Canadian Institute of Actuaries / Institut canadien des actuaires

Practice Resource Document

Actuarial Aspects of Enterprise Risk Management

Committee on Enterprise Risk Management

March 2021

Document 221035

Ce document est disponible en français

The actuary should be familiar with relevant practice resource documents. They do not constitute standards of practice and are, therefore, not binding. They are, however, intended to assist members in considering whether they have addressed all relevant topics within a practice area. These may include skills and knowledge inventories (SKI), a compilation of other relevant material (internal or external to the CIA) related to the practice, as well as recognized best practices, where appropriate.

MEMORANDUM

To: Members in the enterprise risk management area

From: George Wang, Chair
Practice Development Council

Pierre Lepage, Chair
Committee on Enterprise Risk Management

Date: March 31, 2021

Subject: **Practice Resource Document: Actuarial Aspects of Enterprise Risk Management**

The Committee on Enterprise Risk Management (ERMPC) has prepared this practice resource document to assist members in understanding the various elements of Enterprise Risk Management (ERM) and to highlight areas where ERM practices can be of value, and to help achieve greater consistency in knowledge and awareness of various risk topics.

This paper focuses on ERM from an actuarial perspective and is intended to assist practitioners in considering whether they have addressed all of the various potential topics of relevance.

It is important to note that the approaches and methodologies discussed in the note will not definitively address the many various topics on ERM practice. Depending upon the specific circumstances and proportionality there may be other approaches that are more appropriate and other considerations to be taken into account.

In accordance with the Institute's *Policy on Due Process for the Approval of Practice Resource Documents*, this practice resource document has been prepared by the ERMPC and has received approval for distribution to all members from the Practice Development Council on January 19, 2021.

Practice resource documents are intended to assist members in considering whether they have addressed all relevant topics within a practice area. These may include skills and knowledge inventories (SKI), a compilation of other relevant material (internal or external to the CIA) related to the practice, as well as recognized best practices, where appropriate. Such documents may be particularly helpful to members in small or in emerging areas.

The ERMPC would like to acknowledge the contribution of the working group that assisted in the development of this practice resource document: Claude Désilets (chair), Mario Robitaille (former chair), Joel Cornberg, Phil Rivard, Sarah Cheng, Harry Li and Pierre Lepage.

Questions or comments regarding this practice resource document may be directed to Claude Désilets at claudedesilets@hotmail.com or Pierre Lepage at plepage@kpmg.ca.

GW, PL

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this paper is to assist actuaries or other practitioners in relation to enterprise risk management (ERM). Another objective of the paper is to highlight areas where ERM practices can be of value, and to help achieve greater consistency in knowledge and awareness of various risk topics.

The paper is wide ranging and deals with the possible components of an ERM system. The purpose of the paper is not to describe any individual element of ERM in detail but to assist in understanding the various elements of ERM and the various areas for consideration. Therefore, it is considered that the paper is more likely to be of relevance to practitioners who are assisting in the development of an ERM system or where the ERM system is at a relatively early stage of maturity.

It is important to note that the approaches and methodologies discussed in the paper will not definitively address the many various topics on ERM practice. Depending upon the specific circumstances and proportionality there may be other approaches that are more appropriate and other considerations to be taken into account.

This paper focuses on ERM from an actuarial perspective and is intended to assist practitioners in considering whether they have addressed all of the various potential topics of relevance. It is likely that the Canadian Institute of Actuaries (CIA) will produce additional papers on related ERM topics in the future.

The CIA acknowledges and thanks the International Actuarial Association (IAA) for being the primary author of this paper. The paper represents a modified version of an IAA paper entitled "Actuarial Aspects of ERM for Insurance Companies"[1], which primarily focused on risk management in the insurance industry. As the majority of the concepts covered in the IAA paper are also applicable outside of the insurance industry, this paper includes modifications to reflect the generalized application of the ERM concepts to any organization in which an actuary may be involved, as well as changes and examples to reflect relevant Canadian practices.

1.2 Enterprise Risk Management

There are numerous definitions of ERM. This paper has been developed with regard to the common themes and principles that emerge from the various definitions, notably the following:

- ERM is a continuous process.
- ERM adopts a holistic view to risk and assesses risk from the perspective of the organization's aggregate position as well as from a standalone perspective.
- ERM is concerned with all risks, including those that are unquantifiable or difficult to quantify.
- ERM considers uncertainty from both a positive and negative viewpoint.

[1] International Actuarial Association, Actuarial Aspects of ERM for Insurance Companies, January 2016.

- ERM aims to achieve greater value for all stakeholders by assisting in achieving an appropriate risk-reward balance.
- ERM considers both the short-term and the long-term aspects of risk.

It is generally recognized that a key value of an effective ERM is to establish key controls for the organization and to ensure that they are implemented consistently amongst the operations.

1.3 Relevant knowledge

The items discussed in the paper all require that there is a foundation of knowledge regarding the specific circumstances of the organization in question and of all relevant regulatory requirements.

2 Glossary

2.1 General terms

Alternative definitions of these terms are possible and the definitions below are only intended to define the terms as referenced in this paper.

alternative risk transfer (ART): The use of techniques other than insurance or reinsurance to provide risk transfer.

capital at risk (CaR): The capital that would be lost if a predefined event occurs.

Chief Risk Officer (CRO): The executive responsible for the risk management of an organization.

Committee of Sponsoring Organizations of the Treadway Commission (COSO): A joint initiative between five private sector organizations dedicated to providing thought leadership on ERM, internal control and fraud deterrence.

Contagion: When one risk event generates another. Financial contagion is the spread of a financial shock throughout a wider group, such as a financial group, an economy or the world.

earnings at risk (EaR): The reduction in earnings that would occur if a predefined event occurs.

economic capital: The amount of capital an organization requires to cover its obligations with a given degree of confidence over a specific time horizon.

economic capital models (ECM): A model used to calculate economic capital as defined above.

economic scenario generator (ESG): A consistent model that generates all the financial, economic and macro-economic variables required for economic capital calculations.

Financial Stability Board (FSB): Was established to coordinate at the international level the work of national financial authorities and international standard setting bodies and to develop and promote the implementation of effective regulatory, supervisory, and other financial sector policies in the interest of financial stability.

fungibility: The ability to move funds freely from entity to entity within a group of companies in order to absorb losses wherever they arise.

global systemically important insurers (GSIIs): In 2013 the IAIS published a methodology for identifying global systemically important insurers and a set of policy measures that would apply to such companies.

group: Generally represents a group of related organizations or a group of related companies.

ICAAP: The internal capital adequacy assessment process.

International Association of International Supervisors (IAIS): Represents insurance regulators and supervisors of more than 200 jurisdictions in nearly 140 countries.

insurance core principle (ICP): An international set of principles, standards and guidance applicable to insurance supervisors, seeking to foster convergence towards a globally consistent framework, developed by the IAIS.

international financial reporting standards (IFRS): International accounting standards developed by the International Accounting Standards Board®.

life insurance capital adequacy test (LICAT): The Canadian capital framework for life & health insurers.

minimum capital test (MCT): The Canadian capital framework for property & casualty insurers.

National Association of Insurance Commissioners (NAIC): The US standard-setting and regulatory support organization.

organization: Represents an enterprise including an insurance company, bank, pension plan, financial services cooperative, trust company, loan company, or any other financial institution or entity**.**

own risk and solvency assessment (ORSA): An organization's assessment of its risks and of the solvency needs associated with those risks.

PESTLE: A framework used to analyze the impact of external factors on an organization. It analyses the exposure of the organization to political, economic, social, technological, legal, and environmental factors.

risk adjusted return on capital (RAROC): Risk-adjusted return on capital is a measure of return on capital that adjusts the capital to reflect the level of risk associated with that investment.

risk based capital (RBC): Capital requirements that reflect the risk profile of the financial institutions.

risk appetite: The level and type of risk that an organization is willing to accept in order to achieve its objectives.

risk capacity: The extent of risk that an organization is able to support before breaching constraints generally determined by regulatory capital and liquidity needs and its obligations.

risk limit: The maximum amount of risk that can be underwritten generally set at the operational level. Risk limits will often be identified for key risk-taking activities such as insurance underwriting and investment.

risk management control cycle: A cyclical process typically involving identification, analysis, measurement, management and monitoring of risks.

risk profile: A description of the risk exposures of an organization.

risk response: The response of the organization to a particular risk, typically summarized as avoid, accept, transfer or manage.

risk tolerance: A quantitative description of the extent of risk that the organization is willing to take in respect of a specific risk; it is generally set by the organization in its risk appetite statement.

Solvency II: The prudential regime for insurance and reinsurance undertakings in the EU introduced on January 1, 2016.

surplus at risk (SaR): The shift in financial position that would occur if a predefined event occurs.

tail value at risk (TVaR): Quantifies the expected loss given that an event outside a given probability level has occurred over a given time horizon (a.k.a. conditional tail expectation).

time horizon: The time period associated with a given decision or measure.

transferability: the actual ability to transfer funds from one entity to another within a certain time frame.

value at risk (VaR): The maximum loss that could occur with a specified probability over a given time horizon.

2.2 Risks categories referenced in this document

Please note that this is not intended to be a complete list of risks but is solely intended to define the terms as used in this document. Please also note that alternative definitions of these terms are possible.

agency risk: The risk of loss as a result of an agent's pursuance of his or her own interests rather than the interests of the principal.

conduct risk: The risk that firm behaviour will result in poor outcomes for customers.

credit risk: The risk that a counterparty will be unable or unwilling to make payments due under a specific agreement.

emerging risk: A risk which may develop or which may already exist, that is difficult to quantify or may have a high loss potential.

equity risk: The risk of loss associated with exposure to an adverse movement in equity prices.

group risk: The risk of loss associated with exposure to other group companies.

inherent risk: The assessed level of raw or untreated risk; that is, the natural level of risk inherent in a process or activity without doing anything to reduce the likelihood or mitigate the severity of a mishap, or the amount of risk before the application of the risk reduction.

insurance risk: The risk of loss arising from movement in insurance variables including claim incidence, claim termination and persistency.

interest rate risk: The risk of loss associated with exposure to adverse movements in interest rates.

investment risk: The risk of loss relative to the expected return of any investment.

liquidity risk: The risk associated with the ability to trade a particular asset quickly without incurring a loss.

market risk: The risk of loss arising from changes in market variables.

mortality risk: The risk of loss arising from movements in mortality variables including morbidity and longevity.

operational risk: The risk of loss from failed or inadequate internal processes, people and systems, or from external events.

reputational risk: The risk that events could have an adverse impact on an organization's reputation or brand value.

residual risk: The risk remaining with an organization following its risk management process and internal controls.

strategic risk: The risk in relation to the achievement of an organization's strategic business plan and objectives.

3 ERM System

This section of the paper outlines various issues and considerations that might form part of an organization's ERM system.

Key components are risk governance, risk culture, and the steps that make up the core risk management process consisting of risk identification, risk assessment, risk measurement, risk response, risk monitoring, and risk reporting.

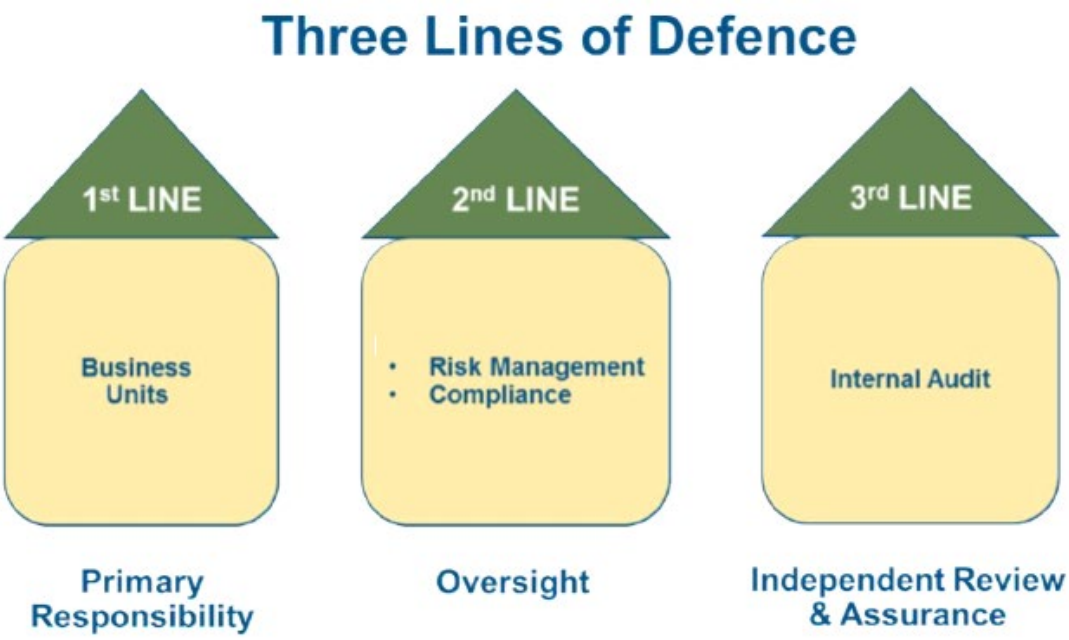
It is important to emphasize the dynamic nature of risk management as part of an ERM system. All of the sections in this document can be viewed as continuous processes that require ongoing review and updating so that they remain appropriate to the organization's circumstances and external environment.

3.1 Risk governance

Many organizations start the review of their ERM system by assessing the appropriateness of risk governance already in place. This encompasses the assignment of roles and responsibilities, policies and procedures, and the internal control system.

3.1.1 Roles and responsibilities

Many organizations adopt a 'three lines of defense' model, as illustrated in the diagram below:



- The first line is responsible for the regular operations of the business and includes business management and staff.
- The second line is responsible for supporting and monitoring the business and oversight of the operations of the first line.
- The third line is responsible for independent review and assurance of the operations of the first and second lines.

It is important to note that various interpretations of the three lines of defense are possible and that the above diagram is just shown as an illustration. It is also important to note that organizations might choose to use a structure other than the 'three lines of defense' model to achieve a similar outcome.

Actuarial duties and responsibilities can lie within any of the three lines of defense or across all three and different organizations will structure themselves in different ways.

It is important that the second line provides an independent challenge to the first line activities, but in order to do so effectively, it also needs to maintain a trusting relationship. It is usually difficult to maintain this balance.

The Board, Board committees and senior management are often considered to be the primary stakeholders served by the three lines. They are typically responsible for setting objectives, defining strategies, and establishing governance structures.

Many organizations assign roles and responsibilities of the various parties to ensure that the ERM system is robust. Key parties to be considered include:

- Board
- Risk committee

- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Chief Risk Officer (CRO)
- Chief Actuary or Appointed Actuary
- Compliance
- Internal audit

While the CRO would typically act as the centralized coordinator of risk activities overseeing and facilitating risk identification, risk evaluation and in some instances, risk response activities, the CEO and/or CFO should be a vigorous champion of ERM with oversight provided by the Board and risk committee.

The organization would typically need to consider whether it has addressed potential conflicts of interest and any independence criteria in the final structure chosen. The organization might also consider agency risk and the potential for management to have different interests to shareholders and/or policy-holders.

3.1.2 Risk policies and procedures

Many organizations document a risk strategy, outlining the high-level attitude towards risk, as outlined in Section 3.2. Many also establish risk policies for various individual risks, for example:

- credit risk
- insurance risk
- liquidity risk
- investment risk
- operational risk

The exact risk policies required for any individual organization will depend upon the individual circumstances of that organization, its risks, and exposures.

It might also be advisable to develop a policy in relation to risk mitigation techniques such as reinsurance and hedging.

Risk policies often outline:

- the organization's objective in relation to the specific risk;
- the link to the risk strategy;
- the tasks to be performed including how the risk is to be measured;
- roles and responsibilities;
- process and reporting procedures to be applied;
- escalation processes in relation to policy breaches (risk tolerances (3.2.1.2) and/or risk limits (3.2.1.3) are approached or breached; and

- frequency of review of the policy.

Procedures are then required to outline how the organization measures and reports risks in these areas on a regular basis.

3.1.3 Internal control system

An internal control system addressing the key processes and controls within the organization is an important consideration for most organizations. A frequently used definition of internal control is that adopted by the COSO Internal Control – Integrated Framework:

"Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."

The COSO internal control framework outlines five components:

- control environment
- risk assessment
- control activities
- information and communication
- monitoring activities

As part of the internal control system there would normally be clear documentation of all processes and controls. Internal audit would normally review the adherence to stated processes and controls on a regular basis.

The compliance function is often considered part of the internal control system, as are the risk policies and procedures detailed in Section 3.1.2 above.

3.1.4 Risk culture

Risk culture can be defined as, "the norms and traditions of behavior of individuals and of groups within an organization that determine the way in which they identify, understand, discuss, and act on the risks the organization confronts and the risks it takes."[2]

It is important to consider whether the organization has an appropriate risk culture, including whether risk management is appropriately supported by senior management. The Board and senior management, in particular the CEO, often determine how much weight is given to views on risk and how important a role the risk management function plays in relation to key business decisions such as new developments that involve taking on new types of risk.

As an example, for an insurance company, risk considerations often form an integral part of product development and pricing. Product development and pricing decisions could take into account economic value creation requirements for shareholders, a fair treatment of customers,

[2] "Reform in the Financial Services Industry: Strengthening Practices for a More Stable System" Institute of International Finance December 2009.

the impact on statutory requirements, the speed of recouping investment of capital, impact on financials and tail event impact on risk tolerances.

For a defined benefit pension plan, risk considerations would encompass investment policy (including asset-liability matching (ALM), liquidity), design of the plan (including indexation, anti-selection for optional benefits), funding policy, plan maturity etc.

Many organizations look to involve all staff in risk management and it is important to ensure that communication is working effectively in both directions. Assessing risk culture on a regular basis can provide insight into attitudes within the organization and trends in risk culture over time.

Risk culture can be measured through staff surveys testing awareness and views on risk issues such as the relative importance of potential adverse risk outcomes versus potential profits or sales targets.

Organizations would often also be conscious of the importance of ensuring that employees escalate potential losses and risks on a timely basis. It is important to signal the gravity of being aware of a risk or potential loss and not reporting it. To protect against risks that have reputational impacts in particular, organizations might also consider the establishment of an independent channel to allow employees to report issues and inappropriate behaviour, potentially on an anonymous basis.

One item which contributes significantly to risk culture and the relative importance of risk management is that of remuneration. Organizations sometimes link remuneration to risk-adjusted performance for certain departments rather than just considering performance. If this is not done then there can be an incentive for employees to take on more risk in order to increase the expected return, but with a corresponding increase in the risk of significant losses.

Similarly, there can be a risk that greater focus is placed on short-term results if remuneration is overly influenced by short-term performance. Some organizations and regulators have introduced longer term measures and other features such as the claw back of bonuses and the mandatory deferral of bonuses to help mitigate this risk.

3.2 Risk strategy

There are a number of different components to risk strategy but typically organizations would look to define and document the organization's objectives, principles, risk appetite, and responsibilities in relation to risk. The risk strategy would normally aim to be consistent with the organization's business strategy.

There is often discussion regarding whether the organization's business strategy is derived from the risk appetite or whether the organization typically defines its business strategy first and then sets its risk appetite. In reality, the two will typically be developed and evolve in tandem with the key point being that they remain internally consistent.

It should be noted that organization practices will vary greatly depending upon the nature, scale and complexity of the underlying business and that some organizations might choose not to use some of the elements discussed in this section (i.e., risk appetite, risk tolerances, and risk limits).

3.2.1 Risk appetite and related measures

3.2.1.1 Risk Appetite

There are many different definitions of risk appetite, a good example being that in the Financial Stability Board (FSB) consultative paper on "Principles for An Effective Risk Appetite Framework", which defines risk appetite as:

*"*The articulation in written form of the aggregate level and types of risk that a financial institution is willing to accept, or avoid, in order to achieve its business objectives. It includes qualitative statements as well as quantitative measures expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate. It should also address more difficult to quantify risks such as reputation and money laundering and financing of terrorism risks, as well as business ethics and conduct.*"*

Organizations' risk appetites will often have evolved informally over time and organizations often start by analyzing the risks that they are currently exposed to and the risks inherent in the organization's current strategy. They may however also consider establishing the Board's appetite to risk directly by surveying Board members on their attitudes to specific risk events, such as the potential for the organization to issue profit warnings or to breach minimum acceptable regulatory solvency levels.

As the analysis of risk exposures is developed, including how the risk exposures diversify/aggregate, how they may evolve over time, and how they may interact in extreme conditions. It may well mean that the risk appetite needs to be reviewed and revised.

3.2.1.2 Risk tolerances

As well as having qualitative elements in risk appetite statements, where possible, organizations will often set risk tolerances for each risk type. These will be used to determine for each material risk the maximum level of risk within which the firm is willing to operate, based on its risk appetite, risk capacity, and risk profile.

Risk tolerances are the typical measures of risk used to monitor exposure compared with the stated risk appetite. In practice, they enable the high-level risk appetite statements to be broken down into measures that are actionable and can be measured and monitored.

The aggregate maximum amount of risk the organization is willing to take is expressed in terms of key measures, which often include:

- capital or funding adequacy (usually economic, or the higher of economic and regulatory) and/or a credit rating target, including objectives in terms of maximum funding requirements or funding volatility;
- earnings or earnings volatility (usually using the published accounting basis but possibly other earning measures such as embedded value);
- liquidity (for example expected or stressed cash requirement over, say, four to 13 weeks); and

- operational risk including conduct risk. As operational risk is often expressed as a mix of qualitative and quantitative statements, it is often difficult to develop risk tolerances for this risk.

Developing risk tolerances helps to ensure that appropriate reporting and monitoring processes can be put in place for the effective management of these risks. As such, these tolerances will benefit from being clearly articulated and readily measurable.

3.2.1.3 Risk limits

While risk tolerances are set for an organization or group as a whole, it is important that risk limits are set at the most granular level for business operations. These translate organization risk tolerances and risk appetite for each risk category into risk-monitoring measures for business units.

The consistency between risk limits and the organization risk tolerance helps the organization to realize its risk objectives and maximize risk-adjusted returns. This tends to be a challenge for various reasons, including:

- the technical challenges of projecting future scenarios and capital requirements;
- the availability of data and their relevance to forecasting future experience, for example in respect of risk dependencies;
- the conflict that can arise between different risks and measures, for example between capital and earnings volatility;
- the interaction of risks and capital, in particular where assumptions have been made about the diversification benefits of certain strategies; and
- maintaining consistency between business unit and group objectives.

Business units are sometimes expected to operate within capital at risk (CaR), earnings at risk and other limits set as part of the group's risk limits framework. So, the metrics for them to do this need be readily available. This may mean that actuaries need to develop proxies to the exact calculations (and validate them and communicate the circumstances under which they may be unreliable).

In circumstances where a limit is at risk of being, or has been, breached, the business units would normally notify the CRO team as soon as they become aware of the matter.

3.2.1.4 Important considerations

Important considerations to some of the key aspects of developing and managing the business in accordance with risk appetite include the following:

- The risk appetite would ideally be sufficiently clear to support the monitoring of risk profile and might also be supported by forward-looking analysis (see Section 3.5.5), and subject to stress and scenario testing (see Section 3.5.6), to ensure that the organization understands what events might push it outside its risk appetite and/or risk limits.

- A clear set of risk metrics supporting the risk appetite statement is often considered to help to shape the risk culture. It is important that the risk metrics achieve a balance between being relatively easy to produce on a regular basis and being sufficiently reflective of the underlying risk exposures to be relevant.

The risk appetite has a direct impact on many operations, including but not limited to the following:

- New business mix/budgeting – the analysis of risks would often include both new business mix (looking at risk concentrations as well as opportunities to improve diversification) and volumes, taking into account both available capital and risk concentrations.
- Capital allocation – an analysis of the risks in different parts of the business will not only identify the capital required but also the uncertainty or volatility associated with the risk profile. This will be an important factor in allocating capital to different parts of the business. An additional consideration will be how, and to what extent, the benefit of diversification of risk at the organization level is allocated to lower levels within the business in the determination of capital requirements and risk appetite.
- Asset allocation – asset allocation would often take into account the respective risk appetite (and how risks diversify/interrelate) in optimizing asset returns against both liabilities and capital requirements.
- ORSA or ICAAP – this could include, among other things, an assessment of how well the risk profile of the business is aligned with the agreed risk appetite and how this is expected to develop in the future over the business planning period.
- Liquidity management – actuarial analysis of circumstances to determine the extent of the need for (short-term) liquidity is an important consideration, particularly when conventional actuarial models are not sufficiently granular for this purpose.
- Performance measurement and management – typically organizations set targets for earnings and/or earnings volatility. Actuarial teams would often play some role in defining and communicating such targets, and whether performance has been achieved by operating within risk appetite.

3.2.2 Stakeholder perspective

Due to their different interests, stakeholders may have different opinions on risk related strategies. Some stakeholders will be more risk averse than others. Stakeholders may include the following:

- *Regulators* – generally look to protect the interests of the public, particularly beneficiaries, and maintain the stability of the financial system.
- *Investors* – in order to profit from their investment, they tend to be less risk averse and more focused on return maximization.

- *Board of directors* – the Board represents the interests of investors but also has to consider all other views and constraints to maximize the organization's long-term value relative to its risk appetite. For mutual companies, the Board represents the mutualists who are generally the policy-holders.
- *Senior management* – they are expected to work to achieve the objectives of the Board but there can sometimes be a risk that they focus on short-term performance to the detriment of longer-term performance.
- *Bond holders* – their interest is in relation to the capacity of the organization to repay the bonds and make interest payments as required.
- *Credit rating agencies* – strategies which result in added volatility and added risk may result in a downgrade, which would increase the cost of borrowing for the organization. It should also be noted that a potential conflict of interest can arise for rating agencies because they are paid by the issuer of bonds rather than by the investors purchasing the bonds.
- *Customers* – their interest is in relation to the capacity of the organization to fulfill their promises.
- *Plan participants* – where the organization is a pension plan and the plan members themselves bear all or a portion of the risks, such members can be viewed as investors, bond holders, customers, or even participating policy-holders.

A risk appetite statement would often cover its desired position regarding major stakeholders. Together with risk tolerances, this may include the desired level of capital adequacy and earnings volatility, target bond ratings and financial strength ratings.

3.3 Risk identification

This section discusses the risk identification process, with specific reference to emerging and group risks.

Best practice would consider emerging risks separately, but not all organizations would treat it as a separate category.

3.3.1 Identification process

The core risk management process is typically structured around a risk management control cycle involving the systematic identification, assessment, measurement, response, monitoring, and reporting of risk. The precise steps in the cycle will vary from organization to organization depending upon circumstances but it is important to have a fully thought through documented process that can be demonstrated as required.

The first stage in the process is typically in relation to risk identification. Most organizations have a process for identifying, categorizing and tracking potential risks, ensuring that risk is not limited to financial or insurance risks but also considers strategic, reputational, and other risks. Conduct risk is another category that many organizations now define as a separate risk category, while others still consider it to be part of operational risk.

The risk identification process can be bottom up or top down or some combination of the two. In a bottom up risk identification process, many people within the organization are asked to identify risks. Those risks are categorized into major groupings and eventually fit into a hierarchy of risks that can be used by senior management in their strategic decision making. In a top down process, senior management identifies the major risk categories that they feel are best suited for management and Board attention. Those major risk categories are then often subdivided as risk management responsibilities are delegated to different levels within the organization.

The organization needs to consider how to ensure that all staff have a common understanding of the various categories so that risk can be reported consistently. Many organizations establish a risk taxonomy clearly defining what risks are considered to fall within various categories.

It is also possible to establish categorization systems using various methodologies. For example, some organizations categorize risks using a PESTLE methodology, where the acronym stands for political, economic, social, technological, legal, and environmental.

Important terminology in categorizing risks are the cause, the event and the adverse impact of a risk and it often helps in the identification process to give meaning to these terms.

There are numerous elements that might be included in the risk identification process, including:

- regular information flows from all departments highlighting key risks within the departments;
- workshops with senior management covering most material risks;
- specific workshops with specialists focused on an individual area;
- analysis of error logs detailing all risks or near misses that have occurred can help to identify risks;
- industry benchmarking which can serve to highlight risks; and
- scenario analysis which can identify particular exposures of the organization.

Once risks are identified, they are typically recorded on a risk register. The risk register might also contain information on the assessment of the risk such as probability, impact, control effectiveness, and residual risk. Sometimes it will also contain information on potential risk responses and any planned actions.

3.3.2 Emerging risk

Emerging risks are sometimes defined as risks which are developing or changing, which are difficult to quantify, and which could have a major impact on the organization. They are often associated with a high degree of uncertainty, a lack of data, and are often beyond the organization's control. Examples would include items such as climate change, cyber risk and the risk of pandemic.

Identification of emerging risks possibly require specific attention given that there can be limited data and they might not be captured by a process that might be otherwise focused on

more routine risks. Environmental scanning can be one method of gathering information on external risks, as can the use of external experts facilitating the identification of emerging risks in internal workshops.

3.3.3 Group risk

Group risk is another category for companies that are members of groups to consider. Companies that are members of a group might be adversely affected by an event that happens within a different group entity and group risk can arise in a number of different forms including contagion, leveraging, multiple gearing of capital, concentrations, and large exposures. Examples of these issues are outlined below:

- Contagion can occur where financial difficulties in one entity in the group results in other group members also experiencing financial difficulties.
- Leveraging can arise where a parent issues debt or other instruments which are ineligible as regulatory capital and down-streams the proceeds as regulatory capital to a subsidiary.
- Multiple gearing occurs when an insurer invests in a capital instrument that counts as regulatory capital of its subsidiary, its parent, or another group entity. In effect, the same capital is used twice to cover regulatory requirements.
- A concentration of risk can occur when relatively small exposures to an entity in separate group companies accumulates to a large exposure when aggregated to a group and parent level. This can also contribute to some of the other issues mentioned above.

3.3.3.1 Considerations for entities within a group

Groups typically consider ERM across the entire group. In fact, the sound management of a group often comprises intra-group transactions that allow, amongst other purposes, the diversification of risks within its component entities. Certain integral functions of the group, such as funding or liquidity management, are often carried out by designated entities that have the requisite licenses or ratings.

However, when carrying out ERM effectively throughout the group, insofar as business decisions are made locally or where the local business environment has specific features warranting additional consideration, circumstances of local entities can be separately analyzed. The local business' contribution towards the wider group's overall risk profile can be articulated as well.

This could allow the local management team to better understand the risks inherent within their businesses, and how they fit into the wider group's risk profile. Considerations such as when the local entity would start to monitor local capital or liquidity requirements more closely, and when they may start to request additional capital or transactional support from the group, can be articulated within the local risk management framework.

There may be differences in approach where the local entity is a legal entity (subsidiary of a group or holding entity), or where the local entity is a branch. A legal entity would probably have its own Board, which could be staffed with either internal senior management, or

potentially also independent Board members. In these circumstances, the local Board will potentially want to require or request a separate ORSA or ICAAP and other ERM frameworks or reports.

A branch, however, is unlikely to have a separate Board, but will generally have a management team. In order to aid them in a proper risk-based decision-making process, a proportionally appropriate element of ERM can be brought to a branch level. For example, the Office of the Superintendent of Financial Institutions (OSFI) Guideline E–19 (Own Risk and Solvency Assessment) applies equally to Canadian insurers and Canadian branches of foreign insurers. Liquidity and other considerations could be more important in the context of a branch.

3.4 Risk assessment

Once risks have been identified, many organizations will undertake some form of assessment or profiling. This is often done via an assessment of the likelihood of the risk occurring and the impact on the organization if the risk were to occur. This assessment is often performed in addition to the risk measurement, which is more focused on statistical and actuarial methods, detailed in Section 3.5. The results of the risk assessment and risk measurement are often combined into one integrated analysis.

There would often be an assessment of both the inherent and the residual risk, following the application of controls or risk mitigation. As described earlier, the inherent risk represents the assessed level of raw or untreated risk; that is, the natural level of risk inherent in a process or activity without doing anything to reduce the likelihood or mitigate the severity of a mishap, or the amount of risk before the application of the risk reduction. The residual risk represents the risk remaining with an organization following its risk management process and internal controls.

This assessment allows organizations to form some view on the effectiveness of the controls that are applied to risks and also on the extent of reliance on controls. A risk assessment or profile might include:

- a description of the risk in sufficient detail;
- the consequence of the risk, considering both financial and non-financial impacts;
- an appropriate categorization of the risk;
- an inherent risk assessment that considers the likelihood and impact of the risk, often expressed in qualitative terms as high/medium/low;
- an assessment of the effectiveness of the controls or risk mitigation strategies;
- a residual risk assessment after the application of controls or risk mitigation; and
- a description of any actions required to reduce unacceptable residual risk below an appropriate limit.

Section 3.8 on risk reporting outlines how the risk profile report can often provide a useful snapshot of the organization’s risk positions and can be effective in communicating those risks.

Due to their nature, assessing emerging risks often require specific consideration, with scenario analyses often playing an important role.

3.5 Risk measurement

Risk measurement is used to support the organization decision making and processes (including capital management and performance measurement) by providing important quantitative information related to the risks it faces. The nature, scale, and complexity of the risks in question would normally dictate the techniques used to measure risk with materiality and proportionality (i.e., whether the extent of effort is proportional to the size of the risk or potential losses) also being important considerations.

This section focuses on risk measures which are the output of risk models. It is divided into a number of subsections with the main subsections consisting of:

1) risk measures
2) models
3) aggregation
4) forward-looking assessment
5) stress and scenario testing
6) risk measurement documentation and reporting

3.5.1 Features of risk measures

This section focuses on the desired outcome and generic features of risk measures. This will drive many of the other choices that are made when performing other elements of the risk measurement process (including calibration, modelling, and stress testing).

3.5.1.1 Risk measurement selection criteria

There are several criteria that contribute to the selection of which risk measure to use, including the objective of the analysis being undertaken, the stakeholders involved (internal/external), limitations in available data to perform calculations and available modelling approaches given resource and time constraints. These criteria are important because they inform the desired level of sophistication for risk measures as well as limitations actuaries or other risk practitioners may face in selecting a risk measure.

Objective of analysis

The objectives for performing an economic capital calculation are quite different to the objectives for determining the annual volatility of incentive compensation (for example). The risk measures utilized for each of these may be different, and when combined with the other selection criteria, may warrant different levels of sophistication in the risk measure chosen.

Stakeholders

Taking account of the various stakeholders that use or contribute to the analysis is another important consideration when selecting the risk measure to be modelled and subsequently reported. While some level of education and disclosure is always recommended, if a highly

sophisticated measure is chosen, actuaries can expect to dedicate significant time for education related to the risk measurement methodology and definition of the risk measure provided. Diligence on the audience and intended use of risk measures will help ensure proper understanding and use of risk measures.

Data and modelling limitations

Data and modelling limitations are key pieces of information that contribute to the understanding of the sophistication of the risk measure that might be used to satisfy a specific objective. For example, using 99.5th percentile value at risk output from models that only capture 1 in 50-year event. Prior to deciding on a risk measure, the capabilities for both data and modelling might be assessed against the requirements for data and modelling of the risk measure chosen. Guidance on the proper use of models can be found in the CIA's educational note entitled *Use of Models*[3]. Addressing this at the outset will help to mitigate the risk of costly implementation projects that do not justify value add and will limit the amount of unnecessary investment on systems/data requirements.

3.5.1.2 Common risk measures

There are several risk measures that are commonly used for risk measurement purposes. It is important to understand their limitations as well as their advantages. An understanding of risk measure limitations provides additional information that helps to inform the selection of an appropriate risk measure. Common risk measures include:

- standard deviation
- value at risk (or VaR)
- conditional tail expectation (or tail value at risk).

These risk measures are outlined in Appendix A in terms of their definition, advantages, and limitations.

3.5.1.3 Risk metrics for business planning

In order to ensure effectiveness, risk management would ideally be integrated with business planning. Business planning covers many areas such as new business targets, asset allocation, and capital allocation. Actuaries are often required to predict the future financial outcomes of different strategies. The predictions usually cover not only the best estimate but also the volatility of the outcomes. These predictions are valuable inputs and have significant influences on the decision-making.

Risk metrics are used to measure the risk and its impact in business planning; and subsequently assess risk vs. reward of different strategies. We can classify risk measures into two broad categories – pure risk measures vs risk adjusted measures. Below are examples of each kind of risk measure.

[3] CIA Educational Note, Use of Models, Modelling Task Force, January 2017.

Pure risk measures:

- *Capital at risk (CaR)* – It can be described as the loss of capital/equity that is projected to occur with a probability of Y% over a specific time period. For example, there would be a loss of $100 million in a 99.5% scenario over a one-year time period. Some companies focus on the potential capital ratio change due to the loss, as the risk might not only lead to a reduction in available capital but also to an increase in required capital.
- *Earnings at risk (EaR)* – It can be described as the probability of an X% loss of expected/target earning in one year is less than Y%. Alternatively, with a probability of Y%, the earnings will be non-negative.
- Surplus at Risk (SaR) – For a pension plan, it can be described as the probability of an X% loss relative to the funding target in one year is less than Y%. Such a measure captures how risk events can affect both sides of a balance sheet.

Risk adjusted measures:

- *Risk adjusted return* – the measure of expected return adjusted for level of risk. For example, with risk adjusted return on capital (RAROC), the adjustment could be a reduction of cash flow by cost of capital or an increase in the discount rate for net income in the numerator or adopt risk adjusted capital (or economic capital) in the denominator.
- *Risk adjusted value* – the measure of expected value that is adjusted according to the level of risk. The adjustment cold be a reduction of the cash flows or an increase in the discount rate. For example, embedded value calculation techniques that explicitly take into account the riskiness of modelled cash flows.

Different valuation bases and accounting bases are used for different purposes. For insurance companies IFRS®, generally accepted accounting principles (GAAP), and economic basis may be used for measuring the EaR and risk adjusted return and value. Solvency II, NAIC RBC, LICAT, MCT, other local solvency frameworks, economic capital framework, and rating agency capital framework may be used to measure the CaR. The appropriateness of the basis being used for these measures might be a factor to consider. The basis would often be consistent with those used in the organization's risk appetite framework and how performance is measured in practice.

It is worth noting that 99.5% VaR over a one-year time period is a minimum level of regulatory capital in many territories and by convention approximates to a BBB credit rating. Many firms target a higher credit rating and accordingly target a higher level of confidence such as 99.95% VaR.

The selection of appropriate risk metrics is a factor for actuaries to consider. For CaR and EaR, when the loss distribution is heavily skewed, tail value at risk may be used instead of the VaR. For risk adjusted return and value, the risk adjustment can be made to the discount rates for future cash flows or to the cash flows directly using the cost of capital approach. Judgment is often needed to decide the most appropriate approach under each specific circumstance.

When selecting between two alternative capital projects or strategies, pure risk measures act like constraints, for example ensuring that a given risk exposure falls within agreed limits, and risk adjusted measures act like a combined measure of return and risk, or a way of assessing value on a risk adjusted basis. When two strategies work within the constraints, risk adjusted measures might be used to compare them.

3.5.2 Models

This section focuses on models in the context of risk measurement. This includes guidance to actuaries when contemplating the design, development, selection, review and/or the maintenance of a model to measure risk. The section includes a description of models which measure specific risk factors and models that simultaneously cover all risks. Risk is commonly measured in terms of impact on capital, and therefore this section also covers economic capital models.

3.5.2.1 Types of models

Models vary in sophistication and complexity depending on factors such as the materiality of the risk measurement result and the risk type being modelled. The following paragraphs outline various model types that an actuary can consider using when measuring risk. Models are described as those that vary by the level of sophistication employed and those that vary according to the individual risks being modelled.

It is also important to bear in mind that depending upon the specific purpose a model can encompass a lot more than just the calculation kernel or the software used. For example, a model could be considered to encompass (noting that this list is an example and not definitive):

- data
- methodology
- assumptions
- expert judgement
- documentation
- calculation kernel
- software
- model governance

<u>Models that vary by sophistication</u>

In selecting a model, the actuary might examine the materiality and complexity of the underlying risks being modelled. For small organizations and less material risks, a less sophisticated model, such as a simple factor model or deterministic stress tests, may be appropriate for measuring risk. As complexity and/or the materiality of the risk increases, the actuary might consider the use of a more sophisticated model, such as a full stochastic internal model. The development of a full internal model takes significant time, effort, and expense. If the development of a full model is not feasible, the use of a partial model (i.e., a combination of

standard regulatory stress tests for certain risks and more detailed organization-specific calibrations for others) can be a prudent alternative and can be used as a transitional step while the full model is being developed.

- *Simple factor models* – This is the simplest form of model that can be used to measure risk. A prescribed factor is multiplied by a known base amount to estimate the amount of risk. As examples, factor-based models are used in rating agency risk based capital models, US statutory risk-based capital models, and simplified calculations for the EU Solvency II Standard formula. A common use is in measurement of asset default risk, where ratings-specific credit default charges are applied to the value of assets held.
- *Standard shocks (stress tests)* – A risk can be measured by assessing the financial impact of a prescribed risk factor stress or set of stresses. Examples of this type of model are the standard stress tests applied in the EU Solvency II Standard Formula and Swiss Solvency Test; or on-going scenarios prescribed by OSFI for federally regulated insurers in Canada. In Solvency II, for example, mortality risk is assessed by calculating the financial impact of a 15% increase to best-estimate mortality rates, while longevity risk is measured based on a 20% decrease in mortality rates.
- *Own shocks (stress tests)* – Instead of applying prescribed stress tests, the actuary can measure the risk using stress tests calibrated to the specifics of their particular risks instead of the standard prudent industry stresses determined by regulators. For example, companies are required to create organization-specific adverse but plausible scenarios that involves multiple risk factors and assess financial impacts from such scenarios via annual ORSA process and Appointed Actuary's Report Financial Condition Testing.
- *Partial models* – If the actuary determines that a simple model cannot produce an accurate measure, or if an organization is particularly concerned with a subset of risk types, a more complex model might be developed for those particular risks. The model can be based on a probability distribution or distribution of scenarios, determined either stochastically or deterministically. The partial model can be used in conjunction with simpler models for other risks to create an aggregate measure of organization risk. An example of this in practice is the C-3 phase II portion of the US NAIC risk-based capital model, where a stochastic model is used to measure the risks of variable annuity contracts.
- *Full internal models* – The most comprehensive (and most complex) way to measure an insurer's risk is with a full internal model. To develop this model, one method is to use a multivariate probability distribution function as a basis to measure all risks simultaneously. Another method is to model each risk separately and aggregate the results using copulas as an aggregation approach. For underwriting risks with thin tails, where little data are available, it may not add value to develop a full simultaneous probability distribution function. However, a holistic model is more appropriate for risks with great risk dependencies, especially in the tail, which is our main area of focus. Once the model is developed, the risks can be assessed based on a set of underlying

stochastic or deterministic scenarios. Results of stochastic scenarios will produce a distribution of financial results, and the risk can be assessed by analyzing the tail scenarios. Results of deterministic scenarios are useful for understanding the impact of extreme scenarios under stress and scenario testing.

Models that vary by risk type

Risks that are material to the organization or entity should be quantified as much as possible. The following sections discusses some risks that are likely material to the type of organization or risks entity under consideration.

Models will vary based on the type of risk they are measuring. Different types of models may be appropriate for different categories of risk, such as market, credit, life underwriting, property and casualty underwriting and operational risk.

- *Market risks* – These risks, including interest rate risk, spread risk, foreign exchange risk, real estate risk, and equity risk, are largely dependent on external economic factors. These risks are often measured using stochastic models, which may make use of sub-models such as economic scenario generators. Asset/liability mismatch risks are less important in shorter-term business, although they might still be considered.
- *Credit risks* – These risks, including default risk and counterparty credit risk, are commonly measured using a factor model, where ratings-specific credit default charges are applied to the corresponding asset values or exposures. More sophisticated stochastic models can also be used to measure these risks, using a statistical distribution that defines the probabilities of default and loss given default for each underlying instrument or counterparty. Financial contagion might be another factor to consider in relation to credit risk, where the default or financial difficulties of one entity could result in financial difficulties for other linked entities.
- *Biometric risks* – These risks, including mortality, disability, and longevity, can be modelled using factors, stress tests, or more sophisticated stochastic models. Since these risks are often long-term in nature, the stress tests and models tend to be structured as cash-flow projection models, which could include stochastic elements.
- *Property and casualty insurance risks* – these risks include underwriting risk, reserving risk and catastrophic risk, are usually modelled separately and aggregated by correlation matrix or dependency models in economic capital models. Underwriting risk, the risk from in force exposure is usually decomposed into attritional and large loss components. Large loss is modelled via loss frequency and severity distributions whereas loss ratio model is used directly to model attritional loss. Reserving risk, the risk from past exposures, can be modelled stochastically with predictive distribution, i.e., bootstrapping, simulation techniques or generalized linear models. Catastrophic risk, the risk of multiple claims due to a single event from the in-force exposure. Property cat risk is usually estimated by supplementing the organization's loss experience with proprietary catastrophe model – cat event generator. In modelling both underwriting and reserving risks, actuaries should exercise their judgment in selecting the level of

granularity – i.e., whether to model individual line of business or combine similar risks (long-tail vs. short-tail coverages) to improve credibility.

- Behaviour risks – These risks, including persistency, contribution patterns, exercise of embedded options, and management expenses, can be modelled using various methods depending on the context. Interactions with other modelled risks must be monitored for consistency.
- Maturity risks – Certain organizations, such as a public pension plan, adopt investment strategies consistent with the organization's current risk profile and ability to bear risk. Where the underlying risk profile shifts over time due to gradual or sudden demographics shifts, the organization may encounter a dichotomy of being unable the bear the risks that are foundational to the success and objectives of the organization itself. Developing robust models to analyze maturity risks can be challenging due to demographic vagaries.
- *Operational risks* – These risks include fraud and risks related to information systems, compliance, business processing, human resources, business continuity, outsourcing, distribution channels, changes in the legal, regulatory, and taxation environments, and changes to the insurer's reputation. Due to the difficulty in quantifying these risks, a highly subjective scenario-based approach is often adopted, relying on the opinion of subject matter experts. Regulatory regimes and rating agencies vary on their assessment of this risk with many ignoring it or using a simple factor model. Particular diligence might be required in the understanding and mitigation of these risks wherever possible. If the measurement of operational risks is undertaken, the actuary might consider documenting any assumptions made, and seeking assistance from subject matter experts in the business, due to the high level of judgment and subjectivity involved. Some literature has suggested that, although the results may not be particularly robust, the quantification exercise may provide stakeholders with a better understanding of the true nature of operational risks.

<u>Economic capital models</u>

Economic capital models (ECMs) are a key component of risk modelling for some companies. A common definition of economic capital is the value-at-risk assessed on the market value of assets over liabilities. However, this is not necessarily the only definition of economic capital. More generally, an economic capital model allows an organization to quantify, assess and communicate its complete risk exposure using internally defined methods and assumptions.

The primary purpose of an ECM is to assess capital adequacy by comparing the ECMs calculation of required capital to the organization's actual available capital. The results can be used by the organization to make decisions regarding business strategy and capital allocation. ECMs can also be used to compare this internal risk assessment to rating agency and regulatory model assessments, which can assist in the communication of an organization's risk profile to external stakeholders. Most large insurance organizations have developed some form of ECM, but the range of structure, complexity, and use of these models varies widely.

ECMs can only provide useful results if they adequately reflect all the underlying risks of the organization and the range of scenarios that it may encounter. The model would normally be proportionate to the nature, scale, and complexity of the organization's risks. The ECM can be constructed using any combination of the model types listed above (factor, stress tests, partial), or it can be a fully integrated internal model either with stochastic scenarios and/or deterministic scenarios and stress tests.

3.5.3 Aggregation

The objective of many risk measurement activities is to develop a comprehensive view of the risks taken across an organization. As opposed to individual risk measurement, when performing risk measurement across multiple risk types, there is an added element of risk measure aggregation to consider. Risk aggregation takes into account diversification across risk types, geography, entities, or lines of business and dependencies among them, so that management could have a holistic and quantitative view of risks facing the organization and potentially exploit opportunities.

- There are several approaches to aggregating risk measures ranging from simple to complex. The appropriate approach to use in a given situation might be determined by the actuary and other key stakeholders involved in the process. The factors often considered are the extent of computing power, end-user sophistication, and the balance between complexity and additional accuracy.
- Model risk of dependence in risk aggregation.

The approach towards aggregation can be a very significant factor in determining the overall capital requirement. Thus actuaries should exercise their expert judgment in accordance with standards of practice and best practices.

3.5.4 Forward-Looking Assessment

The ORSA is discussed in Section 3.9. One of the objectives of the ORSA is to understand how risk and capital metrics are expected to develop in future, linked to an organization's business planning process, and is seen as an important tool in the development of risk and capital management strategies.

3.5.4.1 Forward-looking assessments in context

In order for the projection process to be most useful to an organization, and increasingly required in international ORSA principles, the forward assessment of risk and capital information could be an integrated part of the business planning process. Projection of risk and capital information within the business plan helps to ensure that strategic decisions made by senior management have regard to the implications on risk and capital on a forward-looking basis.

Without such information, the organization may pursue a strategy which unwittingly results in the accumulation of excessive levels of specific risks. For example, a property insurer may target growth in British Columbia without measuring its increased earthquake risk. A pension plan may decide to reduce its exposure to equity risk without considering the consequent additional exposure to interest rate risk.

Risk measures projected would include those that are used within the organization to determine risk exposure against agreed risk appetite limits, internal capital measures such as economic capital, as well as regulatory and rating agency capital measures. The time horizon used for the forward-looking assessment would normally be consistent with the projection of other business plan metrics, usually a 3 to 5-year projection. The projection is also likely to take the form of a base case projection, potentially together with additional scenarios to test a range of different business and/or external market scenarios.

Instead of being a once-off exercise as part of the business plan, the forward assessment of risk and capital is typically iterative as part of the risk appetite and limit setting process. Initial forward-looking assessments, perhaps performed using approximate methods, are used to assist management in determining risk appetite, translated into limits on key risk measures that strategic business planning can adhere to. In addition, an initial assessment will help inform the organization's risk strategy, or decisions on which risks are to be avoided, reduced, maintained or increased as part of the risk strategy to ensure that risk and capital metrics are optimized in the strategic planning process.

3.5.4.2 Consistency with other forward-looking projections

It is important to consider whether the risk measurement projections produced are consistent with the other business planning metrics produced.

In addition, risk metrics by their nature describe the effect of changes in markets or other risk variables on specific business outcomes. The maintenance of consistency between risk measurement outcomes and business plan projection outcomes where both describe similar changes in the business or external market environment is a factor to consider.

For example, a risk measure describing the impact of a fall in equity markets on capital resources could be compared to the direct projection of a downside equity scenario as part of the business planning process to consider whether both movements in capital resources are consistent.

The level of sophistication used for the risk measurement projection process could recognize the importance of the projection for strategic decision-making purposes, i.e., whether the specific risk measure in question is a peripheral consideration or part of a key risk/capital constraint in the given projection. The modelling approach chosen could also consider the accuracy and sophistication of projection models used for other projected metrics that act as inputs to the projection of risk measures, such as earnings and new business value. A complex modelling approach that uses simplified projection inputs as a calculation basis will risk producing results that are spuriously accurate.

Whatever modelling approach is chosen and level of sophistication employed, the understanding and communication of the limitations of the method chosen is something to consider.

3.5.5 Stress and scenario testing (SST)

Models assume that the external economic and internal business environment is stationary on a forward-looking basis, and in most cases that it can be predicted using average historic

experience and/or relationships between risk variables. From a theoretical perspective, SST is used to understand what happens if the environment is non-stationary. SST is a complementary process to risk measurement that assists in the understanding of key business outcomes.

- *Scenario* – A scenario is a possible future environment, either at a point in time or over a period of time. The effect of these events or changes in circumstances in a scenario can be generated from a shock to the system resulting from a sudden change in a single variable or risk factor. Scenarios can also be complex, involving changes to and interactions among many factors over time, perhaps generated by a set of cascading events.
- *Stress test* – A stress test is a projection of the financial condition of a firm or economy under a specific set of severely adverse conditions that may be the result of several risk factors over several time periods with severe consequences that can extend over months or years. Alternatively, the severe conditions might be just one risk factor, acting over a short duration. The likelihood of the scenario underlying a stress test is referred to as extreme but plausible.

A robust SST framework will aim to test:

- the adequacy of resources held within a business;
- the validity of current strategic business plans and risk appetite; and
- the appropriateness of some aspects of resolution and recovery plans.

It will also aim to assist in the process of identifying new risks that might have been overlooked via the usual base case business plan projections.

As such, SST is both a management tool and a supervisory tool, with regulators increasingly using this approach to test both robustness of individual organization resources and plans, and the vulnerability and systemic risks associated with the entire national insurance industries.

Sources which provide further detailed insight into this topic include the:

- July 2013 IAA paper on stress testing and scenario analysis;
- April 2020 CIA educational note on financial condition testing;
- December 2009 OSFI guideline E-18 on stress testing;
- June 2012 L'Autorité des marchés financiers (AMF) guidelines on stress testing; and
- April 2020 CIA educational note, financial condition testing, Committee on Risk Management and Capital Requirements

3.5.5.1 Stress and scenario testing as part of the ERM process

Key aspects of the ERM process that involve SST include:

Assist in determining risk appetite

SST could help management understand the reasonability of risk appetite limits through understanding what conditions would result in risk exposure measures exceeding risk appetite

limits. Alternatively, if a risk appetite of an organization is defined in terms of a specific adverse business outcome, such as a ratings downgrade, SST can help management understand the factors that contribute to that outcome and risk tolerances, or risk appetite limits, that might be defined as a result.

For example, a firm might identify that a loss of $200M will lead to a reduction in resources and capital cover that would lead rating agencies to consider reducing an organization's credit rating. Senior management could then use $200M as a risk appetite limit related to an earnings risk measure.

Strategic decision making

Analogous to the usefulness of senior management being involved in the forward-looking assessment of risk and capital metrics, it is also useful to involve senior management through the entire SST process. The SST process is a useful risk communication tool and can help senior management to understand the implications of strategic decisions, together with the trade-offs of taking different courses of action.

Model validation

SST, or more specifically reverse stress testing, is a key aspect to model validation because it can focus on the tail events which are rarely observed. For example, if a small change in the severity of such an event materially impacts the organization's financial strength, model users would likely view this as a weakness.

Compliance with accounting requirements

Some accounting bases, e.g., IFRS 17, require that risk margins be calibrated in a consistent manner. They may also require that the level of that calibration be disclosed using metrics such as those described in Appendix A. SST facilitates the consistency necessary to comply with such requirements.

Interactions with regulators

Regulators also find SST analysis useful, including the wider application to potential systemic risks, where a regulator may ask a number of firms to test the impact of the same scenario. Reverse stress testing is a useful way for regulators to assess the robustness of the firm's financial position and/or business model.

3.5.5.2 Types of stress and scenario tests used in practice

SST can be prescribed by regulation or as part of a risk management framework in order to populate a risk dashboard. SST can also be used as a communication tool as part of risk workshops for senior management or as part of the risk measurement process. The following types of scenarios are often used in practice:

- Reverse scenarios (or reverse stress testing), with the purpose of back-solving a specific financial outcome.
- Historical scenarios, where one typically has a lot of detail of the sequence of events and risk factor outcomes over multiple time periods.

- Synthetic scenarios derived as what-if prospective scenarios by extrapolating an extreme version of a recent trend or movement in risk factors.
- Organization-specific scenarios that test specific outcomes unique to given organization, or industry wide scenarios.
- Single and multi-event scenarios, where either single or multiple events contribute to a specific future scenario outcome.
- Global scenarios that test the impact of an event that happens on a global scale (e.g., climate change).

3.5.5.3 Reverse stress testing

As described above, reverse stress testing is the process used to back-solve the required stress and/or scenario events that will give rise to a specific adverse business outcome. This is an iterative process that may involve an initial assessment of a plausible stress test based on estimates and desktop analyses, followed by a more rigorous bottom-up process once the appropriate stress test has been identified and chosen.

The adverse business outcome could be the point at which the organization becomes insolvent under local regulatory guidelines or could be a less adverse scenario that is defined according to "business model failure", e.g., a scenario that would cause a credit ratings downgrade.

As there are many different possible combinations of risk factor outcomes that could give rise to a targeted adverse business outcome, it is important to derive the stress test in a way that gives rise to the most likely combination of risk factor events.

Reverse stress testing in this manner allows organizations the opportunity to learn from consideration of the stress test and to modify their business strategies to reduce the likelihood or consequence of failure.

Reverse stress testing is also a particularly useful way of describing the result of a risk measure calculation in a simplified way, for example describing a capital requirement result as the outcome of a few key risk factors instead of reproducing the mathematics behind the risk factor and aggregation calculations. In addition to testing the likelihood of a chosen scenario, derived reverse stress test scenarios can also be tested for stability over time, which will greatly assist in communicating modelled results. The analogous use for SST is for model validation purposes to consider whether the outcome of a risk measurement model makes intuitive sense. A change in reverse stress test scenarios over time could be checked for consistency against changes in business conditions or modelled approach adopted.

Global systemically important insurers (G-SIIs) are required to complete recovery plans addressing such failure scenarios, which focus on the options available to support the business in recovering and the prioritization of those actions to form the plan.

3.5.5.4 Constructing scenarios for stress testing

A comprehensive understanding of a scenario begins with a narrative and a trigger event. It is important to understand the purpose of the scenario to consider whether it is applicable to the business outcome that management wants to explore. To be most useful, scenarios could be

constructed with input from the management committee or Board that is responsible for approving the business strategy and can sign-off actions to mitigate risk. It is often worthwhile to get a wide range of opinions on plausible scenarios from external industry experts or economists as well as internal experts from business subject matter experts. Scenarios might also need regular updating over time to maintain relevance when internal or external market conditions change.

A scenario chosen by senior management will often be a combination of quantitative outcomes for specific risk factors and a qualitative assessment of other variables or business impacts. It is important that the scenario definition is translated into a comprehensive and consistent set of risk variables that can be used to model specific business outcomes. This may involve either considering the impact on a fuller suite of risk variables where models are more complex or the impact on fewer variables if the modelling is more simplistic.

For example, a chosen scenario might describe a stagflation scenario where interest rates are low, equity markets are flat, and inflation is high. Risk variables used in chosen models might need more defined information on the evolution of the entire term structure of interest rates and different types of inflation that might affect general economic forecasts vs. policy-holders.

A key dimension to describing a given scenario is whether the entire industry is affected in a similar way or whether a scenario is isolated to impacts on a given organization in isolation. If scenarios are isolated, there are likely to be substantial effects on the organization from stakeholder reaction, including customers and debt-holders, where stakeholders are likely to select against the organization, reducing ability to attract business, retain clients and maintain a given credit rating.

For example, potential new policy-holders might avoid an organization or existing policy-holders might surrender policies if they are made aware of a substantial drop in an organization's credit rating. This will differ from the situation where all insurance companies are affected similarly and policy-holders don't have the ability to move to an alternative provider for the same insurance product. Similarly, a scenario in which one insurer's real estate investments decline materially in value would have significantly different ripple effects than a scenario in which all real estate values decline.

Scenarios can consider inter-dependencies between risk variables to consider whether a coherent set of impacts are explored. Two variables may have an immediate dependency (direct immediate causal linkage), time-lagged dependency, feedback dependency (where risk variables interact with each other over time) or phase-shift dependency (where a variable affects another only after a change has reached a certain threshold).

It is important to consider whether the chosen scenario would have a knock-on effect on underlying risk distributions being modelled. The decision of whether or not to rebase underlying distributions would depend on the risk factor calibration process itself and whether rebasing forms an automatic part of the approach chosen.

For example, if equity risk calibration within a capital model incorporates some form of mean reversion and would be rebased after a sudden change in market levels, this change could be incorporated into the scenario modelling.

3.5.5.5 Practical considerations in producing stress and scenario test results

Knock-on business effects

It is important to outline the scenario narrative clearly to consider whether risk variables can be appropriately modelled to describe the scenario. One could also consider whether any knock-on effects on business operations are carefully understood and modelled.

For example, if derivative transactions require the posting of additional collateral where credit ratings fall, this could be incorporated into the modelling results.

As another example, if an epidemic is being modelled that affects the insured population and hence claims pay-outs; one could also consider the impact of the scenario on illness rates among staff and costs to find temporary replacements.

Management actions

Allowance for the impact of management actions taken could be based on approved and plausible actions that will be taken in the given scenario. Interpretations of 'plausible' actions could differ widely among key stakeholders in the modelling process and it is therefore important to specifically agree on actions that are being modelled. For example, some stakeholders may believe that exercising rights to increase pension plan contribution rates or insurance premium rates may have unacceptable ripple effects. It is also useful to produce information before and after the impacts of management actions to assist in the understanding and disclosure of the impact.

Qualitative assessments

Results of detailed scenario calculations might be supplemented with qualitative assessments of specific scenario outcomes by subject matter experts that may have an intuitive sense of scenario impacts from experience in a particular field. Qualitative assessments are particularly useful as they are likely to highlight potential limitations of the chosen modelling approach.

3.5.6 Risk measurement documentation and reporting

This section describes best practice principles for documenting risk measurement models and results. Documentation is a key way of reducing model risk by ensuring that key stakeholders understand the modelled results and key judgment areas, and also helps to ensure continuity in the modelling process where there is staff turnover.

3.5.6.1 General best practice principles

Reports would typically conform to internal corporate guidelines, applicable local actuarial guidelines and external regulatory guidelines if required. Information contained within reports would ideally be sufficiently accurate, with the level of independent verification and checking appropriate for the intended purpose of the report.

The information included within reports would ideally be unbiased and complete to minimize the risk of document users interpreting information incorrectly or making incorrect decisions as a result of information contained within the report. The sources of data and other information contained within reports would normally be clearly stated. Information contained within

reports might also be reconciled to information quoted previously, with restatements of prior information clearly noted with impacts of restatements provided.

Actuaries would typically consider writing reports in such a way that they can be understood by the intended audience, with access to further detailed technical/risk practitioner information available on request.

3.5.6.2 Business requirements

In order to provide context to reported information, and to ensure that the model is developed in line with its intended use, the business rationale and objectives for the risk measurement calculation would normally be clearly specified in the documentation, including the role of the documentation in the overall ERM and/or governance framework. This is likely to include some form of cost benefit analysis covering the research undertaken to develop the model and the costs of producing calculated information on a regular basis.

In addition, reports might specify upfront the level of robustness employed in the modelling of risk measures and the implications of any practical compromises have been made given scarce time and resources.

3.5.6.3 Modelling technical specification and governance

The technical specification could include the theoretical justification for the chosen approach with information on alternative approaches and the justification for the chosen approach. The consideration of alternatives could be set out in an unbiased way instead of being focused on the ultimate method chosen.

Documentation on model procedures can help to minimize key-person risk by accurately specifying each step in the modelling process. The documentation might also include specified governance procedures, including requirements for evidencing model reviews and sign-off and any independent verification procedures required for each step in the modelling process.

Documentation might extend to the steps in the model development lifecycle, including research and development, implementation of model changes, and post-implementation modelling. Model weaknesses and limitations could be clearly addressed in documentation, including the specific model risk that the weakness gives rise to and ways of mitigating this risk.

Guidance on modelling technical specification and governance can be found in the CIA's educational note entitled *Use of Models*[4].

3.5.6.4 Communicating modelled results

Communication of results could include information on the external business environment and internal business context to ensure that the reader is informed of key issues that have either affected results for the current reporting period, or which may affect results in future reporting periods. All material considerations could be provided in the report to help in ensuring that the report users are fully informed and can make appropriate decisions as a result of the information presented.

[4] CIA educational note, *Use of Models*, Modelling Task Force, January 2017.

The granularity of the presentation of results per risk factor, or broader risk category, is something to consider so that information is presented in enough detail to explain the impact of key risk drivers, but not so much detail that key messages can be lost when trying to interpret the results. Features of the aggregation process, such as the impact of the chosen dependency structure and allowance for fungibility and transferability and non-separability can be separately disclosed to ensure that these impacts are clearly understood. Other result features that can be separately disclosed are the effects of changes in assumed tax assets and liabilities, as well as any out-of-model add-ons/estimations that have not gone through the usual defined bottom-up model process.

Noting material judgments made in preparing the results is something to consider, with the rationale for using the chosen approach and commentary on the impact of different possible judgements that could have been made. This disclosure might extend to a discussion of any material estimates or use of approximate methods to derive results.

Information included in reports could be validated (or reconciled) against previous reported results, preferably using an 'analysis of movement' type of approach, with the restatement of prior period results clearly noted. It is also useful to reconcile information at a high level with other related information that may have been produced for the current period in order to prove the consistency of different measures.

Any material events that have occurred after the date of the risk measure calculations could be noted and discussed. Although quantitative impacts might not be available, a qualitative discussion on the impact of such events will help ensure that the user of the results report is fully informed.

As may be required in ERM frameworks in some organizations, documentation could include detail of the independent review and challenge process that was conducted, with examples given of investigations into components of modelled results and any changes made as a result of the challenge process. Potential reviewers may include external parties, internal oversight functions, or simply staff who were not involved in performing the underlying work.

3.6 Risk response

Once risk has been identified, analyzed, and measured the Board and management are faced with responding to the risks. This section outlines some of the potential responses to risks.

3.6.1 Potential risk responses

Responses are often characterized into the following four categories (or a combination of the four):

- avoid
- accept
- mitigate
- share

The Board's response to risks can be reflected in its risk appetite, risk tolerances, and risk limits. One factor to consider is that the options to mitigate or share risk often create new forms of risk that might in turn require monitoring.

When making the decision regarding whether to accept/avoid/mitigate/share a risk the organization might consider the risk-return profile of that risk and its impact on the organization's overall risk-return profile. The impact of the risk on the organization's capital position is an important consideration and the methodologies previously discussed in respect of aggregation in Section 3.5.3 are relevant.

From the perspective of customer fairness principles, the decision tree to take or accept a risk could start with the question of whether a customer need is served by accepting this risk. In many cases, customers are served by offering products that transfer risk from them to an insurance company e.g., mortality risk, longevity risk, and equity risk through minimum return guarantees. Customer needs can also be served by taking on a risk so that customers have access to attractive returns that can be used in the design of savings products e.g., credit or equity risk through the offering of savings products that invest in investment funds.

Pricing in respect of new business and reserving for the specific risks in question are other aspects of risk response. If the organization decides that it wants to avoid the risk in question, then pricing for new business would normally be consistent with that decision. The analysis of the risk might provide information that would be useful when reserving for the specific risk.

Once it is decided to mitigate or share a risk, then the organization can proceed to:

- identify the options to mitigate or share the risks;
- assess the options through cost-benefit analyses; and
- prepare a plan to implement the response.

3.6.1.1 Avoid

The Board can decide that it wants to avoid the risk. Therefore, actions are taken to reduce the organization's exposure to the risk or not to enter a new development or area, noting that it is often difficult to totally avoid risks. Actuaries might be careful of statements regarding zero appetite for risks as often the actions necessary to totally eliminate the risk don't follow that statement.

3.6.1.2 Accept

The Board can decide that it is willing to accept the risk in its current form. Therefore, no additional action is taken to change the nature of the risk other than to monitor the risk and ensure that the appropriate technical provisions and capital are held in respect of it.

3.6.1.3 Mitigate

The Board can decide that it wants to mitigate the risk in some way. It can be useful to consider mitigating either or both of the likelihood of the risk occurring and the impact of the risk.

The actions that are taken to mitigate the risk will depend upon the type of risk in consideration. For example, certain operational risks might be mitigated by:

- installing new control processes;
- training and supervision;
- specific audit, compliance, and quality assurance programs; and
- contract and policy conditions.

Actions that can be taken to reduce the impact of certain risks might include:

- contingency planning;
- emergency procedures; and
- disaster recovery and business continuity plans.

Other risks might require:

- diversification of the risk (geographically or across other risks) which can be achieved by changing business mix, distribution, or products;
- hedging can be used for certain financial risks and in relation to credit risk through the use of credit default swaps;
- additional financing might be necessary to mitigate liquidity risk; and
- collateral can be used to mitigate certain credit risks.

It is important to be aware of risk transformation in that some of the actions taken to mitigate risks could result in the creation of risk of a different nature, so that risk has been transformed rather than eliminated. For example, using collateral might reduce credit risk but could result in additional operational risk.

3.6.1.4 Share

The Board can decide to share the risk with a third party, through insurance or reinsurance for certain demographic risks. Reinsurance can be used to mitigate the frequency and/or the severity of certain risks.

Capital markets and alternative risk transfer (ART) can also be used to share certain risks. Sometimes risks can be shared with policy-holders through features such as policy excesses and profit sharing, where permitted under product rules and policy-holder fairness principles.

Outsourcing of activities or functions can be used to share certain operational and financial risks, although residual risks and risks created through the outsourcing processes need to be carefully considered.

Joint ventures or partnerships can be used to share risks associated with new developments where the organization might lack expertise or simply where the organization wants to reduce the financial risk associated with an exposure.

Sharing a risk often results in some reliance upon a third party, such as a reinsurer. Therefore, it often results in credit risk and the organization might need to consider whether this new risk is taken into consideration when deciding whether or not to proceed.

3.7 Risk monitoring

This section outlines some of the considerations in relation to the monitoring of risks and monitoring of the risk management system more generally.

3.7.1 Risk monitoring activities

Monitoring is linked to risk measurement and reporting in that the quality of measurement and reporting often determines the extent of monitoring possible at various levels. Therefore, risk monitoring will include monitoring of all the various risk measures used by the organization.

Monitoring would normally be done with a frequency that is appropriate to the risk in question. For some risks it might be sufficient to monitor on a monthly basis whereas other risks might be monitored as close to real-time as possible. Monitoring should be sufficiently frequent to allow decisions to be made and for action to be taken on an informed basis.

Organizations might need to monitor a range of risk related items. These might include:

- output of risk evaluations;
- risk control self-assessments;
- observation of defined risk limits, tolerances, and appetite;
- external environment;
- key risk indicators; and
- risk management action plans.

These items are discussed in greater detail below.

3.7.1.1 Output of risk evaluations

Risks might be monitored on an ongoing basis using the output from the risk evaluation. The organization should monitor the extent of individual risks as well as the relationships between risks in order to monitor the total exposure of the organization. It is useful to monitor total risk positions as well as effectiveness of internal controls and residual risk positions.

3.7.1.2 Risk Control Self-Assessments

Self-assessment reporting from various internal units can be very useful to provide insight from the operational units regarding risk positions and effectiveness of internal controls. Trends in these self-assessments are often indicative of some change which might impact upon the organization’s risk position.

3.7.1.3 Observation of defined risk limits, tolerances, and appetite

The organization also might monitor the observation of its defined risk limits, tolerances, and overall risk appetite. The actions taken in respect of any breaches would normally be assessed relative to the defined escalation plan.

3.7.1.4 External environment

It is also necessary to monitor the external environment in order to contribute to risk evaluation. This includes monitoring of tax and regulatory developments in order to understand their impact on risk positions as well as the regulations themselves.

3.7.1.5 Key risk indicators

Many companies use key risk indicators to provide insight into risk positions, as part of their risk appetite framework for setting risk tolerances and risk limits or as additional information as they often provide insight into changes in risk exposures, likelihood and the external environment. They can serve to complement the core risk evaluations and to evaluate certain risks which are hard to measure precisely.

For example, operational risk is difficult to quantify. However, risk indicators can provide useful insight into changes that might increase operational risk (e.g., staff turnover could act as an indicator for operational risk). Therefore, the indicators can indicate when a risk exposure is increasing or when the likelihood of a risk occurring is increasing. The organization might decide to use this information in different ways depending upon the circumstances and the reliability and importance of the indicator. It could:

- use the information to gain insight into the applicable risk;
- set risk tolerances and limits based on this information; and
- incorporate the information into the organization's economic capital model.

3.7.1.6 Risk management action plans

Many organizations also monitor the progress of any risk management action plans that have been agreed and are in the process of being implemented.

3.8 Risk reporting

This section outlines some of the considerations in relation to reporting of risks and outlines some common methods for communicating risk.

Section 3.5.6 outlined considerations in relation to risk measurement reporting and documentation. Many of those considerations are also relevant to more general risk reporting, in particular Section 3.5.6.1 which outlined general best practice principles.

3.8.1 Risk management information

Effective ERM requires quality risk management information that contains certain attributes. Those attributes include the following:

- *Timely* – Information on risks would ideally be provided with sufficient speed to allow companies to make decisions to manage those risks appropriately while also meeting the other data requirements outlined. The frequency of reporting might vary depending upon the risks, the organization's situation and the external environment.
- *Comprehensive* – The information provided would ideally be comprehensive, covering all risks in an appropriate level of detail. It is important to note that too much

information can be as inappropriate as too little information depending upon the circumstances. Reporting can be tailored to the audience with recognition of the different needs of the Board, senior management, and other levels and would ideally be clear and concise.

- *Consistent* – The information provided would ideally be consistent, in terms of both production and reporting to allow consistent evaluation.
- *Accurate* – All risk information would ideally be accurate and reflect the underlying risks appropriately. Risk data could be reconciled and validated.
- *Auditable* – All risk information would ideally be auditable, and the entire process could be transparent and adequately documented.
- *Forward-looking* – Risk management information provided could incorporate a forward-looking element rather than rely solely on current and past data.

There are different ways of achieving these objectives and risk management information might vary so that it is appropriate to the specific organization and situation.

3.8.2 Assurance regarding information

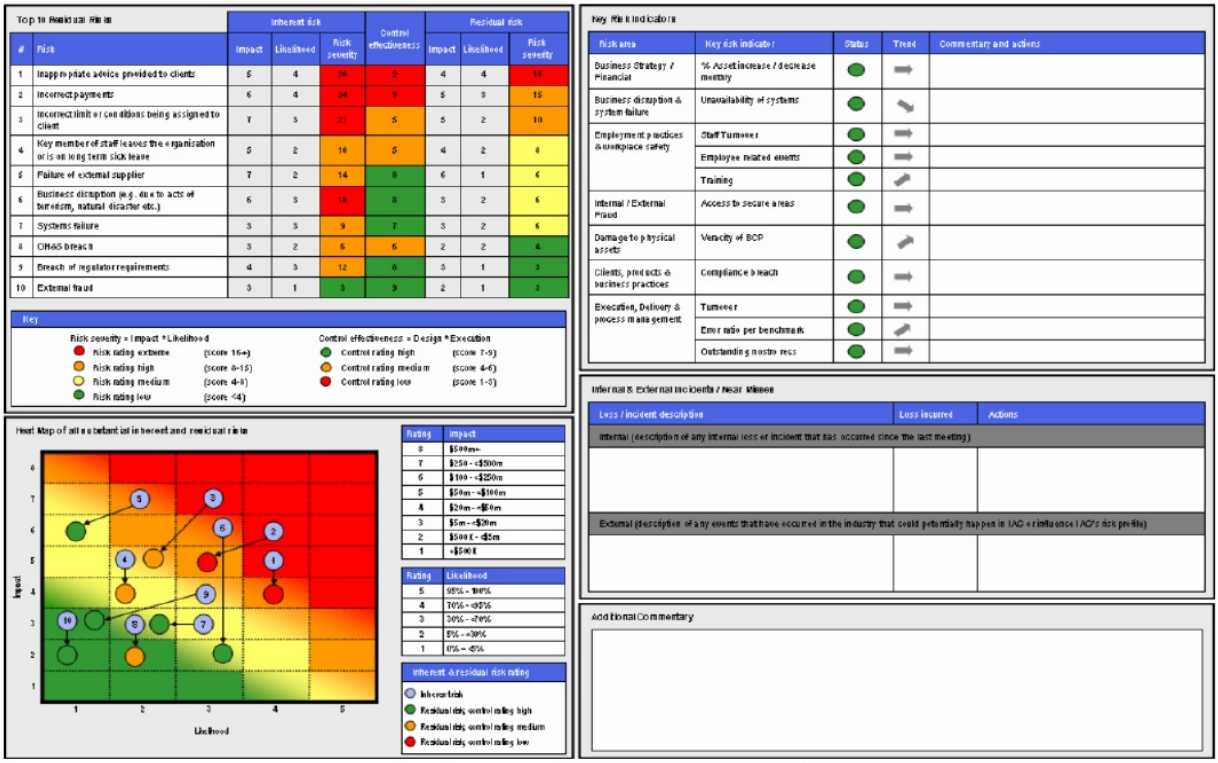
There are a number of considerations that could help to provide assurance regarding risk management information and which might be appropriate, depending upon the circumstances:

- Independent verification in relation to certain processes/information.
- Reconciliation of information between previous and current reports.
- Appropriate documentation of all processes and procedures.

3.8.3 Reporting methodologies

There are a number of methodologies commonly used in industry to communicate risk management information including:

- top 10 residual risks
- heat maps
- key risk indicators
- event logs



3.8.3.1 Top 10 residual risks

Many companies use an assessment of likelihood and impact to assess risks. This can be assessed both gross and net of controls, or alternatively gross risk and control effectiveness can be assessed with residual risk emerging from those assessments. It is important to define the scale that is used to categorize risks and this scale could include a number of measures such as solvency loss, regulatory fine, reputational impact.

3.8.3.2 Heat maps

Heat maps are an effective method of communicating risk in a simple, straightforward manner. Movements in assessments can also be incorporated as illustrated above.

3.8.3.3 Key risk indicators

Key risk indicators are a useful means of incorporating factors that might indicate increased risk, but which might not be apparent otherwise. For example, staff turnover might indicate increased risk of operational losses but would not be apparent unless specifically reported.

3.8.3.4 Event logs

Event logs are important in monitoring actual events that either led to losses or were “near misses”. Reporting of event logs is important to allow insight into the events that are creating risk and losses for the organization, recognizing that low probability events might not feature in event logs for long periods.

3.8.4 Internal and external reporting

The type and depth of information provided will vary depending upon whether it is to be provided internally or externally. Nevertheless, similar considerations apply to both.

Different information is required for different levels within the organization and the organization might consider separately the needs of the Board, of business units, and of individuals. Relevant reports could be distributed to all relevant parties and contain information appropriately tailored to the audience.

The organization might consider how to achieve consistent usage of risk management terminology by defining exactly what is meant by certain terms and ensuring that these are understood internally. The organization might also consider the establishment of reporting standards and risk management information systems to assist in the production of consistent, coherent risk reporting.

3.8.5 Disclosures

Appropriate disclosures are something to consider in relation to any actuarial report on ERM. The following are areas that might be appropriate for disclosure:

- *Purpose* – The purpose of the report and scope would normally be disclosed.
- *Data* – Any limitations of risk management information could be disclosed, including an assessment of the potential impact of those limitations.
- *Assumptions* – Key judgments, assumptions, and reliance upon expert opinion. It might also be appropriate to discuss sensitivities and uncertainties.
- *Methodologies* – Appropriateness of methodologies chosen, any shortcomings and reasons for using them.
- *Changes* – Any material changes to systems or processes, and the impact of those changes, could be disclosed.
- *Validation* – Any validation of results or models could be disclosed.

3.9 ORSA and financial condition testing

The Own Risk and Solvency Assessment (ORSA) is becoming an increasingly international requirement, with regulators in many countries incorporating the requirement into supervisory plans The International Association of Insurance Supervisors adopted Insurance Core Principle 16 (ICP16) in October 2010 and the requirement for an ORSA was one of the key elements of ICP16. In Canada, insurers must also submit annually a financial condition testing (FCT) report prepared by their Appointed Actuary.

3.9.1 Key requirements of an ORSA

ORSA is a wide-ranging topic but the following are among the key requirements outlined in ICP16:

- Regular assessment of the adequacy of risk management.

- Regular assessment of the adequacy of current, and likely future, solvency position.
- Board and senior management to be responsible for the ORSA.
- All material risks to be encompassed, including underwriting, credit, market, operational, liquidity and group membership.
- Determination of the financial resources needed to manage its business.
- Risk management actions to be based on consideration of capital and financial resources.
- Assessment of the quality of capital resources.
- Analysis of the ability to continue in business including projections of future financial position and ability to meet capital requirements.

Section 3.5.4 of this document addressed some of the issues related to the forward-looking perspective of the ORSA.

3.9.2 Key elements of an FCT (Section 2500 of the standards)

FCT is one of a number of stress-testing processes that would fit within the insurer's overall risk management process. Stress testing includes scenario testing and sensitivity testing.

FCT has the following key elements:

- development of a base scenario;
- analysis of the impact of plausible adverse scenarios;
- identification and analysis of the effectiveness of various corrective management actions to mitigate risks;
- a report on the results of the analysis and recommendations to the insurer's management and the Board; and
- an opinion signed by the Appointed Actuary and included in the report of the financial condition of the insurer.

3.10 Evaluation of an ERM system

In some situations, actuaries may be called upon to give an opinion regarding the quality of an ERM system. The following discussion provides an example of a process for forming such an opinion.

The actuary might first come to agreement with their audience on the elements of the ERM system that are to be included in the review. The topics in this report could be used to help define such a list of elements.

Subsequently, the actuary could receive or propose a scale which defines the possible opinions both in range of detail and levels of classification required. The following is an example of a possible scale. Practices would be reviewed to determine whether they are any of the following:

- *Ad Hoc* – Incomplete and undeveloped. No ERM goals underlying or considered in developing current oversight.
- *Basic* – Minimal tools and systems. Low sophistication. Objective of ERM is to meet external minimal expectations.
- *Standard* – Complete framework with adequate tools. Average sophistication in all areas. Competent execution in all risk areas.
- *Advanced* – Proprietary value-added components to ERM tools and systems. Leading edge sophistication in some major risk areas.

An even number of categories is suggested above to encourage differentiation of the scores. Scoring systems with an odd number of categories might attract a disproportionate number of results in the middle category.

For each area of practice that is evaluated, a separate score would be determined. Appendix B provides an example of scoring for one risk management practice area: risk identification. The examples of practice are provided to help guide the reviewer rather than to restrict the reviewer to those particular practices. ERM practices are continuously evolving and including a static set of practices into an evaluation process could result in the process becoming outdated because it would not include new practices that emerge after the development of the document.

Bibliography

Actuarial Standards Board (2004), Actuarial Standard of Practice No. 23 Data Quality

Actuarial Standards Board (2012), Actuarial Standard of Practice No. 46 Risk Evaluation in Enterprise Risk Management

American Academy of Actuaries (2013), Insurance Enterprise Risk Management Practices

Bank for International Settlements, Developments in Modelling Risk Aggregation, October 2010.

Bank for International Settlements (2013), Principles for effective risk data aggregation and risk reporting

C.C. Heyde, S. K. (2007). What Is a Good External Risk Measure: Bridging the Gaps between Robustness, Subadditivity, and Insurance Risk Measures. Columbia University.

Dowd, K. (2005). Measuring Market Risk. West Sussex, England: John Wiley & Sons, Ltd.

Financial Services Authority (2008), Stress and Scenario Testing CP08/24

Hardy, M. (2006). An Introduction to Risk Measures for Actuarial Applications. Society of Actuaries.

Institute of International Finance. (2009). Reform in the Financial Services Industry: Strengthening Practices for a More Stable System.

International Actuarial Association (2009), Practice Note on Enterprise Risk Management for Capital and Solvency Purposes in the Insurance Industry

International Actuarial Association (2010), Comprehensive Actuarial Risk Evaluation

International Actuarial Association (2010), Note on the use of Internal Models for Risk and Capital Management Purposes by Insurers

International Actuarial Association (2013), Stress Testing and Scenario Analysis International Actuarial Association (2015), Deriving value from ORSA – Board Perspective

Kaye, P. (2005). Risk measurement in Insurance: A Guide to Risk Measurement, Capital Allocation And Related Decision Support Issues. Casualty Actuarial Society Discussion Paper Program, 1–34.

Milliman (2013), ORSA – An international requirement

P. Artzner, F. D.-M. (1999). Coherent measures of risk. Mathematical Finance, 9, 203–208.

PwC (2013), A Closer Look at Financial Services Regulation – Model risk mitigation and cost reduction through effective documentation.

S.S. Wang, V. R. (1997). Axiomatic characterisation of insurance prices. Insurance: Mathematics and Economics, 173–183

Appendix A – Common risk measures

This appendix outlines three common risk measures in terms of their definition, advantages, and limitations.

Standard deviation

- *Definition* – Standard deviation is the square root of the variance of a distribution and measures the dispersion around the mean of a distribution. The variance is known as the second central moment of a distribution.
- *Advantages* – Standard deviation is easy to calculate and is commonly understood by most informed audiences. This decreases the amount of time needed to educate and describe the risk measure itself.
- *Limitations* – Standard deviation is not a coherent risk measure as it fails the monotonicity criteria and variance fails the sub-additivity criteria. Another drawback is that it does not explain the entire distribution of a given modelled risk factor. Distributions chosen to model risk factors can have the same standard deviation and dramatic differences in other aspects of the distribution, which could lead to a significantly different view of the risk profile. Information on the skewness or kurtosis (the third and fourth central moments) might be needed to understand the shape of the "tails" of the distribution. When measuring risk, this is often the area actuaries are most concerned with.

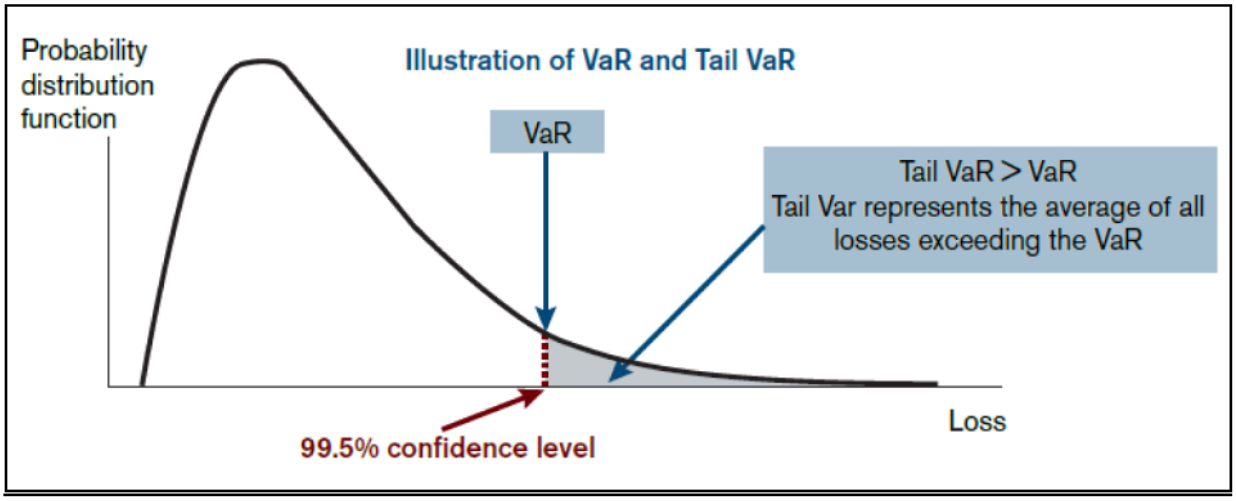
Value at risk

- *Definition* – Value at risk or VaR measure is often defined as the smallest loss that is greater than a predetermined percentile of the loss distribution or in other words, the quantile at a pre-defined probability level. The predetermined percentile used in calculating VaR is often expressed as a confidence level, α, commonly 95% or 99% for risk analysis and a time interval over which the loss is expected to occur.
- *Advantages* – VaR is a well-known risk measure and is commonly used in the financial sector leading to greater comprehension from stakeholders. It is intuitive and can be explained in layman's terms as "with a probability of α, we will suffer a loss no greater than $Y over a n-week period." There are also various options to calculate VaR including both parametric, non-parametric methods, Monte Carlo simulation, and approximations such as the delta-normal method, which uses first order sensitivities to approximate simulation results.
- *Limitations* – VaR is not a coherent risk measure because it fails the sub-additivity coherence axiom. Additionally, it provides information at one point of the distribution and does not provide information in the area of the distribution above the specified confidence level. This area or "tail" is commonly of most interest when performing risk analysis. Lastly, while VaR is a popular measure that is in use today, it is often misinterpreted by users.

Conditional tail expectation (or tail value at risk)

- *Definition* – Conditional tail expectation or CTE or tail value at risk (TVaR) is the mean of the distribution above a certain percentile or confidence level (α) or in other words, the expected value of a loss given that the loss is above a specified threshold, which is defined according to a specified percentile value α. This risk measure has many other names including tail value at risk, tail conditional expectation, and expected shortfall.
- *Advantages* – The CTE is a coherent risk measure as it satisfies all of the coherence requirements. The risk measure does not focus only a single point of the distribution and provides information about the values above the threshold or in the tail. Additionally, CTE is used across the financial services industry and by regulators for determining reserve and capital requirements.
- *Limitations* – The CTE is more difficult to calculate compared to the standard deviation and the VaR measures as information related to the entire tail of the distribution is needed as opposed to a point measure. CTE is more complex than VaR and backtesting CTE can be significantly more challenging than backtesting VaR.

The graphic below displays the difference between the VaR and Tail VaR risk measures for a 99.5% confidence interval:



Source: CEA working paper on the risk measures VaR and Tail VaR, November 2006.

The risk measures described above are also commonly used within regulatory frameworks in addition to being employed within insurance companies for management purposes.

The following table summarizes the measures and their advantages and disadvantages:

Table: High-level summary of risk measures and their limitations

Risk Measure	Description	Advantages	Disadvantages
Standard Deviation	• Measures dispersion around the mean	• Easy to calculate • Commonly understood	• Not a coherent risk measure • Doesn't explain the entire distribution with limited focus on the tail distribution
Value at Risk	• The quantile at a pre-defined probability level	• Well known and commonly used • Allows different calculation methodologies	• Not a coherent risk measure • Only provides information about one point in the distribution • Sometimes misinterpreted
Conditional Tail Expectation (Tail Value at Risk)	• The mean of the distribution above a certain percentile	• Coherent risk measure • Doesn't only focus on one point in the distribution	• Somewhat more difficult to calculate • Somewhat more complex

Appendix B – Example evaluation of a practice area

This appendix deals with risk identification from the senior management perspective, whether the risk identification process started or ended at that level. The following table outlines some potential examples of practices that might be used when categorizing the risk identification process. It should be noted that the examples are subjective and intended to illustrate possibilities rather than representing a definitive categorization.

Ad Hoc	Basic	Standard	Advanced
1. Management will assert that "everyone knows" the top risks of the firm. But if polled, each member of management will list different risks. 2. No risk identification process. 3. Management risk focus is primarily on the most recent problem topic.	1. Management has a list of identified risks. 2. List is taken from an outside source and does not use terminology that matches with company language. 3. List of risks does not match up with senior management responsibilities. Several risks fall under multiple senior management areas or none. 4. List of risks that is used in reports to senior management and the board contains more than 20 top risks. 5. Most of senior management cannot recall the risks on the list. 6. List of risks is missing one or several of the top insurance related risks that generally impact insurance companies but there are many operational risks on the list.	1. Management has a list of top risks that they have reviewed carefully and/or that they have created. 2. Most of senior management can recall the entire list. 3. The list of risks is less than 20 elements. 4. Management has identified a short list that they discuss with the board. 5. List of risks will include all of the major categories that are found in many sources that affect insurance companies and often the very largest risks for the company are sub divided into parts that are managed separately.	1. All of the Standard elements. 2. Management has processes for regularly reassessing and renewing the identified risks. 3. Management is open to ad hoc changes to the risk list as situations change in between scheduled updates. 4. Companies that have used bottom up process are able to incorporate top down modifications without disrupting that process. 5. Companies that have used top down processes also have a process to allow input from around the organisation.