

A PUBLIC POLICY PRACTICE NOTE

EXPOSURE DRAFT

# Insurance Enterprise Risk Management Practices

*March 2013*

Developed by the ERM Committee  
of the American Academy of Actuaries



---

AMERICAN ACADEMY *of* ACTUARIES

---

The American Academy of Actuaries is a 17,000-member professional association whose mission is to serve the public and the U.S. actuarial profession. The Academy assists public policymakers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

## ERM PRACTICE NOTE

This Practice Note was prepared by the ERM Committee of the Risk Management and Financial Reporting Council of the American Academy of Actuaries. The Committee developed an overview of the practices used by U.S. actuaries when performing or assessing the effectiveness of Enterprise Risk Management (ERM). While this Practice Note discusses some common approaches used in ERM, we make no representation of completeness; other approaches may also be in use.

This practice note is not a promulgation of the Actuarial Standards Board, is not an actuarial standard of practice, is not binding upon any actuary and is not a definitive statement as to what constitutes generally accepted practice in the area under discussion. Events occurring subsequent to this publication of the practice note may make the practices described in this practice note irrelevant or obsolete.

This practice note was prepared by the ERM Committee of the American Academy of Actuaries. Please address all communications to [rmfrcpolicyanalyst@actuary.org](mailto:rmfrcpolicyanalyst@actuary.org).

### **Participating Members from the 2011-2012 ERM Committee**

Bruce Jones, *Chairperson*

Mark Bergstrom  
Maryellen Coggins  
Patricia Matson  
Kevin Madigan

Malgorzata Jankowiak-  
Roslanowska  
Mary Bahna-Nolan  
Alistair Macpherson  
Seong-Min Eom



---

AMERICAN ACADEMY *of* ACTUARIES

1850 M Street N.W., Suite 300  
Washington, D.C. 20036-5805

## TABLE OF CONTENTS

I. Purpose/Introduction .....	4
II. Role of the Actuary in ERM .....	6
III. Concepts relevant to the practice and review of ERM	
A. Risk culture, risk organization, and risk governance .....	6
B. Policies and procedures .....	8
IV. Identifying and evaluating risks, setting strategy, and monitoring results	
A. Risk identification and categorization.....	10
B. Risk evaluation .....	12
1. Economic Capital Models .....	13
2. Model approach and key considerations .....	14
3. Model assumptions and parameterization.....	14
4. Risk Measures .....	15
5. Using economic capital models .....	15
6. Stress and scenario testing .....	16
7. Controlling model risk environment .....	17
8. Data collection and exposure monitoring .....	19
C. Risk Treatment	
1. Risk tolerance, risk limits, and risk appetite .....	21
2. Consistency of risk appetite and financial planning .....	22
3. Risk limits and authority guidelines.....	22
4. Local risk limit protocols .....	22
D. Strategic Treatment of Risk	
1. Goals/Strategies.....	23
2. Identifying strategic risk treatment options.....	23
3. Evaluating strategic risk options .....	23
4. Risk Mitigation.....	24
E. Risk Monitoring.....	24
F. External Impacts and Influences .....	25
V. Future Developments in ERM.....	27
Appendix 1: ERM definitions .....	29
Appendix 2: Relevant Actuarial Standards of Practice (ASOPs) .....	31
Reference Materials .....	34

## I. Purpose and Introduction

This Practice Note discusses Enterprise Risk Management (ERM) practices within insurance organizations<sup>1</sup>. According to the Casualty Actuarial Society, ERM is defined as “the discipline by which an enterprise in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.” The Committee of Sponsoring Organizations (COSO) of the Treadway Commission defines ERM as “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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” Both definitions recognize ERM as a corporate function that motivates an enterprise-wide understanding of risk and encourages commitment to the discipline of risk-based decision-making.

The practice of ERM within the insurance industry continues to evolve. Those insurers that had committed to the discipline of ERM several years ago have begun to realize tangible benefits from their investment; many more insurance organizations continue to work to implement or enhance the discipline within their management framework. Meanwhile, interest in these practices continues to grow among rating agencies and regulators who are interested in how insurers utilize ERM in the day-to-day management of their businesses and pursuit of their goals.

Effective ERM is supported by a substantial amount of quantitative analysis. While certain technical risk measurement approaches are referenced within this Practice Note, a thorough discussion of these approaches is outside the scope of this Practice Note. In addition, we recognize that the ERM practices of any given insurance organization may differ from those discussed within this Practice Note, since the practice of ERM and regulatory oversight of ERM continue to evolve.

At the time of the writing of this Practice Note, the National Association of Insurance Commissioners (NAIC) is developing regulatory requirements regarding an insurer's Own Risk and Solvency Assessment (ORSA). In general, the regulatory requirements for an ORSA leverage the existing risk management processes used by an insurer, rather than create a separate and distinct process or set of reports. The ORSA would generally reflect the iterative process of identifying and evaluating risks, setting strategy, and monitoring results that an insurance company does as part of its overall ERM program. The information regarding this iterative process can be helpful to insurers as they consider what type of information they will be providing to regulators to meet the ORSA requirements. Other than a brief commentary on ORSA in the section on external impacts and influences, this Practice Note does not describe ORSA requirements separately given that regulatory reporting of an insurer's ORSA will likely leverage existing ERM practices.

Effective ERM relies on two primary goals:

- To identify, evaluate and, where possible, quantify risks and their correlations and/or dependencies from all sources across an organization; and
- To ensure that the organization actively implements risk treatment strategies that leverage knowledge of its risks to achieve appropriate risk and return tradeoffs in accordance with an organization's values and goals.

---

<sup>1</sup> For the purpose of this practice note, “organization” is defined as an entity in the insurance industry for which ERM is being performed.

While there are many ways to illustrate the ERM process, the following diagram highlights key concepts that insurance organizations have used to employ ERM frameworks. These concepts include:

- A core risk culture, risk organization, and risk governance;
- An iterative process of identifying and evaluating risks, setting risk treatment strategies, and monitoring results, often called an ERM control cycle; and
- Recognition of the external impacts and influences of the economy, marketplace and views of regulators, the investment community and rating agencies.



This Practice Note seeks to treat each of these concepts in turn. It should be noted, however, that successful ERM frameworks provide for an integrated and iterative approach with a commitment to continuous improvement. Attempts within this Practice Note to treat concepts sequentially are purely for practical reasons and no inferences should be drawn from the order or segmentation. The iterative nature of the ERM process is fundamental to realizing its full value. In this note, insurance includes all types of products, (including reinsurance and co-insurance, for example).

## II. Role of the Actuary in ERM

Actuaries undergo extensive training and develop specialized experience in dealing with uncertainty within many areas of an insurance organization. Therefore, actuaries often play key

roles in all aspects of the ERM control cycle. Chief Risk Officers (CROs) may be credentialed actuaries. This practice note provides a summary of the principal elements of an insurance ERM framework and is intended for actuaries who currently serve in an ERM role, are in the process of considering such a role or have been asked to perform an independent review of certain aspects of an ERM program.

Throughout this practice note, references are made to practices by actuaries and practices by organizations. Due to the evolving nature of ERM and the typical need for an individual ERM practitioner to understand the overall ERM framework, these references regarding the ERM practices of insurers is included to provide broader context to the readers of this practice note.

While the intent of this practice note is to provide information to actuaries practicing in ERM, other professionals may find value in the note as well.

### **III. Concepts relevant to the practice and review of ERM**

#### **A. Risk culture, risk organization, and risk governance**

Effective ERM is generally characterized by an enterprise culture that supports accountability in risk-based decision making. Traits of organizations with an effective risk culture include an established risk governance framework, characterized by:

- broad risk management competency throughout the organization with a consensus that risk management is everyone's responsibility;
- an informed board of directors;
- appropriate risk committees and subcommittees with clearly defined roles and responsibilities;
- a CRO and/or ERM team with effective leadership and quantitative skills;
- effective risk management leaders undertaking coordinated efforts throughout the business; and
- a common risk language in support of a consistent enterprise-wide view of risk.

Such a governance structure provides an organization the platform necessary for the encouragement of effective dialogue among parts of the organization and among different levels of leadership. Often, a governance structure will support executive commitment to the organizational and infrastructure requirements needed to execute risk-based decisions. Practical considerations including the size, complexity, risk profile, and strategies of an organization can influence roles and responsibilities of the ERM governance structure.

Actuaries directly involved with ERM would typically develop a thorough understanding of management's and the board of director's commitment to effective ERM; such a commitment could be revealed through a close inspection of an organization's risk governance program. Members of the governance structure overseeing an effective ERM program are typically strong advocates of ERM and often convey a belief that ERM is a fundamental requirement for both the survival – and ultimately the success – of the organization. In organizations with effective ERM it is common for an executive at the highest level, such as Chief Executive Officer (CEO) or Chief Financial Officer (CFO), to be a vigorous champion of ERM. Each member of the governance structure would typically have a clear understanding of their risk management roles and responsibilities.

The CRO (or individual with CRO responsibilities) typically acts as a centralized coordinator of risk activities overseeing and facilitating business units' risk identification, risk evaluation and in some instances, risk treatment activities. It is most common for the CRO to report directly to the CEO, the CFO, the board of directors, and/or a sub-committee of the board.

Actuaries practicing in ERM typically develop an understanding of the roles and responsibilities assigned to an organization's CRO. A CRO's roles and responsibilities might include:

- Overseeing enterprise-wide risks, the management of those risks, and the enterprise's overall risk profile;
- Facilitating the development of a formalized risk appetite statement and tolerance limits;
- Ensuring appropriate governance and controls are in place to manage and quantify risks;
- Achieving compliance with regulatory requirements imposed on the organization.
- Implementing a risk identification process throughout the organization. This includes ensuring risk policies are in place around the roles and responsibilities of risk owners, the identification, measurement and management of key risks and the escalation process for when risk tolerances are breached or near breach;
- Chairing the organization's internal risk management committee (or similar management function) and coordinating the reporting of key risks being managed within the organization, including insurance, investment, liquidity and operational risks;
- Being one of the key authorities who manage significant risk events or crises;
- Working with management and risk owners to ensure key risks are assessed and quantified and to ensure key metrics for measuring risks are appropriate;
- Ensuring key risk assessments are considered in business and strategic planning in a manner consistent with the overall enterprise risk management framework; and
- Preparing a risk report or dashboard which monitors the key risks, measurement relative to the defined risk appetite for the organization, and the impact of risk treatment strategies employed. The risk report is typically prepared and conveyed to the senior management team, the risk management committee and the board of directors and/or its risk subcommittee(s) on a periodic basis.

An ongoing challenge for a CRO when overseeing an ERM function is the “bringing together” of the various risk-related functions and specialists within the insurance organization under a common framework and structure. Such risk-related functions may include: a business continuity team; an internal audit function; a treasury function; a credit risk function; a capital management function; a market risk assessment function (which may reside within asset management operations); an actuarial function; a reinsurance department or reinsurance buying function; fraud and investigations experts; health and safety experts reporting to the human resources (HR) function; and compliance teams in business units or in a central location.

It may be impractical or inappropriate for an insurer to combine all risk functions within a management structure headed by a CRO. However, it is important that processes are established to ensure that risk functions act and are seen to be acting in a coordinated fashion and viewed through a common lens.

The CRO might lead a corporate ERM team within which actuaries often play key roles. This team may include a broad mix of capabilities and skills to support the delivery of ERM objectives. Technical expertise alone might not be sufficient. The function may need project and change management skills as well as broader relationship management skills. Major roles and responsibilities of a corporate ERM team often include:

- Building, maintaining, and enhancing the ERM infrastructure;
- Building risk management buy-in;
- Ensuring consistency in the approach used for identification, quantification, treatment, and monitoring of risk;
- Acting as central clearing house for risk-based data and information;
- Supporting the business in the identification, assessment, and quantification of risks;
- Monitoring accumulations of exposure;
- Identifying and measuring - to the extent possible – correlations and/or dependencies between risks;
- Preparing enterprise risk reports; and
- Developing and maintaining technical models that support the ERM function (e.g., economic capital models, stress testing tools, etc.).

Effective ERM typically relies upon oversight provided by the board of directors. Boards will often approve the organization’s risk management policies and provide ongoing review of the organization’s ERM practices including those relating to the identification and assessment of risks that could have a material impact on the organization— often referred to as “key risks.” In addition to approving an organization’s risk management policy, its board of directors could periodically review and discuss with management the following:

- Implementation, execution and performance of the organization’s ERM program;
- Any changes to the organization’s risk appetite due to new strategies or changes in the business environment;
- Management of the organization’s most significant exposures (e.g., catastrophe exposures, investment exposures, exposure to credit risk across investments and insurance operations);
- The organization’s determination of appropriate risk mitigation strategies;
- Any material changes to the enterprise’s operations, including information technology;
- Any material changes to the legal and regulatory environments in which the enterprise operates;
- Strategic decisions that would alter the risk profile of the organization;
- Reports relating to material breaches of policy or limits;
- The organization’s business continuity and executive crisis management plans; and
- Any specific operational segments of the organization that could contribute unusual or significant risks that could have a material impact on the risk profile of the organization.

The primary stakeholders of an insurance organization can include policyholders, investors, active and retired employees, management, creditors, and claimants. The potential view of risk and risk management objectives of different stakeholder groups are unlikely to be uniform and therefore appropriate consideration needs to be given to conflicts of interest and the equitable treatment of each group.

## B. Policies and procedures

A risk management policy (or policies) is a means by which an insurance organization describes its ERM framework, communicates risk management expectations and defines risk management roles and responsibilities.

A published set of enterprise risk management policies and procedures generally improves the effectiveness of ERM. These are typically created and then reviewed and updated on a regular



basis with senior management, the board of directors, risk committees and business leaders. Effective risk governance typically involves a clear policy which includes accountability for adherence in fundamental areas, including:

- Well-defined risk preferences, risk appetite, risk tolerances and limits;
- Escalation procedures when the limits are approached or breached;
- Portfolio risk assessment of assets and liabilities and their inter-relationships;
- Effective assessment of results and feedback mechanisms
- Risk mitigation supported with cost benefit analysis;
- Communication by management of the risk responses and metrics for the organization;
- Risk and reward assessment of opportunities;
- Business continuity for the organization in the face of extreme events;
- Efficient and effective use of capital or other options in the reinsurance and capital markets;
- Performance measurements based on risk adjusted returns; and
- Management of and reaction to influences external to the organization.

Controls and procedures integrated into ERM policy would typically include:

- Purpose and objectives, and how these tie into an organization's strategy and risk profile;
- List of key activities, responsibilities, and accountabilities;
- Schedule identifying sequence and timing of tasks and milestones;
- Identification of key deliverables;
- Exception handling process;
- Change management process for modification and enhancements;
- Impact assessment to identify key assumptions and inputs; and
- Consistent reporting of key metrics used to monitor/mitigate/manage all key risks.

One area of potential importance with respect to policy setting is risk-adjusted performance management. Strategies are better executed when the interests of individuals and the organization are aligned, and risk-adjusted performance metrics are one way that companies introduce such alignment. Some organizations have developed performance metrics based on risk-adjusted metrics to facilitate comparison and evaluation of alternatives. The design of appropriate risk-adjusted performance metrics that are practical and accepted by stakeholders can be challenging. Policies designed to avoid conflicts of interest are frequently integrated into processes and governance as appropriate to help address this challenge.

## IV. Identifying & evaluating risks, setting strategy, and monitoring result

### A. Risk identification and categorization

In order to effectively manage risk it is important to first define and understand the risk to which an insurance organization is exposed. The spectrum of risks considered should not be driven solely by recent losses or by rating agency and regulatory considerations; it often includes a broader range of risks than might have been considered in the past and, critically, the interrelationships among those risks under a range of economic, financial and marketplace conditions. For an insurance organization, the sources of risk include the assets of the organization, the liabilities generated from underwriting the insurance risks, and the strategies and operations of the organization itself.

ERM requires the introduction of efficient processes for the routine identification, assessment, mitigation and monitoring of the key risks to which the organization is exposed. For efficiency, ease of communication and to assist in the development of a common risk language, many insurance organizations aggregate these risks into several broad categories as follows:

- Insurance risk: unexpected changes associated with non-investment related events impacting the underlying insured population, such as mortality, morbidity, policyholder behavior, accident, catastrophe, and theft.
- Investment risk: unexpected changes in external markets, asset prices, interest and exchange rates, credit spreads, and liquidity characteristics.
- Operational risk: unexpected changes in elements related to operations, such as human resources, technology, processes and controls.
- Strategic risk: unexpected changes in key elements of strategy formulation or execution.

It is also common for organizations to build a risk taxonomy as part of their ERM processes, which identifies the subrisks associated with each broad risk category, allowing for further classification, and then management, of risks at a granular level.

Desired characteristics of an insurance organization's risk identification process are that it is:

- Comprehensive: covers all material and emerging risks.
- Inclusive: all risk-taking functions within the organization are involved in the risk identification process.
- Efficient: any "bottom up" risk identification processes utilized should be balanced by "top down" processes thereby limiting consideration of risks that pose little or no likelihood of material impact on the organization.
- Consistent: all risks identified are defined in the context of a common framework and consider both the inherent risks to which an organization is exposed as well as the net effect of mitigation strategies that may be in place (i.e., residual risk).
- Focused: on a qualitative and quantitative assessment (likelihood, impact and speed of onset of risks) and prioritization of key risks.

Enterprise-wide risk identification is typically performed on a routine basis or if the risk profile of the organization materially changes, and actuaries are frequently involved in this process. An

effective method adopted by many insurance organizations for identifying enterprise-wide risks is to conduct periodic senior management risk workshops, the development and facilitation of which may involve the following considerations:

- Workshop participants: participants are typically those that are actively involved in risk taking or risk management functions and have a "stake in the game." Since the workshops involve qualitative assessments of risk, participants typically possess a strong intuition about the most significant risks of the organization. Workshop participants often include: the CEO, General Counsel, head of internal audit, CRO or equivalent, head of HR, heads of major business units, Chief Technology Officer (CTO), head of marketing, CFO, head of compliance, head of strategic planning, CIO, Chief Underwriting Officer (CUO), Chief Actuary, etc.
- Advance communication: prior to the workshops, participants typically receive and review advance communication that prepares participants on the workshop objectives, including background on the organization's ERM program, a clear description of what is expected from participants, definitions of risk categories and an overview of prioritization framework (for example, likelihood, impact, and speed-of-onset metrics).
- Risk registries, risk assessment surveys or interviews: risk registries and surveys or selected interviews may be provided or conducted in advance of the workshop to encourage a common risk language, motivate thinking and establish an initial risk ranking prior to the senior management workshop.
- Senior management workshop: attendees of the workshop typically review the rankings, discuss the highly ranked risks and decide on where to delineate between key and non-key risks. The result of the workshop is usually a prioritized list of key risks which will be regularly reviewed and periodically updated in response to the organization's changing risk profile.

In addition to a process for the identification of known risks, the organization typically also has in place a process to regularly identify and assess potential emerging risks. Environmental scanning for emerging risks involves the collection and processing of information from multiple sources, for example:

- Attending industry conferences;
- Researching industry and academic journals;
- Serving on industry committees;
- Conducting discussions with industry experts;
- Conducting comparative analysis of risks disclosed by competitors; and
- Understanding general socio-economic and technological trends
- Reading ERM surveys and analyses.

Coupled with the external environmental scan could be an introspective review of the exposures, claims, policyholder populations, terms and conditions of the policies written etc., to anticipate additional sources of emerging risk.

## B. Risk evaluation

Risk evaluation typically follows the risk identification phase of the ERM cycle and may involve a wide range of methodologies and approaches. Actuaries have long been involved with risk evaluations, examining the potential impact of risk outcomes and the likelihood that these risk outcomes might occur.

Typical risk evaluation tools may be developed using a variety of methods for the quantification of risk. Common risk quantification methods include:

- **Stress Tests**—Stress testing involves an assumption of a specific degree of adversity and measures the financial impact of that adverse experience upon the organization.
- **Reverse Stress Tests** – Reverse stress tests identify scenarios that cause insolvency and then investigate their probability and possible mitigation.
- **Stochastic Models**—Stochastic modeling involves estimating probability distributions of potential outcomes using random variables for one or more inputs over time. In many cases, this could include an ESG that simulates potential outcomes of the economies and financial markets. The distributions of potential outcomes and, in particular, the extreme losses indicated by stochastic models often form the basis for computing key risk metrics of the organization.
- **Reference to Standard Measures**—Regulatory and rating agency capital models use standard measures of the risk of organizations. These models are often factor-based, involving the use of a fixed formula for material risks and the assignment of risk loads to exposure amounts from financially reported sources.
- **Hybrid Methods**- These include some combination or averaging of the prior methods.

Assets and insurance product-related risks can be evaluated on their own individual merits; however, ERM typically involves a holistic view through the examination of the incremental impact of these activities on the full portfolio of risks of the organization. Risk evaluation can require the quantification of both individual and aggregate risk positions. Evaluating risk for the entire organization usually requires well-defined risk metrics and methodologies. These risk metrics and methodologies typically recognize both current and potential internal activities and risk positions of the organization as well as the external economic and marketplace environments. To keep metrics and methodologies current, there is often an advantage if the evaluation process occurs frequently.

An organization's view towards risk may change as the organization's risk management capabilities and risk evaluation models evolve. An ongoing flexible evaluation structure provides the opportunity to make regular changes to an organization's risk treatment strategies, including those used within its claim and underwriting practices. In some cases, risk models need to be updated or recalibrated to reflect the new view of an organization's risk exposures.

Risk models are evaluated as "fit for purpose", or appropriate for the model's intended use, by considering a range of criteria including but not limited to the following:

- the degree to which the models need to be reproducible and adaptable to new risks;
- the trade-off between precision and simplicity;
- the complexity of the models and model components in proportion to the materiality of the risks they cover;
- the practical considerations for the models, including usability, transparency, reliability, timeliness, process effectiveness, technological capabilities, and cost efficiency;
- the inherent statistical and theoretical limitations of the models;
- the quality, accuracy, appropriateness, and completeness of data underlying the models;
- the appropriateness of the methodologies used for model validation, calibration, and sensitivity testing;
- the appropriateness of the methodologies used for modeling dependencies and interactions among risks; and
- the appropriateness of the cash flow and discounting methodologies used in the models.

Commonly, substantial amounts of professional judgment are embedded within risk evaluation models and therefore the independent validation of these models is a fundamental step in the risk evaluation process. Techniques such as back testing and stress testing provide insight into the strengths and limitations of the models. Models provide valuable information and points of reference for the organization, provided model risk is understood by the risk management team and business leaders alike.

### *1. Economic capital models*

In this document, we use the term economic capital to refer to an organization's risk capital, regardless of the underlying framework (economic, statutory, etc.) used.

Economic capital models can be used to measure "the amount of capital an organization requires to survive or to meet a business objective over a specified period of time at a selected confidence level, given its risk profile."<sup>2</sup> Economic capital models are often used to assess capital adequacy and develop risk strategies by comparing the results of the economic capital model (measures of "required" capital) to "available" capital in order to understand the amount of capital available for other strategic purposes or for returning to capital providers such as shareholders and policyholders. In addition, economic capital models can be used to compare internal assessments of risk to rating agency and regulatory measures of required capital which can also serve to improve discussions with these external stakeholders about the risk profile of the organization. Many of the largest insurance organizations rely upon some form of economic capital models, but the range of structure, complexity, and use of these models is wide.

An economic capital model can provide a core utility in risk evaluation. A robust capital model can generate key metrics for strategic capital and risk decisions for the organization. Models provide useful metrics only if they adequately reflect the risks of the organization and the range of scenarios that it may encounter. Economic capital models can provide key insight into the impacts of potential economic and catastrophic events that expose the organization to material

---

<sup>2</sup> ASOP No. 46. *Risk Evaluation in Enterprise Risk Management*

loss. The modeling process itself - one that is proportionate to the nature, scale and complexity of the risks faced by an enterprise - can add value to the risk management process beyond the model outputs, by clearly defining risk and requiring the collection of data that provide information on risks and their interactions. Also, an economic capital model and the modeling process can help provide a framework to support a common understanding of the organization's risk profile, support the articulation of an organization's risk appetite, and help embed a risk-focused culture.

### *2. Model approach and key considerations*

The design and development of an economic capital model involves the consideration of several factors, including but not limited to:

- the nature, scale and complexity of the risks faced by the organization;
- the appropriateness of the selected time frame;
- the basis of measuring loss (for example, solvency, regulatory standards, earnings loss, reputation damage, etc.)
- the confidence level underlying the organization's definition of economic capital relative to how it is used to support strategic decisions;
- the degree to which the economic capital model reflects significant risks of the organization in a consistent and comprehensive manner;
- the appropriateness of the method (i.e., stochastic or deterministic) used to model each risk; and
- the references to and reliance on accounting frameworks, which should be consistent throughout the model and appropriate for the model's intended use.

### *3. Model assumptions and parameterization*

Economic capital models incorporate a wide range of underlying assumptions and could include complex parameterization processes. Often, the selection of assumptions will be based upon informed judgment since economic capital models generally focus on remote, unlikely losses that might be experienced by an organization. Due to the nature of economic capital and the focus on tail risk, the development of assumptions and their interrelationships in tail events can be challenging. Therefore, techniques beyond those used for more traditional models may be needed to develop appropriate parameterization.

Considerations for model assumptions and parameterization may include:

- historical data;
- the fit of assumed distributions to the available data in terms of expected value, variance, and extreme values;
- prices in the marketplace;
- use of benchmark data from regulators, rating organizations, or other industry experts;
- opinions of experts;
- sensitivity of results to changes in baseline assumptions;
- internal consistency of the assumptions; and
- the consistency in the application of assumptions over time.

Since economic capital models measure the aggregate risk of an organization, assumptions characterizing the dependency structure of risks are vital for the development of meaningful results. Often, the interaction between risks is described using statistical measures of dependence such as correlations, copulas, or shared risk drivers. Although these statistical measures may broadly capture the dependencies between risks, they are limited in their ability to adequately characterize severe or compound risk interactions that are remote but possible. In addition, they can be challenging to develop due to data limitations and may be difficult to implement and understand. Therefore, scenario tests can serve to supplement the evaluation of risk interactions using economic capital models under extreme events.

#### 4. Risk measures

When measuring economic capital (or other key risk metrics), organizations may rely upon a variety of risk measures to define acceptable levels of risk. Many organizations make use of multiple measures to avoid overreliance on a single metric. An organization's selection of specific risk measurement metrics may reflect its risk management objectives, model assumptions or the availability of data. Examples of common risk metrics include:

- Value at Risk (VaR): given a confidence level  $\alpha$  between 0 and 1, the VaR at the confidence level  $\alpha$  is the maximum loss amount  $x$  such that the probability that the loss exceeds  $x$  in a given time horizon is no more than  $(1-\alpha)$ .
- Tail-Value at Risk (TVaR): the expected amount of loss in the worst  $(1-\alpha)$  % of the distribution. It is also called Conditional Tail Expectation (CTE) or Worst Conditional Expectation (WCE).
- Risk Adjusted Performance Measurement (RAPM): major categories are Risk-Adjusted Return on Capital (RAROC), Return on Risk-Adjusted Capital (RORAC) and Risk-Adjusted Return on Risk-Adjusted Capital (RARORAC).
  - RAROC: (Risk-Adjusted Net Income) / (Allocated Economic Capital). The numerator is adjusted to reflect risks that are not captured in accounting-based net income, and the denominator uses economic capital that is allocated to the specific unit being measured. The method for making risk adjustments varies widely. This metric is also sometimes referred to as Risk-Adjusted Return on Risk-Adjusted Capital, or RARORAC.
  - RORAC: (Net Income) / (Allocated Economic Capital). The numerator is typically based on accounting basis net income without risk adjustment. The denominator is typically consistent with the denominator used in RAROC. In addition, sometimes RAROC and RORAC are used interchangeably, so it is important to understand how the term is defined in each situation.
- Return on Equity (ROE): (Net Income After-Tax) / (Shareholder Equity).

#### 5. Using economic capital models

As stated above, organizations utilize economic capital models to support a broad range of objectives, from assessing risk and solvency to supporting strategic initiatives. Some of the more common uses of economic capital models are as follows:

- Assessing capital adequacy: Many organizations use economic capital models to effectively ensure adequate capital is maintained both in aggregate relative to internal and rating agency targets and for each legal entity or group relative to local regulatory requirements. In addition, economic capital models can be used to evaluate different operational structures to gain efficiencies and improve capital fungibility.
- Determining appropriate risk treatment strategies: To the extent material risks are quantified through economic capital metrics, changes in economic capital associated with various risk mitigation options can be used in evaluating risk treatment strategies.
- Analyzing financial performance: Organizations can use economic capital models to establish a variety of performance targets by business unit, by region, by product line, etc. These targets can be used by business leaders to assess and manage their underwriting and operational effectiveness. Economic capital models can provide quantitative feedback on actual results relative to targets that can then be shared with senior management and the board of directors— which, in turn, helps them to understand the nature and magnitude of the risk inherent in the enterprise.
- Pricing: Outputs from the economic capital model can be used to align product pricing with risk adjusted performance metrics.
- Developing business strategies: When developing strategies, organizations determine (and articulate via a risk appetite statement) the aggregate risk they are willing to take in pursuit of those strategies. Economic capital models are frequently used to support this analysis.
- Determining relative risk and reward: Economic capital often serves as the risk metric that is used in analyzing the relative risk and reward associated with various strategic decisions, and can in turn support a company in optimal deployment of capital in pursuit of its strategic objectives.

#### 6. *Stress and Scenario Testing*

Stress testing is a process for measuring the impact of adverse changes in one or relatively few factors affecting an organization’s financial position, while scenario testing is a process for assessing the impact of several simultaneously occurring events on an organization’s financial position. Stress and scenario testing have long been used for many risk management and regulatory purposes. These tests are emerging as key sources of information for solvency assessment by regulators.

When performing stress and scenario testing, several considerations are important:

- the degree to which various stress tests reflect a similar degree of adversity (i.e., assumed likelihood of occurring) and are therefore comparable;
- any items in the organization’s business plan that describe how the organization will function during a catastrophic event(s) as well as any historical organizational examples;
- an extreme event scenario may be a single catastrophic event or a series of events that, taken together, have catastrophic results;



- how actions and reactions of various stakeholders and markets during extreme events differ from those during “normal” times;
- whether the assumed interdependencies are appropriate under the stress or scenario testing assumptions due to the possibility of unanticipated consequences when risks interact in ways not seen historically (for example, a stress to one risk could result in a change in exposure to another risk);
- how to define situations that result in a non-quantifiable risk and how to show plausible financial effects on the organization;
- that some stress and scenario tests will be hypothetical situations which may not require validation of whether the scenario is realistic; and
- For major trigger events (e.g., catastrophes, events that have an adverse impact on an insurer’s reputation, downgrade by rating agency) the behaviors of the risks may need to be more carefully analyzed than with less adverse outcomes.

A basic requirement for a stress or scenario test is a forecasting process or system to project outcomes under alternative assumptions. Management should consider whether the objectives of the stress or scenario test will be accomplished based on the forecasting process or system used. Approaches that may be used for stress and scenario testing include the following:

- Models of single subsystems of the organization: Some very simple stress tests can be performed with forecasts of a single assumption that is being stressed. However, in most cases, even the simplest stress test requires the consideration of contagion effects throughout the organization.
- Integrated forecasting model: Economic capital models or business forecasting models may be designed to reflect the interdependency of various elements or assumptions and may be more appropriate for complex stress and scenario tests.
- Event footprints: For catastrophe risks, it is helpful to take an event footprint and overlay it over the geography of exposures. As the footprint is moved around, areas of risk (and mitigation opportunities) are uncovered.

#### 7. *Controlling model risk environment*

An organization’s economic capital model and stress testing tools are typically supported by documentation providing appropriately detailed descriptions and explanations of risks, the measurement approaches used, the key assumptions made, the scope of application, and restrictions or limitations. Since actuaries are often responsible for risk models within an ERM function, they may become responsible for the documentation of these models as well. This documentation can provide the foundation for the model control environment and for supporting regulatory and rating agency requirements. Actuaries can also play a critical role in explaining the technical concepts to non-technical stakeholders.

The ERM team is typically involved in establishing effective controls related to the risk modeling process. One significant component of the controls is typically *documentation of the process flow* from source to model. Full documentation of the flow helps ensure that the process is adhered to and that if there is a breakdown, the full process can be quickly reestablished. In addition, senior management and/or outside entities (regulators and rating agencies) may require a re-calculation or comparison of previous model output, and the documentation will help

facilitate this. Also, as an economic capital model is typically designed to be flexible and adaptable, comprehensive and accurate documentation will facilitate efficient future changes. The process flow documentation itself is typically controlled to ensure that only approved changes are incorporated. Risk model documentation may aid internal audit and other internal group efforts to assess model outputs for accuracy and completeness, back-testing and stress testing results, and communications to other committees, individuals and groups.

*Control steps* are typically identified, including expectations of work performed, schedule of expected confirmations and documentation and control of output. Each control step typically has processes and control evidence and identification of key individuals and backup responsibilities for each checklist activity.

In addition to independent validation of an economic capital model, an *accuracy and completeness assessment* of the data input into the economic capital model, the model's software environment, and the resulting model outputs is often completed on regular basis. The following are examples of model risk control strategy options that may be used:

- *Data reconciliation* – random and specific cross checks of data inputs to the source business units, IT systems, external models, etc. to ensure completeness, accuracy, relevance, conformity with goals and strategies and protection.
- *Peer reviews* – specific output provided on a regular basis to business experts and owners to obtain their endorsement.
- *Reasonability checks* – review of inputs to assess whether they appropriately reflect underlying data and risk assumptions; analytical tests on the output to assess reasonability as well as consistency with inputs.
- *Affirmations* – a defined control process to ensure that key individuals/business units asked to review and confirm specific data do so in a timely fashion and can provide support for their conclusions.
- *Supporting documentation* – a defined control process to ensure all supporting documentation is maintained in a secure environment at intervals defined by the CRO.
- *Independent validation* – use of independent parties (internal and/or external) that understand the business and its goals and strategies and perform analysis to periodically verify the accuracy of the model and the relevance and completeness of its parameterization. Since economic capital is often determined based on the results of stochastic models that produce a large number of outcomes, model users should ensure that these complex models are appropriately validated. Model users and independent validators should devise appropriate tests of the distribution of outcomes calculated by the model (for example, in comparison to the range of results in similar models or to historical outcomes over time) and the sensitivity of those distributions to changes in the assumptions and parameters. Modelers should also perform validation tests to determine whether the model reasonably reproduces relevant items of the underlying balance sheet and income statements of the organization. Results and feedback from review with regulators and ratings agencies can be used to this end.

- *Controls* over software, servers and proprietary modeling are essential. The size and importance of most economic capital models implies a need for effective control over security access of the software and the server(s) it resides on and change controls to prevent unwanted errors. Additionally, many models have frequent version changes to enhance or correct modeling activity. The organization's data management team often provides testing and quality assurance to check that new versions produce the improvements intended and do not introduce additional issues. Contractual obligations related to third-party software/models are also an important consideration.

8. *Data collection and exposure monitoring*

The scope of data needed for ERM typically begins with an understanding of the current risk profile of the organization and the current risk metrics in use by the organization to support its risk strategies. Data considerations require an understanding of:

- The organization's current key risks and their relationships to each other
- The organization's enterprise risk management objectives for understanding, controlling or optimizing risk versus reward
- The underlying data and models that are needed to appropriately examine these risks and their outcomes

ERM processes typically rely on a wide range of different types of data. While balance sheets and income statements are important elements of risk/reward analysis, they are typically not sufficient by themselves. Since risk evaluation typically involves estimating both the "expected" or average results and the distribution of possible future outcomes, unique data governance and data management requirements are often introduced. Data such as distributional statistics from a set of stochastic projections; comparable market data; company experience data; and management insights could be required as part of the risk evaluation process.

Data governance and data management therefore typically provide the framework to capture and calculate:

- The fundamental drivers of the insurance, asset, operational, and other key risk exposures of the organization;
- The parameterization of the corresponding distributional outcomes of these exposures;
- The interactive relationships that exist for these exposures under different scenarios;
- The stochastic and/or deterministic events used to examine distributions of risk outcomes; and
- The key risk metrics used to mitigate risks or evaluate the risk management strategies of the organization.

Because of the close relationship between outcomes and assumptions, the associated relationships between data governance and management for outcomes and assumptions may be significantly greater than in a reporting only environment. ERM data collection and exposure monitoring typically works best when there is:

- A full inventory of the risk exposures including information, when available, regarding historical incidence and management of the exposure;

- Sufficient and accurate data to support the development of distributions of possible outcomes given the risk exposures, economic conditions and the proper interrelationship of the risk bearing activities of the organization;
- Effective governance which supports meaningful and reasonable results, a stable environment and provides the underlying assumptions that are communicated, documented and appropriately vetted; and
- As needed, metadata and data dictionaries to describe how, when and by whom a particular set of data was collected, and how the data is related to other data.

While much of the exposure information will come from internal sources, for many risks/enterprises a significant amount of external data is needed to produce a realistic view of outcomes.

Data requirements and risk model selections are interrelated. The appropriateness of a model is typically evaluated based on the reasonableness of the outcomes, the organization's ability to provide the model with the data required and management's expert judgment relating to model input and parameterization. Some models will also have data quality or heuristics (intuitive judgment) packages to identify problems in the received data.

The choice of risk model will affect data requirements. Based on these requirements the governance process would typically include identification, evaluation and selection of the target data sources. In this process, the actuary often examines the availability and quality of the informational elements, the level of detail available and the completeness of the exposures captured. For the insurance risk exposures, much of this information can be collected as part of underwriting and pricing. Therefore, the data capture in the primary rating engines can provide a good source for capturing risk exposure data elements.

It is also important to understand the data input requirements to any stochastic modeling processes employed. Economic Capital Models or Dynamic Financial Analysis (DFA) models have many different data structures and requirements. Translation and/or conversion activities may be needed to properly process modeling data values. Modeling complexities and options might involve data element choices. To effectively prioritize data quality efforts, actuaries often must understand the impact of the values of the data elements on the key risk metrics used by the organization.

Many stochastic modeling software packages require an Economic Scenario Generator (ESG) to produce the range of possible outcomes. ESG output is typically evaluated for its quality, applicability, currency, frequency of updates and completeness to create the risk metrics for the organization.

Successful modeling efforts typically require data structures that appropriately reflect the corporate structure and products. They also typically capture how various business units and products are impacted by severe events as well as management's response to those events. Lastly, they often capture the cumulative and/or distributional results of this activity. Key considerations typically include:

- Corporate structure – What are the key businesses entities of the organization and what are their financial relationships?
- Business enterprises and product portfolios – What are the actual businesses of the organization and the products that are sold?

For each individual business unit above, the data structure must recognize both the inputs and the corresponding outputs. These elements would include:

- Inputs – Corporate and product structure, balance sheet items, planning data, parameters for pricing, reserve variability, correlations, reinsurance, investments, catastrophe probability curves and decision rules; and
- Outputs – Stochastic event sets, stress tests results, key risk indications, risk factors and capital requirements.

The number of data elements, parameters, relationships and stochastic events can create significant data storage and access issues. Good data modeling and design are often needed to make smart decisions about hardware and data reporting environments. The sheer size of the model typically requires effective control over security access and change activity to prevent errors. Additionally, many models have frequent version changes to enhance or correct modeling activity. The organization’s data management team often provides testing, quality assurance and production environments to properly evaluate that the versions produce the improvements intended and do not introduce additional issues.

Like ERM itself, good ERM data collection and exposure monitoring typically focuses not only on the individual elements but their relationships to each other and reflects the total activity of the organization.

### C. Risk Treatment

The ERM control cycle includes risk treatment activities including risk avoidance, risk mitigation, and the setting of limits associated with the identified risks. Organizations with effective ERM typically have a formal, documented risk appetite statement which drives the development of specific risk limits and governance for monitoring and enforcing those limits.

#### *1. Risk appetite, risk tolerance, and risk limits*

*Risk appetite, risk tolerance and risk limits* provide three important working concepts for the risk treatment process.

- *Risk appetite* is the amount of specific risk and aggregate risk that an organization chooses to take during a defined time period in pursuit of its objectives.
- *Risk tolerance* is the level of risk to which an organization is willing and able to be exposed, taking into account the organization’s financial strength, its nature, scale and complexity, the organization’s liquidity, and the physical resources needed to adequately manage the risk.
- *Risk limit* is a threshold used to monitor the actual risk exposure of a specific risk or activity unit of the organization to ensure that the level of actual risk remains within the risk tolerance.

Using these concepts, prospective opportunities can then be evaluated through the proper assessment of incremental risk to the organization, the strength of the organization and the marketplace opportunity for return.

Risks to the organization are typically viewed in terms of the magnitude of adverse consequence (severity), the likelihood (frequency) and the time until the impact occurs (speed of onset). This frequency, severity and speed of onset of adverse outcomes across all risks can provide important insight needed to assess capital and/or risk charges to businesses, products, geography and customers.

### *2. Consistency of risk appetite and financial planning*

A good risk treatment process generally includes some consideration of both the current risk appetite and the prospective plan of the organization. When the risk appetite and the financial plan are closely linked, various options can be more easily evaluated. This typically allows for a better management and board discussion of the organization's chosen position on the risk and reward continuum. It can also provide the opportunity to more easily integrate risk goals into employee incentive plans along with other profitability and production metrics.

### *3. Risk limits and authority guidelines*

Enterprise risk tolerance and risk limit monitoring is often supported by more granular activities that occur within specific subsets of the business. These activities may include avoidance of specific risks (identified qualitatively or quantitatively) that are outside of the risk tolerance of the organization or not appropriately priced in the marketplace.

Many organizations guide the identification, monitoring, quantification and management of risk through the development of risk-specific policies such as underwriting and investment policies, which should be reviewed and updated as appropriate. These policies are typically supported by specific authority guidelines which identify the individuals and/or committees that have the authority to accept such risks, as well as guidelines as to who has responsibility for the ongoing monitoring, measurement and management of such risks.

Effective ERM control environments usually involve the establishment and enforcement of key risk authority levels throughout the organization, across all business and operations units and by individual. A good system of authority level governance typically will include the establishment of specific steps regarding an elevation process so that the right person is involved in every aspect of risk assumption and risk mitigation. This process typically strikes a balance between being thorough and well controlled, but also unencumbered by unreasonable restrictions or delays that could jeopardize key decision-making with potential negative commercial impacts. In some cases, an additional independent review is warranted and would be included in the risk review process.

### *4. Local risk limit protocols*

When several businesses within an organization are competing to make use of capacity in associated risk limits, effective protocols are often required. Good protocols require real time

knowledge of the organization's current risk profile as well as an assessment of marketplace return opportunities.

Strategic risk management may not be effective if it cannot be translated into action at the local level. Effective aggregate risk limits and risk appetite position at the corporate level are often connected to local authority and decision making. The required actions and opportunities are put in the proper local context. For each risk limit concern, effective local monitoring of the risk mitigation typically results when it is aligned with the aggregate risk limits and risk appetite position.

#### D. Strategic Treatment of Risk

##### *1. Goals/Strategies*

Strategic risk management involves the assessment, evaluation and effective management of the relationship between risk and reward as the organization pursues its values and goals. Many of the processes, tools, and activities described in the prior sections are components of strategic risk management. Successful risk managers typically consider the basic tension between risk, returns and capital for the organization within the economic, political and marketplace environments. They seek risk strategies and solutions which will enhance the ultimate value of the organization to its stakeholders.

##### *2. Identifying strategic risk treatment options*

As an organization examines its strategic options and the associated risks, the three risk concepts described above (appetite, tolerance, and limits), expected returns and required capital may be modified to reflect appropriate alignment with the strategy. Once risk limits and appetite are aligned with the strategy and finalized, an insurance organization's options to improve its risk and reward position include but are not limited to the following:

- Modifying exposure or coverage;
- Changing prices or expense structure;
- Expanding new or existing risk and reward opportunities;
- Non-renewing risks or narrowing selection criteria of new business;
- Reconsidering reinsurance or other risk mitigation options;
- Modifying claim practices; and
- Modifying and/or reallocating capital.

##### *3. Evaluating strategic risk options*

Current market and economic conditions play a major role in evaluating and optimizing strategic risk options. How customers and agents react to changes from their insurer can be substantially affected by their perception of the marketplace around them. While models are often used to select the best option, the choice of assumptions is an important consideration – for example, customer and agent perceptions are difficult to measure and are subject to rapid change. Effective strategic risk management typically examines not only current risk positions but also future plans and potential acquisitions, and includes the management of change-related risks.

The interrelationships of current and new risks are typically examined together as opposed to evaluated independently.

#### 4. Risk Mitigation

An actuary may be called upon to review or recommend an organization's risk mitigation strategy, or may be involved in designing or using processes to mitigate risks relative to the organization's risk appetite, risk tolerance, and risk limits.

Risk mitigation involves the identification, quantification, and implementation of specific processes, strategies, or solutions to eliminate, reduce, or transfer enterprise risk. Examples of risk mitigation strategies include:

- Insurance or reinsurance
- Hedging
- Capital market products and alternative risk transfer (ART)
- Implementation of policyholder awareness, education programs, or loss control measures
- Changes in governance or process controls
- Changes in mix of business, distribution, or target markets
- Exiting specific markets and products or reducing coverage

Actuaries are often called upon to identify mitigation strategies based on the risk exposures to the enterprise, and often support the quantification of the impact of various risk mitigation options. Tools such as stochastic models, deterministic stress tests, and factor-based analysis can be used to assess the risk and reward impact of implementing risk mitigation strategies. Actuaries may be involved in quantifying the impact of strategies on risk tolerance limits. Ongoing monitoring of risk mitigation programs is also important, to ensure that the expected benefits continue to be realized.

#### E. Risk Monitoring

One of the fundamental building blocks of ERM is an effective risk monitoring framework. This framework typically comprises both quantitative and qualitative elements at key levels: local, regional and enterprise-wide. To be effective, monitoring needs to be timely and accurate and performed relatively consistently across the organization so that management decisions can be made efficiently.

Faced with myriad risks and opportunities, it can be hard to determine what should be monitored given limited resources. It is therefore typically important that risk monitoring is aligned with the strategic goals and objectives and incorporates appropriate reference to the risk limits, risk tolerances and overall risk appetite and preferences defined by management. Risk monitoring generally necessitates some risk quantification. Examples of metrics that may be used for monitoring include accounting ratios such as liquidity ratios, statistics such as combined ratios or asset and liability durations, and risk measures such as economic capital or coefficients of variation. When a limit is breached or a defined opportunity presents itself, the corresponding response can be launched. Typical responses could include the transfer of capital from one entity



to another within an organization, a change in the investment strategy and portfolio, a change in reinsurance purchases and/or a change in the underwriting activity in a specific area or areas.

Key Risk Indicators (KRIs) or other measures of accumulated risk exposure are often required for risk monitoring. KRIs mapped to specific risks enable active monitoring of potential losses or increasing risk exposures, and facilitate appropriate risk mitigation decisions. KRIs are typically relatively easy to measure and are usually integrated with regular risk assessments and dynamically updated. KRIs can provide significant risk-related insights to the management of a business unit. Therefore, KRIs are often incorporated within the organization/business unit objectives and strategies.

An important aspect of risk monitoring is the risk aggregation process. This process facilitates understanding of the interactions and diversification benefits among risks. Management information at an aggregate level typically reflects existing offsetting positions to allow for appropriate management actions and avoid overly conservative strategies based on non-diversified risk information. Additional reporting mechanisms are often developed to allow for risk aggregation reporting, since a simple collection of risk monitoring reports from the individual business units may not be sufficient for decision making at an enterprise level.

Successful reviews of risk aggregation could involve identifying clusters of risks that are contributors to adverse outcomes approaching or exceeding enterprise risk limits in terms that the stakeholders of the organization would understand. These may include but are not limited to:

- Businesses and distribution channels;
- Geographic footprints;
- Customer segments;
- Product and investment portfolios;
- Perils or loss categories; and
- Combinations of the above.

In addition to this focused, strategic risk monitoring, a more general risk surveillance process is often used to facilitate the detection of new and emerging risks on a timely basis. The business environment is dynamic; as laws and consumer behavior change, the systems and approach used to monitor risk need to be updated. In some instances more creative approaches are needed in order to detect a risk that has not yet been fully identified or defined. In this context, the ERM function may work closely with research and development (R&D) departments to stay current with new product development, market trends and changes to an organization's systems and procedures. Tools such as risk maps, charts and checklists may be used to enable a dynamic and robust approach.

#### F. External impacts and influences

There are significant stakeholders in an insurance organization's ERM process residing outside of the organization. These include governments, regulators, taxpayers, rating agencies, the broader communities wherein the organization resides, and business partners. These groups may exert significant forces that will likely impact an organization's risk attitude, risk strategy, risk evaluation, risk treatment, and reporting of risk. The actions and requirements of these groups

are considerations within the ERM framework in order to fully assess the organization's risk strategy.

The external economic and marketplace environment shapes the insurance organization itself, including its ERM framework. ERM foundational knowledge includes an awareness of the organization's standards and practices relative to peers and the industry. Core ERM processes may need to be re-evaluated with changes in the market or environment as well as changes to the portfolios, products, capital positions, operational activities, values and goals of the organization. Successful ERM frameworks are responsive to a changing external world. They exhibit an integrated and iterative approach with a commitment to continuous improvement.

Remainder of page intentionally left blank

## V. Future Developments in ERM

ERM is a relatively new area of practice for actuaries. Most U.S. insurance ERM capabilities have been instituted within the last ten to fifteen years, and there are organizations that still do not have formal ERM functions. Because of the relative immaturity of many ERM processes and procedures, practice is expected to continue to evolve, potentially significantly, over the next decade or more. In addition to continued enhancement and development that will occur within organizations, significant change in the regulatory landscape is expected as well. In the U.S., the NAIC and many state regulators are working on developing regulations related to ERM, including a requirement for insurers (unless they are below specified size thresholds) to regularly perform and provide a report on their internal ORSA process. In addition, ERM is an area of interest for the newly formed Federal Insurance Office. Also, there is significant effort underway in Europe with respect to finalizing the requirements of Solvency II, which focuses in part on the ERM practices of insurance organizations.

As a result of these activities – as well as continued academic research, influence from analysts, rating agencies and the public at large – we are likely to see many changes in ERM practices generally and within the insurance sector in the future which may not be addressed in this document. Examples of areas that are likely to evolve include:

- Improved linkage of ERM into overall corporate strategies and decision making;
- Increased “cascading” of risk evaluation (including risk appetite, tolerance, limits, and assessments) down to individual business units, asset segments and products;
- Better integration of economic capital analysis and overall capital management programs;
- Increased use of multiple “lenses” into risk metrics – i.e., using a combination of economic, GAAP and statutory measures;
- Increased consistency of practices across the insurance industry, as regulations are put in place and further disclosures are made;
- Further separation of duties into a “three lines of defense” model, whereby the ERM function serves as a provider of tools and methods, and a reviewer of results (e.g., the “second line”), and the business units own the “first line” risk management. A related change will likely be an increased role of internal auditing in reviewing risk information (the “third line of defense”);
- Improved infrastructure within ERM functions, including use of risk data warehouses, risk modeling and aggregation tools and reporting infrastructure to improve the efficiency, consistency and transparency of risk reporting;
- Improved documentation of ERM practices, as companies prepare both internal and regulatory documentation of their ORSA processes; and

ERM COMMITTEE PRACTICE NOTE

- Increased regulatory scrutiny of ERM practices and how they relate to an organization's risk profile and capital position, due to the implementation of ORSA and ERM regulations in the U.S. as well as the implementation of Solvency II for certain global organizations.

Remainder of page intentionally left blank

### Appendix 1: ERM Glossary<sup>3</sup>

- Economic Capital—The amount of capital an organization requires to survive or to meet a business objective over a specified period of time at a selected confidence level, given its risk profile.
- Emerging Risks—New or evolving risks that may be difficult to manage since their likelihood, impact, or timing are highly uncertain.
- Enterprise Risk Management—The discipline by which an organization in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the organization’s short- and long-term value to its stakeholders.
- Enterprise Risk Management Control Cycle—The continuing process by which risks are identified, risks are evaluated, risk appetites are chosen, risk limits are set, risks are accepted or avoided, risk mitigation activities are performed, and actions are taken when risk limits are breached.
- Risk—The potential of future losses, or shortfalls from expectations, due to deviation of actual results from expected results.
- Risk Appetite—The level of specific risk and aggregate risk that an organization chooses to take in pursuit of its objectives.
- Risk Limit—A threshold used to monitor the actual risk exposure of a specific unit or units of the organization to ensure that the level of aggregate risk remains within the risk tolerance.
- Risk Management System—A combination of practices, tools and methodologies that an organization uses to identify, assess, measure, mitigate, and manage the risks it faces during the course of conducting its business.
- Risk Metric—A measure of risk. Examples include value at risk, expected policyholders deficit, and conditional tail expectation.
- Risk Mitigation—An action that reduces the frequency or severity of a risk.
- Risk Profile—The risks to which an organization is exposed over a specified period of time.
- Risk Tolerance—The level of risk to which an organization is willing and able to be exposed, taking into account the organization’s financial strength, its nature, scale and

---

<sup>3</sup> All glossary words except for Risk Appetite and Risk Treatment are cited in *ASOP No. 46 Risk Evaluation in Enterprise Risk Management*.

complexity, the organization's liquidity, and the physical resources needed to adequately manage the risk.

- Risk Treatment<sup>4</sup>—The process of selecting actions and making decisions to transfer, retain, limit, and avoid risk. This can include determining risk tolerance, choosing risk appetites, setting risk limits, performing risk mitigation activities, and optimizing organizational objectives relative to risk.
- Scenario Test—A process for assessing the impact of several simultaneously occurring possible events on an organization's financial position.
- Stress Test—A process for measuring the impact of adverse changes in one or relatively few factors affecting an organization's financial position.

Remainder of page intentionally left blank

---

<sup>4</sup> *ASOP No. 47 Risk Treatment in Enterprise Risk Management*

## Appendix 2: Relevant Actuarial Standards of Practice (ASOPs)

Below are references to Actuarial Standards of Practice in place at the time of the writing of this note. This information is being included in this document to provide non-authoritative information regarding instances in which existing ASOPs reference specific risks, and also where existing ASOPs may apply to an actuary performing ERM services. However this list is for reference only, and is not intended to serve as guidance regarding applicability of specific ASOPs. It is the responsibility of the individual actuary to determine which ASOPs apply to their work and follow the requirements accordingly.

Examples of ASOPs that may be applicable to actuaries performing ERM work are as follows:

- ASOP 46: Risk Evaluation in Enterprise Risk Management. This ASOP provides guidance to actuaries when performing professional services with respect to risk evaluation systems.
- ASOP 47: Risk Treatment and Enterprise Risk Management. This ASOP provides guidance to actuaries when performing professional services related to risk treatment within a risk management system.
- ASOP 41 – Actuarial Communications. This ASOP applies to a broad range of actuarial communications, and therefore may provide helpful guidance to actuaries performing ERM services.
- ASOP 38 – Using Models Outside the Actuary’s Area of Expertise. While this ASOP applies to work regarding Property and Casualty insurance coverages, ERM actuaries of all disciplines may find themselves using models and simulations that are outside of the actuary’s area of expertise and therefore may want to review this ASOP.
- ASOP 7 – Analysis of Life, Health, or Property/Casualty Insurer Cash Flows. In determining solvency, capital, and other risk measurement, the actuary will be analyzing cash flows. This ASOP may provide useful guidance, whether it is or is not directly applicable.
- ASOP 23: Data Quality. This ASOP provides guidance to the actuary when selecting, relying upon, reviewing and using data, and when making appropriate disclosures with regard to data quality.

Several risks are addressed by adhering to the Actuarial Standards of Practice. The table provided below is intended as a summary and quick reference guide to some of risks addressed by the ASOPs.

Title of ASOP	Risks
1. Nonguaranteed Charges or Benefits for Life Insurance Policies and Annuity Contracts	Model risk, insurance risk
3. Practices Relating to Continuing Care Retirement Communities	Market risk, insurance risk, mortality risk, morbidity risk, operational risk, model risk, legal risk, asset-liability mismatch risk
4. Measuring Pension Obligations	Market risk, insurance risk, mortality risk, model risk, legal risk, Asset-liability mismatch risk
5. Incurred Health and Disability Claims	Model risk

ERM COMMITTEE PRACTICE NOTE

Title of ASOP	Risks
6. Measuring Retiree Group Benefit Obligations	Market risk, mortality risk, morbidity risk, model risk, asset-liability mismatch risk
7. Analysis of Life, Health, or Property/Casualty Insurer Cash Flows	Market risk, insurance risk, mortality risk, morbidity risk, model risk, asset-liability mismatch risk
8. Regulatory Filings for Health Plan Entities	Morbidity risk, insurance risk, operational risk, legal risk
10. Methods and Assumptions for Use in Life Insurance Company Financial Statements Prepared in Accordance with U.S. GAAP	Model risk, legal risk, operational risk
11. Financial Statement Treatment of Reinsurance Transactions Involving Life or Health Insurance	Operational risk, insurance risk
12. Risk Classification (for All Practice Areas)	Risk classification
13. Trending Procedures in Property/Casualty Insurance	Model risk
15. Dividends for Individual Participating Life Insurance, Annuities, and Disability Insurance	Model risk, insurance risk, market risk
17. Expert Testimony by Actuaries	Legal risk
18. Long-Term Care Insurance	Market risk, insurance risk, mortality risk, morbidity risk, model risk
19. Appraisals of Casualty, Health, and Life Insurance Businesses	Market risk, catastrophe risk, mortality risk, morbidity risk, operational risk, model risk, legal risk, asset-liability mismatch risk
20. Discounting of Property/Casualty Unpaid Claim Estimates	Market risk, model risk, credit risk, insurance risk
21. Responding to or Assisting Auditors or Examiners in Connection with Financial Statements for All Practice Areas	Legal risk, operational risk
22. Statements of Opinion Based on Asset Adequacy Analysis by Actuaries for Life or Health Insurers	Insurance risk, market risk, asset-liability mismatch risk, model risk
23. Data Quality	Model risk, operational risk
24. Compliance with the NAIC Life Insurance Illustrations Model Regulation	Model risk, legal risk
25. Credibility Procedures Applicable to Accident and Health, Group Term Life, and Property/Casualty Coverages	Data collection and exposure monitoring
26. Compliance with Statutory and Regulatory Requirements for the Actuarial Certification of Small Employer Health Benefit Plans	Model risk, legal risk, morbidity risk
27. Selection of Economic Assumptions for Measuring Pension Obligations	Market risk, model risk, legal risk



ERM COMMITTEE PRACTICE NOTE

Title of ASOP	Risks
28. Statements of Actuarial Opinion Regarding Health Insurance Liabilities and Assets	Model risk, morbidity risk, market risk, legal risk
29. Expense Provisions in Property/Casualty Insurance Ratemaking	Market risk, insurance risk, catastrophe risk
30. Treatment of Profit and Contingency Provisions and the Cost of Capital in Property/Casualty Insurance Ratemaking	Model risk, market risk, insurance risk, legal risk
32. Social Insurance	Insurance risk, model risk
33. Actuarial Responsibilities with Respect to Closed Blocks in Mutual Life Insurance Company Conversions	Market risk, insurance risk, mortality risk, morbidity risk, operational risk, model risk, legal risk, asset-liability mismatch risk
34. Actuarial Practice Concerning Retirement Plan Benefits in Domestic Relations Actions	Model risk, legal risk
35. Selection of Demographic and Other Noneconomic Assumptions for Measuring Pension Obligations	Model risk, legal risk
36. Statement of Actuarial Opinion Regarding Property/Casualty Loss and Loss Adjustment Expense Reserves	Insurance risk, model risk, operational risk, market risk
37. Allocation of Policyholder Consideration in Mutual Life Insurance Company Demutualizations	Market risk, model risk, legal risk, insurance risk
38. Using Models Outside The Actuary's Area of Expertise (Property and Casualty)	Model risk, legal risk
39. Treatment of Catastrophe Losses in Property/Casualty Insurance Ratemaking	Catastrophe risk, model risk, insurance risk
40. Compliance with the NAIC Valuation of Life Insurance Policies Model Regulation with Respect to Deficiency Reserve Mortality	Insurance risk, mortality risk, model risk
41. Actuarial Communications	Legal risk, operational risk
42. Determining Health and Disability Liabilities Other Than Liabilities for Incurred Claims	Model risk, insurance risk
43. Property/Casualty Unpaid Claim Estimates	Model risk, insurance risk, operational risk
44. Selection and Use of Asset Valuation Methods for Pension Valuations	Model risk, market risk
45. The Use of Health Status Based Risk Adjustment Methodologies	Model risk, operational risk
46. Risk Evaluation in Enterprise Risk Management	All risk types
47. Risk Treatment and Enterprise Risk Management	All risk types

## Reference Materials

Acharyya, Madhu (2007). *Proposing a Conceptual Framework to Measure the Performance of Enterprise Risk Management from an Empirical Study of Four Major European Insurers*

Basel Committee on Banking Supervision (2004). *International Convergence of Capital Measurement and Capital Standards A Revised Framework*

Berliet, Jean Pierre. (2008) 'Increasing the Usefulness of ERM to Insurance Companies', Risk Management Issue No:13.

Casualty Actuarial Society (2003). *Overview of Enterprise Risk Management*.

The Committee of Sponsoring Organization of the Treadway Commission (2004). *Enterprise Risk Management-Integrated Framework*.

Doherty, Neil (2000). *Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*. New York: McGraw-Hill Companies, Inc.

Hardy, M.R. (2003) *Investment Guarantees: Modeling and Risk Management for Equity-Linked Life Insurance*. Hoboken, NJ: John Wiley & Sons, Inc.

Lam, James (2003). *Enterprise Risk Management: From Incentives to Controls*. Hoboken, NJ: John Wiley & Sons, Inc.

Lloyd's (2010). *Solvency II Detailed Guidance Notes for Dry Run Processes*.

Segal, Sim (2011). *Corporate Value of Enterprise Risk Management: The Next Step in Business Management*. Hoboken, NJ: John Wiley & Sons, Inc.

Society of Actuaries, the Casualty Actuarial Society, and the Canadian Institute of Actuaries (2008). *Risk Management: The Current Financial Crisis, Lessons Learned and Future Implications*.

Standard & Poors (2006). *Insurance Criteria: Refining the Focus of Insurer Enterprise Risk Management Criteria*.

Standard & Poors (2007). *Criteria: Summary Of Standard & Poor's Enterprise Risk Management Evaluation Process For Insurers*.

Standard & Poors (2010). *A New Level Of Enterprise Risk Management Analysis: Methodology For Assessing Insurers' Economic Capital Models*.