Enterprise Risk Management Specialty Guide

May 2006

Table of Contents

Foreword

Recently, the Society of Actuaries has undertaken an initiative to educate the public, and especially industry leaders who are in need of guidance in matters involving risk assessment and control, about actuaries' unique set of skills that are particularly relevant in today's climate of risk quantification, classification and mitigation.

This Specialty Guide on Enterprise Risk Management (ERM) is a work in progress, begun in the spring of 2004 by members of the ERM Working Group of the Society of Actuaries Risk Management Section to serve as a fundamental resource for a basic understanding of ERM, as well as a guide to further study of the subject. Members of the Casualty Actuarial Society have participated in the effort, as well.

Because ERM is a relatively new discipline, and because the background and expertise of the people contributing to and reviewing this Specialty Guide lie predominantly in the insurance industry, we decided that in this first phase it would be best not to stray too far from the insurance industry, and also that our target audience would be actuaries or actuarial students.

In subsequent phases, we would like to provide more in-depth treatment of specific risks, either by inclusion of more details within the document or by links to other sources. We would also like to expand the scope to more industries.

Although this effort benefited from input and feedback of many people, acknowledgements go to the following contributors for their exceptional efforts in the development of this resource:

Jennifer K. Bowen
Renee Cassel
Charlene Collins
Kevin Dickson
Melinda Fleet
Dave Ingram
Steve Meyers
Hubert Mueller
Zenaida Samaniego
José Siberón
Suzanne Wille
Mark Yu

Executive Summary

Chapter 1. Introduction

In its "Overview of Enterprise Risk Management," the Casualty Actuarial Society describes Enterprise Risk Management as:

> "…the discipline by which an organization in any industry assesses, controls, exploits, finances and monitors risk from all sources for the purposes of increasing the organization's short- and long-term value to its stakeholders."

Similarly, COSO defines ERM as:

> "…a process, affected 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 goals."

The definitions are compared and contrasted, and ERM is differentiated from traditional risk management (RM). It is the holistic aspect of the enterprise that makes the difference—the contribution to the overall portfolio risk, rather than the risk associated with each individual investment.

Generally, the appropriate risk context is that of the entire enterprise. The enterprise view is consistent with the economic decisions facing the organization. If an insurance company is able to reduce risk, it will be able to reduce capital and hence, costs. A second reason supporting the enterprise context is that it aligns with stakeholders' perspectives. An investor in an insurance company, like an investor in a particular mutual fund, is only concerned with the risk and return of the company in total.

With their technical backgrounds, actuaries are experts in quantifying insurance risk and by way of training are well positioned to quantify other types of risks and their interactions as well.

Chapter 2. Why is ERM Important?

Subsection 2a. Drivers of change and development of the discipline of ERM

1. Regulatory developments
2. Rating agency views
3. The COSO Report
4. Basel

5. Economic Capital
6. Conglomerates
7. Convergence of financial products, markets, globalization
8. Board attention due to public's demands for certain assurances

Subsection 2b. ERM Impact on Management Practices

The company's mindset toward ERM determines the efficacy of the risk management. Perhaps no single effort can produce greater results than developing the risk management culture—training, supporting, communicating, and compensating risk-smart behavior. As a risk management expert serving at the executive level, the Chief Risk Officer establishes a channel for two-way communication throughout the organization.

Through crisis planning, modeling and stress testing the company can train for a liquidity risk event in advance of its occurrence. Liquidity crisis management teams are selected to identify and manage risk events.

Subsection 2c. Other ways that ERM can contribute to value creation

Enterprises want to optimize capital and reduce exposure to risk. This is when ERM is an extremely valuable tool.

All enterprises have operational and financial risks thereby needing capital to cover these risks. Managing capital implies that there will be enough financial resources to cover operational and financial risk and managing risk implies that operational and financial risks are covered by capital.

Subsection 2d. Organizational objectives for pursuing ERM

1. Competitive advantage
2. Strategic goals
3. Shareholder value
4. Transparency of management (reduction of agency costs)
5. Decision-making
6. Policyholder as a stakeholder

Chapter 3. Enterprise Risk Management Process

The activities of ERM can be organized into four themes: Risk Control, Strategic Risk Management, Catastrophic Risk Management, and Risk Management Culture.

Risk Control is the process of identifying, monitoring, limiting, avoiding, offsetting, and transferring risks.

Strategic Risk Management is the process of reflecting risk and risk capital in the strategic choices that a company makes.

Catastrophic Risk Management is the process of envisioning and preparing for extreme events that could threaten the viability of the enterprise.

Risk Management Culture is the general approach of the firm to dealing with its risks.

Chapter 4. Decision-making

A key step is clarifying a company's risk appetite so ongoing strategic decisions can be made within an established risk-based context. Specific risks can be addressed on an ad hoc basis, but a more integrated assessment can be gained by performing a more complete analysis. This section describes a top-down process that could be applied to a specific risk as well as a broad overview.

The process unfolds by addressing the following questions:

- What is risk appetite?
- How can risk appetite be measured?
- How can your company define its risk appetite?
- Who are your stakeholders and what do they demand?
  - What will it take to meet key stakeholder demands?
    - Board of directors and management
    - Employees
    - Policyholders
    - Stockholders
  - What will it take to meet supporting stakeholder demands?
    - Rating agencies
    - Regulators
  - How do you create the strategies to meet these demands?
  - How will decisions be made within your risk management framework?
  - What are your risks to succeeding in these strategies?

Chapter 5. ERM Implementation

There must be an individual, or a small team, whose primary responsibility is to implement ERM. The business unit risk managers need to have a close relationship with the Chief Risk Officer (CRO) even though they report up through the business unit management.

Just as GAAP results and ROE are now key components in measuring an executive's performance, it is important that risk-adjusted ROE become a key component in executive compensation.

One of the key challenges in a conglomerate is specifying a uniform time horizon. In banks, the convention for modeling risks and assessing capital is to adopt a one-year horizon. Alternatively, insurance companies are typically capitalized for longer decision horizons.

Chapter 6. Examples of real-life situations in which implementing ERM has added value and/or avoided significant losses

Recent failures:

> A highly rated insurer was threatened with financial ruin and had to sell itself to a larger rival because it miscalculated the financial risks associated with a major reinsurance treaty.
>
> A large multi-line carrier with both primary and reinsurance operations was unaware of its total exposure, through its various business units, to a single natural catastrophe—until the catastrophe occurred.
>
> Some of the best-known names in the U.S. life insurance industry now face millions of dollars in fines, billions in policyholder restitution and near-crippling damage to their reputations because of the misleading sales practices of not much more than a handful of their agency sales force.

ERM has **added** value where management teams make decisions that:

> Exploit their firm's true risk-taking capacity
> Complement their existing risk profile
> Further their overall strategic objectives

Typically, these are also the companies that achieve higher ratings, as well as higher returns and higher valuations, with less capital than their peers.

Chapter 1. Introduction

This Specialty Guide is designed to be a source of information on Enterprise Risk Management (ERM) both for those new to the field and those more experienced. The Guide begins by defining ERM, discussing risk in the context of ERM and making a case for actuaries as prominent or leading players in the field. Subsequent sections cover:

- The importance of ERM and how it creates value for an organization
- The ERM process
- Decision-making
- Implementing an ERM program
- Real-world ERM examples
- A Glossary of ERM and related terms, and
- A Bibliography

The Guide is intended to inform interested parties as best as possible, but should not be taken to define or endorse a particular set of "Best Practices."

Enterprise Risk Management Defined

As a relatively new field of practice, ERM has quickly taken on a number of different meanings. This leads to confusion as people talk about ERM and it may appear that they are talking about seemingly different things. Therefore, it is important to begin by examining these meanings in order to be aware of the potential uses of ERM and to begin to develop a common understanding of the term.

In its "Overview of Enterprise Risk Management," the Casualty Actuarial Society describes Enterprise Risk Management as:

> "… the discipline by which an organization in any industry assesses, controls, exploits, finances and monitors risk from all sources for the purposes of increasing the organization's short- and long-term value to its stakeholders."[1]

Similarly, COSO defines ERM as:

> "… a process, affected 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 goals"[2]

These two definitions have several points in common. Both definitions speak of ERM as a process. ERM is an organized, systematic way of managing risks throughout the organization. ERM is not a once-and-done activity, but an ongoing process. A further reading of these publications suggests similar process steps (the subject of Section 3 of this Guide)–identifying, measuring, prioritizing, managing and the on going monitoring of risks. That ERM is described as a process suggests that it is intended to become an integral part of how an organization operates.

Both definitions speak of ERM as applying broadly both in terms of the risks it encompasses and to the organizations to which it applies. Risk is not limited to a set of financial or insurance risks. Instead, "risk" applies broadly to all things threatening the achievement of organizational objectives. In the same way, ERM is not meant to apply merely to insurance companies or to financial institutions. Instead, ERM applies broadly to all organizations. Even the use of the term "organizations" rather than "companies" reflects this broadness. Combining the "process" and "broadness" aspects suggests that

the ERM process is generic. While the specific risks and the details of the ERM process play out differently from organization to organization, there is a single, common foundational process. As a result, ERM practitioners may find they have more in common with those from fields far removed from insurance or financial services.

Lastly, both definitions stress the value creation. By more effectively managing risk, organizations can better achieve their objectives and create value for stakeholders. In both publications, the term risk is not limited to threats, but also includes opportunities. Therefore, appropriate risk management actions consist not only of risk avoidance and mitigation, but may include risk acceptance and even risk-seeking activities. Instead of risk minimization, the goal is seeking an appropriate "risk-return position."

It is also important to consider how these definitions differ from traditional risk management. After all, risk management itself is not new. Risk managers have been about the business of anticipating, managing and monitoring risks for a long time. What then is it about Enterprise Risk Management that is new and different?

To answer that question it is instructive to focus on the term "enterprise." What do organizations mean when they talk about ERM? What does the "enterprise" stand for? Again, while there are many definitions depending on the situation and the organization, there are perhaps two main definitions. In many instances, the term has an Auditing/Process Control nuance. In this sense, "enterprise" speaks to processes used consistently and effectively throughout the enterprise. Risks are managed by establishing control processes. It also speaks to a consistent and comprehensive approach. All significant organizational risks should be included within the scope of ERM processes.

As an offshoot to this "process control" sense, it may also mean the linking of strategic planning and organizational objectives to ERM processes. As an illustration, consider a company with an earning target of $X for the upcoming year. That company may choose to employ ERM processes to identify and prioritize threats to achieving the earnings target. It may establish control processes regulating the most significant risks, seeking to reduce the possibility and severity of an earnings shortfall. Over time, the organization should be able to exert more effective controls and, therefore, have greater confidence of achieving earnings targets. This can be thought of as a Quality Control approach to achieving organizational objectives.

A second main definition has roots in Investments and Finance in which "enterprise" has a meaning synonymous to "portfolio." The idea is that an organization is a collection of risky activities in the same way that a mutual fund is a collection of risky investments. A skilled portfolio manager faced with a universe of potential investments–each risky on a stand-alone basis–may be able to combine them into a low-risk portfolio. Portfolio risk depends not simply on the risk of the individual investments on a stand-alone basis, but also how they interact with each other. In a sense, the risky investments lose their identity when combined into the portfolio.

In the same way, an organization can be thought of as a collection of risky activities. Now "investments" may be a collection of insurance policies or other financial products, customer, geographical, or other categorization segments. There is wide latitude as to how "investment" is defined. As before, each individual investment has some risk and return expectation. A skilled enterprise risk manager may be able to combine these risky investments into a low-risk portfolio. As before, risk associated with each individual investment is no longer relevant, ***but only their contribution to the overall portfolio risk.*** This is a subtle, but critical, distinction to which we shall return to shortly.

Both the “control” and “portfolio” definitions are in use today. In fact, there are likely many other functional definitions differing in details. Multiple definitions create confusion, but it is hoped that confusion can be avoided by recognizing that multiple definitions exist. This Guide does not select between the “control” and “portfolio” definitions, but instead, suggests that both are legitimate uses of the term and both should be pursued as part of an ERM program.

A Context for Risk

The goal of ERM is to effectively manage risks facing the organization. Returning to the portfolio concept, enterprise risk managers should be focused on the business of effectively managing risk and return. Within the portfolio, “return” is relatively straightforward and easily understood. It has a common, shared context. Expected return is the weighted sum of the expected returns of the individual investments.

Risk is not so easily understood. Consider, for example, a collection of insurance policies. One might think about risk in terms of the variation in underwriting results of those policies and mentally compare that risk to the expected return of those policies. This would be one “context” or mental method of comprehending risk. Further, if these policies are volatile then one would conclude that they are “risky” compared to their potential return.

In another situation, a person’s risk context might be to think of the risk of these policies relative to an entire product line. Depending on the circumstances, the policies may or may not appear to be “risky.” A person might naturally compare the risk based on some management-delegated authority limit. For instance, a manager with authority over a particular geographical region may naturally compare the risk of those policies to some metric representing that region. Again, depending on the circumstances, the polices may or may not appear risky and depending on the perception, certain risk management actions would take place.

Further, another person’s risk context may be the entire enterprise. That person would compare the risk of the subject polices to the entire enterprise. Again, depending on the circumstances, these polices may no longer appear to be risky. In fact, they may now be viewed as having little risk in comparison to the enterprise as a whole and adding little risk to the enterprise.

By now it should be clear that the “risk context” does matter in terms of how risk is perceived and consequently, what risk management actions may be taken. Further, it may seem that no context is any more or less appropriate than another. Depending on the circumstances and one’s preferences, it may seem that one is free to select any risk context. But Portfolio Theory does not allow such freedom. A foundational principle of Portfolio Theory is that the portfolio in total is the appropriate risk context.

This Specialty Guide supports the view that, generally, the appropriate context is that of the entire enterprise. In addition to aligning with Portfolio Theory, there are two reasons we would give as support. First, the enterprise view is consistent with the economic decisions facing the organization. An insurance company holds costly capital to support its operations. If it is able to reduce risk, it will be able to reduce capital and hence, costs. The company has many risk management actions available. If it used reinsurance, for example, it would estimate the total or portfolio risk reduced, translate the marginal capital reduction to a marginal dollar reduction (through the cost of capital or other means) and then be able to compare that amount versus the cost of reinsurance. As with any economic decision, if marginal revenues exceed marginal costs, the decision adds value to the firm. Viewing risks in isolation, in a “silo,” gives a misleading reading on overall risk reduction and therefore, does not line up with the economic decision the firm faces.

A second reason supporting the enterprise context is that it aligns with stakeholders' perspectives. As regards risk, an investor in a particular mutual fund is only interested in overall risk and return–not risk of the individual investments that make up the fund. (A contention that investors are only interested in systematic risk does not detract from the argument. In that case, the point remains that investors are only interested in systematic risk of the portfolio. They are concerned about the systematic risk of the individual investments only to the extent that they have an impact on the systematic risk of the portfolio.) Once the investor has purchased the fund, they are subject to the risk and return prospects of the fund in total and not the individual components of the fund. Likewise, an investor in an insurance company is only concerned with the risk and return of the company in total. That investor is only concerned with individual products or other components to the extent of their impact on total company risk and return. Insurance company claimants are concerned that the enterprise in total has the financial strength to pay potential claims. This concept can be extended to other organizations as well.

Nonetheless, whether through the delegation of authority for some other reason, one is easily reminded of examples where the risk context is something other than the portfolio in total. A risk-adjusted performance incentive scheme, where risk is measured or compared to some subset of the organization, would be one example. Without going further than advocating a general practice of using the portfolio context, it is suggested that organizations give serious thought to the risk context and how that context impacts risk measurement and management in their organizations. If not, organizations may find that risk management is at odds with stakeholder interests and leads to sub-optimal actions.

A Case for Actuaries

Since the portfolio context establishes the basis for risk measurement and management, and hence, economic decisions, it is important to think about portfolio risk and to try to measure and estimate it as best as possible. This involves measuring individual risks and all their interactions. And while one may very quickly think of any number of real and significant technical issues involved in the measurement process, this should not deter the enterprise risk manager from having an enterprise risk mindset and attempting to measure risk as best as possible.

Therefore, it would seem that actuaries are in an ideal position to be effective enterprise risk managers. With their technical backgrounds, actuaries are experts in quantifying insurance risk and, by way of training, are well positioned to quantify other types of risks and their interactions as well. And while risk managers increasingly acknowledge the value and need for enterprise, holistic modeling, to date it appears there are few working models. Again, this is likely due to the current real and significant barriers to quantitative modeling. But one can assume that advances in technology and quantitative expertise will continue and, therefore, it makes sense for the profession to take steps now to best position itself to be the risk modelers and Enterprise Risk Managers of choice in the future.

Of course, Enterprise Risk Management is more than simply quantifying risks, but this is a key step and one in which the actuarial profession would do well to consider as a means to be more effective players in ERM.

Conclusion

After explaining the case for the value of ERM to an organization in the next chapter, the Guide will go on to cover the ERM process in detail, describe how risk and return decisions are made in an ERM context and covers real examples of how ERM adds value to an organization.

Chapter 2. Why is ERM Important?

Subsection 2a. Drivers of change and development of the discipline of ERM

1. Regulatory developments[17],[18],[19]

Risk Management is not new. The concept has been around in investment, banking, insurance, artificial intelligence, and public policy processes, for example. It is important to note that the types of risk and focus vary by industry, and may encompass related corporate governance and accounting practices. Following is a chronology of regulatory and related developments.

The Basel Committee on Banking Supervision was formed in 1974 from among central bank governors and regulators from major industrialized countries. At the committee's 1988 meeting at the BIS (Bank for International Settlements) in Basel, the "Basel Capital Accord" was reached, setting forth a new framework for minimum risk-based capital requirements for internationally active banks which has been adopted by over 100 countries worldwide. The accord has undergone various revisions leading to the latest "Basel II" accord in 2004.

In 1985, COSO (Committee of Sponsoring Organizations) formed an independent, national commission to undertake a private sector study of factors that cause fraudulent financial reporting. The COSO framework that was developed subsequently set forth recommendations for internal controls needed to identify and monitor risks. This led to the practice of senior executive workshops that utilize risk registers or risk maps to rate and track the likelihood and impact of risks. Another resulting common practice was the use of control self-assessments.

In 1992, the London Stock Exchange introduced new regulations following a series of high profile corporate frauds and accounting scandals. The new rules are based on the Cadbury Committee's Code of Best Practice covering financial aspects of corporate governance that would apply to publicly held companies. The current United Kingdom rules are contained in the Hampel Committee's "Combined Code," whereby U.K. listed companies are required to evaluate their internal controls covering all types of risks.

Following the debacle in the insurance industry resulting from the collapse of insurers and their failure to honor insured pensions and other guaranteed benefits, the U.S. Department of Labor promulgated an interpretive bulletin in 1995 dealing with the selection of safe annuity providers. A year earlier, the NAIC (National Association of Insurance Commissioners) issued a major solvency regulation in the form of risk-based capital requirements for property/casualty

insurance companies. The new rules are predicated on an actuarial and financial analysis framework that formulates minimum capital charges and co-variance adjustments for the various risk components that insurers must set up by law.

A string of corporate accounting scandals had profound implications in the U.S. and worldwide, and led to the passage of the Sarbanes-Oxley Act of 2002. The new laws included risk management processes aimed to keep internal controls up to date. One of the key provisions requires that SEC registered companies evaluate the effectiveness of internal controls over information issued in the capital markets and have such evaluation audited and made public.

The development of national standards on Risk Management began with the first-ever AS/NZS (Australia/New Zealand Risk Management Standard), which was issued in 1995 (updated in 1999) creating a generic framework for the risk management process as part of an organization's culture. This presaged similar standards in Canada (Dey report, 1997) and Japan, and in the United Kingdom (2000). The ISO (International Standards Organization) is working with other countries and regions in Europe who are considering similar standards, particularly in the area of common global terminology.

There are information technology security management-related frameworks as well, including COBIT (Control Objectives for Information and Related Technology) framework developed by ISACF (Information Systems Audit and Control Foundation). One standard that applies to effective project management, PRINCE2 (Projects in Controlled Environments) is widely recognized in the United Kingdom and internationally.

The supervisory authorities for the financial services industry include Canada's OSFI (the Office of the Superintendent of Financial Institutions), the United Kingdom's Financial Services Authority system of risk based supervision, and in the United States, S&P (Standard & Poor's) with their risk-based capital adequacy model for financial products companies and Moody's Financial Institutions with their ERM model to deal with corporate governance guidelines for the general industry. Within the insurance industry, the regulatory framework is embodied in APRA (the Australian Prudential Regulation Authority) and in the United States, the NAIC, A.M. Best's ERM holistic model for capital adequacy measurement, and Moody's C-3a risk-based capital component.

2. Rating agency views

In the last ten years, the U.S. life insurance industry has become more effective in managing risks. But, in general, the industry is three to five years behind where they should be in terms of enterprise risk management's best practices compared to other countries and financial institutions.

The rating agencies have also increased their surveillance on the topic of enterprise risk management. The ratings of insurance companies have always included the view of the company's ability to manage its risks. In addition, since the early 1990s, the industry was one of the first to implement the concept of the risk-adjusted view of capital and earnings. The main difference is that companies, through new technology and advancements in the area of enterprise risk management, are becoming more capable of answering questions about frequency and severity of both known and unknown risks affecting the enterprise.

Some rating agencies are taking a more proactive approach at evaluating the strengths of an organization with respect to enterprise risk management. In general, this evaluation is starting to affect the views of the individual companies' prospective financial strengths because of the increased levels of information available to better evaluate the risk adjusted capital and

earnings power. In addition, more companies with strong enterprise risk management culture and capabilities are better positioned to understand the vulnerabilities of the organization and create strategies to mitigate any potential negative impact to the enterprise and its stakeholders. As a result, some companies are using these tools to generate competitive advantages through innovative product development and pricing, or by avoiding large losses in down cycles of the markets, or acquiring less efficient companies.

The rating agencies are starting to ask questions about the companies' internally developed economic capital models. Unfortunately, as of 2004, only a handful of companies have developed an economic capital model that could be shared with the rating agencies or other interested parties. The main benefit of these models is to develop a good dialogue between the company and the rating agencies about the difference in views of certain risks and the risk based capital analysis. Economic capital models help to quantify these differences and to better understand the dynamics of various risks as well as their impact on the company's capitalization strength. Rating agencies can use this information to better understand the strengths and weaknesses (or vulnerabilities) of a company. The information necessary to build an adequate economic capital model is too large and the tools too complex for the rating agency to properly build its own economic capital model. Therefore, static capital models will continue to be used to compare risk-adjusted capitalization among companies in the industry. The economic capital models developed internally by companies would be reviewed and validated by the rating agencies and they could be used as additional tools to opine on the capitalization strength of the enterprise.

The first aspects of enterprise risk management upon which rating agencies are focusing most of their attention are ALM, investment risks, liability or pricing risk, and the area of risk transfer.

In general, risk management should start at the product development. If the risks of the products being manufactured are not well understood, the company will be vulnerable to surprises that could impact its financial strength and ratings, and ultimately it could become insolvent. Usually, by the time a product is launched in the market it is already too late to re-price the product or to adjust it for unforeseen risks that weren't captured during the product development process. Actuaries have always played a very important role in this part of the enterprise risk management process. But, the complexity of the products being developed today and the increased competition from banks, mutual funds, and other financial institutions, are forcing actuaries to increase their risk analysis skills and perform more testing before launching a new product into the market. In addition, using traditional actuarial techniques such as looking at historical experience is no longer practical because the world has become more complex and better equipped to take advantage of ineffective products. Now, more sales are coming from non-proprietary distribution channels such as independent agents, banks, and brokers/ dealers that are constantly testing the adequacy of the prices of the products being launched today. Investment bankers are finding arbitrage opportunities in the options embedded in insurance products and more life insurance products are sold in the secondary markets. This is something that the insurance companies and their actuaries have never faced before because most insurance products are priced assuming that the policyholders will not exercise the options embedded in the insurance products effectively. In the banking world, where a secondary market and more liquid markets exist, pricing assumptions assume that holders of the products will exercise the options available to them efficiently. Otherwise, some smart investors will capture arbitrage opportunities quickly. The insurance industry is not at this stage yet but actuaries and management should look into these potential risks and understand the consequences as proper enterprise risk management.

Standard & Poor's have presented in various forums some key questions related to enterprise risk management that insurance companies need to be prepared to answer to rating agencies. Among them are:

- Does the company have an integrated enterprise risk management function? If yes, how does it fit in the organizational structure? Does the company have a CRO or just an ERM committee? Who does the CRO or the Committee report to?
- Does the company have a well-integrated risk management culture?
- How strong is the support for the risk management function?
- Describe the adequacy of the audit and control systems, quality of management reporting, aggregation of risks, risk limits and guidelines, and how accessible are they?
- How is the Board of Directors informed about the ERM results?
- How is management compensated?
- Are there predetermined limits for levels of risk it will accept?
- What are the company's major risks? How are those risks mitigated? What is the economic impact to those risks over various confidence intervals? Does the company measure the tail risks? How does it protect from catastrophic events?
- How does ERM add value to the corporation?
- What is the level of connectivity between the product development area and other areas such as valuation, investment department, corporate, etc.? How does the company price its products and how does it know that it is compensated to the level of risks being taken?
- Describe your ALM and what are you doing to optimize your returns?
- Describe the major options offered in your liabilities and how are those mitigated or accounted for in the company's economic capital?

Since 2004, rating agencies have been increasing the importance of their analysis by assessing whether enterprise risk management is engrained in the culture of the corporation and in the way its business units and employees make everyday decisions. Although this is becoming an increasingly important subject of conversation with the insurance company's management, it is just another exercise in the overall analysis of the rating.

3. The COSO Report [28],[29]

In 2001 the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, led by PricewaterhouseCoopers, initiated a study to develop practices for managing risk across an organization. By identifying the key issues and proposing guidelines and applications, COSO formalized a reporting structure to support Enterprise Risk Management.

The COSO methodology inspires confidence by offering a definite framework for ERM. Furthermore, COSO stresses ERM as an iterative process that aligns risk response with the strategic objectives of the enterprise. This approach produces a dynamic audit of the risks identified.

However, a framework alone does not enable an organization to explore the risk landscape. Going beyond the discipline of an ERM structure, the present ERM Specialty Guide advocates the use of risk analytics that produce quantifiable data for risk-smart decision-making. Risk analytics can expose the circumstances that give rise to risk and can quantify the severity of risk. If ERM stops at procedures and controls, unknown risk can easily remain concealed. By contrast, risk analytics have the potential to reveal hidden risks before negative events occur, and to exploit opportunities that would otherwise be missed. With the emphasis on gaining insight into risks rather than on categorizing risk activities, such analysis allows management to shape the ERM framework and tools around the risk environment. By providing building blocks for understanding and managing the risks specific to the organization, risk analytics add value well beyond general best practices.

To summarize and compare the two approaches, a detailed discussion of the COSO Report is followed by the Academy of Actuaries response.

The foundation for the ERM methodology was based on COSO's 1992 Internal Control–Integrated Framework, a publication that formulated a uniform approach to managing internal control systems. Working from this document, COSO expanded the approach by integrating these controls throughout an enterprise. COSO's resulting document, Enterprise Risk Management Framework, provides a risk management architecture in terms of eight components to be considered under each of four categories of objectives. This blueprint is followed at every level of the organization, for the entity, the divisions, the business units and the subsidiaries.

The Four Categories of Objectives:

Each level of the organization applies the eight components for ERM to the following four categories of objectives. A particular objective may be classified into one or more categories. Hence, the classification may delineate the objective into multiple lines of authority.

Because ERM is applied in a strategy setting, the strategic objectives are designed to encompass the entity's mission or vision. The implementation of all other categories of objectives must align with the strategic objectives.

1. Strategic–High-level goals designed to support the entity's mission or vision.

2. Operations--Efficiency of operations, including achievement of performance goals and safeguarding against loss.

3. Reporting--Reliable financial and operational data and reports.

4. Compliance--Compliance with laws and regulation.

The Eight Components:

ERM is a multi-directional iterative process in which the eight components influence one another. The dynamic application of ERM recognizes the inter-relationships between components and considers the impact of each component on the others. These eight components for achieving the four categories of objectives form the framework of ERM.

1. Internal Environment: The Internal Environment is the context within which the enterprise functions. The organization's reporting structure, assignment of authority, development of

personnel, risk appetite, management style and ethical values are key elements of the Internal Environment. This foundation and culture set the course for how risk will be handled across the enterprise; the independence and involvement of the board of directors and the tone set by management have a critical influence on the internal environment. Companies will differ in the level of formality of lines of authority and operating procedures; however, risk practices developed under the consideration of management will preclude the spontaneous formation of a haphazard risk culture throughout the organization.

2. Objective Setting: A mission or vision is enacted through the objectives set by the organization's management. ERM requires that objectives are established that lead toward achievement of the mission or vision in a manner consistent with the organization's risk appetite. Objectives are a focal point of risk strategy. This is because risk events are identified in terms of their effect on the achievement of the objectives.

3. Event Identification: Both internal and external events are considered in terms of their impact on the achievement of objectives. Identifying potential events and distinguishing between those representing loss, opportunity or a combination of both, allows categorization of events into a common risk language, and creates a basis from which a portfolio view of risk can be formulated.

4. Risk Assessment: Identified risk events are analyzed in terms of the likelihood and impact of the range of potential outcomes. Management prepares for the effect of risk events on a given objective.

5. Risk Response: Because the response to a risk event must align with the entity's objectives and risk appetite, a silo approach considering only the immediate context of the business level in question will not yield effective risk management. Rather, a portfolio view encompassing the organization in aggregate must always be maintained. Four categories of response are available:

    - Avoidance–Exit the activity, giving rise to risk
    - Acceptance–Do nothing to alter either the likelihood or the impact of risk
    - Reduction–Reduce the likelihood and/or impact of risk, often via everyday business decisions and processes
    - Sharing–Mitigate the impact and/or likelihood of risks through purchasing insurance products, pooling risks, and hedging and outsourcing risky activities

6. Control Activities: The risk responses are established and executed according to policies and procedures that comprise the control activities.

7. Information and Communication: Management ensures that risk policy is communicated to all levels throughout the organization. All employees understand their roles and responsibilities within the organization. They also provide insight into their respective areas regarding the effectiveness of risk policy and raise awareness of risk events that have not been addressed.

8. Monitoring: A dynamic risk management system is established by responding to ongoing assessment by management as well as to independent audit results.

Limitations of ERM

ERM does not provide absolute assurance that the organization's objectives will be met as actual risk events are subject to the uncertainty of the future. Instead, ERM identifies and monitors risk events deemed significant to the organization's mandates. Further, ERM is limited by the imperfections of the people entrusted with its implementation. Five factors influence the quality of ERM:

- Judgment–Human judgment can falter under the pressures of time and information constraints.
- Breakdowns–Mistakes and errors can result from fatigue, distractions, or lack of training and experience.
- Collusion–Two or more individuals may collude to circumvent controls, conceal activity or alter data.
- Cost versus Benefit–The benefit of a risk concern must be weighed against resource constraints. Valuation of costs and benefits may be directly measurable or may be subjective assessments. For example the cost of a training program to assess creditworthiness is quantifiable, whereas customer response to cumbersome qualification procedures is not.
- Management Override–Management override suspends prescribed controls for illegitimate purposes. Whereas management intervention may be necessary for processing exceptional transactions, management override misuses authority for proscribed activities.

Actuaries' Response to COSO

To take full advantage of the opportunistic side of risk, the guidelines for ERM would benefit from further development of the strategic objectives. As discussed below (Section 2B, 4), the banking industry offers sophisticated controls for financial risk management. Additionally, the actuarial profession possesses a wealth of experience in exploiting risk as opportunity; it has long-standing record of converting risk mitigation into profitable products. Greater emphasis and detail on the following topics would provide more extensive guidance for the strategic, high-level objectives.

- Risks external to the entity and outside of management's control
- Interdependent risks and cross-functional issues
- Coordination of risk management within the entity
- Transparency of the risk management system
- Reputation of the firm
- Quantification of risk, including consideration of risks for which not much data exists–such as future or infrequent risks, or correlated risks
- Long-term evaluation of risk, including scenario planning and stress testing

4. Basel[20,21]

The 1988 Basel Capital Accord was a major initiative toward the creation of a global framework for measuring capital adequacy and developing a minimum standard that would be fair and consistent in ensuring a sound and stable international banking system. The basic components of capital are defined as equity capital and disclosed reserves, which are common to all countries' banking systems as the basis for market judgments of capital adequacy. For supervisory purposes, a second tier or supplementary element of capital would be required consisting of various reserves and debt capital instruments. A weighted risk ratio approach relates capital to different asset and other categories according to relative degrees of risk. Countries may hold higher levels of minimum capital.

The 2004 Basel II accord recognizes changes in banking and risk management practices and has more risk sensitive capital requirements and assessments based on banks' internal systems as inputs to capital calculations. Augmenting the minimum capital standards (pillar 1) are a robust implementation of supervisory review of capital assessments (pillar 2) and market discipline (pillar 3). A proactive dialogue in the global community will be necessary to prevent inappropriate disparities between regulatory and accounting standards. A dynamic approach will help ensure a capacity to evolve with time and modern developments.

5. Economic Capital[22,23]

A corporation needs economic capital to fund its operations and meet financial obligations, even under adverse conditions. To regulators and the public, the level of capital a corporation holds is also used as a measure of financial soundness.

Capital and risk are related. An effective capital and risk management system uses a basic risk-return framework that assigns economic capital to various risk exposures.

As each company is unique, so are the risk exposures and the methodologies used to measure these risks and allocate economic capital to such risks.

To be successful, the system needs to be an integral part of the corporate culture, with management buy-in and support from stakeholders. It must therefore be consistent and coherent, dynamic and up to date, well researched and balanced (information versus judgment), inclusive and cooperative across the organization.

6. Conglomerates[24,25]

A conglomerate is a company that is engaged in a variety of business operations, which are mostly unrelated to its primary activity. By design, the diversity of its operations is aimed to reduce risks to the company due to varying impact of business conditions over time. Typically conglomerates are global giants that arise from mergers and buyouts, which if not done with care can make the ultimate structure too unwieldy and out of sync. Interlocking directorates and clientele can often lead to conflicts of interest, and when conglomerates fail, based on sheer size and reach, the fallout can be vast and far-reaching. While this sounds rather extreme, the need for good corporate governance and coherent risk management are more necessary than ever in a conglomerate setting.

The unraveling of some old monopolies was a response to public and regulatory concerns. However, the recent demise of mega accounting firms, communication and other industry giants, has pointed to the lack of internal controls and coordinated regulatory oversight, among others, as common culprits.

7. Convergence of financial products, markets, globalization[26,27]

Conglomerates have been popular among investors during the 1960s, less so in the 1970s and 1980s. Never the less, the consolidation and globalization of financial products and markets have continued unabated. The banking industry has taken a lead in risk management practices, and consortiums of European countries and other financial authorities have set standards and guidelines in this area. In the insurance industry, property and casualty companies have also made significant advances.

Banks and insurance companies face many of the same risks and some different risks, likewise some similar and some different approaches to risk management have been developed. It is critical that business planning, product development and strategic systems are integrated, so must enterprise controls and regulatory standards that have such impact on the markets for private and publicly held companies alike. It does not matter who lags whom, but it is important that we learn and start with the existing infrastructure and latest and best methodology and technology that are available for our use. For example, there are models in both the private and public sectors that embody capital markets and economic paradigms in forecasts and projections of product liabilities and other risks.

There are countries like Canada whose regulatory authority encompasses both banking and insurance industries. International standards for accounting and capital markets discipline are converging, even while new financial products and markets continue to be formed and cross-sold and cross-marketed in many countries by worldwide institutions.

8. Board attention due to public's demands for certain assurances[13,14,15, 16]

In response to corporate scandals that have created distrust in public company financial reporting, the Sarbanes-Oxley Act of 2002 established the Public Company Accounting Oversight Board (PCAOB). This private, non-profit organization is charged with overseeing the audit of public companies--those companies having securities held by public investors and subject to security laws. Although auditing is not risk management, it can be made an integral part of the process. By creating and enforcing standards for the auditors of public companies, the PCAOB aims to provide public investors assurance of "informative, accurate and independent audit reports." (Sarbanes-Oxley Act, Section 101(a))

All U.S. accounting firms that prepare audit reports for U.S. public companies must register with the PCAOB. The Board's powers include establishing standards for auditing, quality control, ethics, and independence for the registered public accounting firms. Further, the Board is authorized to conduct routine inspections and investigations into alleged misconduct. Areas not traditionally covered by audit firms, but essential to ERM, will be incorporated into the standards required by the PCAOB, such as:

- the "tone at the top"–the expectations conveyed by leadership, and their efficacy
- the compensation and promotion of audit partners, including reinforced behaviors
- the communication and training practices for audit professionals

Under the rules adopted by the Board in September 2003 and approved by the Securities and Exchange Commission (SEC) in May 2004, the Board can enforce compliance and determine disciplinary actions for the registered firms and the persons associated with such firms.

Sanctions available to the Board range from imposing monetary penalties or remedial measures to barring firms or individuals from the practice of auditing public companies.

To ensure the integrity of its own operations, the PCAOB has an internal oversight committee, the Office of Internal Oversight and Performance Assurance (IOPA). Moreover, the Board will open its meetings for observer status and speaking rights to four organizations, Financial Accounting Standards Board, the Government Accountability Office, the International Auditing and Assurance Standards Board, and the SEC.

Subsection 2b. ERM Impact on Management Practices

Enterprise Risk Management standards must accommodate a range of company environments from small to large, decentralized to hierarchical, and informal to formal lines of authority. Also, because different industries face, and tolerate, different risk profiles, controls that are appropriate for one industry may not be meaningful to another. Rather than controlling risk from a canned prescription, a company's management team must design ERM around a set of guiding principles.

The company's mindset toward ERM determines the efficacy of the risk management. Developing a culture of risk management rallies company-wide cooperation, talent and expertise to bear on any and every aspect of risk. Perhaps no single effort can produce greater results than developing the risk management culture–training, supporting, communicating, and compensating risk smart behavior. Employees persuaded of the company's attitude toward risk can contribute to the design of risk practices within their areas of expertise and are better equipped to detect hidden risks in routine operations. The practice of building an ERM infrastructure and tailoring compensation to support RM values will be elaborated in Sections 5D and 5F.

With an ERM infrastructure in place, line management can be relied on to perform the initial risk analysis. Competent managers, already experts in their unit's role within the company, can fold risk controls into business decisions to protect the company from inappropriate risk exposure. Under a strong RM culture, the value of RM is broadly recognized within the company and no competent manager would suggest a product that inappropriately exposed the company to risk. The results of the risk analysis may or may not roll up to the formal ERM team depending on how they can be used; the analysis may facilitate the unit's own business decisions, or it may reveal risks that should be considered in aggregate with the company's portfolio of risk by the ERM team's executive management (Section 3F). Ideally, risk information is shared where risks are most strongly linked.

To be truly embedded in the company culture, ERM must have a voice at the executive management level. The board of directors is responsible for making certain that senior management establishes RM strategies that optimize available resources. Senior management must have sufficient knowledge of and expertise in the company's activities to develop RM systems and controls and to judge their success. As an RM expert serving at the executive level, the Chief Risk Officer (CRO) (Section 5A item 2) establishes a channel for two-way communication throughout the organization. Responsibility for RM must be independent of risk-taking functions to prevent conflicts of interest. The role of oversight for RM must be clearly documented, and relationships between compliance, internal audit and management functions should be unambiguous. Company culture, involvement by line management, two-way communication, support at the executive level, and expert use of appropriate ERM guidelines determine the efficacy of RM in achieving the company's goals.

Once in place, the ERM team charged with overseeing RM affords the company an enterprise-wide view of opportunities and threats. By understanding individual unit risk, or silo risk, and by assessing the individual risks in aggregate, the ERM team can evaluate an accurate cost of the company's risk exposure. The company can then charge back the cost of risk to the individual business units by requiring them to hold appropriate reserves (economic capital). Analogous to the capital budgeting

process, the allocation of risk capital according to the reserve requirement achieves an efficient use of company resources.

The ERM team can yet again add value by taking further advantage of the portfolio view of risk. The mitigation of silo risk viewed through the lens of corporate strength may reveal opportunities for new products and investment strategies that would otherwise remain hidden. Diversification of division risk may expose lucrative opportunities for the company in instances that show no or negative significance for the individual unit; pooled risks present a different profile than the constituent risks at the individual level, as discussed in the Introduction–Enterprise Risk Management Defined.

As an example of integrating risk management across an organization, consider a company's liquidity--its ability to raise cash. This key element of financial strength can be a source of profit or drain. Failure to meet obligations can quickly throw a company into financial ruin.

Yet even generous reserves and economic capital cannot obviate liquidity risk. Instead, an over supply of cash may harm the company by tying up limited resources needed to realize the company's objectives. A well-designed risk management strategy is essential to preparing for uncertain events without undermining corporate strength.

Through crisis planning, modeling and stress testing the company can train for a liquidity risk event in advance of its occurrence. Liquidity crisis management teams are selected to identify and manage risk events. Risks identified for study can include historical examples experienced by the organization itself or by another organization, and "what if" scenarios of the kind or magnitude not yet experience. Topics covered by a liquidity crisis management team include:

- Organization, such as how often the team will meet
- Who is authorized to declare an event
- What event is being measured
- How an event is identified, or an example of what an event looks like
- How the severity of an event is categorized–"heightened awareness" or "crisis level"
- What actions and steps are to be taken
- Who is to be notified
- What reporting is needed

Stress testing uncovers the responses available to the company in the event of a crisis by reproducing the historical examples, or by modeling pressures affecting liquidity with the "what if" scenarios such as "run on the bank" and "impaired markets." Estimates of the company's ability to raise cash, such as through the sale of assets, show whether the various scenarios can be covered. The test results can also be used to price for liquidity risk in the product development stage. Furthermore, the stress testing can be applied to all divisions of the company, down to the business unit level, to determine the viability of each division under a risk event.

Once all material risks are identified for a new product or project, crisis planning and ERM consideration of company risks in aggregate can be applied to each risk type (liquidity, etc.) to determine the risk cost or opportunity. The total burden or benefit of the associated risks will affect the decision to pursue the new product or project. This methodology can also inform the evaluation of strategic alternatives, and the assessment of new market opportunities or investment strategies.

Subsection 2c Other ways that ERM can contribute to value creation

In the past decade, there have been many mergers of companies of all sizes. Companies have combined with companies within their industry as well as outside their industry, i.e. banks with insurance companies. When a company is small, there are few employees and even fewer at the

helm. It is easy for a handful of people to manage both the assets and liabilities at small companies. Whether or not the asset and liabilities are properly handled is another matter. However, as companies grow, more people are employed to run the different departments that begin to emerge. Along with the growing pains, employees begin to have a better understanding of their particular department but tend to know less and less about the workings and issues of other departments. This compartmentalization magnifies with growth and mergers. Large companies tend to have departments just to manage debt portfolios, equity portfolios, and different product lines, i.e. life versus health, and the very large companies have companies within companies.

Although, practitioners of each component of an enterprise may be quite skilled, there must be an overall risk management plan and system for an entire enterprise. Enterprises want to optimize capital and reduce exposure to risk. This is when ERM is an extremely valuable tool.

All enterprises have operational and financial risks thereby needing capital to cover these risks. Managing capital implies that there will be enough financial resources to cover operational and financial risk and managing risk implies that operational and financial risks are covered by capital (Shimpi 2003). Thus, efficiently managing capital and risk together is essential to survival and will reduce the enterprise risk.

The first step is to outline risks of the firm and quantify each one. Next, a dynamic financial model can be developed. Most importantly, the model should recognize all courses of capital available–including equity (for capital adequacy), debt (for financial leverage), and insurance (for risk leverage). Shimpi (1999) defines the term "Insurative" as "any corporate capital resource, be it debt, equity, insurance, derivative, contingent capital or any other." He then builds an Insurative Model defining total average cost of capital (TACC):

- TACC = cost of debt x debt value/firm value
- + cost of equity x equity value/firm value
- + cost of insurance x insurance value/firm value

This model helps determine how capital can be used to increase efficiency by using all sources of capital. As Shimpi (2003) explains, "the term 'insurative' recognizes that each form of capital carries some risk of the firm and can therefore be thought of as insurance or a derivative." For detailed description of the Insurative Model, see Shimpi (1999, 2003).

Once the Insurative model is completed, then the ERM team can review their findings with the enterprise employees. From there, any nuances can be discussed along with any new developments. Then decisions can be made as to how to best manage the capital and risk in the future. This is an ongoing process involving all levels of the enterprise.

Subsection 2d. Organizational objectives for pursuing ERM

1. Competitive advantage

   For organizations that are in the business of taking risks, risk management plays a crucial role in the success and survival of the organizations. Traditionally, companies treat different types of risks as separate matters and deal with them independently. Enterprise Risk Management, on the contrary, treats all risks as a combined portfolio and manages them holistically.

   This holistic approach agrees with the Modern Portfolio Theory, which states that it is possible to construct a portfolio that is reasonably safe even if it contains a number of uncorrelated high-risk investments. Organizations using integrated ERM obviously have competitive advantages over companies using traditional risk management in the sense that ERM not only

passively engages risk controls, but also actively pursues risk optimizations, which further translates into value creation.

2. Strategic goals

In order to succeed, organizations need to set business strategies, both offensive and defensive. Sometimes being a market pioneer and taking on specific risks might pave the way to become the market leader. However, an organization needs to make sure it understands what it gets itself into before jumping in. On the other hand, merely maintaining the market share and playing safe might not be the best way to utilize capital. ERM can influence business strategies by identifying potential adjustments related to previously unidentified opportunities and risks.

In addition, ERM provides a way for senior executives to not only translate the vision into sound strategies, but also makes sure these strategies achieve sustainable competitive advantages. Aligning ERM resources and actions with the business strategy can maximize organizational effectiveness. Moreover, by linking ERM with business strategy, risk process can be carried out in the context of where a business is headed, not just based on where it is today.

3. Shareholder value

Enterprise Risk Management can help an organization achieve its business objectives and maximize shareholder value. Companies that undertake a risk-based program for shareholder value management typically can add 20- to 30-percent [32] or more to shareholder value.

A 1998 study[32] by George Allayannis and James Weston has suggested that active risk management contributes to shareholder value. Risk management adds value not only to individual companies, but also supports overall economic growth by lowering the cost of capital and reducing the uncertainty of commercial activities. Organizations that develop an ERM framework for linking critical risks with business strategies can become highly formidable competitors in the quest to add value for shareholders.

4. Transparency of management (reduction of agency costs)

ERM involves (1) setting risk appetite and policy, (2) determining organizational structure, and (3) establishing corporate culture and values. These three tasks are closely allied to the work of the board. With ERM in place, they can be more easily communicated to the employees and further increase the transparency of management.

Senior executives with a significant portion of their wealth tied up in company stocks and options have a direct financial interest in the success and survival of the firm. These incentives, if structured appropriately, work to put the “skin in the game” for managers, resulting in a strong alignment between management and shareholder interests. Risk management provides managers with a higher degree of job security and protects their financial interests in their firm. This substantially reduces the agency cost.

5. Decision-making

In order to make sound and effective decisions, senior managers need sufficient information. When making business decisions, risk adjusted return plays an important role. Senior managers need to evaluate business opportunities based on not only total returns, but also the risks associated with them, i.e., risk adjusted return. ERM, which controls risks in a combined portfolio approach, substantially enhances the decision making process.

Furthermore, ERM requires the integration of risk management into the business processes of a company. Rather than the defensive or control-oriented approaches used to manage downside risk and earnings volatility, ERM optimizes business performance by supporting and influencing pricing, resource allocation, and other business decisions. It becomes an offensive weapon.

6. Policyholder as a stakeholder

When people think about a company's stakeholders, they often think only about those who hold its equity and perhaps those who hold its debt. However, a truer picture is that the stakeholders include any group or individual that supports and participates in the survival and success of a company. In the case of an insurance company, individual policyholders are an important stakeholder. After all, an insurance company cannot survive without policyholders, and hence there is obviously a great need for customer management.

For traditional insurance business, a company normally incurs upfront investment when issuing a policy and it needs to keep policies in force to recoup the cost. With an ERM infrastructure in place, the insurance company can improve the risk transparency to regulators, rating agencies and equity analysts. Through timely and effective communication and reporting, the insurance company provides assurance to its policyholders that appropriate risk management strategies are in effect. Policyholders, as a stakeholder, will have confidence in the company's ability to meet future obligations and are less likely to lapse.

Chapter 3. Enterprise Risk Management Process

The activities of ERM can be organized into four themes: Risk Control, Strategic Risk Management, Catastrophic Risk Management and Risk Management Culture.

Risk Control

Risk Control is the process of identifying, monitoring, limiting, avoiding, offsetting and transferring risks.

The primary objective of Risk Control is to maintain the risks that have been retained by the enterprise at levels that are consistent with company risk appetites and company plans.

Risk Control is most effective if it is applied universally throughout the organization, but can still be very useful if applied separately to divisions or business units of an enterprise.

Risk Control Process

1. Identifying the risks. This process can be performed bottom-up or top-down.
2. Risk evaluation. Based on the information available as augmented by the judgment of management, the frequency and severity of the risks is determined and risks are ranked to determine the highest priority risks. For each priority risk, a senior level company manager is identified who is personally responsible for the management of that risk.
3. Monitor the risks. Sources of information on the amount of each priority risk are identified and a periodic monitoring and centralized reporting process is developed.
4. Risk limits. Checkpoints are established for each priority risk that are to be used with the risk reporting. For each priority risk, an action plan is identified for each checkpoint. Action plans could include review of the situation with Risk Committee, expansion of risk offset or transfer programs or limiting (or cessation) of activities driving risks.
5. Risk avoidance. This is accomplished by the design of product offerings, investment programs and operational procedures.
6. Offsetting risks. Risk offsetting is accomplished through risk management programs such as ALM and hedging. The design of the risk offsets determines the characteristics of the retained risks.
7. Transferring risks. For insurance companies, this is usually accomplished by reinsurance. Via reinsurance treaty, risks are transferred to the reinsurer. Careful analysis may be needed to determine the significance of any retained risk after reinsurance and of any significant counterparty risk that results from the riskiness of the reinsurer's ability to satisfy the obligations that have been transferred to them.
8. New product review. New products are evaluated and the risks identified, a monitoring process initiated, plans for risk offsetting and/or transferring made and risk limits are set.

Strategic Risk Management

Strategic Risk Management is the process of reflecting risk and risk capital in the strategic choices that a company makes.

Strategic Risk Management usually has as its objective the optimization of risk adjusted results for the organization. That is accomplished by choosing the strategic alternatives that have the best return for the level of risk that is associated with them.

Strategic Risk Management is only effective if it is applied universally throughout the organization. In fact, uneven application of Strategic Risk Management can actually hurt the risk adjusted return of the company by thwarting options with moderate risk reward profiles in areas that are practicing Strategic Risk Management while allowing areas without Strategic Risk Management discipline to pursue plans that have poor risk adjusted returns.

The Risk Control process is used in conjunction with the Strategic Risk Management process to ensure that risks that are retained by the company do not exceed expectation during implementation of the company's plans.

Strategic Risk Management Process

1. Economic Capital. Realistic risk capital for the actual risks of the company is calculated for all risks and adjustments are made for the imperfect correlation of the risks. The correlation benefit is allocated in a manner that does not bias the organization to excessive risk taking.
2. Risk Adjusted Product Pricing. Product pricing reflects the cost of capital associated with the economic capital of the product as well as volatility of expected income. Product profit projections show the pure profit as well as the return for risk of the product.
3. Capital Budgeting. The capital needed to fulfill proposed business plans is projected based on the economic capital associated with the plans. Acceptance of strategic plans includes consideration of these capital needs and the returns associated with the capital that will be used.
4. Risk Adjusted Performance Measurement (RAPM). Financial results of business plans are measured on a risk-adjusted basis. This includes recognition of the economic capital that is necessary to support each business as well as the risk premiums and loss reserves for multi-period risks such as credit losses.

Catastrophic Risk Management

Catastrophic Risk Management is the process of envisioning and preparing for extreme events that could threaten the viability of the enterprise.

The primary objective of Catastrophic Risk Management is to anticipate potential disasters that could destroy the enterprise for the purpose of developing contingency plans to minimize the impact of those disasters on the enterprise and to produce the environmental monitoring that would provide potential advance warning of the disasters.

Catastrophic Risk Management Process

1. Trend Analysis–looking for patterns that suggest potential emergence of negative situations
2. Stress Testing–Determine the impact on the firm of imagined extreme adverse situations. Impacts include financial, reputational, regulatory, credit ratings, etc. Stress tests are often repeated periodically and changes in the impact on the company from successive tests are noted.
3. Contingency Planning–For some or all of the scenarios that are being stress tested and/or are suspected possibilities from trend analysis, the company develops a set of specific action plans detailed enough to be helpful in a fast moving situation, but flexible enough to be useful in an emergency that is not exactly the same as what was anticipated.

4. Active Catastrophic Risk Management–When catastrophe strikes, the firm is prepared to take decisive timely action and clear communications to all stakeholders and media about those actions and does initiate and complete those actions and communications effectively.
5. Problem Post Mortem–After any serious problem situation, whether it results in a loss or if the loss is forestalled by the ERM process, the firm uses the situation as a learning opportunity and identifies what went well and poorly with the ERM process and communicates that learning broadly
6. Catastrophic Risk Transfer--Involves consideration of insurance or capital markets transactions that would transfer catastrophic risk exposure to either insurance companies or the capital markets.

Risk Management Culture

Risk Management Culture is the general approach of the firm to dealing with its risks. A positive Risk Management Culture will incorporate ERM thinking automatically into all management decision-making.

The primary objective of Risk Management Culture is to create a situation where Operational, Strategic and Catastrophic Risk Management take place in an organization without the direct oversight or intervention of the Risk Officer or the Risk Committee. In a positive Risk Management Culture, management across the firm will be aware of the risk tolerance, the risk governance process and the return for risk expectations of the firm.

Risk Management Culture Process

1. Risk Assessment–Identifying and quantifying all of the risks to the firm.
2. Best Practices–Identifying the best risk management practices that are the most important to the firm.
3. Support–Developing full support for the risk management effort includes direct involvement of senior management as well as adequate staffing of the support positions for performing risk management processes. Support takes the form of budget, priority, access, authority and public statements.
4. Communications--Transparency is a major component of Risk Management. Transparency means that everyone can see what is happening. Risk reports are broadly available, not closely held. Successes and failures are disclosed and discussed. The firm seeks to learn from problems not hide them.
5. Reinforcement–Firm must continually feed the Risk Management Culture; incorporating new employees and providing training and growth for existing employees. The Risk Assessment Phase and the Best Practices Phase are periodically revisited. The firm then revises or reaffirms the risk management path.

Chapter 4: Decision-making

A well-designed ERM framework should promote a holistic approach to enterprise decision-making, consistent with long-term corporate objectives. Improved risk and capital management may cause changes in decisions made in many critical areas including:

- Asset/investment strategy
- Product pricing
- Annual business planning
- Reinsurance purchasing
- Strategic planning process
- Product design
- Product/business mix

A key step is clarifying a company's risk appetite so ongoing strategic decisions can be made within an established risk-based context. Specific risks can be addressed on an ad hoc basis, but a more integrated assessment can be gained by performing a more complete analysis. This section will describe a top-down process that could be applied to a specific risk as well as a broad overview. The process may be done on an iterative basis, becoming more refined as more understanding is gained through each loop.

The process unfolds by addressing the following questions:

- What is Risk Appetite?
- How can Risk Appetite be measured?
- How can your company define its Risk Appetite?
- Who are your stakeholders and what do they demand?
    - What will it take to meet key stakeholder demands?
        - Board of Directors and Management
        - Employees
        - Policyholders
        - Stockholders
    - What will it take to meet supporting stakeholder demands?
    - Rating agencies
    - Regulators
- How do you create the strategies to meet these demands?
- How will decisions be made within your Risk Management framework?
- What are your risks to succeeding in these strategies?

What is Risk Appetite?

Risk appetite is the level of aggregate risk that a company can undertake and successfully manage over an extended period of time (Tavan). The capacity for undertaking risk will vary by company and depend on circumstances unique to the company. To determine its capacity, a company will need to initially establish a set of corporate objectives, e.g., minimum surplus ratio, industry rating. Ultimately, a company will need to develop corresponding risk-management strategies to successfully manage its risks.

Objectives will be driven by stakeholder demands. To determine the risk appetite, the risks to each objective need to be identified and assigned a specific risk limit or tolerance that sets the boundaries of what is acceptable. To test what is acceptable will require calculating the range of possible future outcomes that achieve the risk-specific performance goals. A practical test suggested by Fred Tavan for establishing the tolerance range for each risk is:

- high end: the level of risk you're happy to live with before you do something about it
- low end: the amount of risk you're prepared to take that is high enough to produce the reward necessary to achieve company objectives.

Trigger points within these boundaries will be set and provide an early warning indicator for certain action(s) that should be taken to avoid hitting the upper and lower limits. The risk appetite is the aggregate of these risk limits/tolerances.

How can Risk Appetite be Measured?

The basis used to measure the impact of the risk will depend on the company's focus and sensitivity to stakeholder expectations. The stakeholders will also influence the metrics used, e.g., regulators and rating agencies may require certain measurements, stockholders may require measures that are more readily explained.

- Regulatory or statutory basis--regulatory compliance and policyholder protection
  - Profits
  - Capital and surplus
  - Ability to pay claims
- GAAP or IAS basis--shareholder interests
  - Profits
  - Equity
- Economic basis--comprehensive understanding of the impact of the risks
  - Economic value
  - Economic profits
  - Embedded value
  - Embedded value earnings

Measures for risk tolerance include:

- Probability of ruin
- Tail value at risk (TVAR) or conditional tail expectation (CTE)
- Below target risk
- Economic cost of ruin
- Value at risk

More refined measures for specific risks may be defined in terms of loss amounts, error rates, or other types of units. For example, establishing a tolerance of +/- 0.5 years of duration mismatch for interest rate risk.

In theory, it would be optimal to apply a single risk metric, regardless of the risk, so the potential impact on the risk capacity could be judged on a consistent basis. This would make aggregating results and taking a more holistic approach easier. However, in practice, the many differences between types of risks and the practicality for developing a sufficiently complex single measure make it difficult to simplify.

How can a Company Define its Risk Appetite?

Defining its risk appetite will start a company on a self-discovery process and ultimately lead to a better understanding of its culture, its marketplace, its technology, its processes, its strategic positioning, its financial sensitivity to changes, and other factors. Through this discovery process, a company can clarify its risk capacity and determine the methods to successfully manage within it over the long term. The criteria for success and the priority placed on each attribute will primarily depend on the desires and relative dominance of the company's stakeholders, e.g., board of directors, management, employees, policyholders and stockholders.

A general process could be defined as follows and applied to all companies:

- Who are your stakeholders and what do they demand? At a high level, criteria may include attaining a certain rating from an industry agency, maintaining certain regulatory standards, achieving a degree of public confidence, being an employer of choice, etc. So, supporting stakeholders become rating agencies, regulators, current and potential employees, etc.

- What will it take to meet these criteria? Supporting goals could include maintaining specified capital requirements, earnings stability, customer service level, employee benefits, etc.

- What risk analyses will have to be done to create strategies for managing to these goals? What metrics should be established to represent these risks? Is access to the necessary technology and expertise to perform these analyses available?

- How will a tolerance range for each specific risk be established? How will these tolerances be translated into specific risk limits? What are the early warning indicators to provide information on the direction and/or magnitude of changes in risks? At what level(s) of risk will specific action be taken?

- What governance will need to be established and what circumstances have to change to successfully manage to these tolerances over the long run? How will you support this process and keep it under periodic review to ensure it remains consistent with changes in circumstances?

- How will this process be integrated into enterprise-wide decision making? What are the critical decisions that are impacted by this approach? How will responsibility for these decisions be delegated? What risks need higher level review, i.e., corporate, and what risks are more appropriately handled at the line of business, i.e., operational?

Who Are Your Stakeholders and What Do They Demand?

Key stakeholders would include the board of directors and management, employees, policyholders and stockholders. Each type of stakeholder has a different perspective that influences what each considers most important. However, the company mission/culture will exert strong influence--Establishing the organization's risk management culture will help create a shared high-level view by all key stakeholders that will promote consistent goals, better decision-making, coordinated efforts and greater results.

Key Stakeholders

Board of Directors and Management

Creating and improving shareholder value is a key high-level goal. Over the long run, good risk-based decision-making and effective use of capital are critical.

To guide them in managing their capital, a company needs to determine the capital position it wishes to maintain. There are four different approaches that are taken by various companies:

- A quantitative modeling company will determine its capital needs via sophisticated stochastic modeling of the business and developing an economic capital position of the company.
- A maintain rating company will use a rating agency capital formula or a multiple of the rating formula that will develop a capital position that is adequate to maintain the desired rating.
- A regulator solvency company will judge its capital position against the lowest level that a regulator would allow, providing only minimal margin above that level.
- A personal judgment company will base its capital position on the judgment of management as to the level of required capital.

In practice, most companies apply a mixture of these approaches.

Other management objectives may include:

- Manage earnings volatility
- Comply with regulatory changes
- Improve corporate governance
- Manage tail risk
- Improve industry rating
- Improve communications

Once the critical objectives are defined and the key underlying drivers are identified, they can be used to uncover the company's risk appetite. A document created by the Risk Metrics Subgroup of the RMTF includes techniques that can be applied.

Potential Methods/Tools that can be used to identify risk appetite at the executive/board level:

1. Survey and discussion
2. Analyze past and historical choices
3. Risk analysis on a single alternative
4. Risk analysis on multiple alternatives
5. Delphi method (using CEO, CFO, CIO, COO, etc.)
6. DFA-type stress analysis
7. Ask directly
8. Etc.

Some threshold concepts that CEO/Board may be interested in are:

1 Are we keeping a certain credit risk rating, (e.g. we're AAA and would like to stay that way?)?
2. Where did you bet the company, (i.e. where are the risks that could cause us to lose everything?)?

3. What is the cost of hedging the risk? Can we get a reinsurance price for hedging it and compare against keeping it?
4. Etc.

Potential threshold lines for risk appetite:

1. Book Value or Market Value of surplus
2. X percent of BV or MV of surplus (e.g. we are willing to risk 50 percent of surplus)
3. X percent of minimum regulatory capital (e.g. difference from current to X percent is the appetite)
4. Change in credit risk rating
5. Damage to reputation
6. Earnings fluctuations (e.g. are not willing to have more than $X million in any quarter)
7. Capital fluctuations
8. Etc.

Employees

What will attract and retain employees who properly represent the organization? What are the risks of losing key personnel? Employee will consider the following when determining whether to choose or remain with a company:

1. Company culture
2. Physical workplace environment
3. Salary and benefits
4. Flexibility of work hours
5. Opportunities
6. Qualities of direct manager
7. Performance measures
8. Etc.

Uncovering what truly motivates and retains employees will require less analytical approaches:

- Surveys
- Employee/manager discussions
- Good communication regarding performance measures, benefits, growth opportunities, etc.
- Work/life balance flexibility
- Etc.

Policyholders

What is reasonable for policyholders to expect with respect to company operations? Reasonable expectations could include:

1. company maintains its (good) standing with the regulators and rating agencies
2. payments of non-guaranteed elements remain at acceptable levels anticipated **at time of sale**
3. attractive and competitive product offerings
4. fair claim payment practices
5. Etc.

Stockholders

There is a presumed alignment between board of directors, executive and stockholder. Otherwise, this is outside scope of document.

Supporting Stakeholders

Rating Agencies

Capital requirements from rating agencies affect the risk tolerances established by company. Capital requirement is a key criterion used to assess financial strength and financial strength is a critical factor in determining a rating. Both quantitative and qualitative approaches are used to finalize the rating. The emphasis of quantitative versus qualitative has shifted over the years and, consequently, insurers' approaches to meeting the capital requirements have evolved in order to attain desired agency ratings.

Quantifiable or formulaic measures allow an insurer to manage toward predetermined levels with specific strategies focused on influencing the measurements' triggers. The qualitative review is based on a more holistic viewpoint of corporate management and has become an increasing part of the rating review. To better manage (to) this review, an insurer should clearly understand what high-level questions the agency is trying to address through its subjective reasoning. The insurer may have to adjust its decision-making and support processes to be in line with addressing these questions. This will continue the evolution.

As agencies move closer to using an ERM or risk management perspective for their capital reviews, the more an insurer will have to move toward a more holistic approach to managing its capital rather than formulaic. This will be consistent with the industry's move toward an Economic Capital approach for determining required capital. Economic Capital has the potential for becoming the standard for all audiences–rating agencies, regulators, management and boards.

If having good ERM helps its rating, a company will consider making additional investments in technology, expertise, resources, etc. Ideally, up-front expenses would be recouped through improved process efficiencies, better decision-making and other cost-effective results.

Regulators

Regulations exist to protect policyholders and promote the long-term solvency of the company. Data must be received in standardized format and developed using very specifically defined rules and methodologies. These constraints will have an impact on risk measures and tolerances used by insurance companies. These requirements include operating limits, minimum capital requirements and procedures for supervisory reviews.

Operating Limits

In the United States companies operate under legal limits, particularly with regard to allowable amounts of various special investment classes. (See Investments of Insurers Model Act)

Minimum Capital Requirements

U.S. minimum capital requirements are called the Risk-Based Capital. Risk-Based Capital defines capital requirements in terms of Credit Risk (C1), Insurance Risk (C2), ALM Risk (C3), Business Risk (C4) and Fraud and Mismanagement (C5).

In the EU, capital requirements have been broadly related to volume of business, with little regard to specific risk of company practices. In the United Kingdom there are also three resiliency tests, relating to equity returns, credit spreads, and real estate market returns. EU solvency standards are being replaced by "Solvency II" standards that are modeled from Basel II capital standards for banks, with three pillars of Capital Standards, supervisory review and market disclosure as the three pillars.[38]

Other countries have also been adopting risk-based capital requirements.

Supervisory Reviews

Canadian regulators (OSFI–the Office of the Superintendent of Financial Institutions) have adopted a risk-based supervisory review process that is driven by a risk mapping grid process. The NAIC in the United States has been exploring adoption of a similar process. The U.K. regulator (FSA – Financial Services Authority) has declared that they will be driving their review process on a risk-based approach.

Company risk tolerances are impacted by all these regulatory practices. Companies will form their risk tolerances so that they avoid coming close to operating limits, avoid generating risk-based capital in excess of their expected capital and avoid undertakings that would draw special attention under a risk-based supervisory review approach, all other things being equal.

Sources:

1. NAIC Investments of Insurers Model Act
2. Risk-Based Capital (RBC) for Insurers Model Act
3. 2004 NAIC Health, Risk-Based Capital Report, Including Overview and Instructions for Companies
4. 2004 NAIC Life Risk-Based Capital Report Including Overview and Instructions for Companies
5. NAIC Standard Valuation Law
6. OSFI Supervisory Framework
7. NAIC–Risk Focused Surveillance Framework

How Do You Create the Strategies to Meet These Demands?

Existing strategies would be reviewed and new strategies developed by understanding their impact on high-level company goals and objectives for profit, growth, market share, etc., as well as for the satisfaction of specific risk tolerances and risk limits. Risk becomes one more necessary dimension in the multi-dimensioned decision-making process and the company's risk management philosophy becomes an inherent part of its culture.

Insurers are more likely prepared to quantitatively measure market and insurance risks than operational risks. Business processes and responsibilities have been established for managing market and insurance risks:

- Risk modeling and measurement
- Economic capital calculation
- Risk identification and prioritization
- Internal risk monitoring and reporting
- Risk control and mitigation
- Risk aggregation
- External risk communication
- Risk-related performance measurement

Specific risks the insurer is likely to measure include:

- Interest rate
- Equity
- Credit
- Currency
- Liquidity
- Mortality
- Morbidity
- Lapse/surrender
- Property/real estate
- Catastrophe
- Event

Insurers are taking a closer look at what actions should be taken for a better trade-off between risk and return through:

- More advanced ALM strategies
  - Closer duration matching
  - Duration and convexity management with derivatives
- Strategies for hedging equity risk
  - Purchasing derivatives
  - Dynamic hedging
- Risk transfer vehicles
  - Reinsurance
  - Securitization of XXX reserves
  - Factoring of trail commissions

Quantifying operational risk is more difficult and less developed. Since operational risk stems from people, processes, systems and events, it presents a challenge that may differ from other risks. Operational risk can be managed using a control framework. Risk from external events has been effectively managed through the use of insurance. It is important to address where the risk will be managed. James Lam describes one approach--unified ORM (Operational Risk Management)--in a paper titled, "A Unified Management and Capital Framework for Operational Risk" available at the SOA Web site: http://rmtf.soa.org/rma_op_risk.pdf.

New tools can be established that will provide new or improved information that will lead to more targeted strategies:

- Economic capital
- Optimization routines
- Fuzzy logic
- Risk mapping and correlation

Ultimately, controls would be established that reflect the company's risk appetite. Examples include:

- Redline limits on asset classes, to ensure diversification and limit certain types of asset risk
- Individual name limits taking into account bond and equity holdings, derivative counter-parties, reinsurance partners, to control credit risk

- Limits on certain types of business to ensure diversification and limit certain types of risk that cannot be mitigated in another manner, such as through the use of reinsurance
- Duration mismatch targets to mitigate interest rate risk

How Will Decisions be Made Within a Risk Management Control/Committee Framework?

The decision-making can only be as good as the quality and timing of the information provided. To achieve a holistic perspective, the information needs to be integrated. Higher levels of integration include:

- Global
- Entity
- Risk category
- Function
- Business

Though aggregation through sophisticated modeling or other techniques may not be possible in the short term, establishing a risk culture, properly aligning organization structure and improving communication can set a foundation for better risk management.

While going through the process of establishing an ERM framework, it will be important to consider what controls and limits need to be put in place and how accountability will be assigned. Both operational controls as well as financial will be needed. These will help identify the key decision points within the process. The ERM framework would define at what level of the structure decisions are to be made, with the decisions having the greatest impact on the organization being made at the executive level.

Sources include:

- Enterprise Governance–Getting the Balance Right, by the Professional Accountants in Business Committee of the International Federation of Accountants, defines Enterprise Governance as “the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization’s resources are used responsibly.” They go on to state that Enterprise Governance is made up of two pieces, Corporate Governance (conformance) and performance, and effective Enterprise Governance balances these. The performance aspect ensures that risk management is integrated into the company’s decision-making process.

- Enterprise Governance--Getting the Balance Right, The Chartered Institute of Management Accountants and the Professional Accountants in Business Committee of the International Federation of Accountants, available at www.cimaglobal.com

A Risk Management Committee structure would be defined as part of this larger Enterprise Governance role. In response to the corporate scandals of recent years, a wealth of information on Corporate Governance has been developed, including the following.

- The Turnbull Report, The Institute of Chartered Accountants in England and Wales, available at www.icaew.co.uk

- Implementing the Turnbull Report, The Institute of Chartered Accountants in England and Wales, available at www.icaew.co.uk

- Restoring Trust ("The Breeden Report"), Report to The Hon. Jed S. Rakoff, The United States District Court for the Southern District of New York on Corporate Governance for the Future of MCI, Inc. prepared by Richard C. Breeden, Corporate Monitor, available at http://www.law.harvard.edu/programs/olin_center/corporate_governance/papers/Restoring-Trust.Breeden.pdf

What Are the Risks to Succeeding at These Strategies?

Risk management must have support from the Board of Directors and upper management in order to be successful. Decisions must be made within an established framework to maintain consistency and lead to more effective use of resources. The types of risk framework that could work will vary by the company structure and may include a specific chief risk officer ("CRO"), risk committee, line risk managers, etc.

Additional up-front time and resources will be needed to identify the risks, develop the appropriate measures and tools, monitor the metrics, improve communications and manage the risks more holistically. Roadblocks to having a more extensive risk management include:

- Resource issues
- Modeling or measurement issues
- Data or information system constraints
- Level of complexity
- Lack of clarity, of objections or benefits
- Credibility of results

Risks may never appear threatening enough to justify the extra time and resources assigned to improve risk management. It will be important to communicate how the improved decision-making has mitigated the risk potential in addition to the timely monitoring and reporting of actionable information.

Risk management will never be fully integrated until it becomes a part of the performance management or incentive compensation plans. Some ideas of how this may be included are:

- Return on risk-based capital--actual versus target
- Adherence to specific risk guidelines
- Increase in risk-adjusted value

Chapter 5. ERM Implementation

ERM implementation is an exercise in change management. There will be those that embrace the change as a welcome improvement in the management of the company. There will be those that view the change as more unnecessary work. In order to be successful there must be an individual, or a small team, whose primary responsibility is to implement ERM. The Chief Risk Officer (CRO) needs to work with the corporate management and the management of the business units to determine the form of the risk management function (see section x). No one structure is correct for all companies. What is important is the process, rather than who plays what role.

When addressing the needs for ERM with the business management, emphasis should be on the benefits to the organization. Few business people can argue against the benefits of understanding all the risks an organization faces or in demanding that a business unit's return should reflect the amount of risk that they are taking. However, there will be those whose above average results as measured by GAAP and ROE will look less stellar when measured with a risk adjusted ROE. Acceptance by these business managers may not be readily obtained. Just as GAAP results and ROE are now key components in measuring an executive's performance it is important that risk adjusted ROE become a key component in executive compensation.

In most risk management structures it is necessary for each business unit to put in place a process to evaluate and manage their risks. The business unit risk managers need to have a close relationship with the CRO even though they report up through the business unit management. Since most business units will not have a full-time team dedicated to ERM, it is important that the annual objectives, performance review and bonus include a significant factor related to the implementation and success of the business unit ERM.

Accurate and consistent risk measurement is a prerequisite for good risk management. Risk measurement typically starts bottom-up in the different businesses within a financial conglomerate. As a result, many different approaches to risk measurement have been developed between insurance and banking businesses and even within each of these areas (e.g. life and non-life insurance).

Many different ways of classifying risk are possible, and no single taxonomy is inherently better than another. The classification of risk types often follows the relative importance of risk types to a financial services provider.

A common risk measurement framework is the prerequisite to an effective measurement and management of risk and used capital. To construct a common risk language across the whole of a financial conglomerate, differences in the sector-specific frameworks should be identified and agreement should be reached consistently covering all relevant risks. One of the key challenges in a conglomerate is specifying a uniform time horizon. In banks, the convention for modeling risks and assessing capital is to adopt a one-year horizon. Alternatively, insurance companies are typically capitalized for longer decision horizons. In order to have a "common currency" for risk, a common time horizon needs to be specified, at least at the group level where risk aggregation across banking and insurance takes place.

Risk Management Structure

In order to organize an adequate risk management structure, the link between central risk management and local risk management (within operating companies) should be clearly defined. From this point of view, the following question arises: Who is in the driver's seat in the measurement and management of the risks and returns of each of the activities at a stand-alone and aggregated level?

Whether you are at the helm of a bancassurance group or a financial holding company (with stakes in banks, life or P&C insurance companies), you must rely on an integrated risk-management framework throughout the whole organization. The legal structure may evolve over time. Approaches to organizing the risk management function include the following:

1. Group Risk Reporting
   a. Operating companies decide their risk appetite
   b. Operating companies measure their risks how (if) they want
   c. Group risk aggregates the results
   d. Operating companies decide how (if) to manage risk/return

2. Group Risk Quality Control
   a. Operating companies decide their risk appetite
   b. Operating companies measure their risks
   c. Group risk checks the quality of the risk measures and issues suggestions for improvement
   d. Operating companies decide how to manage risk/return

3. Group Risk Monitoring
   a. Group risk and operating companies decide risk appetite (at business line level) as part of annual planning process
   b. Operating companies measure their risks
   c. Group risk analyzes the results and raises issues
   d. Operating companies decide how to manage risk/return, and how to address any issues raised by group risk

4. Group Risk Management
   a. Group risk and operating companies decide risk appetite (at sector/risk factor level) on a dynamic basis
   b. Group risk measures all risks
   c. Group risk analyzes the results and makes recommendations
   d. Operating companies decide how to maximize return given their risk limits

5. Group Risk/Return Management
   a. Group risk decides risk appetite overall for each operating company
   b. Group risk measures all risks
   c. Group risk decide what to do to change the risk/return profile
   d. Operating companies execute group risk's decisions

The management of risk within a diversified organization requires both top-down and bottom-up approaches. The financial system has witnessed considerable economic turbulence over the last five years. While these conditions have generally not been focused on G-10 countries directly, the risks that financial conglomerates have had to deal with have become more complex and challenging. The Corporate Risk Department of financial institutions should frequently test and monitor reserves and capital adequacy. Significant resources are needed in order to measure capital adequacy from different points of view.

The Corporate Risk Department also needs to be responsible for limit setting. Counter party exposure limits are set to constrain the maximum impact of any single default on the capital base of a financial conglomerate. Portfolio risk models allow the calculation of risk contribution of individual counterparties or subportfolios taking into account the (un)expected losses, correlation effects and thus the economic capital. If risk contributions of certain counterparties are high, senior management could decide to set limits for approval of additional credits to these counterparties. In a financial

conglomerate it is important to apply the “one obligor principle” which implies that one global vision of all risks on one obligor throughout all entities (no matter the location) and risk types (no matter the nature of the underlying risk) should be taken into account.

Relationship Performance Measurement

The local business should be responsible for developing and recommending methodologies of risks as they are assessed at the individual asset level. Financial institutions have to adapt their organization and their incentive systems in order to be successful in the future. Management must have the incentive to use risk information to support better decision-making. The performance of the relationship of a client or relationship manager should not solely be evaluated on revenue and revenue growth rates. The recognition of capital utilization and return of on capital are also important.

Risk-Based Pricing

Rarely do prices consistently reflect risk. Risk measurement techniques, can be applied to analyze and price transactions against the expected loss and required economic capital. On the one hand, the narrowing profitability of traditional business implies little room for error, either in selecting or pricing individual transactions. On the other hand, the attractiveness of less traditional but higher margin businesses can only be evaluated by taking into account not only their margins but also their potential impact on the risk of the portfolio. Although the use of internal credit rating models to support the pricing and classification on a master scale is a step in the right direction, it is not sufficient. It is also important to look at a portfolio level because diversification and timing effects increasingly lead to the difference between profit and loss.

Transfer Pricing

The local business units should also be responsible for transfer pricing. Transfer pricing, or the price at which one unit of a firm sells goods or services to another unit of the same firm, should truly reflect arm’s-length prices. Banks, for example, use risk management tools to transfer banking book exposures to the trading book where possible in order to hedge interest rate risks internally. For insurance companies, basically a comparable approach is used via replicating portfolios. Unlike banks, life insurance company liabilities are intertwined with assets, but this should not prevent the company from tracking the performance of assets and liabilities.

Chapter 6. Examples of Real-Life Situations in Which Implementing ERM Has Added Value and/or Avoided Significant Losses

The need for a true strategic approach to ERM is clear from recent events in this industry. We all know examples of recent failures:

- A large multi-line carrier with both primary and reinsurance operations was unaware of its total exposure, through its various business units, to a single natural catastrophe—until the catastrophe occurred. The severe aggregation of losses and substantial loss of capital that resulted led to the carrier's hasty and premature exit from an entire business segment—one that has proven quite profitable for their competitors over the long run.

- Some of the best known names in the U.S. life insurance industry now face millions of dollars in fines, billions in policyholder restitution and near-crippling damage to their reputations because of the misleading sales practices of not much more than a handful of their agency sales force. These faulty practices could occur because the companies misjudged the adequacy of their monitoring systems.

Less sensational, but no less real, are the other stories: companies that continually "beat the odds" by cleverly "betting" on the right product/distribution strategies, the right growth/acquisition choices and the right investment/hedging tactics. Management teams at these companies make decisions that exploit their firm's true risk-taking capacity, complement their existing risk profile and further their overall strategic objectives. Typically, these are also the companies that achieve higher ratings, not to mention higher returns and higher valuations, with less capital than their peers. These companies do not win by accident.

The remainder of this section includes a number of recent situations where ERM has created value by either:

- Adding to profits of the organization; and/or

- Avoiding losses for the organization.

These are further described below.[36]

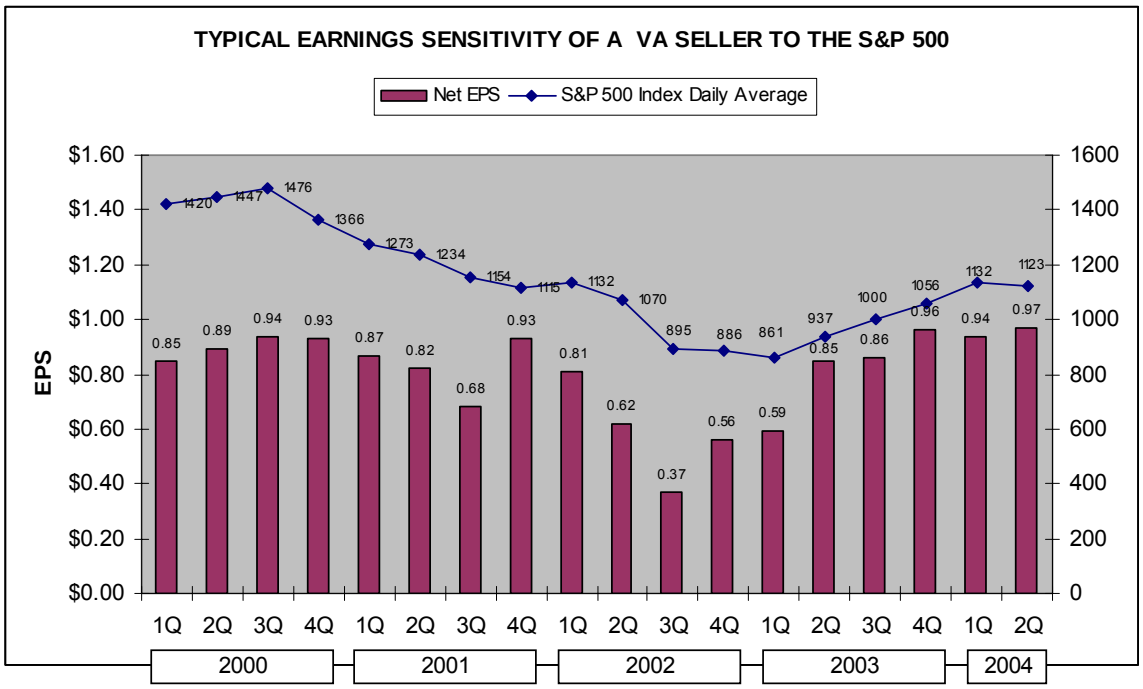
1. Variable Annuity (VA) Risk Management

   For sellers of VA products, earnings are generally based on a fixed percentage of the underlying assets and hence, they are sensitive to market movements (see Exhibit 6.1).

   A company selling VAs decided in the spring of 2002 to incorporate a static portfolio hedge for their VA business, designed to offset losses from lower revenues because of a potential decline in assets. The hedge was put in place in June of 2002, protecting the company against a decline in the S&P 500 below a strike price of 995. The quarterly cost for the hedge was approximately $10 million. At the end of 2002, with the S&P below 900, the hedge was sold for a realized gain in excess of $200 million. This was used to offset the loss in revenue from the drop-off in assets.

Thus, the hedge did what it was supposed to do–it protected the company against a decline in earnings in a declining equity market.

EXHIBIT 6.1

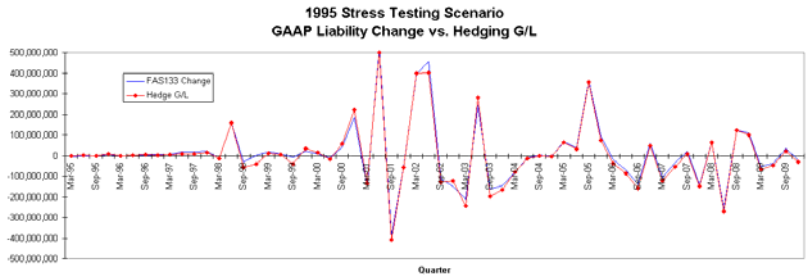


Source: Tillinghast

Other leading-edge sellers of VA products protect their statutory and GAAP earnings and tail risk through a sophisticated dynamic hedging program, including the matching of Delta, Vega and Rho. The impact of hedging on earnings volatility and tail risk is further illustrated in Exhibits 6.2 and 6.3 below.

EXHIBIT 6.2

Impact of Hedging on GAAP Income Volatility



Hedge tightly matches changes in GAAP liability.

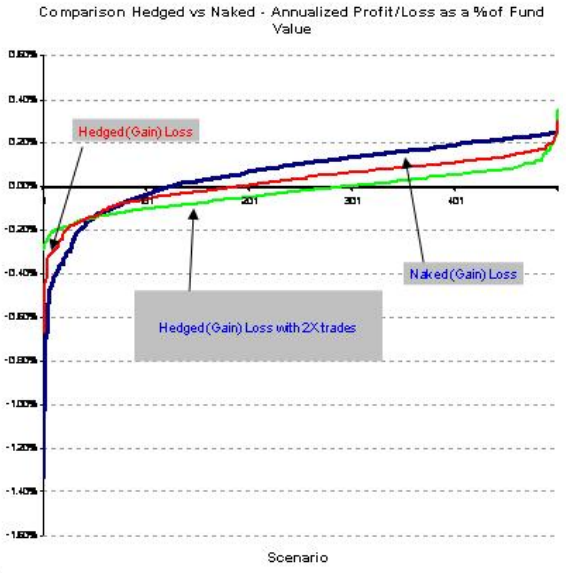
Hedge significantly reduces GAAP net income volatility.

Based on $10 billion block of new business with GMWB benefits issued in 1st quarter of 1995.

Source: Hartford Life

EXHIBIT 6.3

Impact of Hedging on Statutory Earnings



Source: Tillinghast

2. Securitization

Recently, the concept of securitization of cash flows is utilized increasingly by insurance companies in the United States to raise capital and transfer risk.

(a) United States

A variety of different life insurance securitizations have occurred in the United States in recent years, including:

- Closed block securitizations
- Regulation XXX securitizations
- Securitizations of variable annuity fees
- Mortality catastrophe bonds

The first two categories have generated the highest level of interest and are discussed below.[37]

- Closed Block Securitizations. These refer to transactions involving the closed blocks of participating life insurance policies that are formed in the United States at the time a former mutual life insurance company demutualizes and converts to a stock life insurance company. In most of the U.S. demutualizations, a closed block was formed to protect the reasonable policyholder dividend expectations of participating life policyholders. The closed block is funded with high-quality assets that, together with future revenues from the closed block, are expected to be sufficient to pay future benefits for the closed block policies, including policyholder dividends.

  Typically, the closed block is initially funded with assets covering 80 percent to 90 percent of the closed block liabilities (policy reserves). The insurer is obligated to manage the dividend scales for the closed block policies so that the closed block assets are just sufficient to support the liabilities until the final policy matures.

  In addition to the assets assigned to the closed block, other assets are allocated to support the closed block policies in order to satisfy regulatory requirements. These other assets are referred to as surplus and related assets, and are not expected to be needed to pay benefits on the closed block policies.

- Regulation XXX Securitizations. Effective in 2000, Regulation XXX clarified the statutory reserve requirements for most long-duration term life insurance policies. In addition, the closely related Guideline AXXX mandated additional reserves for many types of universal life (UL) insurance policies that contain “no lapse” guarantees. The additional reserves can be very significant and are considered by many to be largely redundant.

  Capital markets solutions are being explored as an alternative to reinsurance. One company completed a successful securitization of its Regulation XXX term insurance business in 2003, and other companies are exploring similar structures for their term and universal life business. There is intense current interest in this area, with the potential for many deals in the near term.

  These structures involve the issuance of non-recourse debt capital to fund the redundant portion of statutory reserves. The viability of these securitizations is predicated on the redundancy of a large proportion of the excess XXX and AXXX reserves (i.e., the excess reserves are not required to pay policy benefits, even under

moderately adverse scenarios). Interest and principal payments on the underlying debt are at risk if the securitized business significantly underperforms.

(b) United Kingdom

In the United Kingdom, recent securitizations have included Barclays Bank in 2003 and National Provident Institution (NPI) in 1998. In each case, the companies utilized the concept of Embedded Value (EV) to securitize the underlying value of the business involved.

The securitization of EV, which is based on a set of expected future cash flows, provides a way for life insurance companies to mitigate new business strain and regulatory solvency capital. Insurance companies have found that they can take a block of existing business off the balance sheet and effectively securitize the future cash flows relating to that block of business. They give the future cash flows to investors in securitized notes and in exchange, they get an up front cash payment from those investors.

3. Economic Capital (EC)

In North America, insurance companies' capital has come under increased scrutiny as of late. The recent bear market and a drop of interest rates to levels not seen since the 1960s have led to dramatic falls in investment income. The quest for higher yields has led insurers to invest in riskier fixed income assets, leading to a record level of realized capital losses in 2002. As a result, many insurance companies have seen downgrades in their financial strength ratings over the last two years.

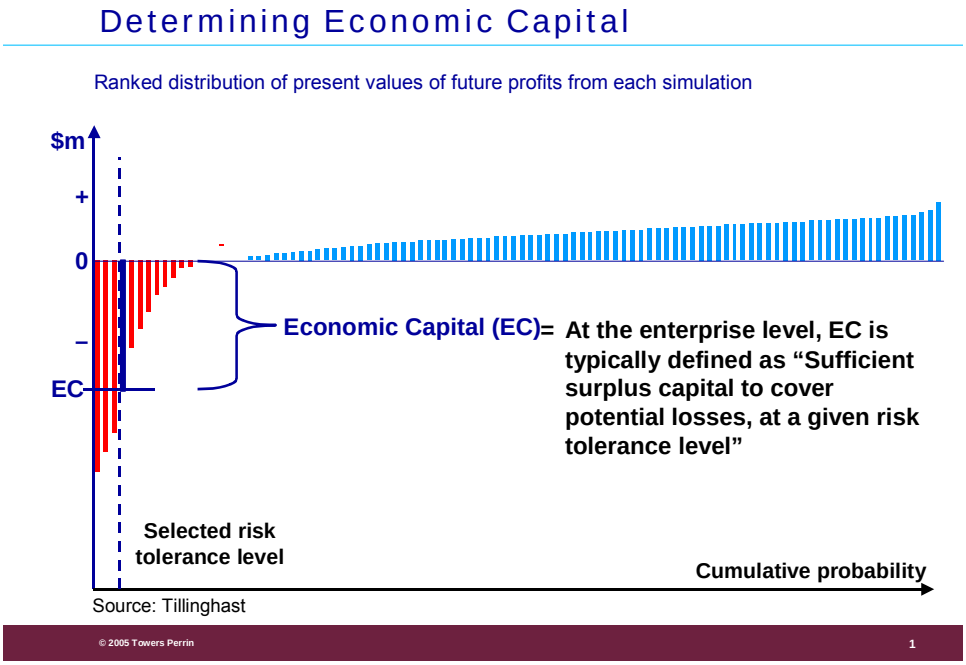
At the same time, U.S. regulatory bodies are introducing new capital and reserving requirements for life insurance products with equity guarantees that will lead to increased pressure on capital. Given this background, it is not surprising to find a growing number of life insurance companies paying greater attention to calculating the appropriate level of capital for their business and risk profile.

(a) Calculation of Economic Capital

First of all, we need to distinguish EC from Regulatory or Rating Agency Capital. EC is based on calculations that are specific to the company's risks, while Regulatory or Rating Agency Capital formulas are based on industry averages that may or may not be suitable to any particular company. In addition, EC is typically calculated on the basis of expected future cash flows, whereas Regulatory or Rating Agency models often use accounting statements as a starting point. Furthermore, economic capital models are often underpinned by explicit stochastic distribution models, therefore allowing more sophisticated calibration and interpretation, whereas Rating Agency or Regulatory models are only loosely calibrated to stochastic distributions.

In North America, EC is typically defined as "sufficient surplus capital to cover potential losses at a given risk tolerance level and over a specified time horizon." This is illustrated in Exhibit 6.4.

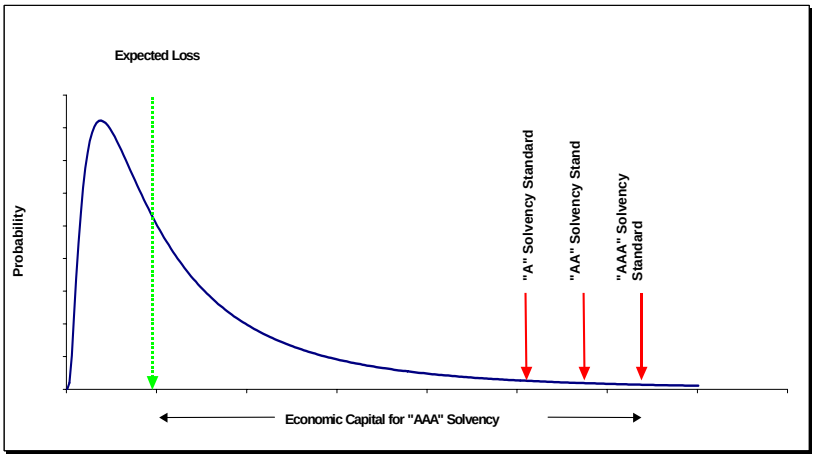
EXHIBIT 6.4



There are various methods for determining Economic Capital. A common methodology is to base EC on the probability of ruin, amount of ruin or other expected shortfall measures. Probability of (statutory) ruin is the probability that liabilities will exceed assets on a present value basis at a given future valuation date, resulting in technical insolvency. It can be calculated from the probability density function of the present value of future surplus by measuring the area under the curve corresponding to the section where liabilities exceed assets. This is shown in Exhibit 6.5 as the shaded area, and is consistent with the Conditional Tail Expectation (CTE) measure defined below. Alternatively, it can be calculated from the cumulative distribution function shown in Exhibit 6.4 by determining the probability point (on the y-axis) where liabilities equal assets (on the x-axis). This is consistent with the "specified percentile" approach described earlier. These probability graphs are generated by running computer simulations of liabilities and assets using a stochastic financial model.

Economic Capital based on the probability of ruin is determined by calculating the amount of additional assets needed to reduce the probability of ruin to the probability target specified by management. The target probability of ruin is set by management in consideration of several factors, primary among them the solvency concerns of policyholders—usually expressed in terms of the minimum financial strength rating that management desires from the rating agencies.

EXHIBIT 6.5



(b) Types of Risk Covered

Most respondents to a recent Society of Actuaries (SOA) Survey agreed that EC should cover various types of risks, including:

- Interest rate risk (96%)
- Pricing risk (93%)
- Credit risk (92%)
- Equity market risk (91%)
- Liquidity risk (86%)
- Operational risk (79%)

It should be noted that in contrast to banking risks, insurance company risks tend to have much longer terms, in some cases going out more than 40 years.

According to an audience poll at a recent SOA seminar, almost 60 percent of respondents have been calculating EC on a total company or a line of business basis. Of the remainder, 24 percent plan to do so within the near future.

The main reasons for companies implementing EC to date have included risk and performance measurement. Going forward, we expect the impetus to come more from competitive forces and rating agency pressures. A majority of SOA Survey participants expect EC to have even greater significance in the near future.

Chapter 7. Notes

1. Overview of Risk Management

2. COSO Enterprise Risk Management–Integrated Framework and Application

3. Petition in Lakin v. Morgan Stanley & Co. Inc., et al., Cause No: 042-07300 (Missouri Circuit Court, 22nd Judicial Circuit, St. Louis City; filed [2004]). [Please note: This citation is a Petition, not a decided court case.]

4. Desloge, Rick, St. Louis Business Journal, *Copyright American City Business Journal,* Aug. 13, 2004.

4.b. "Missouri Insurance Department Sues KPMG over Accounting at General American Life", *Insurance Journal*, Dec. 16, 2002. www.insurancejournal.com Click on News, then Archives. Search by *KPMG* and the date.

5. Daly, Matthew Associated Press, "Probe widens into Air Force-Boeing contracts," *The Orange County Register*, Nov. 10, 2004.

6. Associated Press, "Defense division boosts Boeing," *The Orange County Register,* Oct. 28, 2004.

7. Karp, Jonathan and Pasztor, Andy, "Lockheed, BAE Protest Boeing Pacts," *The Wall Street Journal,* (Eastern Edition), New York, N.Y., Oct. 13, 2004.

8. Wayne, Leslie, "Lockheed and BAE Protest Boeing Contract," *The New York Times* (Late Edition (East Coast)), New York, N.Y., Oct. 13, 2004.

9. Pasztor, Andy and Lunsford, Lynn J., "U.S. Intensifies Probe of Boeing Hire," *The Wall Street Journal,* Aug. 27, 2004.

10. "General American Agrees to $55 Million Settlement with Missouri DOI," *Insurance Journal*, Sept. 8, 2000. www.insurancejournal.com Click on News, then Archives. Search by *General American* and the date.

11. "Principal Settles Class Action," *Insurance Journal*, Dec. 9, 2000. www.insurancejournal.com Click on News, then Archives. Search by *Principal* and the date.

11.b. Williams, Heather, "Lincoln National settles vanishing premium lawsuits for $28.3 million," *Insure.com*, Jan. 3, 2001. info.insure.com Use the search engine to find *Lincoln National*.

11.c. Cybulski, Mark, "New England Life Insurance Co., settles lawsuits for $172 million," *Insure.com*, May 25, 2000. info.insure.com Use the search engine to find *New England Life.*

11.d. Cybulski, Mark, "Provident Mutual settles lawsuits for $45 million," *Insure.com*, Sept. 8, 2000. info.insure.com Use the search engine to find *Provident Mutual*.

12. For more details on vanishing premiums and types of life insurance policies see: Phillips, Richard T., "'Vanishing Premium' Litigation: The Plaintiff's Perspective," A Presentation for THE MISSISSIPPI BAR, July 9, 1996. www.smithphillips.com Click on Publications, then scroll to *"Vanishing Premium" Litigation*.

13. PCAOB Testimony of William J. McDonough before the U.S. Senate, Nov. 20, 2003

14. Sarbanes-Oxley Act, Section 101(a)

15. Sarbanes-Oxley Act, Section 101©

16, PCAOB website, www.pcaobus.org

17. Leitch, Matthew, "Risk management history and regulations (UK)", March 2003

18. Miccolis, J., "The Language of ERM: A Practical Glossary and Discussion of Relevant Terms, Concepts, Models and Measures", Tillinghast-Towers Perrin, May 2002

19. 1998 – 2004 Methodware Limited, "Standards, Methodologies, Recommendations and Legislation"

20. BIS, "International convergence of capital measurement and capital standards", July 1988

21. BIS, "International convergence of capital measurement and capital standards – a revised framework", June 2004

22. Shimpi, Prakash A. (Ed.), 2001, "Integrating Corporate Risk Management", Chapter 3, Thomson Texere (2001); originally published by Swiss Re (1999)

23. "Economic Capital: At the heart of managing risk and value", Price Waterhouse Coopers, 2003

24. David Scott, "Wall Street Words: An A to Z guide to investment terms", Houghton Mifflin Co. 2003

25. Anup Shah, "Corporate influence in the media", April 2004

26. "Risk management: a comparison of the banking and insurance industries", Record, Volume 24, No.3, Society of Actuaries 1999

27. "Risk Management Practices in the insurance industry", Record, Volume 27, No.2, Society of Actuaries 2001

28. *Enterprise Risk Management Framework, Draft*, Committee of Sponsoring Organizations (COSO) of the Treadway Commission, Publication to be released September 2004. Please see www.coso.org

29. Comment on the COSO document, American Academy of Actuaries, October 14, 2003. http://rmft.soa.org/rmtf_erm.html Scroll to *SOA Response to the COSO Framework*

30. Ingram, Wilkinson, Ehrlich, *Best Practices for Life Insurance Company Risk Management*, Milliman Global, 2003. http://www.milliman.com/pubs/LDP24_2003.pdf or http://rmft.soa.org/rmtf_erm.html Scroll to *12 Best Practices*

31. Grondin, *Aegon Risk Management,* Webcast of the SOA Risk Management Task Force, July 2004. http://rmtf.soa.org/rmtf_erm.html Scroll to *SOA ERM Mini Seminar Notes* – *Tom Grondin*

32. G. Allayannis and J. Weston, “The Use of Foreign Exchange Derivatives and Firm Market Value,” working paper, University of Virginia, January 1998

33. “Implementing Turnbull – A Boardroom Briefing”, The Institute of Chartered Accountants in England & Wales, September, 1999

34. “Understanding Enterprise Risk Management: An Emerging Model for Building Shareholder Value”, KPMG, 2001

35. Lam, James, “Enterprise Risk Management: From Incentive to Controls”, 2003

36. “Risk Value Insights™: Creating Value Through Enterprise Risk Management—A Practical Approach for the Insurance Industry”, Tillinghast Monograph (2002), http://www.towersperrin.com/Tillinghast

37. For further reference, see also Tillinghast’s Emphasis Magazine, 2004/2, pages 6-9

38. “Adding Value through Risk and Capital Management” – an ERM Update on the Global Insurance Industry, Tillinghast ERM Survey (2004), http://www.towersperrin.com/Tillinghast

Chapter 8. Glossary

Word	Definition
Analytic Methods	Models whose solutions can be determined in closed form by solving a set of equations; require a restrictive set of assumptions and assumed probability distributions that are mathematically tractable.
Asset Allocation	Determination of the optimal mix of assets by asset class.
Below-Target-Risk (BTR)	The expected value of unfavorable deviations of a random variable from a specified target level.
Candidate Analysis	Restricted form of optimization in which only a finite number of decision options are considered.
Capital Adequacy	The determination of the minimum amount of capital needed to satisfy a specified economic capital constraint, usually calculated at the enterprise level.
Capital Allocation	The deployment of capital to each business segment of the enterprise.
Capital Attribution	The assignment of enterprise level capital to various business segments that make up the enterprise, in recognition of the relative risk of each segment.
Capital Structure	The optimal mix of capital by type (debt, common equity, preferred equity), given the risk profile and performance objectives of the enterprise.
CFROI (Cash Flow Return On Investments)	EBITDA divided by tangible assets.
Chief Risk Officer	Individual responsible for overseeing all aspects of risk within an enterprise; usually responsible for risk policy, capital management, risk analytics and reporting.
Contingency Planning	The process of developing crisis management protocols in advance of crisis conditions.
Corporate Governance	The relationship among various participants in determining the direction and performance of corporations.
Correlation	A measure of the degree to which two risks behave similarly.
Covariance	Statistical measure of the degree to which two random variables are correlated.
Covariance Matrix	Two-dimensional display of the covariances among several random variables.
Credit Risk	The economic loss suffered due to the default of a borrower or counterparty.
Crisis Management	The proactive response of an organization to a severe event that could potentially impair its ability to meet its performance objectives.
Deterministic Models	Models that describe expected outcomes from a given set of inputs without reflecting the probabilities of the outcomes above or below the expected values.
Downside Standard Deviation	Modification of standard deviation in which only unfavorable deviations from a specified target level are included in the calculation.

Word	Definition
Dynamic Financial Analysis (DFA)	The name for a class of structural simulation models of insurance company operations, focusing on certain hazard and financial risks and designed to generate financial pro forma projections.
EBITDA (Earnings Before Interest, Dividends, Taxes, Depreciation and Amortization)	Cash flow measure used for evaluating the operating performance of companies with high levels of debt.
Economic Capital	Market value of assets less fair value of liabilities; the amount of capital required to meet a specified solvency constraint.
ECOR (Economic Cost of Ruin)	Solvency related measure of risk that enhances the shortfall risk and VAR concept in which the severity of ruin is also reflected; the expected value of the shortfall.
Embedded Value	A measure of the value of in force business; comprised of adjusted net worth plus the present value of expected future profits on in force business.
EVA (Economic Value Added)	Net operating profits after tax less the product of required capital times the firm's weighted average cost of capital.
Financial Risks	Risk from price, liquidity, credit, inflation and basis risk.
Hazard Risk	Risk from property damage, theft, business interruption, liability claims, etc.
Investment Strategy	Determination of the optimal mix of assets by asset class.
Market Risk	The exposure to potential loss that would result from changes in market prices or rates.
Operating Earnings	Net income from continuing operations, excluding realized investment gains.
Operational Risks	The risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems or from external events.
Optimization	A process for making decisions under uncertainty; includes the range of decision options, constraints, and the objective to be optimized.
Performance Measurement	The development and implementation of appropriate risk-based metrics for evaluation of business segment performance, reflecting capital consumption, return and volatility.
Probability of Ruin	Solvency related measure of risk; the percentile of the probability distribution that corresponds to the point at which capital is exhausted.
RAROC (Risk-Adjusted Return On Capital)	A target ROE measure in which the numerator is reduced based on the risk associated with the project. Calculated as expected net income divided by economic capital.
RARORAC (Risk-Adjusted Return On Risk-Adjusted Capital)	A combination of RORAC and RAROC in which both the numerator and denominator are adjusted in the ROE calculation.
Return on Equity	Net income divided by net worth.
Risk Aggregation	Combining all of the types of risks within an enterprise, across different business activities and risk types.

Word	Definition
Risk Analytics	Measures and tools used to quantify and evaluate risks.
Risk Based Capital	Formula derived minimum capital standard promulgated by NAIC.
Risk Limits	Specified levels of risk allowed by an enterprise; may be set at corporate and individual levels; prevents the enterprise from engaging in business activities that are too risky.
Risk Mapping	A visual representation of identified risks in a way that easily allows ranking them. Often represented as a two-dimensional grid with frequency on one axis and severity on the other.
Risk Transfer	The act of moving risk from one entity to another through the exchange of probabilistically different cash flows.
RORAC (Return On Risk-Adjusted Capital)	A target ROE measure in which the denominator is adjusted depending on the risk associated with the project.
Shortfall Risk	Solvency related measure of risk; the probability that a specific random variable falls below the specified threshold level.
Simulation Methods	Models that use a large number of computer-generated trials to approximate an answer; relatively robust and flexible; can accommodate complex relationships.
Stakeholders	Any individual or group with a direct interest in the affairs of the enterprise; includes shareholders, employees, suppliers and the general public.
Standard Deviation	The square root of the variance.
Statistical Methods	Models that are based on observed statistical qualities of and among random variables without regard to cause and effect relationships; easier parameterization of model from available data.
Stochastic Models	Models that treat specified inputs as variable; the outcomes then become specified with a probability distribution.
Strategic Planning	The use of structural simulation modeling as a decision tool to assist management in selecting among alternative strategies.
Strategic Risks	Risks from damage to reputation, competition, demographic trends, technological innovation, capital availability and regulatory trends.
Structural Financial Models	Financial models that describe how various inputs affect key performance indicators; explicitly capture the structure of the cause/effect relationships linking inputs to outcomes; often used in developing strategic and operational plans.
Structural Methods	Models that are based on explicit cause and effect relationships; the relationships are derived from both data and expert opinion.
Tail Events	Unlikely, extreme events, usually representing large losses.
TCE (Tail Conditional Expectation)	A solvency related measure of risk; similar to ECOR because it measures both probability and cost; the expected value, from first dollar, of all events beyond the tail threshold event.
VAR (Value at Risk)	Solvency related measure of risk; used primarily in banking industry; the maximum loss an organization can suffer under normal market conditions over a given period of time at a given probability level.

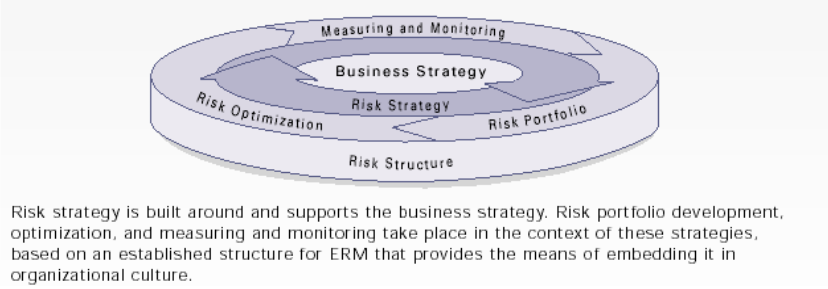
Word	Definition
Variance	The average squared difference between a random variable and its mean.
WACC (Weighted Average Cost of Capital)	The sum of the required market returns of each component of corporate capitalization, weighted by that component's share of the total capitalization.

Chapter 9. Annotated Bibliography

Article/References	Applications
COSO Enterprise Risk Management–Integrated Framework and Application http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf	This framework details the essential components of Enterprise Risk Management and the context in which they are effectively implemented. The context is not limited to the financial/insurance industry; instead, concepts are illustrated from a broader angle to present applicability in all industries. It defines ERM as "*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.* This report identifies the following eight interrelated components for ERM. For each component, detail explanations and case studies are provided to help readers implement the best ERM practice. 1. Internal Environment 2. Objective Setting 3. Event Identification 4. Risk Assessment 5. Risk Response 6. Control Activities 7. Information & Communication 8. Monitoring
Ingram, Wilkinson, Ehrlich, *Best Practices for Life Insurance Company Risk Management*, Milliman Global	This article outlines 12 essential practices for establishing RM in an insurance enterprise, based on the broad experiences of Milliman consultants. Each practice is discussed concisely and with a view to application of the concepts. This article could serve as a practical tool for developing a blueprint or checklist for RM implementation. The categories covered are: • Board and management responsibility for RM within the enterprise • Management's knowledge of all enterprise activities and RM systems • Independence of risk management and risk taking functions • Identifying and measuring risk • Setting limits and controls on risk • Expertise and systems support to perform RM • Risk Capital • Stress Testing • New products and ventures • Financial Reporting • Product Pricing • Monitoring RM and resolving weaknesses

Article/References	Applications
Grondin, *Aegon Risk Management,* Webcast of the SOA Risk Management Task Force, July 2004	Web site: http://rmtf.soa.org/rmtf_erm.html Meeting Minutes SOA ERM Mini-Seminar Notes–Tom Grondin This Webcast is presented in tree structure, flowchart, and bullet point formats. These charts provide a quick framework for RM in a global environment as well as simple definitions of terms. Aegon N. V. is the holding company for a leading insurance group with a focus on life and pension products. Having operations throughout the globe, Aegon's risk management (RM) must accommodate different markets and the interactions between them. To do so, Aegon has developed clear lines of communication and responsibility throughout the enterprise. These are outlined in the webcast. Because the corporate structure for each country represented in the Aegon group may be unique, each country may have a different RM framework; the flow should be practical for the given organization. An example of the U.S. structure is given. Each country's RM tree rolls up to a Risk and Capital Committee (RCC). As the top RM teams at the national level, the RCCs feed into a Group Risk Department for the enterprise. This latter department serves as a reporting task force to the Group Risk & Capital Committee, which ultimately reports to the executive and supervisory board of the enterprise. This framework enables two crucial aspects of ERM: • Risk information is communicated from the bottom to the top of the organization • Risk information is routinely considered within each context of the business itself–division, portfolio, corporate, country, global Five types of financial risk are defined and examples of each are given. The definitions and examples are general enough to provide insight into life and pension insurance companies as well as other industries. A bullet point discussion demonstrates how "what if" scenarios, stress testing, and product pricing are addressed for the various types of risks, and at the different levels of RM throughout the enterprise. The Liquidity Risk scenario outlines a Crisis Planning strategy. • Credit Risk • Liquidity Risk • Market Risk • Operational Risk • Underwriting Risk A comparison is made between the risk based capital (RBC) and the economic capital models (ECM). ECM is found to price risk more appropriately and to provide a balanced picture of risk at different RM levels (e.g. division versus country-wide). For an in-depth discussion of ECM, see http://rmtf.soa.org/rmtf_ecca.html, Economic Capital Calculation and Allocation.

Article/References	Applications
	Lastly, the roles of the Internal Auditor and the Operational Risk Manager are defined.
"Implementing Turnbull – A Boardroom Briefing", The Institute of Chartered Accountants in England & Wales, September, 1999 www.icaew.co.uk/viewer/index.cfm?AUB=TB2I_26539&tb5=1	Companies listed in London Stock Exchange are required in compliance with Turnbull internal control guideline. This 32-page briefing serves as a very practical guidance on how to embed internal control in the business process and further engage effective risk management. It mentions a very good point that companies traditionally emphasize too much on risk identification and not enough on risk management. Companies should focus on the significant risks, which might potentially damage its business objectives. When embedding the process, 1) having right attitude to risk management and 2) keeping the process simple and straightforward should always be kept in mind. The time and expense needed to increase the complexity or accuracy might not be worthwhile. In addition, companies need to make sure employees understand the purpose of controls and have a sense of ownership. Frequently, many fundamentals of good risk management and internal control are in place. Do not replace what is already working well. This figure shows the fundamentals of good risk management and internal control. 
"Understanding Enterprise Risk Management: An Emerging Model for Building Shareholder Value", KPMG, 2001 www.kpmg.com/Rut2000_prod/Documents/9/ERM.pdf	This white paper describes how ERM has evolved and then further addresses how leaders should seek to analyze their critical risks—balancing them with their objectives for improved returns—and then use that information to drive business value. At the end, it outlines a new ERM model, one that can provide organizations with new action steps they may use to enhance business decision-making and, potentially, shareholder value. The following are some highlights from this white paper: • How risk management is evolving: from risk mitigation toward risk portfolio optimization

Article/References	Applications
	• How organizations are deploying ERM: tools and techniques is use today 1. Identification/Assessment tools 2. Categorization tools 3. Financial quantification tools Once risks are identified, categorized, and quantified, organizations need to determine whether centralized or decentralized risk management approach will be implemented. Regardless which approach taken, the key is to create ERM program office and appoint Chief Risk Officer to develop and manage risk management strategy. • Deriving value from risk management: A New ERM model  Risk strategy is built around and supports the business strategy. Risk portfolio development, optimization, and measuring and monitoring take place in the context of these strategies, based on an established structure for ERM that provides the means of embedding it in organizational culture.
Lam, James, “Enterprise Risk Management: From Incentive to Controls”, 2003	This book provides an excellent explanation of Enterprise Risk Management (ERM) and an insightful road map to best practices in risk management. Modern portfolio theory teaches that it is possible to construct a portfolio that is reasonably safe even if it contains a number of high-risk investments, if the investments are either uncorrelated or negatively correlated. ERM treats market, credit, and operational risks as an element in an overall risk portfolio, integrating them three ways: 1. Organizational integration: A single risk management organization, often supervised by a Chief Risk Officer (CRO), manages all three kinds of risk. 2. Strategic integration: To avoid duplication, over-hedging, under-insurance and other missteps, ERM treats insurance, derivatives and other risk transfer instruments as part of a single risk management strategy. 3. Business process integration: ERM becomes part of the effort to optimize business initiatives such as pricing, sourcing, investment and others. ERM has seven key elements. Each of these components must be developed and linked to work as an integrated whole. 1. Corporate governance 2. Line management 3. Portfolio optimization 4. Risk transfer

Article/References	Applications
	5. Analytics 6. Technology 7. Stakeholders Section three, Risk Management Applications, addresses the best practices of risk management from three perspectives: 1) credit risk 2) market risk, 3) operational risk. Credit Risk Management: • Integrated measurement of credit risks • Scenario analysis • Credit scoring, credit surveillance and Credit migration modeling • Risk-adjusted pricing and profitability modeling Market Risk Management: • Hot spot analysis—this breaks risk down into its elements, considering not only VaR but also VaR by risk factors, by asset types, by geographic region, by trading desk and more. • Best hedge analysis—this calculates how much of each asset the trader must buy or sell to minimize portfolio risk. • Best replicating portfolio—this summarizes portfolio risk by using a few assets as proxies or representations. • Implied view—this determines what market view the portfolio's asset combination really expresses. Operational Risk Management: Manage risks from the following perspectives. • People: Human beings are subject to dishonesty and error. • Processes: This includes inadequate or erroneous documentation or pricing errors. • Systems: Computers can fail; models can be flawed and so on. • Events: Consider terrorist attacks, hurricanes, sudden market moves and such. • Business risk: Think of changes in competition, industry structure or technology.