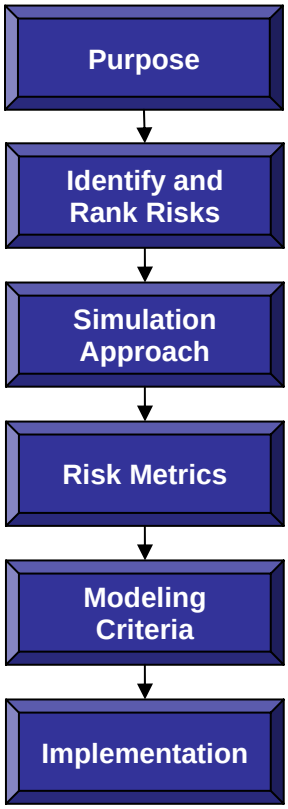
A key decision that will affect the form and use of the ECM will be to what degree the ECM will be integrated into the day to day operations of the business. Various alternatives for this could include:

- Real time running of the ECM for changes (actual or potential) to the business

- Translation of the ECM output into "rules of thumb" that can be used by the businesses on a day to day basis
- Processes used to control centralisation of the ECM, which would usually involve many aspects of the business having their own detailed model which a centralised model could then incorporate to produce more summarised output at a group level that is nevertheless built on a consistent foundation throughout all the insurer's activities.

7.3 Economic Capital Model Process

The ECM process entails a number of steps. The flowchart below provides an elevated summary.



Each step of the ECM process is explained in the following sections.

a) Purpose

Will the ECM be used for supervisory capital requirements or the insurers own solvency assessment? An ECM for supervisory capital purposes must comply with the IAIS solvency requirements for Internal Models[7]. This Note supports the use of an ECM for an insurer's

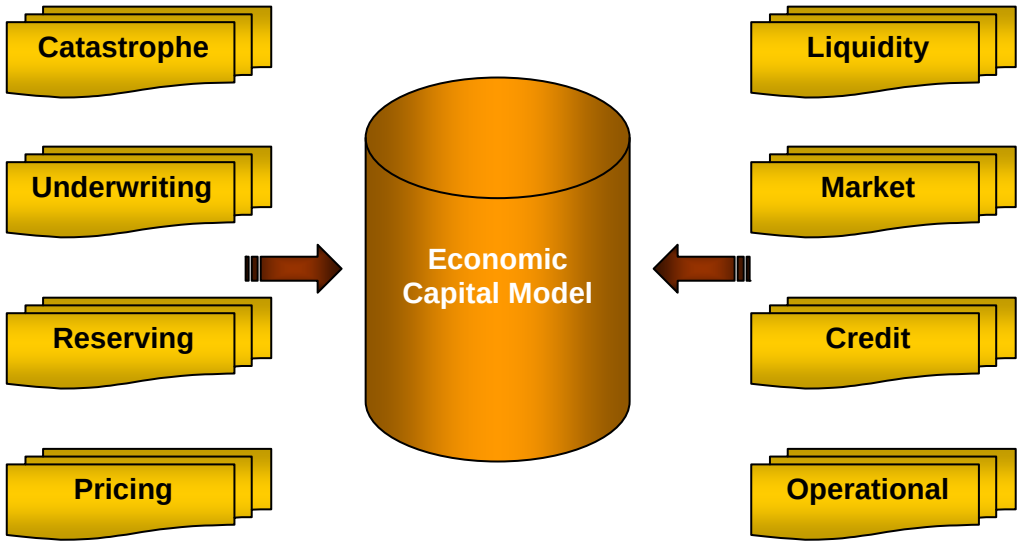
[7] IAIS Guidance paper on the use of internal models for risk and capital management purposes by insurers (October 2007)

own solvency assessment and capital management purposes. It is important to clarify the purpose of the ECM as it will have a significant impact on:

- Who should be responsible for the ECM
- What level of controls and processes need to be incorporated around the ECM
- How flexible and dynamic does the ECM need to be
- What level of detail and accuracy is required from the ECM
- What level of resourcing is required?

b) Identify and Rank Risks

The risks that need to be assessed and ranked according to the particular requirements of each insurer are illustrated below. The dominant risks will vary by insurer.



The sophistication of the model will reflect the risk hierarchy i.e., key risks require more detailed modelling and analysis.

Any diversification recognised between risks (and within risks) is generally built into the model. This may, for example, be via correlation matrices, copulas or other approaches.

Given the scope of operational risk, there needs to be clearly defined guidelines to ensure consistency across the domestic and international insurance industry. An example here is the Basel II definition of operational risk for banks[8].

[8] International Convergence of Capital Measurement and Capital Standards – A Revised Framework, Basel Committee on Banking Supervision, June 2004

> Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputation risk.

Basel II outlines three methods for calculating operational risk. These methods are outlined below in increasing degree of sophistication:

(i) Basic Indicator Approach

- Operational risk capital is a fixed percentage (15%) of positive annual gross income averaged over the previous three years.

(ii) Standardised Approach

- Operational risk capital is a fixed percentage (12%, 15% or 18%) of annual gross income measured for each of eight specified business lines. The positive total across all business lines is averaged over the previous three years.

(iii) Advanced Measurement Approaches

- Operational risk capital is calculated using an approved internal model.

The Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS) outlines in their last quantitative impact study (QIS3 spring 2007) a methodology to calculate the capital charge for operational risk. Operational risk is the minimum of two values:

- A fixed percentage (30%) of the Basic Standard Capital Requirement
- The maximum of a fixed percentage (2% for Non Life and 3% for Life) of total earned premium and a fixed percentage (2% for Non Life and 0.3% for Life) of insurance technical provisions.

The choice of method is a function of the corporate structure (mono-line insurer, multi-line insurer, conglomerate of insurance and non insurance), the maturity of capital modelling within an organisation, resources and cost.

The challenge for the international insurance industry is the establishment of processes to separately record operational losses. There is limited historical data on operational risk which currently limits the sophistication and reliable application of stochastic modelling of this risk.

c) Simulation Approach

There are several techniques to quantify risk which could be used by an insurer to construct its model. In broad terms, these could range from basic deterministic scenarios to complex stochastic models. Deterministic scenarios would typically involve the use of stress and scenario testing reflecting an event with a set probability to model the effect of certain events (such as a drop in equity prices) on the insurer's capital position, in which the underlying assumptions would be fixed. In contrast, stochastic modelling (such as Monte Carlo simulation) often involves multiple scenarios with varying likelihoods, in order to reflect the likely distributions of the capital required by the insurer.

The choice is a function of cost, time and benefit.

Deterministic testing highlights key risks and provides a reasonable check on more sophisticated simulation methods. It is particularly important to understand the interaction between risks and to understand how this interaction changes under stressed scenarios (e.g., previously unrelated impacts may become related under severe stress). A key input into the ECM is often qualitative and subjective decisions that would be considered by the insurer's management at the time of distress (for example changing asset mix or reinsurance levels).

d) Risk Metrics

Traditional risk metrics associated with an ECM includes:

- VaR versus TailVaR
- Time horizon
- Confidence level.

These are a function of the insurer's strategy and risk tolerance.

e) Modelling Criteria

Some examples of modelling criteria include:

- Exit value as measured by absolute ruin
- Ongoing business criteria as measured by supervisory intervention
- Attaining a certain investment rating.

An insurer should seek to apply multiple criteria for each segment of its business.

f) Implementation

- Two main approaches can be taken to the development of the ECM:
- A fully integrated model that considers the interactions of the entire operation or
- A univariate model that considers each division individually and then integrates all components using some combination method (e.g., copulas).

A fully integrated model can readily be applied to mono-line insurers while a univariate model lends itself to multi-line organisations that are involved in insurance and non-insurance business.

The type of model used should be appropriate to the nature, scale and complexity of the insurer's business.

7.4 Relationship with Capital Management

Supervisory capital requirements are just one input into capital requirements. As discussed there can be a multitude of others including:

- Desired rating agency ratings
- Desired earnings volatility
- Desired shareholder return – dividend and capital growth
- Accumulation of risks
- Market expectations.

An ECM will generally present a more accurate and/or complete picture of a business than the application of a supervisory capital prescribed methodology.

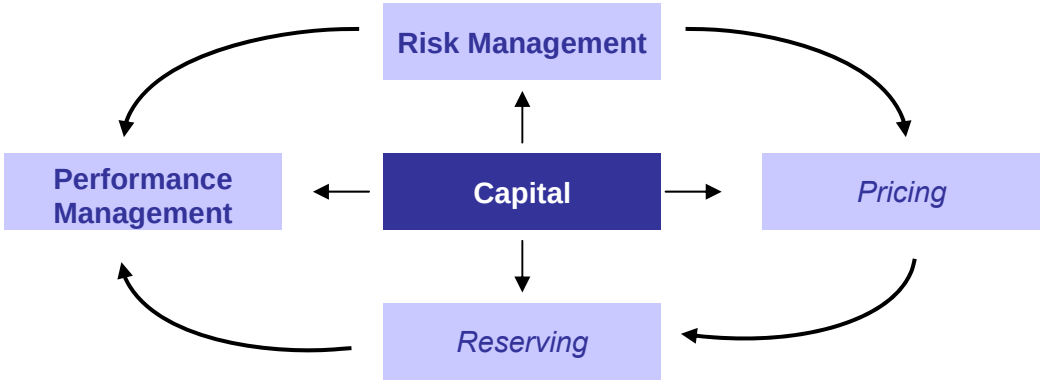
Key potential differences between a supervisory prescribed method and an ECM would often include:

- Different views as to the volatility of various classes of business (both absolute and relative to other classes)
- Different allowances for diversification (often performed by correlation matrices, or sometimes via copulas) between risk types and within risk types
- Different focuses driving capital (i.e., different aims)
- Inclusion of different risk types (e.g., operational risk may not be included or may be implicitly included in supervisory prescribed methods, but may be included explicitly in the ECM)
- Different views may be expressed regarding the availability of various assets for capital (e.g., tax benefits, goodwill, etc).

Even an ECM will likely need to calculate and project supervisory prescribed method capital as the relevant supervisor will want to understand the relativities.

Effective capital management is focussed on turning risk into shareholder value. In operational terms this means ensuring that the “right” amount of capital is ascribed to the appropriate risks so that suitably informed decisions can be made.

The following schematic seeks to articulate the relationship between capital and the core elements of capital management.



Capital plays a central role in the cycle of turning risk into value. It finances growth, capital expenditure and business plans. It also provides support in the face of adverse outcomes from insurance activities, investment performance and support activities.

From a market perspective, one of the roles of pricing is to ensure premiums are competitive and that an adequate return on capital is achieved. Operationally, the objectives of the pricing process are to meet expected claims and operational / administration expenses. Of course, pricing includes other aspects, including consideration of the need to cover fixed costs as well as meeting supervisory requirements where appropriate.

The reserving process establishes a central estimate for outstanding claims, provides a margin to cover the value of uncertainty (the risk margin) and ensures that insurance liabilities are adequate having regard to experience and expectations about future experience and cover against any expected premium rate deficiency.

The allocation of capital to business units / lines commensurate with risk underpins the performance management process and enables measurement of outcomes and returns against those expected. Effective performance management incorporates early warning mechanisms so that the risk management, reserving and pricing processes can be adapted to improve outcomes.

From a capital management perspective, the role of risk management is threefold – establishment of the overall risk tolerance, identification / assessment of risks, and keeping risks in control. The process of establishing risk tolerance relies on systematically deciding which risks to take and which risks to shed. As discussed previously, the articulation of risk tolerance can ultimately be expressed in terms of target financial strength (an acceptable "risk of ruin") but can also encompass strategic components e.g., target credit rating and acceptable earnings volatility.

8. Continuity Analysis

Key Feature 7

As part of its ORSA, an insurer should analyze its ability to continue in business, and the risk management and financial resources required to do so over a longer time horizon than typically used to determine regulatory capital requirements.

Such continuity analysis should address a combination of quantitative and qualitative elements in the medium and longer term business strategy of the insurer and include projections of the insurer's future financial position and

8.1 Introduction

A key benefit of the use of an ECM is the ability to examine scenarios outside of those prescribed by regulation. For example, supervisory capital requirements are often performed on a run-off basis, rather than on an ongoing basis. Likewise, an ECM allows an insurer to look further into the future than most supervisory prescribed methods are based on. This will require explicit decisions to be made regarding (amongst other things):

- What time period of modelling should be used
- Should the financial position of the insurer be assessed at a future point in time, or once all relevant liabilities are modelled to have run-off
- What management actions are likely should results turn to the worst
- What capital reduction (e.g., dividend) / capital injection policy can be assumed
- How reliable are an insurer's longer term forecasts and are they sufficient to form the basis of an ECM.

The modelling approach and the assumptions, fundamentally depend on the time horizon over which risks are modelled. For a one year time horizon actions of an insurer's management can be neglected. However, for modelling over the longer term, the actions of the insurer become more important.

For longer time-horizon models, assumptions based on a static business and asset mix in the absence of actions of the insurer would make the calculations and projections less effective. However when long-horizon models consider assumptions such as the insurer's strategy and management actions, since these are rather subjective, the results of the model need more interpretation and the limitations of the modelling need to be clearly articulated.

Long-term modelling can necessitate the development of separate models from those used for shorter time horizons. For example, in order to model financial market risk over a longer time

horizon requires models that project the relevant risk factors consistently. This requires the use of more explanatory models rather than models that rely to a large degree on purely historical data.

A key part of models that project over longer than one year time horizons is the modelling of management actions and strategies. This encompasses:

- Premium setting: what is the strategy of the firm in case of losses or inadequate profits emerging? Does the firm try to retain or gain market share when prices are low? What is the strategy of the firm during an insurance cycle?
- Asset allocation: How does the firm react in cases of financial stress?
- Discretionary policyholder benefits: What is the insurer's strategy for discretionary policyholder benefits in particular in cases (a) where the firm alone experiences financial distress and (b) where the whole market experiences financial distress
- Dividend policy: What is the dividend strategy, in particular in cases where the firm experiences losses
- Risk mitigation strategy: Reinsurance strategy, ALM strategy, securitizations and other transfers of risk to the market etc.

8.2 Quantitative Analysis - Capital Planning

A truly integrated ECM will be used for a wide range of purposes within an insurer. For example, it can used to provide analysis relating to:

- **Economic capital requirements**
  The ECM is the primary vehicle to calculate the capital requirements based on the risk profile of an organisation. The output of which should be closely integrated into the capital management process of the insurance company.

  However the model can also be utilised to link capital more closely to the way in which the business is managed. It can be used to help clarify or define the risk appetite of the organisation. This could consider for example, the calculation of the risk of ruin, the risk of "regulatory ruin" or as a measure of earnings volatility.

- **Disaster Planning**
  The ECM can also be used to analyse the eventuality of financial distress. This should include a detailed analysis of the legal and supervisory requirements of the jurisdictions in which the firm operates. Included in the analysis should be the potential limitations in capital fundability. The output of this exercise can then be used to alter the capital management strategy, implementing, where appropriate, instruments that mitigate potential capital mobility problems, e.g., via contingent capital solutions.

- **Investment strategy**
  An organisation's approach to their investment strategy considers a number of elements such as risk tolerance and the objectives of the insurer. The future capital need of the organisation also plays a part in this equation. The investment strategy will vary according to the future need for capital in the business.

- **Mergers, acquisitions and divestments**
  ECM can be used to assist the business understand the impact of any mergers, acquisitions and divestments. That is, it can be used to model the effect of diversification of risk on capital requirements and by quantifying the actual dollar amount of additional capital required (or released) due to merger / divestment activity. Economic Capital can also be used as a mechanism to assist in the valuation of acquired (or divested) entities.

- **Capital allocation**
  Capital allocation is one of the primary methods used to measure the performance of Business units. There is not one way of allocating capital to businesses, but the approach should be risk based and provide incentives for the business to effectively manage their risk (demand for capital) and measures to ensure they earn a suitable return on deployed capital.

  The approach taken to capital allocation will depend on the organisation's aim, for example, if it is to build an "optimal portfolio" (in terms of the spread of risk) the risk measures may be derived more from the extremes of the distributions of outcomes by class rather than the middle of the distribution that simple growth targets may suggest. Issues that need to be overcome in the allocation of capital include the treatment of support (i.e., non revenue generating business units) and the approach used; top-down allocation or bottom-up calculation (or a combination of both).

- **Reinsurance programs**
  An ECM can be used to assess the capital required based on the risk profile of the organisation. The more risk that is on an organisation's books the more capital is required to be set aside. Reinsurance is one of the main mechanisms available to insurers to pass on some of this risk to another party, the refore decreasing the amount of capital they are required to hold. Therefore in this instance, the value of reinsurance is derived from it acting as a proxy for capital.

  The cost of holding capital versus the cost of reinsurance can be considered by an organisation, allowing a more information decision to be made.

- **Optimal business mix**
  Setting the optimal business mix is related to the effective allocation of capital to the business. If capital is allocated on the basis of the underlying riskiness of the business, then the risk adjusted performance can be measured. The risk adjusted performance management can then be used to optimise the product or business mix and assist management to make decisions in line with the organisation's strategy. Although capital will not be the only factor considered it provides a good measure for assessing relative performance.

- **Reserving volatility**

In this case, the model acts to effectively treat the risk margins in the claim and premium reserves as "policyholders' capital" (as opposed to the "shareholders' capital" designated by the difference between assets and liabilities in the balance sheet).

- **Capital outflow / inflow policies**
  This is could be considered a subset of Economic Capital Modelling, but is important to treat it separately as it considers risk tolerance in a specific way (i.e., examining the capital adequacy "range" for the entity).

The Solvency II Cost of Capital risk margin (with its origins in the Swiss Solvency Test) actually requires the projection of the capital needs for the existing business. This requires organisations to also assess the long term impact of their business. As a minimum risk management must be able to at least quantify the capital requirements of insurance business over the whole life time of the liabilities.

The OSFI (Canadian regulator) already requires longer term projections via their DCAT (Dynamic Capital Adequacy Testing) requirement (10 year projections of plausible adverse scenarios). (See also *The use of internal models for determining liabilities and capital requirements* by Allan Brender, April 2002, North American Actuarial Journal).

Some supervisors require a more formal assessment of the financial viability of an insurer, often called a Financial Condition Report (or FCR). The FCR usually covers the broad spectrum of risks that are faced by an insurer, and is most useful when it provides a holistic view of the insurer for the Board and supervisor. An FCR usually covers not only the explicit numerical financial condition of the insurer (including financial statements and the outcomes of the ECM mentioned above) but it also usually covers the range of harder-to-quantify risks faced by an insurer, for example operational risks and reputation and brand related risks. The FCR usually includes an assessment of the effectiveness of the risk management framework of an insurer.

8.3 Qualitative Analysis - Business Continuity Planning

Business continuity management is an essential part of operational risk management. Business continuity planning enables a business to anticipate, identify and assess business interruption risks. A properly documented and tested Business Continuity Plan (BCP) reduces the impact of interruptions on key business processes and, most importantly, protects reputation. A robust BCP also allows a business to explain to stakeholders and industry supervisors that risks associated with potential business interruptions can be managed.

8.4 Crisis Management and Contingency Planning

A Crisis Management Plan minimises business impact and loss in the event of a significant incident by providing a clear and organised response strategy supported by predefined response procedures. It outlines the basic actions to be performed by, say, a Crisis Management Group (CMG) during an incident to assess its nature and severity, decide if the

incident requires crisis level response and in itiate the appro priate actions by management and employees.

One way of treating consequences is to undertake planning and preparedness for contingencies so that an insurer can act quickly to take advantage of unexpected gains or stem losses and prevent or limit disruptio n. This req uires plan s to be well f ounded in g ood risk management principles, tested and up-to-date. When an event occurs, t he organisation's management ma y need to respond quickly to mitigate the impact of the eve nt on the a chievement of busine ss objectives such as r evenue stream, produ ct quality, corporate reputation o r customer satisfaction. In most circumstances, these impacts may be mana ged as par t of normal management processe s. However, when the sc ale of the event overwhelms management's normal capacity to cope, a systematic approach to critical incident management is needed.

At the core of critical incident management is Business Co ntinuity Man agement (BCM), which provides an organisatio n with a disciplined cap ability to co ntinue to op erate sustai nably in th e face of potential significant business disruption. Appropriately implemented, BCM can provide a robust framework for addressing disruption risk exposures in a cost effective and timely manner. It provides a key component for the organisation to su stain good corporate g overnance, maintain its customer b ase and market share, retain the confidence o f its st akeholders, and manage its reputation in the face of an increasingly turbulent economic, industrial an d security environment. As a min imum response, effect ive BCM will prevent an emerging crisi s from becoming more persistent or widespread.

EXAMPLE:
UNDER WATER AGAIN!

> *"QUEENSLAND is facing a damage bill of hundreds of millions of dollars as flood waters surge through the state, cutting roads, swamping coal mines, destroying agricultural stock and forcing people from their homes. The state's booming mining industry expects tens of millions of dollars in coal production to be lost from the Bowen Basin. The flooding has caused massive stock losses for some farmers, while irrigation infrastructure and crops have also been destroyed."* (news.com.au 22 January 2008)

Climate change is a major challenge for the insurance sector and the increasing incidence of extreme weather events is a likely manifestation of the changing global environment. In the Australian context, extreme weather events account for the bulk of major property damage and are therefore the key focus for property and casualty insurers. The floods in Queensland were just one of the most recent weather related disasters that the Australian insurance industry has had to respond to, one compounded by the number of remote locations involved.

From a business continuity perspective, what is the appropriate response of an insurer with a focus on customer service and what should their response be if their own buildings or data centres are affected?

In 2008 one 'resilient' insurer had, in line with regulatory requirements, a proven and tested recovery strategy, well-rehearsed continuity plans, clear crisis management procedures and a culture of awareness of the need to ensure that critical services continue to operate. Moreover, with a geographically spread customer base, this insurer had implemented a resilient service model with processing of claims as a number one priority for business function recovery. This operational model ensured that processing was not dependent on any single building, location or data centre. While parts of its infrastructure may be damaged, other parts can take on the workloads in the short term and the impacted areas are quickly brought back on line in alternate facilities.

An important initial response to customer needs used by this insurer was to send mobile assessors into a disaster area. Those assessors were equipped with the necessary technology and authority to accept and process claims, make payouts on claims, approve emergency accommodation and respond to other particular requests for assistance that are within the scope of its policy commitments. The insurer has surplus mobile telephony infrastructure on stand-by for prompt deployment to all personnel so that they are always connected. This insurer also worked in close cooperation with disaster relief and emergency services personnel to ensure that access of its personnel into the affected area was conducted in a responsible manner and did not place people at risk.

Although very rare, large-scale catastrophic events can throw significant challenges at the insurance community and may overwhelm individual insurers. In these circumstances, responsible insurers will work with the national industry umbrella organisation under catastrophe coordination arrangements that have been prepared and rehearsed. By establishing working parties composed of state and federal government agencies, insurance industry organisations, insurance ombudsman services and associations of brokers and loss adjusters, a broad combined response will be mobilised to meet these challenges.

9. Role of Supervision in Risk Management

Key Feature 8

The supervisor should undertake reviews of an insurer's risk management processes and its financial condition. The supervisor should use its powers to require strengthening of the insurer's risk management, including solvency assessment and capital management processes where necessary.

9.1 Introduction

This Section seeks to provide assistance to insurers in developing constructive, transparent and proactive relationships with supervisors.

9.2 The role of the Supervisor

Prudential supervision [9] is accepted worldwide as an integral component of the regulation of financial institutions. The fundamental premise underpinning the supervisory role is that the primary responsibility for financial soundness and prudent risk management within a supervised institution rests with the Board and senior management. In this context the primary emphasis of supervision is on avoidance of problems rather than penalizing those who may be found to have caused problems.

In relation to insurance, prudential supervision involves establishing a system of:

- Financial oversight
- Mandatory licensing
- Ongoing operational requirements e.g., prudential standards
- Procedures and processes for monitoring compliance with licence conditions and ongoing operational requirements
- Where necessary, undertaking enforcement action either to force a non-compliant insurer into compliance or remove it from the industry.

[9] A term used to describe the supervision/regulation of financial institutions such as banks, insurers, building societies, friendly societies where the supervising authority seeks to ensure that the protection of depositors/policyholders is maintained by the institution in question being financially sound.

Supervisors adopt a risk-based approach to supervision. In practice this means that institutions facing greater risks receive closer supervisory attention. Therefore, in order to effectively manage the supervisory process, supervisors must form their own view of risks, and the effectiveness of the management of risks, for each supervised institution.

It is also worth noting that supervisors find themselves in the unique position in a given market of seeing the broad totality of risk management practices in operation across the supervised sector. They are exposed to the full spectrum of worst to best practices. Insurers seeking to improve their risk management practices should therefore not lose sight of the opportunity to engage with supervisors with a view to improving the management of risks.

9.3 Risk-based Supervision

The supervisor's understanding of an insurer typically begins with consideration of the nature of the insurer's business, governance arrangements, strategic/business plans, financial condition reports and strategies and processes to manage risk. Licensing and ongoing supervisory activities typically involve review of documents relating to these areas.

Insurers should proactively engage with supervisors to help them understand, and test, these key aspects of the business. If a supervisor does not have a level of comfort about the strategic and higher level aspects of an insurer's risk management framework, they are more likely to adopt a more intensive supervisory approach than would otherwise be the case. Insurers should therefore seek to promote ongoing and transparent dialogue with supervisors about strategy and framework matters. This will foster a more open and productive relationship over the medium to longer term.

9.4 Supervisor Relationship Management

Relationship Management Principles

Insurers should consider adopting a set of high-level principles to guide engagement with supervisors. In developing a set of appropriate principles, insurers should have regard to:

- Alignment with supervisory objectives
- Preservation and enhancement of corporate reputation
- Proactive and early engagement
- Communication transparency
- Relationship management accountability and coordination.

Strategic Approach

The supervisor is one of the key stakeholders for any insurer and therefore insurers should have a comprehensive understanding of supervisory objectives and processes. A strategic approach to supervisory relationship management involves, amongst other things, maintaining a profile on key supervisors. This includes key contacts at the supervisor and within the insurer, forward supervisory priorities and objectives, pressure points, specific risk areas for focus, relationship analysis, relationship development plans and opportunities for engagement.

Nature of interaction with supervisors

Insurers will typically have a range and variety of interactions and communications with the Supervisors which regulate the various jurisdictions in which they operate. These can be broadly classified as follows:

- Operational / Procedural
    - Submitting standardised, periodic returns and statistics
    - Responding to routine queries relating to standard operations (e.g., claims performance benchmarks).

- Non-standard / Unusual
    - Responding to a supervisor in relation to matters arising from a customer complaint
    - Responding to supervisor about industry issues and company exposure to them e.g., surveys about exposure to Hurricanes/Cyclones/Typhoons
    - Communications from supervisors initiating investigation and/or enforcement action
    - Results from supervision visits reported by supervisors to senior management
    - Reporting material incidents and breaches to a supervisor
    - Seeking relief/ exemption from current/proposed legislation
    - Advice of fines or “please explain” requests
    - Developing strategy, tactics in response to industry or entity-level enforcement actions
    - Responding to non-standard communications (e.g., enforceable undertaking)
    - Any non-routine enquiry which has the capacity to result in the insurer being subject to disciplinary action or adverse consequences.

- Strategic
    - Submission on current/proposed legislation/policy
    - Encouraging a change in a supervisor’s policy position
    - Public statements (e.g., to media and or government) relating to an insurer’s views and policy position
    - Consulting with supervisors in relation to strategic initiatives (e.g., acquisitions, corporate transactions).

In the context of this wide variety of interaction many insurers (and most large insurance groups) develop accountability mechanisms and protocols to ensure the "right people" are engaging supervisors appropriately. For example, supervisor engagement with respect to proposed acquisitions should involve the most senior management of the insurer.

A common approach is for insurers to allocate overall accountability for the supervisory relationship to a single executive, typically the Chief Risk Officer or Chief Financial Officer. In this way supervisory engagement can be effectively planned and coordinated. Under this approach, all non-standard and strategic engagement is transparent to the ultimate relationship manager.

Supervisory Policy Development

It is critical for insurers to engage with supervisors in the area of policy development. This is because in surers are in the best position to assess the practical implications of proposed supervisory change. Supervisors look for constructive feedback on their proposals and look to insurers to test the robustness and proportionality of new proposals.

Supervisors typically set time frames for submissions on new proposals. Insurers should adopt a strategic and proactive stance with respect to responding to submissions. A submission process that involves only written correspondence delivered on the final due date is likely to result in poor outcomes. Rather, insurers should use the policy development process as an opportunity to meet with supervisors to explore implications of proposal and to understand the rationale for change.

In today's environment supervisors are moving in a direction of principles-based supervision. Therefore, insurers should avoid arguments about being unique unless there are compelling reasons for doing so. Instead, insurers should make use of industry bodies to coordinate submissions on proposed new policy.

Supervisory Visits

Supervisory visits provide the supervisor with an opportunity to deep dive into particular aspects of an insurer's operations and/or risk management processes. Insurers should work with supervisors in the first instance to assist them with shaping the overall supervisory plan, typically spanning a one-year time horizon.

Having agreed the overall plan, insurers should seek to work with supervisors to coordinate site visits - agenda development, document submission and overall visit logistics. This process provides an excellent opportunity to strengthen the relationship at an operational level.

Requirements and recommendations arising from supervisory visits should be welcomed, and taken seriously. To the extent that insurers seek to unreasonably challenge supervisory requests and requirements, this may be viewed by the supervisor as in indicator of underlying cultural issues and potentially have the effect of resulting in even more intensive supervision. Insurers should therefore look for every opportunity to promote openness and free exchange of views during site visits.

Reporting of Incidents and/or Breaches

One of the key tests of an effective supervisory relationship is how the insurer deals with the management and reporting of breaches of requirements. In the vast bulk of cases, breaches are inadvertent human and/or process errors as opposed to blatant disregard of rules.

Supervisors typically establish requirements for the mandatory reporting of breaches. These establish materiality thresholds to ensure that only significant matters reach the attention of supervisors. Insurers should therefore seek to operationalise supervisory breach reporting requirements by translating these into processes that result in internal reporting and escalation of material matters and clear accountabilities for reporting to supervisors.

The identification, management and reporting of breaches should be viewed as a process improvement opportunity. No one expects zero breaches. Ironically, an absence of breach reporting to supervisors for an extended period could be viewed as an indicator of ineffective risk management and/or cultural activities.

International Considerations

Insurers operating in multiple jurisdictions have the added complexity of managing multiple supervisor relationships. In these situations the principles outlined above equally apply. There is even a greater need to establish clear accountabilities for relationship management at the country/local level and at the corporate/group level. Insurers should assume that supervisors themselves will establish protocols for the sharing of appropriate information cross-border and therefore establish agreed and transparent processes that recognize this dynamic in the context of international insurance groups.

Governance Aspects - Transparency of Supervisory Engagement

Boards have a key role to play in setting the tone for engagement with supervisors. They should monitor important engagement between the insurer and the supervisor. In particular, strategic and non-standard engagement should be transparent to the board or appropriately delegated committee. For example, summary details of strategic and non-standard engagement should be reported on a periodic basis to the board or relevant board committee. This will enable the board to ensure that its expectations with respect to supervisor relationship management are being met on an ongoing basis.

TIPS: HOW TO ENGAGE WITH SUPERVISORS LOCALLY AND GLOBALLY

KPMG: *Bringing regulation into the boardroom – A global survey of the supervisory function in the communications sector* (December 2007) noted that "With an increasing focus on regulation, companies must be able to both shape and respond to the supervisory agenda in traditional and, increasingly, emerging markets".

With the increasing demands of regulation and supervisors throughout the world, insurers should incorporate regulation as part of everyday operations. Regulation should be part of the "DNA" of the business. The question however is, "how can this be done"? How can we "engage" with supervisors?

Tips:

1) Embracing and understanding the principles of the overall supervisory framework and its mandates / standards throughout all levels of the organisation with the Board / governance committees driving the implementation of the compliance strategy. This should involve linking the supervisory strategy with the overall corporate strategy.

2) Implementation of a transparent and comprehensive supervisory strategy which is communicated to the supervisory bodies and throughout the organisation. The supervisor should be able to evidence the extent of the success of the organisation in achieving its supervisory strategy and the organisation must be able to demonstrate how their supervisory strategy leads to compliance with the standards mandated by the supervisors.

3) Be practical in your feedback on proposed supervisory changes presented by the supervisors e.g., incorporating examples, financial and market impacts, to support the organisations' view and present an unbiased argument at all times, focussing primarily on the critical issues. Never feel the pressure to comment on every aspect of the supervisor's discussion paper.

4) Adopt best practice before it is mandated. The Board / governing committees and senior management should adopt a "forward thinking approach" to ensure compliance with regulations.

5) Be proactive, anticipating supervisory changes and working with industry bodies to influence the supervisors to create the most favourable environment to the business / industry. This will include demonstrating a willingness to participate in supervisory consultations and surveys.

6) Engage in open and regular communication with the supervisors. Establishing a good working relationship with the supervisors' supervisory contacts will therefore be important. This is relevant for all types of communication, and not just relating to matters concerning risk management.

7) Be proactive in the provision of relevant information which will allow the supervisor to discharge its responsibilities. This should encompass: keeping supervisors updated with the progress and results of certain risk management qualification and quantification exercises (and not just providing the results of these when they are due) – i.e., being open in relation to potential issues and how the firm intends to rectify matters. However, it will be important to establish expectations initially since supervisors will not want to be overwhelmed with large volumes of information, not all of which may be relevant to them.

8) Manage the perception of the supervisors internally within the firm. Where the relationship with the supervisor is seen to be confrontational and negative, engagement tends to be on defensive terms, seeking to justify actions as opposed to engaging in open communication by treating the supervisor as a partner and significant stakeholder of the business.

9) Liaise with the supervisor on where they see the next challenges emerging and working with them to minimise the anticipated impacts on the industry.

In summary, an insurer's ERM framework will not be complete if it does not incorporate as a key component the effectiv e management of the r elationship with the su pervisor. I nsurers are therefore encouraged to focus on this aspect as part of the o ngoing development of t he overall ERM framework.

Appendix 1
Published Definitions for Enterprise Risk Management

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

COSO: Enterprise Risk Management – Integrated Framework Executive Summary (September 2004)

ERM is the discipline by which an organisation in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organisation's short- and long-term value to its stakeholders.

CAS ERM Research Committee: Overview of Enterprise Risk Management (2002)

Enterprise Risk Management, as described here, is a holistic management process applicable in all kinds of organisations at all levels and to individuals. ERM differs from a more restricted "risk management" used in some sectors. For example, in some areas the terms "risk management" or "risk control" are used to describe ways of dealing with identified risks, for which we use the term "risk treatment". Some other terms used in this document also have different usages. For example the terms "risk analysis", "risk assessment" and "risk evaluation" are variously used in risk management literature. They often have overlapping and sometimes interchangeable definitions, and they sometimes include the risk identification step.

ERM is a structured and disciplined approach aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value.

KPMG: Enterprise Risk Management – An emerging model for building shareholder value (November 2001)

ERM is the process of planning, organising, leading, and controlling the activities of an organisation to minimise the effects of risk on an organisation's capital and earnings.

KPMG: Viewpoint for Consumer Markets (August 2005)

ERM is defined as a process, effected by an entity's board of directors, management, and other personnel; applied in a strategy setting and across the enterprise; designed to identify potential events that may affect the entity; and manage risk to be within its risk appetite to provide reasonable assurance regarding the achievement of entity's objectives.

The Institute of Internal Auditors: What is ERM and what role in it does internal auditing play? (September 2004)

Appendix 2
Stages of Enterprise Risk Management Maturity

Framework Sophistication	Definitions used in this Attachment
Early	Risk management and internal control activities exist in part, are inconsistently applied and not well understood by management and the relevant employees in limited business areas. Significant opportunities for enhancement remain.
Intermediate	Risk management and internal control activities are established, yet not consistently applied or fully understood by management and relevant employees in key functions/business areas. Moderate opportunities for enhancement remain.
Advanced	Risk management and internal control activities are established, consistently applied and well understood by management and relevant employees across the organisation. Opportunities for enhancement remain to align and coordinate activity across the organisation.

	Early	Intermediate	Advanced
Role of the Board	Board not closely involved in risk management.	Board responsibility for creating the environment and the structures for risk management.	Dedicated board risk management subcommittees, and roles and responsibilities of these committees are publicly available.
	Statement of risk management responsibility.	Board approves the Risk Management Policy.	Board reviews Policy and sets best practice objective.
	No defined risk tolerances.	Board sets the Risk Tolerances.	Any proposed variation to the organisation risk tolerance requires the prior approval of the Board.
			The Board or relevant committees ensures that the risk management framework is appropriately resourced consummate with the risk profile of the organisation.
			The Board and Committee sets the appropriate “tone from the top” with regards to the importance of risk management in the organisation.

	Early	Intermediate	Advanced
Risk Appetite	Risk tolerances are implied in corporate plan but not explicitly applied.	Both risk tolerance and risk limits set boundaries for how much risk the organisation is prepared to accept.	Risk tolerance is determined having regard to organisation's strategy and long term (i.e., over 3 years) Strategic Plan.
	Risk appetite is not tangible, but is understood by the Board and Senior Management for the decision-making process.	Risk appetite is set by the Board and articulated sufficiently to the majority of the organisation. However, not completely embedded within strategic and operational decision-making process.	Risk appetite is set by the Board, articulated sufficiently to the majority of the organisation. It is effectively communicated to internal stakeholders and assists the strategic and operational decision-making process.
			Strategic decisions are independently reviewed against the risk appetite. Areas of weakness are remediated.
Risk Management Policy	Formal policies occasionally set out internal controls responsibilities.	Risk Management Policy outlines the requirements for the management of risk. Policies are supported by protocols, standards and guidelines.	Risk Management Policy covers all major elements of an ERM program.
	Internal controls not linked formally to other corporate governance (e.g., strategy)	Risk Management Policy directly supports the organisation's purpose, and identifies roles and responsibilities for risk management.	Clear alignment between strategic objectives and risk management. Complementary activities on improving the external environment. New acquisitions are integrated into the Risk Management Policy
	Compliance with local laws and supervisory requirements.	Risk management relates to compliance and operational risks.	Risk management linked to business objectives.
	Policies are developed ad hoc.	Risk Management Policy reviewed regularly by the Enterprise-wide Risk Function.	Policy framework exists and is reviewed every 12 months.
Management Accountabilities	Statement of responsibility for internal control is prepared but not owned by CEO or executive team.	Executive management implements the Risk Management Policy.	Management committees oversee Risk Management Policy.
	Do not see business value of compliance activities.	Risk management is integral part of doing business.	The risk management program outcomes are measurable and value creating.
	A senior person (e.g., internal auditor) is responsible for risk management.	Business Units have appropriate structures and processes to meet the requirements contained in the Risk Management Policy.	The Business Unit Risk Functions have a dual matrix reporting line to the management of the Business Unit and Enterprise-wide Risk Function.
	Informal procedures exist for managing risk.	Each Business Unit has a Risk Function that develops tailored Risk & Compliance plans.	Risk functions undertake control self assessments and develop action plans
Management Commitment & Leadership	Risk management seen as responsibility of specialist area (e.g., internal audit).	Managers at all levels are responsible for using the Risk Management Policy in their normal processes and procedures.	Managers see risk management as source of competitive advantage and reflected in employees.

	Early	Intermediate	Advanced
	Internal controls responsibilities not generally included in job descriptions and performance appraisals.	Identification and management of risk is the responsibility of all employees. Roles are formally defined for each employee.	Support and promote the proactive risk management behaviours Encouraging others to report any issues or incidents.
Enterprise Risk Function	Internal controls are delegated to Internal Audit.	A CRO position has responsibility for the Risk Management Policy.	The Enterprise-wide Risk Function develops and maintains the Risk Management Policy.
	Resources provided to specialist risk area.	Executive management is responsible for establishing Business Unit Risk Functions sufficiently resourced and supporting their activities.	Efficiency and effectiveness of risk resourcing is periodically reviewed.
Risk Language	No common usage of risk terms.	Shared understanding of risk language.	Use of consistent risk management terminology/lexicon, internationally accepted risk categories, ratings, and reporting.
	Definitions provided do not materially assist the identification and management of risks. Some risks that have been identified and managed are not material risks, but causes or consequences.	Definitions provided allow for sufficient identification and management of material risks. A significant amount of risks have been incorrectly classified.	Definitions clear, concise and allow for all risks to be identified and categorised correctly, enabling the efficient management of these risks.
Risk Management Culture	Corporate plan refers to values.	The organisation aims to ensure: Role Clarity Training Accountability	Developed a behavioural model to underpin and promote the desired proactive risk management culture. Executive promotes and reinforces the risk management culture. Processes exist to identify, evaluate, assess and exploit opportunity risks
	Code of Conduct exists and training is included in orientation for new staff.	Training to support people in understanding how to use proactive behaviours.	Measurement each year of the risk management culture.
	Employees do not see internal control as a personal responsibility.	Risk Management Policy is reflected in employee and management training.	Employees take responsibility for proactively managing risk to benefit the business.
Performance Management & Reward Systems	Incentives exist for employee performance.	Some incentives for management aimed at encouraging a proactive risk management culture.	Each year a risk goal is set as part of an incentive bonus scheme.
Own Risk & Solvency Assessment	Ad hoc analysis on a reactive basis.	An Economic Capital Model provides assessment of the key risk drivers and risk management techniques to address these risks.	Economic capital model comprises forecast future balance sheet, profit and loss accounts, and projected distributions of profit; capital and return on capital. The allocation of capital to business units / lines commensurate with risk underpins the performance management process and enables measurement of outcomes and returns against those expected.

	Early	Intermediate	Advanced
Risk Management Processes	Controls are not explicitly linked to risks.	There is a clear identification of all the relevant risk categories.	Materiality limits for reporting incidents/risk issues are agreed on at least an annual basis by the executive management.
	Controls are generally detective in nature.	Risk management processes are applied.	Risk management processes are applied & the risk assessment includes the quantification of operational risk.
	A formal risk management plan is produced on a periodic basis that includes actions to be taken in respect of risks.	Risk Profiling is undertaken regularly at Business Unit level and organisation level.	Process for identifying and evaluating emerging risks (i.e., developing subject to uncertainty and difficult to quantify).
	Financial and compliance objectives and taken into account in the risk assessment process.	The risk analysis and treatment processes allows for the assessment and quantification of “Inherent” and “Residual” risk and the effectiveness of controls.	Scenario planning is used to evaluate high impact/low probability events.
	Loss events are monitored by central function (e.g., internal audit),	Loss events and risk profiling undertaken.	Able to integrate loss events with key risk indicators (lead and lag) and risk profiling.
	Controls focus on financial reporting and compliance.	Controls are all risk based and reviewed regularly.	Control activities cover all risks and undertaken within each Business Unit and business processes are documented and incorporate policies and procedures.
Reporting & Monitoring	Reporting of significant control weaknesses are communicated to certain parties e.g., internal audit, and without a strong sense of urgency.	Any breaches of these requirements are reported to the Enterprise-wide Risk Function.	Assurance is provided to executive management, the Audit Committee, and the Board via controlled risk self-assessments. The responses to the controlled risk self-assessments are reviewed by the internal audit team, and the results of their review are reported to a Board Committee.
	Information captured sometimes enables line management to effectively identify and deal with risks.	Internal risk reporting covers all key aspects of the Risk Management Policy. Risk & Compliance plans developed by the Business Units identify the external reporting requirements, timings and responsibilities.	The Enterprise-wide Risk Function undertakes the: Central collection, collation and analysis of enterprise-level risk-related data Establishment of common reporting standards, tools and risk management information systems Production of risk management reports.
	Some oversight / monitoring of middle management actions and the organisation’s activities.	Business Unit are responsible for monitoring control activities.	Consistent Key Risk Indicators are applied across the organisation, enabling aggregation.

	Early	Intermediate	Advanced
	Employees are encouraged to raise issues with management regarding inappropriate behaviour.	Formal internal channels exist for raising inappropriate behaviour.	Formal and independent channels exist for raising inappropriate behaviour, and these are used.
	Internal Audit plays integral role in reviewing effectives of controls.	Management undertakes overall responsibility for periodic reviews of the risk management system.	Risk management is monitored and evaluated on an ongoing basis by management and employees.
Internal Audit	Internal audit has limited access to Executives or Audit Committee.	Effective implementation and compliance with the Risk Management Policy is monitored by the Internal Audit Function, as well as the organisation's external auditors.	Internal Audit Function conducts an annual audit of the Risk Management Policy, and the Enterprise-wide Risk Function.
New activities	Major projects have cost benefit analysis with risk factored in.	Risk and controls exist for major projects.	Risk, controls and assurance testing new programs, projects and ongoing change tasks, and strategic developments (e.g., acquisitions).
Continuity Analysis	A disaster recovery plan exists for information system applications	A properly documented and tested Business Continuity Plan.	Risk & financial condition assessment of the ability of the insurer to stay in business for more than one year.
			Crisis Management Plan that minimises business impact and loss in the event of a significant incident.

Appendix 3
ERM Implementation Case Studies

ERM Implementation – Incorporating a Capital Model

A large insurer was seeking to implement an ERM strategy throughout the organisation, and an integral aspect of this strategy was building a capital model. There were several drivers for insurance companies to build capital models. Supervisors and rating agencies now considered capital modelling incorporated into an ERM framework as vital for a well run insurance company. As well as reducing capital requirements, capital models provide employees with a tool to better understand the risks in their business, and therefore manage those risks more effectively.

Before the project started, the insurer recognised that it is important to get support within the business to develop a capital model. This is possibly the most important step, since building a capital model that will be useful for the business as a whole required input from across the organisation. Therefore, the project sponsor for the European capital model was the Chief Actuarial Officer (who was part of the Board Executive), and the project sponsor for the Group capital modelling project was the Chief Executive Officer of the Group. This high profile project sponsor provided a clear vision to implementing the ERM strategy. This in turn was helped increase the businesses' enthusiasm to participate in the project and enabled the project team to overcome obstacles through the project's lifetime.

Next a steering committee was formed to monitor development of the modelling. Membership included a good mix of business skills to help resolve any major issues. For instance, the European capital model steering committee consisted of:

- Chief Actuarial Officer (Chair)
- Chief Executive Officer
- Chief Finance Officer
- Chief Underwriting Officer
- Two operations directors
- Two senior underwriters.

Use of project disciples with a well-developed project plan ensured effective tracking of progress and ability to report in a timely and comprehensive manner to the Steering Committee.

During the implementation phase, the key internal stakeholders were managed through the steering committee, and a concerted effort was also made to extend publicity as far as possible. External stakeholders were also brought on-board at an early stage. The insurer recognised that it is much easier to include them on the capital modelling journey, rather than hand them a large report at the end of the project, for which they do not have the necessary resources to review. With the European model, the insurer held a number of meetings with the two UK supervisors; Lloyd's of London and the FSA. These meetings were beneficial in that it provided consensus that the general approach was sound. During the development phase of the capital

model, the modelling team held one hour meetings with most of the underwriting teams within the business.

Incorporating all key risks into the capital model, as part of a wider ERM implementation, required the insurer to include the following:

- Underwriting risk – It was found that employees were familiar with the risks that business they are currently writing faces, and the underwriters were familiar with considering the uncertainty around business they are about to write
- Credit risk - The most common source of credit risk was external reinsurers, since this was typically one of the larger debtors on the balance sheet. The insurer incorporated reinsurance credit by considering the credit quality of the different reinsurers on the insurer's balance sheet
- Asset (market) risk – In seeking to avoid too much investment risk, the insurer was investing in high quality corporate bonds. Yet, even though these are secure, due to their market value being dependant on the prevailing yield curve, the market value of the bonds were modelled stochastically
- Liquidity risk – Although liquidity risk tends to be an immaterial risk for non-life insurance companies, in the event of a natural catastrophe, there could be a liquidity crunch. To allow for liquidity issues, the insurer considered short-term cash flows within the model
- Operational risk – The insurer combined a robust operational risk scenario analysis along with a risk register as the operational risk assessment within the capital model.

Once the various parts of the capital model were assessed, they were reviewed by the relevant business experts:

- Underwriters and pricing actuaries for underwriting risk
- Reinsurance function and security committee for credit risk
- Investment function for market risk
- Risk management for operational risk and group risk
- Senior management and Board for overall reasonableness of the aggregate capital model.

Due to the comprehensiveness of the capital model, as part of a wider ERM strategy, the ERM implementation process achieved a high confidence level with the Board of this insurance organisation. However, the insurer also recognised that a continual review of their ERM strategy is necessary in order to increase focus on managing risk at an organisation-wide level and to effectively address pragmatic issues.

ERM Implementation – A Cautionary Tale

A large insurer initiated a project to design and implement an ERM process throughout the organisation. Project management and project ownership was assigned to the Internal Audit department because they were considered the owners of risk identification. Internal Audit quickly set about identifying the risks for each business unit and creating a draft Risk Profile. However the risk profiles produced were limited because they only addressed the areas which were understood and monitored by Internal Audit. Not only did the Executive not accept these

risk profiles as true reflections of their businesses but some "key risks" were omitted entirely. As a result of this resistance the process of implementing ERM was significantly slowed down.

In response to the problems being experienced in the implementation of ERM, the Board decided to reassign ownership of the ERM project to the business units. The business units worked collectively to establish a project team of people with the right attitude for the project. However, these individuals ended up being part time resources due to their continued responsibility for their day to day roles and again the project ran into delays.

Additional risk champions in the businesses were identified. These were managers with full day jobs already who were not part of the risk community. Due to budgetary constraints and time availability no training was provided to these new champions. It was considered that they were talented mangers who would soon pick it up. By now the Board had decided that to ensure ERM was implemented to be "leading practice" in the industry. This added pressure to the project team and the new champions as they strove to meet these higher level criteria for success. Nevertheless after several months the ERM implementation was complete.

A post implementation survey of business managers was conducted to assess both the project and views about the usefulness of the ERM framework. The feedback was quite critical. The ERM process was considered "over-engineered" in some areas and the implementation patchy in other areas of the business. They also observed that there was a lack of training and support provided to the business unit risk teams / risk champions and that the solution for the risk management tool was decided before the development of the Group framework. In addition, the roll-out would have benefited from detailed implementation planning. This lead to frustrations and actually resulted in risk awareness going backwards. People found it was difficult to understand what the objectives were, what the desired inputs were and what output and benefit was being received. The process became very user-unfriendly.

The Board subsequently initiated a new project to "simplify" the existing ERM process and noted the following learning to avoid problems in future:

- Board and senior management "buy-in" into the ERM process is required from the beginning; with a clear vision and agreed achievable outcomes
- The project owner of ERM design and implementation should never be just one department within the organisation, always include ownership across the business from the start
- Use project plans, project disciplines and full time resources, don't ask people to do this work in addition to their day jobs, build the project over time
- Engaging risk champions at the lower levels of the organisation is critical prior to roll-out and ensure they receive the relevant training
- The time and resources for a roll-out of a Group framework should not be under-estimated
- Introducing new technology is typically harder than expected so plan for the worst not the best case scenario
- Understand that implementing ERM involves cultural change which will take time so build these expectations into the project plan
- AND do not over-engineer the process; keep it easy and simple.

ERM Implementation: Success is whatever you define success to be!

A large Global Insurer embarked on an ERM implementation program. Taking the prevailing standards, guidance and academic material the organisation set out to deliver holistic, strategic, integrated risk management to the entire enterprise to meet the needs of supervisors, investors, customers and policy holders and management all in one program.

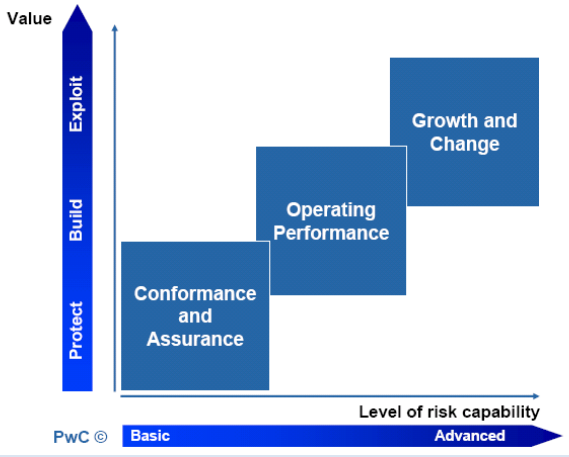
The ERM program defined measures of success in terms of project activities, achieving project milestones, number of workshops, frequency and volume of reporting outputs, sophistication of tools and techniques and many process- or activity- related success measures. But the outcome was unsuccessful and much of the work and investment was unwound and written off. Many of the staff in the risk management function lost their jobs.

So what went wrong? Fundamentally, the ERM program did not have a definable impact on business objectives or outcomes. There was:

- No significant changes to the risk profile or risk management capability of the organisation
- No defined business outcomes for ERM that were aligned/ sufficiently connected to the business objectives and outcomes
- Increased cost, work load and time put on management that did not deliver any greater insight to the business than already obtained through other management practices and capabilities
- Duplication of existing analysis, processes and reports for little marginal economic benefit.

What should be done differently? The definition of success for ERM needs to be defined in terms of the business outcomes and value contribution to the business.

1. Be very specific on the scope and focus of the ERM activity. For example the illustration below provides a view on where ERM is to have an impact:



Conformance and assurance; reduction in losses or greater cost avoidance

Operating performance; reduction in uncertainty or downside variability in operational costs and outcomes – operational stability and cost avoidance

Growth and change; increase the likelihood or probability of success in growth and change decisions – taking the right bets with greater confidence

Where is the primary business focus for the ERM implementation?

2. There must be qualitative, quantitative and economic measures of success and impact of ERM on the business.
3. The Stakeholders must agree and support th e measures of succe ss, with the ERM sponsors held accountable for delivering this success.
4. There must be continuous assessment and c hallenge of the status quo to ensure the investment in ERM continues to be relevant to the business outcomes.

Appendix 4
Example of a Risk Committee Charter

What should be included in a risk committee charter?

- The purpose of the Risk Committee e.g., to perform centralised oversight, policy setting, information gathering, and communication to senior management and the Board of Directors, regarding important risks and its related risk management activities
- Outline of the responsibilities of the Risk Committee e.g., identify and monitor important existing and emerging risks to the achievement of the company's strategic and operating objectives, formulate appropriate policies and monitoring and reporting frameworks etc.
- Minimum pre-requisites for its members / committee composition e.g., nominated by senior management, a third of the committee members are required to be external etc.
- Frequency of meetings for the Risk Committee e.g., meet one month in advance of each Board of Directors' meeting
- Outline of the Key Performance Indicators ("KPI") which will be used by the Risk Committee to annually assess its performance e.g., number of policies considered by the Risk Committee in a year, number of policies recommended for adoption to the Board which were adopted in a year, number of meetings held during the year, number of policies approved for adoption by the Board which were successfully implemented etc.
- Outline the resources which the Risk Committee shall have direct access to and open communication with e.g., senior management, assistance / liaison from internal audit, internal legal, finance and other advisors within and external to the organisation.

Example Charter

1. PURPOSE

The Risk Committee's primary purpose is to perform centralised oversight, policy-setting, information gathering, and communication to the Board of Directors, regarding important risks and its related risk management activities. In addition, the Committee shall assist the Board of Directors in fulfilling its oversight responsibilities related to the company's risk assessment and management processes.

2. RESPONSIBILITIES

- *The Risk Committee shall be responsible for the following activities:*
- *Identify and monitor important existing and emerging risks to the achievement of the company's strategic and operating objectives.*
- *Formulate appropriate policies and monitoring and reporting frameworks to support effective management of important risks.*

- *Review and evaluate the effectiveness of management processes and action plans to address such risks.*
- *Advise on and recommend to senior management any significant actions or initiatives that the Committee believes necessary to effectively manage risk.*
- *Ensure that activities of discrete risk management disciplines within the company are appropriately coordinated.*
- *Report to the Board of Directors on the status of the company's important risks and related risk management processes.*

3. MEMBERSHIP AND MEETINGS

The Chief Executive Officer / Board hereby resolves to establish a Risk Committee consisting of representatives from the Board of Directors. The Risk Committee shall have a Chair appointed by the Board / Chief Executive Officer, who will be responsible for providing overall leadership of Committee activities and setting agendas for the Committee meetings.

The Risk Committee shall meet [bi-monthly / quarterly] and additionally when needed.

PERFORMANCE AND CHARTER

Annually, the Risk Committee shall perform a self-assessment against the Key Performance Indicators ("KPIs"), a review of the Committee membership and recommendations as to any changes thereto. In addition, the Committee shall annually review its Charter and make any recommended changes thereto.

RESOURCES AND AUTHORITY OF THE COMMITTEE

The Committee shall have direct access to and open communication with senior management and liaison / assistance from internal audit, internal legal, finance function and other advisors to assist with decision making and monitoring. The Committee shall also have access to external advisors to assist if required.

KEY PERFORMANCE INDICATORS FOR ASSESSMENT OF COMMITTEE PERFORMANCE

Examples:

- *Number of policies approved by the Committee per annum;*
- *Number of policies considered by the Committee per annum;*
- *Number of meetings held per annum; and /or*
- *Average number of attendees at each Committee meeting.*

Appendix 5
Chief Risk Officer – Key Roles & Responsibilities

Chief Risk Officer

The Chief Risk Officer will oversee market risk, asset/liability management, credit risk, investment risk, operational and supervisory risk and actuarial issues throughout the organisation and service the Risk Committee and its subcommittees.

In accordance with the organisation's Operating Philosophy, the role of the Chief Risk Officer is to provide:

- Policy Guidance and establish Minimum Standards for the conduct of risk management activities throughout the organisation
- Oversight of risk management activities across the organisation to ensure Minimum Standards are met, including monitoring of aggregate risk data
- Lead the risk committee and ensure it adheres to its charter
- Functional leadership for the organisation's specialist personnel involved in risk management activities throughout the organisation to ensure a professional cadre of risk management personnel operates at high standards throughout the organisation
- Monitor leading practice trends to ensure the organisation's ERM program continually evolves
- Research capability to ensure the organisation is kept abreast of the latest developments and harnesses such developments for the benefit of the organisation
- Ensure there is an independent view on the effectiveness and efficiency of the risk management arrangements
- Liaise with ratings agencies and provide the relevant information as required
- Provide additional services deemed necessary by the organisation or at the request of individual operating units that does not conflict with their role
- The Chief Risk Officer where necessary, challenges business decisions on key risk areas and has the ability to escalate issues that cannot be resolved with individual operating units to the Operating Units Managing Director / Chief Executive Officers. In the very rare event that a matter of significant business risk cannot be resolved with an Operating Unit Managing Director, then the matter is referred to the Chief Executive.

In addition the Operating Unit Managing Directors / Chief Executive Officers ensure that appropriate consultation takes place with the Chief Risk Officer on all issues involving organisational policy or otherwise within their remit.

The following example is how these responsibilities might be described in a role specification.

EXAMPLE:
GENERIC ROLE SPECIFICATION

Reports to: INSURER Group Chief Executive Officer

Principle Role & Accountability:

The Chief Risk Officer is responsible for the leadership, direction and co-ordination of the Group-wide application of risk management at INSURER including line management responsibility for [Group Risk Management, Internal Audit, Health, Safety, Welfare and Environment.] and to ensure that the principles and requirements of managing risk are consistently adopted throughout the Group, and to establish a risk management framework and appropriate resource to assist the Group in its realisation of business objectives and continual development.

Principle Responsibilities:

Policy and Strategy

a) *To design and oversee the group-wide risk management strategy, aligning all risk management and associated internal control activities to support the delivery of shareholder value in the INSURER Group.*
b) *To present INSURER Group risk management policy for discussion and approval by the INSURER Group Risk Management Committee and/or INSURER Group Board.*
c) *To canvass senior management views on the continual development of risk management across the Group and review whether organisational structure to support the INSURER Group risk management strategy remains appropriate.*
d) *To maintain awareness of trends and developments in risk management that may be significant to the INSURER Group and its operating subsidiaries.*
e) *To oversee the procurement of all Group insurance, broker and underwriter contracts and where appropriate, identify professional advisors to support the delivery of best practice risk management across the INSURER Group.*
f) *To facilitate the integration of risk management policy and strategy into all INSURER Group business strategy and activity, including the consideration of risk management in investment decisions.*
g) *Ensure that appropriate information regarding risk and internal controls is provided to the investment market including shareholders in conjunction with the Chairman and Chief Executive Officer.*
h) *To liaise with the Supervisors on existing regulations, new regulations and emerging regulations. Liaison will include participation in providing feedback to the Supervisors on framework and principles as well as responding to the Supervisors questions and requests.*

Risk Identification & Assessment

a) *To monitor and report to the INSURER Group Risk Management Committee on the total level of INSURER Group risk exposure.*

b) To maintain independent challenge on risk and assurance issues through the management of INSURER Group risk and assurance functions.

c) Ensure that risk identification and assessment activities performed across the INSURER Group and operating subsidiaries are reviewed and challenged where necessary and appropriate escalation procedures are in place at the highest level.

Management and Reporting Framework

a) To be responsible for management and co-ordination of Group Risk Management [(to include Group Insurance), Internal audit and Health, Safety, Welfare and Environment (including Corporate Social Responsibility).]

b) To ensure appropriate risk management and reporting frameworks are in place across the INSURER Group and operating subsidiaries, commensurate with risks to Group.

c) To provide an annual INSURER Group risk management performance report to the INSURER Chief Executive Officer.

Reporting and Stakeholder Engagement

a) To monitor the overall risk management performance at Group level and to ensure the effective and timely reporting of risk management information within the Group operating subsidiaries and at Group level.

b) To be an attendee of the INSURER Group Risk Management Committee and ensure that the Committee engages in the development of best practice risk management across the INSURER Group.

c) To present, discuss and challenge Strategic Risk Review summary reports, reporting key risks and associated internal control procedures, to the INSURER Group Risk Management Committee.

d) To represent INSURER Group risk management positions, strategy and experiences at internal and external forums to maintain a high reputation.

e) To develop and maintain appropriate engagement processes with INSURER Group stakeholders, and ensure that equivalent and consistent risk management processes are implemented within INSURER Group operating subsidiaries.

f) With Strategy & Communications and others as appropriate, to advise the investment community, Credit Rating Agencies, on risk management performance, particularly with reference to Socially Responsible Investment.

Line Support and Knowledge Sharing

a) To facilitate risk management knowledge and best practice sharing across the Group, with reference to external indices and benchmarks as appropriate.

b) To Chair the INSURER Group Risk Management Co-ordinators Forum, providing expertise and support and communicating risk and associated internal control procedures arising from the INSURER Group Risk Committee and act as an information conduit for the Forum to the Risk Management Committee.

c) *To support senior management with any aspect of risk management development and oversee key risk management training initiatives including key senior management training and to incorporate risk management into employee induction programs.*

Appendix 6
Topics and structure of a typical risk management policy

1 INTRODUCTION

1.1 Definitions of Risk and Enterprise Management

1.2 Objective of Enterprise Risk Management

2 RISK MANAGEMENT POLICY

2.1 Objectives of Risk Management Policy

2.2 Categories of Risk and Definitions

[Example risks for an insurer:

- *Operational*
- *Corporate and strategic*
- *Underwriting and pricing*
- *Reserving*
- *Liquidity*
- *Credit*
- *Market*
- *Legal and compliance*
- *Financial]*

2.3 Potential Benefits of ERM

2.4 Success Criteria

3 RISK MANAGEMENT STRUCTURE

[*Include organisational chart along with details on the roles of each position.]*

3.1 Risk management organisational structure

3.1.1 Role of Risk Committee

e.g., Performs centralised oversight, policy-setting, information gathering, and communication to executive management and Board of Directors.

3.1.2 Role of CEO

3.1.3 Role of CRO

3.1.4 Role of Executive Management

3.1.5 Role of Risk Sponsors

e.g., Represents each of the Company's major business units and support functions, and to whom given risks are "assigned" for helping to ensure that the Committee's objectives are carried out.

3.1.6 Role of Risk Owners

e.g., Individuals responsible for managing a specific risk or risks.

3.1.7 Role of Risk Manager

3.1.8 Role of Monitors

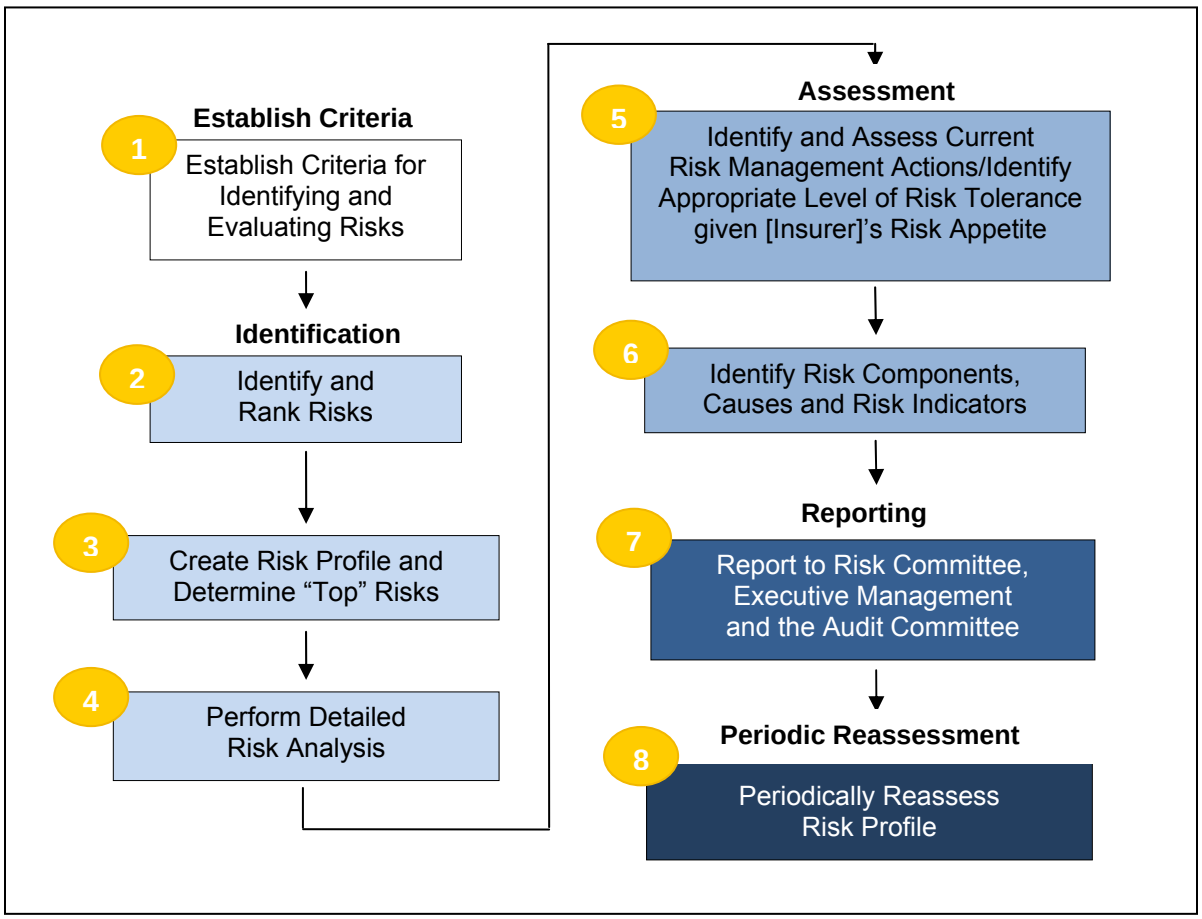
e.g., The company's risk control processes are monitored at the Risk Owner and Risk Committee level, as well as by risk control functions (e.g., Internal Audit, Compliance, and Legal)

4 RISK IDENTIFICATION AND ASSESSMENT PROCESS

[Define the enterprise identification and assessment process.]

4.1 Overview of the risk assessment process

The overall risk assessment process is illustrated in the following diagram. Each of the steps is explained further below.



4.2 Step 1 – Establish Criteria

4.2.1 Risk Ranking Criteria

4.2.2 Current Risk Management Action Effectiveness Score

4.2.3 Risk Appetite

4.2.4 Risk Tolerance

4.3 Step 2 – Identify, Assess and Rank Risks

4.4 Step 3 – Create Risk Profile and Determine "Top" Risks

4.5 Step 4 – Perform Detailed Risk Analysis

4.6 Step 5 – Identify and Assess Current Risk Management Actions / Identify Appropriate Level of Risk Tolerance Given [Insurer]'s Risk Appetite

4.6.1 Identify and Assess Current Risk Mitigating Actions

4.6.2 Identify Appropriate Level of Risk Tolerance Given [Insurer]'s Risk Appetite

4.7 Step 6 – Identify Components, Causes and Risk Indicators (applicable to Top Risks only)

4.8 Step 7 – Report to Risk Committee, Executive Management and the Audit Committee

4.9 Step 8 – Periodically Reassess Risk Profile

5 RISK REPORTING

[Define the risk reporting process and include example template where applicable.]

5.1 Format and timing of the risk reporting

For Example:

Reporting to	Frequency of reporting	Reporting format
Risk Committee	*Quarterly*	
Executive Management	*Quarterly*	
Audit Committee	*Quarterly for Top Risks*	

APPENDICES

Appendix A: Risk Committee Charter

Appendix B: List of Risk Committee members

Appendix C: Risk Register Template

Appendix D: Risk Ranking Criteria (Likelihood and Consequence)

Appendix E: Current Risk Management Action Assessment Criteria

Appendix F: Risk Profile

Appendix G: Sensitivity Analysis for Top Risks

Appendix H: Top Risk Management Actions Report

Appendix I: Effectiveness in Light of Risk Tolerance

Appendix J: Risk Status Report – Top Risks

Appendix K: Risk Status Report – Remaining Risks

Appendix L: Risk Content Report

GLOSSARY OF TERMS

For Example:

- Risk Committee: reviews the Company's policies with respect to risk assessment and risk management, and contingent liabilities and risks that may be material
- Enterprise Risk Management (ERM): a structured and disciplined approach aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing risks a company faces as it creates value
- Monitoring: the Company's risk control processes are monitored at the Risk Owner and Risk Committee level, as well as by risk control functions
- Risk: the threat of an event, action, or loss of opportunity that, if it occurs, may adversely affect values of the Company
- Risk Appetite: phrase used to express the overall level of risk the Company is willing to take to achieve its objectives.
- Risk Committee: performs centralised oversight, policy setting, information gathering, and communication to executive management and Board of Directors
- Risk Owners: individuals responsible for managing a specific risk or risks
- Risk Sponsors: represent each of the Company's major business units and support functions, and to whom given risks are "assigned" for helping to ensure that the Committee's objectives are carried out
- Risk Tolerance: quantitatively defines the level of risk we are willing to accept with respect to each of the Company's important risks.

Appendix 7
Useful Emerging Risk Web Links

CRO Forum home page: http://www.croforum.org/

CRO Forum Emerging Risks Initiative page: http://www.croforum.org/emergingrisc.ecp

CRO Forum Emerging Risks Initiative – "Position paper - Climate change & tropical cyclones": http://www.croforum.org/emergingrisc.ecp

CRO Forum Emerging Risks Initiative "Position paper – Pandemic": http://www.croforum.org/publications/20080201_1_resource/File.ecr?fd=true&dn=cro_pandemie_final

CRO Forum Emerging Risks Initiative "Position paper – Terrorism": http://www.croforum.org/publications/20072711_resource/File.ecr?fd=true&dn=terrorismpositionpaper_nov07

Swiss Re emerging risk initiate: http://www.swissre.com/pws/media%20centre/online%20magazine/market%20trends/the%20cro%20emerging%20risk%20initiative.html

Ernst & Young report - "Strategic Business Risk 2008 – the Top 10 Risks for Business with Oceania Perspectives": http://www.ey.com/Global/assets.nsf/Australia/AABS_Strategic_Business_Risk/$file/SBR.pdf

Ernst & Young report - "Property/Casualty Insurance Industry 2007 Outlook": http://www.ey.com/Global/assets.nsf/International/Industry_Insurance_US_Property_Casualty_Insurance_Industry_Outlook_2007/$file/EY_USProperty_Casualty_Insurance2007Outlook.pdf

Ernst & Young report - "Strategic Business Risk - Insurance 2008": http://www.ey.com/Global/assets.nsf/International/Industry_Insurance_StrategicBusinessRisk_2008/$file/Industry_Insurance_StrategicBusinessRisk_2008.pdf

World Economic Forum report "Global Risks 2008 - A Global Risk Network Report": http://www.weforum.org/pdf/globalrisk/report2008.pdf

OECD Report – "Emerging Risks in the 21st Century – An OECD International Futures Project": http://www.oecd.org/dataoecd/23/56/19134071.pdf

Economist Intelligence Unit Report – "Risk 2018. Planning for an unpredictable decade": http://www.btglobalservices.com/business/global/en/docs/other/risk_2018_planning_for_an_unpredictable_decade.pdf

Deloitte report – "2008 Industry Outlook. Insurance overview. A look around the corner": http://www.deloitte.com/dtt/cda/doc/content/us_2008CrossIndustryOutlook_insurance.pdf

Appendix 8
Useful References

Note: All websites accessed on 1 July 2008.

Acharyya, M. 2007. *Proposing a conceptual framework to measure the performance of Enterprise Risk Management from an empirical study of four major European insurers.* http://www.egrie2007.de/EGRIE%20Papers/EGRIE_2007_Acharyya.pdf

A.M. Best. 2006. A.*M. Best Comments on Enterprise Risk Management and Capital Models.* http://www.ambest.com/ratings/methodology/enterpriserisk.pdf

American Academy of Actuaries. 2001. *Risk Management in the Insurance Industry.* http://www.actuary.org/pdf/finreport/risk_09dec01.pdf

Bennet C.; Cusick, K. (Trowbridge Deloitte Limited) 2007. *Risk Appetite: Practical Issues for the Global Financial Services Industry*. http://www.actuaries.asn.au/IAA/upload/public/4.a_Conv07_Paper_Bennet%20Cusick_Risk%20Appetite.pdf

Bohn, C.; Kemp, B. 2006. *Enterprise Risk Management Quantification - An Opportunity*. http://www.soa.org/library/monographs/other-monographs/2006/july/Bohn-abstract.pdf

Casualty Actuarial Society. May 2003. *Overview of Enterprise Risk Management.* http://www.ucop.edu/riskmgt/erm/documents/overview.pdf

Committee of Sponsoring Organizations of the Treadway Commission. 2004 *Enterprise Risk Management – Integrated Framework: Executive Summary.* http://www.coso.org/publications/ERM/COSO_ERM_ExecutiveSummary.pdf

Continuity Central. 2007. *Emerging Governance Practices in Enterprise Risk Management*. http://www.continuitycentral.com/feature0439.htm

D'Arcy, S. 2006. *Enterprise Risk Management in the Insurance Industry*. http://www.business.uiuc.edu/~s-darcy/present/ERM%20Symposium%20-%202006%20-%20Workshop%202%20(D'Arcy%203-31-06)%20with%20Template.ppt#258,2,Overview

Deloitte. 2006. *The Risk Intelligent Enterprise: ERM Done Right.* http://www.deloitte.com/dtt/cda/doc/content/us_risk_RIPOV.pdf

Ernst & Young. 2006. *Insurance Risk Leadership Roundtable: Setting Risk Appetite, Tolerance and Limits.* http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Insurance_Risk_Leadership_Roundtable_Corporate_Risk/$file/AABS_RAS_Insurance_Risk_Leadership_Roundtable_CorporateRisk.pdf

Ernst & Young. 2006. *Insurance Risk Leadership Roundtable: Preparing for the new ERM Environment.*
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Insurance_Risk_Leadership_Roundtable/$file/AABS_RAS_Insurance_Risk_Leadership_Roundtable.pdf

Ernst & Young. 2005. *Managing Risk across the Enterprise: Connecting New Challenges With Opportunities.*
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Managing_Risk_Across_Enterprise/$file/AABS_RAS_Managing_Risk_Across_Enterprise.pdf

Ernst & Young. 2006. *Managing Risk Across the Enterprise: The Value of Enterprise Risk Management* .
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Value_ERM/$file/RAS_Value_ERM.pdf

Ernst & Young. 2007. *Managing Risk Across the Enterprise: Building a Comprehensive Approach to Risk.*
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Manag_Risk_Enterprise/$file/AABS_RAS_Manag_Risk_Enterprise.pdf

Financial Services Authority. 2006. *Insurance Sector Briefing: Risk Management in Insurers.*
http://www.fsa.gov.uk/pubs/other/isb_risk.pdf

Financial Services Authority (McDonnell, William). 2002. *Managing Risk: Practical Lessons from Recent "Failures" of EU insurers.* http://www.fsa.gov.uk/pubs/occpapers/OP20.pdf

Gates, Stephen. 2006. *Incorporating Strategic Risk into Enterprise Risk Management XV^{ème} Conférence Internationale de Management Stratégique, Annecy / Genève 2006.*
http://www.strategie-aims.com/aims06/www.irege.univ-savoie.fr/aims/Programme/pdf/SP26%20GATES.pdf

Hoyt, R.E; Liebenberg, A.P. 2008. *The Value of Enterprise Risk Management: Evidence from the U.S. Insurance Industry.* http://www.ermsymposium.org/pdf/papers/Hoyt.pdf

Ingram, D. 2003. Life Insurance Industry Risk Management.
http://www.iafe.org/upload/Ingram_Talk.pdf

Institute of Internal Auditors. 2004. *The Role of Internal Audit in Enterprise-wide Risk Management.* http://www.ucop.edu/riskmgt/erm/documents/erm1.pdf

International Association of Insurance Supervisors. 2007. *Guidance Paper On Enterprise Risk Management For Capital Adequacy And Solvency Purposes.*
http://www.iaisweb.org/__temp/2_2_6_Guidance_paper_on_enterprise_risk_management_for_capital_adequacy_and_solvency_purposes.pdf

International Association of Insurance Supervisors.2007. *Guidance Paper On The Use Of Internal Models For Risk And Capital Management Purposes By Insurers.*
http://www.iaisweb.org/__temp/15__Guidance_paper_No__2_2_6_on_the_use_of_internal_models_for_risk_and_capital_management_by_insurers.pdf

International Electrotechnical Commission (IEC). *Draft IEC 31010 Risk Management - Risk Assessment Techniques.*
http://www.rmia.org.au/LinkClick.aspx?fileticket=uXc91tcaLVU%3d&tabid=85&mid=634

International Organisation for Standardization (ISO). 2008. *Draft International Standard ISO/DIS 31000: Risk management – Principles and guidelines on implementation.*
http://rmia.org.au/LinkClick.aspx?fileticket=AWkZuS%2bB6Wc%3d&tabid=85&mid=634

KPMG. 2001. *Enterprise Risk Management: An Emerging Model for Building Shareholder Value.* http://www.kpmg.com.au/aci/docs/ent-risk-mgt.pdf

KPMG. 2006. Risk and Capital Management for Insurers.
http://www.kpmg.cz/czech/images/but/Risk_Capital_Management_for_Insurers_2006.pdf

Lam, J. 2000. *Enterprise-wide risk management and the role of the chief risk officer.*
http://www.erisk.com/Learning/Research/011_lamriskoff.pdf

Matthews, A.; Wang, S.; Cassidy, P.; Faber, R.; Newton, T. 2007. *Enterprise Risk Management and Exploring Best Practice in Commercial Insurance Pricing and Underwriting.*
http://www.actuaries.asn.au/IAA/upload/public/2.c_Conv07_Paper_Matthews_putting%20enterprise%20risk%20mgt%20into%20best%20practice.pdf

McConnell, Patrick. 2004. *A 'Standards Based' approach to Operational Risk Management under Basel II.* http://www.m-bryonic.co.uk/library/ORStandards.pdf

PWC. 2004. *Enterprise-wide Risk Management for the Insurance Industry - Global Study.*
http://www.pwc.com/extweb/pwcpublications.nsf/docid/57b887e9d239274785256e470020a3a5

Rech, J. E. 2005. Enterprise *Risk Management for Insurers: Theory in Practice.*
http://www.contingencies.org/novdec05/enterprise_1105.asp

Schmidt Bies, S. 2006. *A Bank Supervisor's Perspective on Enterprise Risk Management*, BIS Review, publication 34/2006. http://www.bis.org/review/r060502d.pdf

Shamieh, C. 2007. *Implementing EC – Recent experience.*
http://riskisopportunity.com/files/pdf/2007-chicago-shamieh.pdf

Society of Actuaries, 2006. *Enterprise Risk Management Specialty Guide.*
http://soa.org/library/professional-actuarial-specialty-guides/enterprise-risk-management/2005/august/spg0605erm.pdf

Standard and Poor's. 2005. *Enterprise Risk Management For Financial Institutions: Rating Criteria And Best Practices.*
http://www.mgt.ncsu.edu/erm/documents/sp_erm_busdevbk.pdf

Standard and Poor's. 2007. *Enterprise Risk Management Can Help U.S. Commercial Lines Insurers Ward Off Irrational Pricing.*
http://www.rims.org/resources/ERM/Documents/ERMReportCard4-30-07.pdf

Standard and Poor's. 2006. *Insurance Criteria: Refining The Focus of Insurer Enterprise Risk Management Criteria.* http://www.actuaries.org.hk/doc/ET060808_Ref4.pdf

Teuten, P. 2005. *Enterprise Risk Management: Its Evolution And Where It Stands Today.* http://www.keanebrms.com/portals/0/JLR-Fall%202005.pdf

Tillinghast - Towers Perrin. 2000. *Enterprise Risk Management: An Analytic Approach*. http://www.towersperrin.com/tillinghast/publications/reports/Enterprise_Risk_Management_An_Analytic_Approach/erm2000.pdf

Tillinghast - Towers Perrin. 2001. *Creating Value Through Enterprise Risk Management – A Practical Approach for the Insurance Industry*. http://www.towersperrin.com/tillinghast/publications/reports/Creating_Value_through_Ent_Risk_Mgmt/2002051306.pdf

Treasury Board of Canada. 2004. Integrated Risk Management – Implementation Guide http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/guide01_e.asp

Tripp, M.H; Chan, C; Haria, S; Hilary, N; Morgan, K; Orros, G.C; Perry, G.R; Tahir-Thomson, K. 2008. *Enterprise risk management from the General Insurance perspective.* http://www.actuaries.org.uk/__data/assets/pdf_file/0017/132038/sm20080428.pdf

UK Cabinet Office. Government Strategy Unit Report. 2008. *Risk: Improving Government Ability to Handle Uncertainty.* http://www.cabinetoffice.gov.uk/strategy/work_areas/risk.aspx

Wang, S; Faber, R. 2006. *Enterprise Risk Management for Property-Casualty Insurance Companies.* http://www.ermii.org/Research/downloads/erm_paper080106.pdf

Warrier, S.R; Chandrashekhar, P. 2006. *Enterprise Risk Management: From the boardroom to shop floor.* http://www.infosys.com/industries/insurance/white-papers/enterprise-risk-management-paper.pdf

Wason, S. 2007. *Repositioning ERM.* http://www.actuaries.asn.au/IAA/upload/public/1.a_Conv07_Paper_Wason_repositioning%20ERM.pdf

Yow, S; Sherris, M. 2007. *Enterprise Risk Management, Insurer Pricing, and Capital Allocation.* http://wwwdocs.fce.unsw.edu.au/actuarial/research/papers/2007/iisyowsherrisfinal.pdf