Actuaries Institute Australia

LIFE INSURANCE AND RETIREMENT VALUATION

MODULE 13: RISK MANAGEMENT FRAMEWORKS

Education Program
ACTUARIES INSTITUTE

Education that Counts

Fellowship Program

Module 13

RISK MANAGEMENT FRAMEWORKS

Education that Counts

Table of contents

13.1. Introduction **5**

13.2. Enterprise Risk Management (ERM) **6**

13.2.1. Background to ERM 6

13.2.2. Definition of ERM and reasons for its evolution 9

13.2.3. Defining risk 12

13.2.4. Risk classification 15

13.2.5. Interconnectedness of risks 19

13.3. Risk Management Frameworks **19**

13.3.1. Strategic plan 21

13.3.2. Risk appetite 22

13.3.3. Risk management policy 24

13.3.4. Governance 24

13.4. Risk Management Process **30**

13.4.1. Risk assessment 32

13.4.2. Risk treatment 36

13.4.3. Risk reporting 37

13.4.4. Risk culture 39

13.4.5. Role of other stakeholders 40

13.5. Key learning points **42**

13.6. Answers to exercises **44**

13. Risk Management Frameworks

This module addresses the following learning objectives:

Item	Unit/Key Performance Objective/Learning Objective
6.	**Analyse the components of risk management frameworks applicable to life insurers and retirement funds, covering risk assessment, risk management, risk reporting, governance and culture.**
6.1.	**Consider the relationship between objectives, risks and capital**
6.2.	**Identify, and assess, the different types of risks and their potential impact**
6.3.	**Design a new, or critique an existing, risk management framework**
6.4.	**Examine the impact of the internal and external environment on risk management, including the role of regulators**
6.5.	**Plan the implementation of risk management processes within a business function**

13.1. Introduction

Students will be familiar with many of the concepts in this module from their studies of the Control Cycle subject (Core Actuarial Management from 2020), particularly Chapters 2 and 6 of the textbook *Understanding Actuarial Management*.

This module builds upon the concept of enterprise risk management (ERM) and some of the tools associated with it. The content of the module is focused on a top-down view of implementing a risk management framework. Nowadays, there is a strong link between managing capital and risks. Risk-based capital is discussed in Module 14 (Capital).

This module begins by reviewing the relationship between objectives, risks and capital and discusses the evolution of holistic approaches to managing risk across a company or fund. It looks at the definition of risk and some of the consequences of that definition, as well as the need to place risk management in the centre of a company or fund's governance framework. A definition of ERM follows, with a discussion on the importance of leadership, entity culture and risk management processes to the overall success of ERM. The more quantitative aspects of ERM are also covered.

Next, the various categories of risk are discussed. Some of these are financial in nature and therefore familiar to actuaries. Other risks are not financial and perhaps less familiar to actuaries. The key outcome is a broad awareness of the various risks entities may face, together with an awareness that the ultimate objective of ERM is to assist the integrated management of all the material (identified) risks that may impact an entity's value and long-term success.

The important risk management techniques of underwriting, claims management, asset-liability matching and reinsurance are discussed in depth in the LI&R Product Development subject.

13.2. Enterprise Risk Management (ERM)

13.2.1. Background to ERM

For any objective that an organisation may seek to achieve, there is:

- uncertainty about the likelihood of achieving the objective; and
- capital which may be required to support the achievement of the objective.

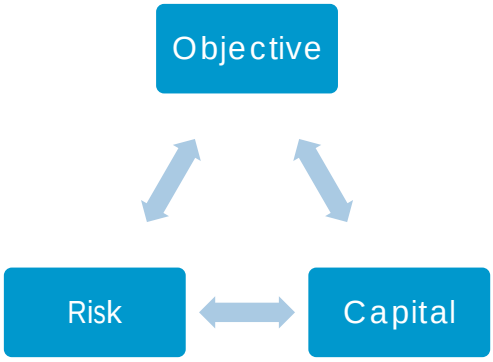
For example, suppose a life insurance company planned to receive $100m of single premium endowment assurance participating business within one year. Six months into the year, sales have exceeded expectations and the business has received $500m in premiums. This might appear to be a very good outcome, but the objective was not met which will likely have capital implications for the company. The additional sales will lead to more capital being allocated to this one line of business and that may impede business development in other, potentially more profitable, areas. There could be solvency issues or potentially a negative effect on policyholders if the unexpected increase in business forces the company to adopt a less risky investment strategy that leads to potentially lower future policy owner returns.

Exercise 13.1

Consider how news of the sales volumes in the scenario outlined above would be received within various departments within a mutual life insurance organisation. How would the news be reported to the board?

The term "uncertainty about the likelihood of achieving the objective" can be replaced with the word "risk". There is a formal relationship, albeit one which is difficult to quantify, between an objective, risk and capital.

Figure 13.1: Relationship between objective, risk and capital



When an objective is set, a company or fund needs to consider the risks and capital requirements relating to the objective. An extreme approach would be for each department in an organisation to list the risks it faces in achieving its objectives and somehow decide a suitable amount of capital required to cover those risks.

Exercise 13.2

Explain why asking each department to calculate its required amount of capital is not adopted in practice.

The definition of *insurance* involves a transfer of risk between members and the insurance company. Consequently, the management of that risk is required by the insurer.

Many students believe that actuaries are the natural risk managers in insurance companies and retirement funds. Actuaries have certainly been heavily involved in the quantification and management of significant risks in these organisations. There are many specific areas where actuaries advise on the management of risk, particularly financial risks. We discussed earlier, in Modules 4 to 10, how actuaries advise companies and funds in the management of their liabilities. The quantification of capital is an area where actuaries utilise their skills in assisting companies understand their regulatory and economic capital requirements. We discuss the general process of risk-based capital in Module 14 (Capital). The LI&R Product Development subject describes how actuaries advise on profit and risk management during the product development cycle.

However, the risks faced by an insurer or retirement fund are wider than the traditional financial risks actuaries are most familiar with. Two common non-financial risks are *operational risk* (i.e. the possibility that processes are not operating as expected) and *strategic risk* (i.e. the risks surrounding a potential, or actual, strategy). There are always emerging risks and much effort is now being expended on, for example, *cyber risk* (financial loss, disruption or reputational issues arising from a failure in I.T. systems). A topical issue in Australia is *conduct risk*, with the Haynes Royal Commission (2018-19) examining misconduct in the banking, superannuation and financial services industries. Module 2 (Cash flows) discussed social risk and its implications on the reputation of financial firms.

A common theme across these non-financial risks is the difficulty in quantifying statistical distributions that capture the potential financial consequences of the risks eventuating.

A board of directors or trustees of a retirement fund need to be satisfied that the risks they face are understood and well managed. Historically, risks were managed through functional lines, such as:

- compliance: checking the company or fund is meeting the specified regulations;
- marketing: ensuring products align with customer expectations;
- actuarial: ensuring the solvency of the entity, the equitable distribution of participating business bonuses, and advising marketing on published material;
- customer service: making sure complaints are dealt with promptly and resolved.

Within the last twenty years, there has been a move to manage risks in a more coherent, holistic framework. This framework is known as enterprise risk management (ERM).

13.2.2. Definition of ERM and reasons for its evolution

There are various definitions for ERM, but they all share the common themes of having a holistic approach to risk across the entity and a focus on value optimisation rather than risk avoidance.

This definition from the Casualty Actuarial Society (CAS) is a good example:

> *"ERM is the process by which organizations in all industries assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organization's short and long term value to its stakeholders."*

ERM is a process which:

- flows through an entity at every level and unit, on an ongoing basis, encouraging systematic organisation of and coordination between risk functions, so as to avoid "silos" (i.e. individual areas of a company operating in isolation of other areas);
- identifies potential events which, if they occur, will affect the entity and its ability to manage risk within its risk appetite;
- holistically considers quantifiable and non-quantifiable risks, taking into consideration past events or losses, current performance and potential future outcomes;
- manages both the downside and upside of risk;
- is effected by people at every level of an organisation so it becomes part of the culture (i.e. "how we do things around here");
- employs a common risk management language across the organisation; and
- is applied in strategy setting and integrated into business decision making, so is key to how the business grows and generates value.

The concept of ERM has become well-established around the world, in both financial services and the broader business community. However, the idea of appropriately managing a portfolio of disparate risks is relatively new and still developing. Not only are there new risks to assess but an understanding of the interactions between different risks is needed in the context of the entity being managed. Additionally, given that many (but not all) retirement funds and other financial institutions have survived, with some thriving, over relatively long periods, there can be some resistance to the need to manage disparate risks on a portfolio basis.

The fundamental idea of ERM is that any entity, including life insurers and retirement funds, faces a wide (and potentially evolving) variety of risks in meeting its objectives. Consequently, these risks need to be managed in a way that reflects not only the individual risks but also their cumulative impact. This implies the need to understand specific risks in isolation as well as their interaction with, and relative importance in relation to, other risks and events so the overall behaviour of the entity can be properly managed in accordance with its strategy, objectives and risk tolerances. The risks faced must be managed at all levels of the company or fund and this may require a culture shift.

Management of financial risks lies at the core of actuarial work. However, there are non-financial risks that also impact on a company or fund's success or demise. Extending the range of issues included under the ERM banner means that actuaries, while strong in the areas of financial risk management, need to acquire a well-developed understanding of the broader and more qualitative aspects of modern risk management methodologies, techniques and thinking.

The International Actuarial Association (IAA) recommends that:

> *"An insurer should establish, and operate within, a sound ERM framework which is appropriate to the nature, scale and complexity of its business and risks. The ERM framework should be integrated with the insurer's business operations, reflecting desired business culture and behavioural expectations and addressing all reasonably foreseeable and relevant material risks faced by the insurer in accordance with a properly constructed risk management policy."*

Exercise 13.3

Think about how you would adapt the IAA recommendation for the following organisation types:

a) A medium-sized manufacturing company that offered a defined benefit fund for employees until closing to new entrants three years ago.
b) A captive insurer for a worldwide oil and gas company.
c) A new life insurer set up to sell post-retirement annuities to retirees. The minimum purchase price per policy is $1m.

The evolution of ERM has been driven by a number of (often interrelated) internal and external forces, including:

- sharper focus on risk by ratings agencies, especially in the United States;
- regulatory changes from a variety of sources, such as the new professional standards adopted by the Australia Prudential Regulation Authority (APRA) and new international standards such as Basel II and SolvencyII;
- legislative changes, for example, Sarbanes Oxley legislation in the US;
- listing requirements of stock exchanges, for example, the Australian Stock Exchange (ASX) or the New York Stock Exchange (NYSE);
- growing industry appreciation of the value that can arise through controlled risk-taking;
- increasing recognition of the complexity and interdependency of markets and risks, accentuated by increasing globalisation and the pervasive impact of technology;
- increasing recognition and evaluation of the financial impact of social risks (trust, license to operate, environmental impact, sustainability, governance);
- rapid development of financial products, including the use of derivatives in the development of retail products as well as in financial risk management;
- improved understanding of risk-based capital and its use by regulators;
- understanding and use of risk-adjusted returns; and
- increasing sophistication of risk-management techniques.

The principles of ERM are now well-established in both financial services and the broader business community. Consequently, the number of actuaries involved in providing specialist ERM advice to organisations is growing.

13.2.3. Defining risk

We defined *risk* as the uncertainty related to achieving objectives. Risk is often characterised by reference to potential events and consequences, or a combination of these.

While this may initially seem to be a straightforward statement, it is not. Consider the observations in Table 13.1:

Table 13.1: Definitions

Need for objectives	If an entity or person has not explicitly defined objectives, then the issue of risk, in the sense of not meeting objectives, disappears. Without objectives, there is no benchmark against which to assess the possibility or consequences of not meeting them. Objectives cover both the core purposes of an entity (e.g. Google's core objective is "to organize the world's information and make it universally accessible and useful") as well as an entity's strategic objectives (i.e. how it intends to grow or otherwise change).
Risk management	Risk management is the process of identifying, assessing, mitigating and reporting the risks faced by an entity. That is, understanding the inherent risks faced, implementing appropriate risk controls, and monitoring, managing and reporting the resultant residual risks. Depending on the type of risks faced and the level of control an entity has over them, management approaches may vary. For example, consider the difference between accepting the residual risk of adverse mortality experience (and holding capital against it) compared with the processes involved with establishing a business continuity plan.

Risk measurement	To assess the consequences of a risk implicitly presumes some ability to measure the risk, typically in terms of likelihood and consequences (or frequency and severity). However, the assumption that the consequences of risk can be measured may not always be valid. The question then becomes how to address risks that cannot be measured. An example is the "measurement" of reputational consequences from a risk event or managing the outcome of a natural catastrophe. If a particular risk cannot be usefully measured, then it does not follow that it can be ignored, as it needs to be managed.
Risk and the rear-view mirror	There is a natural tendency to seek to manage what is known or what has happened. However, there are past risk events that are poorly understood, at least from the perspective of their quantification, and new risks that emerge through changes in the environment, as well as changes in the consequences of already identified risks. To presume that all relevant risks can be identified (leaving aside being measured and, if necessary, mitigated) is to presume no new risks will emerge. This is a dangerous perspective to take, particularly when the timeframes we are concerned with are long. For example, in a life insurance context, consider the changes in asset risks due to new investment vehicles being developed, the impact of medical advances on underwriting and the applicability of policy definitions, the impact of technology on all aspects of business processes including policy acquisition, administration and performance measurement, and the worldwide rise of cybercrime.
Risk is two sided	There is the possibility of either not meeting or exceeding objectives. While one may be a positive outcome against expectations and the other a negative outcome, both are possible depending on how the objectives are phrased. In some discussions of risk there is an undue emphasis on not meeting expectations, which entirely misses the point that some outcomes may exceed objectives. On the other side, fortunate success is sometimes celebrated and rewarded even though unfortunate failure was just as likely.

	In some of the literature, the positive side of risk is classified as "opportunity". The use of different terms for positive or negative outcomes relative to expectations is generally not helpful, albeit that some stakeholders, e.g. prudential regulators, will only be interested in the management and mitigation of downside risk. The view that risk management is merely about avoiding adverse outcomes is narrow and potentially dangerous, as it precludes the significant value-adding aspect that good risk management should lead to, even in difficult circumstances.
Risk is inherently statistical/random in nature	We do not know what will happen in the future. Every financial services business is built around its ability to manage future uncertainty, not around its ability to remove future uncertainty. This means that there remains a possibility, however small (but certainly not zero!), that an adverse outcome may emerge. If such an outcome does eventuate, it doesn't automatically mean the risk management process failed or the risk was not, in a statistical sense, adequately managed. It may simply mean that an "outlier" result occurred. After all, if we knew what the future held, then both the entities actuaries work for and the actuarial profession would be out of work! Equally, but more substantially, if there is an expectation from management that adverse results will not occur, then it indicates the risks have not been properly communicated or analysed prior to taking them on, or management has zero tolerance for that risk. The key issue is how risks are communicated and managed and, where an adverse event occurs, what is learned from the experience.
Risk is best managed in aggregate	The inherently statistical nature of risk and, hence, risk management, was noted above. A direct consequence is that there are aggregation benefits to be gained when managing a portfolio of risks to the extent that risks can be diversified. A simple example of aggregation is the pooling of term assurance risks for similar lives. If you have a large group of people to manage then one can use the law of large numbers to apply a probability of death to the group to estimate the number of future deaths. If you are the only member in the group, then you are either dead or alive. More complicated examples on risk aggregation are considered in Module 14 (Capital).

Risk and capital	From a capital adequacy perspective (which is the perspective of the prudential regulator), holding capital to provide security against adverse outcomes is appropriate. However, the key to management of downside risks is not curative action (i.e. holding capital for risks) but prevention (i.e. managing risks to reduce their likelihood of occurring). This is particularly the case as it is inefficient and not always possible to hold extra capital. This implies the need for an open and pro-active risk management approach.

13.2.4. Risk classification

Taking the broad perspective of ERM, there are a range of quantitative and qualitative risks to consider. Entities have varying degrees of influence or control over risks, ranging from strong internal control through to minimal internal control and the consequent need for the capacity to react under externally imposed stress. Taking a narrower quantitative perspective, the focus tends to be on those risks that can be assessed financially and, to a point, controlled more internally. Within this context, the actuarial perspective of risk has broadened well beyond its traditional liability focus.

While groupings of risks may be useful to aid discussion, there are not yet any universally accepted classifications of risks. Care therefore needs to be taken in interpreting any terminology used in reference materials. In any case, the more important outcome for students is a broad awareness of the various risks entities may face and an awareness that the ultimate objective of ERM is to assist the integrated management of all the material (identified) risks that may impact on the entity's value, both in the short and long terms. As actuarial practice moves from one area to another, the relative importance of some of the risks listed below may change. Having an awareness of the various risks that may arise, even if different terminology is used in different areas, provides an actuary with a strong framework to apply.

Financial risks include:

- **Insurance Risk**: Risks taken on through contracts or obligations to provide future benefits to policy owners, retirement fund members and other beneficiaries. Measurement of these risks was discussed in Modules 4–10 and extreme events will be discussed in Module 14 (Capital). The LI&R Product Development subject discusses why consumers buy these products and describes the pricing process and management of their associated risks.
- **Credit Risk**: The risk of default or change in credit quality of issuers of securities, counter parties and intermediaries. This risk is discussed in Module 14 (Capital).
- **Market Risk**: The exposure to movement in the level of financial variables, including effects of asset liability mismatching. This risk is discussed in Module 14 (Capital).
- **Liquidity Risk**: There are a variety of different risks that fall under this category, and the two main types discussed briefly in Module 14 (Capital) are:
  - Funding risk: Insufficient liquid assets to meet obligations as they fall due; and
  - Trading risk: Inability to raise sufficient cash to roll over debt or meet cash, margin or collateral requirements.

Non-financial risks include:

- **Operational Risk:** The risk of loss resulting from inadequate or failed internal processes, people, systems or external events. Operational risk typically includes legal risk but excludes strategic, reputational or systemic risks. It can impact the value of assets and liabilities through errors made in processes (e.g. poor product development) and systems (e.g. modelling errors). The actuary's role as an advisor in operational issues will be discussed in depth in the LI&R Product Development subject. This risk is discussed further in Module 14 (Capital).
- **Strategic Risk:** The risk that a particular strategy will not work effectively or will fail;
- **Application/Execution Risk:** The risk that, while the intended result was acceptable, the actual result was not. In other words, while the theory or intent behind a decision or action may be appropriate in the context of an entity's governance, strategy and/or risk management objectives, there is still a risk that the implementation of the decision fails.

As a result of past risk management failures and the move toward enterprise-wide risk management, the past decade has seen an increasing focus on operational risk. Committees and regulators have implemented standards and guidelines to ensure all financial institutions have robust operational risk management frameworks in place.

It is important to note that operational risk (and other non-financial risks) can lead to financial risks, including traditional insurance, market and credit risks.

For example, imagine an insurer launches a new innovative life insurance product to the market. A few months after the launch, the company is forced to pay a significant number of ex-gratia claim payments due to ambiguous policy wording. An internal audit reveals that the due diligence process for sign-off of the product disclosure statement was not adhered to correctly. The failed internal process has resulted in significant financial loss to the company.

Companies commonly outsource roles and functions to other organisations, particularly IT-based functions. Where companies use an external provider, there is a risk that the supplier is unable to provide the goods or service (either temporarily or on a permanent basis). Typical risks under an outsourcing arrangement include the inability of a supplier to offer adequate or competent resources, adequate service levels or flexibility to accommodate business changes. Business continuity planning is critical to ensure a company can continue to operate in the event of outsourcing issues.

There are many other possible sub-divisions of risks, particularly of operational risk. Some examples, not necessarily mutually exclusive, are risks relating to:

- entity culture and empowerment;
- contagion and related parties;
- competition;
- reputation;
- legislation and the judicial process;
- regulation and/or politics;
- technological change;
- systemic impacts;
- extreme events;
- changing social attitudes; and
- environment change.

Exercise 13.4

Can you think of other risks facing a life insurer or retirement fund that are not covered in the above lists? Which of the above risks do you think are hardest to quantify or measure? Why is this the case?

Exercise 13.5

Review and discuss recent commercial and financial services history and find examples of significant impacts, such as entities failing, for each of the types of operational risk specified.

Significant events leading to shareholder loss of value are strategic and operational risks (i.e. risks associated with poor business decisions, failure to respond appropriately to the environment or failure to execute decisions or strategies). This emphasises the importance of taking a holistic view through ERM and not focusing only on financial risks.

An interesting question for risk managers is how to identify emerging risks in a timely way (i.e. how to detect new or changing risks early, while risk management is still a possibility, rather than after the risk has impacted an organisation). A risk manager's answer to this question may give a useful insight into their attitude to risk management (i.e. whether they take a proactive or reactive approach).

It is a business reality that, ultimately, judgements are made on results and not on intentions, so the issues raised though the ERM process can be significant. This is an area where experienced and pragmatic actuaries can add great value to an entity by assisting them with successful implementation of plans. One only has to reflect on projects that run over time and over budget and then do not meet (perhaps evolving) business needs to begin to appreciate the potential enormity of application risk. Application risk applies from an entity's highest level to its lowest. Poor implementation of board obligations, such as lack of adequate monitoring of business progress and risk management, can be fatal to an entity when it comes under stress.

13.2.5. Interconnectedness of risks

In practice, risks do not operate in isolation. Where risks are interrelated, the occurrence of one event can trigger another. For example, if a company's reputation is severely damaged through some poor claims decisions, this may lead to lower volumes of new business, higher lapse rates for in-force policies and loss of key members of staff which, in turn, could have further operational consequences.

In its simplest form, a correlation matrix can be used in modelling to allow for dependency between risks. This approach is described in Module 14 (Capital). More complex methods are sometimes employed. It is important that students are able to step aside from technical risk modelling and be able to understand and explain the principles and drivers of these interrelationships. This will be considered further in the LI&R Product Development subject.

Exercise 13.6

What other risks from the lists provided in the previous section might be interrelated? Explain how they are interrelated.

13.3. Risk Management Frameworks

To manage risk across a company or fund in accordance with ERM, there needs to be a clear and consistent risk management framework applied to all identified risks, which incorporates the totality of systems, structures, policies, processes and people.

An effective framework will consider a company or fund's strategic plan and risk appetite and will include the following elements:

- a risk appetite statement;
- a risk management policy;
- a designated risk management function;
- defined roles, responsibilities and formal reporting structures for the management of material risks throughout the entity (with risks being reported to and managed at appropriate levels within the organisation, depending on the nature of the risk);

- policies and procedures supporting the management of all material risks;
- a risk management process that informs decision makers of the entity's risks, how the entity intends to mitigate those risks, and how much current and future capital is necessary;
- a management information system (MIS) that is adequate, both under normal circumstances and in periods of stress, for measuring, assessing and reporting on all material risks across the entity; and
- a review process to ensure that the risk management framework is effective in identifying, measuring, evaluating, monitoring, reporting and controlling or mitigating material risks.

In best practice implementations, the risk management framework operates in a dynamic fashion. New risks are identified and assessed, new controls are devised, and the performance of these controls and related residual risks are included in reporting through to senior management and boards or trustees, as shown in Figure 13.2.

Figure 13.2: Risk management process

In other cases, the risk management framework is reassessed on an annual or other regular cycle and is a key component of an entity's annual business plan.

Each of the key components of the risk management framework are discussed below. The risk management process steps shown in the diagram above are discussed in Section 13.4.

13.3.1. Strategic plan

A key objective of ERM is to integrate risk management into business processes so that it influences strategic decision making.

Change usually follows a strategic planning exercise. The company or fund may choose to develop new products, expand into other markets, change the operational model of its business or launch something completely new.

Any change to a business brings risks with it. Equally, deciding to operate an existing business model without change can increase risk if changing market conditions render a once-effective business model obsolete. Whenever business objectives are set as part of a strategic planning exercise, whether or not this results in a change to the existing objectives, it is prudent to conduct a risk assessment of the objectives and the effect of the associated risks upon the business.

While it could be said that, for example, starting up a new and different operation would not affect the existing business, this is not the case if one looks at this from an operational risk management point of view. Taking this example, the questions that immediately spring to mind are:

- Which employees will be deployed from the existing business to make the new venture operational?
- How will these employees be replaced?
- How will this change the risk profile of the existing business?
- What capital is required to back the new venture?
- What are the debt repayment requirements resulting from this?
- If the new venture consumes capital, will profits from the existing business be required to support the new venture?

There are many other questions that will arise in a more detailed analysis, covering issues such as position in the market, conflict with competitors, distribution channels, regulators, and the reputational consequences of a risk event.

Thus, it can be seen that ERM is an important part of any strategic planning exercise.

13.3.2. Risk appetite

Risk appetite is the amount and type of risk an organisation is willing (and able) to take on in pursuit of its business goals. Clearly defining risk appetite is an essential part of a risk management framework, as it sets the boundaries and expectations for the business.

Risk appetite can be qualitative; for example, "the fund has a low appetite for reputational risk exposure", or quantitative; for example, "available capital will not drop below 120% of the regulatory capital requirements."

The board of an insurer, or trustees of a retirement fund, are responsible for setting the risk appetite. Considerations in setting a risk appetite include:

- the current competitive environment (including regulations, competitors, economy, technology);
- the company or fund's strategy, assessing which risks are needed to help achieve the strategy;
- the company's risk capacity (including capital, liquidity, knowledge/skills, market influence); and
- key stakeholder expectations.

A risk appetite statement summarises the company or fund's risk appetite and should cover:

- the degree of risk that the institution is prepared to accept in pursuit of its strategic objectives and business plan, giving consideration to the interests of policy owners and members;
- for each material risk, the maximum level of risk that the institution is willing to operate within, expressed as a risk limit and based on its risk appetite, risk profile and capital strength. This is known as the *risk tolerance*;

- the process for ensuring that risk tolerances are set at appropriate levels, based on estimates of the impacts of risk tolerance breaches and the likelihood of each material risk being realised;
- the process for monitoring compliance with each risk tolerance and for taking appropriate action in the event that it is breached; and
- the timing and process for review of the risk appetite and risk tolerance.

A risk appetite statement should make clear to stakeholders (e.g. shareholders, regulators, customers and market analysts) the nature and size of the risks which will be managed in order to achieve the business goals. It should also define the entity's culture with respect to risk-taking so employees understand how to behave accordingly.

Once a risk appetite is defined, the next challenge is to ensure that it is embedded into the company's culture and operations on a consistent basis as part of the risk management model. Communication and management of culture are key in embedding the risk appetite. The use of risk tolerance levels, risk targets and risk limits will assist business units in assessing business decisions relative to the risk appetite. Further, the risk management function can provide risk training, supervision and oversight relative to the risk appetite.

Risk appetite, tolerances, targets and limits are not static. They must be reviewed regularly and updated as needed to reflect changes in the environment and changes in the company or fund's strategy. Regular risk monitoring, scenario analysis and stress testing should be performed to test the continued appropriateness of the risk appetite statement, risk tolerances, targets and limits.

Exercise 13.7

Search the internet to find examples of risk appetite statements for several life insurers and retirement funds. How do the examples differ from one another? How might risk appetite statements for life insurers differ from those for retirement funds?

13.3.3. Risk management policy

A risk management policy provides an overview of how risk is managed in an organisation. A risk management policy would normally include:

- background and context, including connections between the business plan (business strategy and objectives) and risk management;
- risk appetite and risk tolerances as set by the company's board or the fund's trustees (the governing body);
- the risk management process to be used;
- how the company or fund assesses its key risks;
- the respective responsibilities of the governing body, senior management, relevant committees and frontline staff;
- how risk management performance is monitored;
- the nature, frequency and timeliness of risk reporting; and
- the process and timing for review of the risk management policy.

13.3.4. Governance

Risk governance is the formal structure used to support risk decision making and oversight. There are various ways in which the risk management function may be structured within an organisation. Four potential models are described below.

'Offence and defence' model

- Day-to-day management takes as much risk as it can get away with. It acts as if risk is solely within the domain of the (separate) risk management function.
- The risk management function is set up as opposition and reduces risk as much as possible to minimise losses.

Under this model, the risk management function stifles risk taking and can limit profitable opportunities. At its worst, individuals anticipate opposition by the risk management function and either do not inform the risk management team of issues or actively evade any oversight.

Policy and policing model

- The risk management function sets policies and monitors compliance with these policies.

Under this model, the risk management function is often too 'hands-off' from the rest of the business to be effective.

Partnership model

- The risk management function sets up close working relationships with key operational areas of the business, possibly by embedding risk professionals into operational teams.

A criticism of this model is that too close an involvement may impair the necessary independence of thought for the risk professional.

Three lines of defence model

This is a model suggested by prudential regulators. Each department is classified into one of three lines of defence:

- First line of defence: Day-to-day management such as product development and valuation. These departments are the risk owners.
- Second line of defence: The risk management function. It should review and challenge the first line functions. The risk management function is independent of the risk owners.
- Third line of defence: Internal and external audits. Their purpose is to provide assurance of the framework.

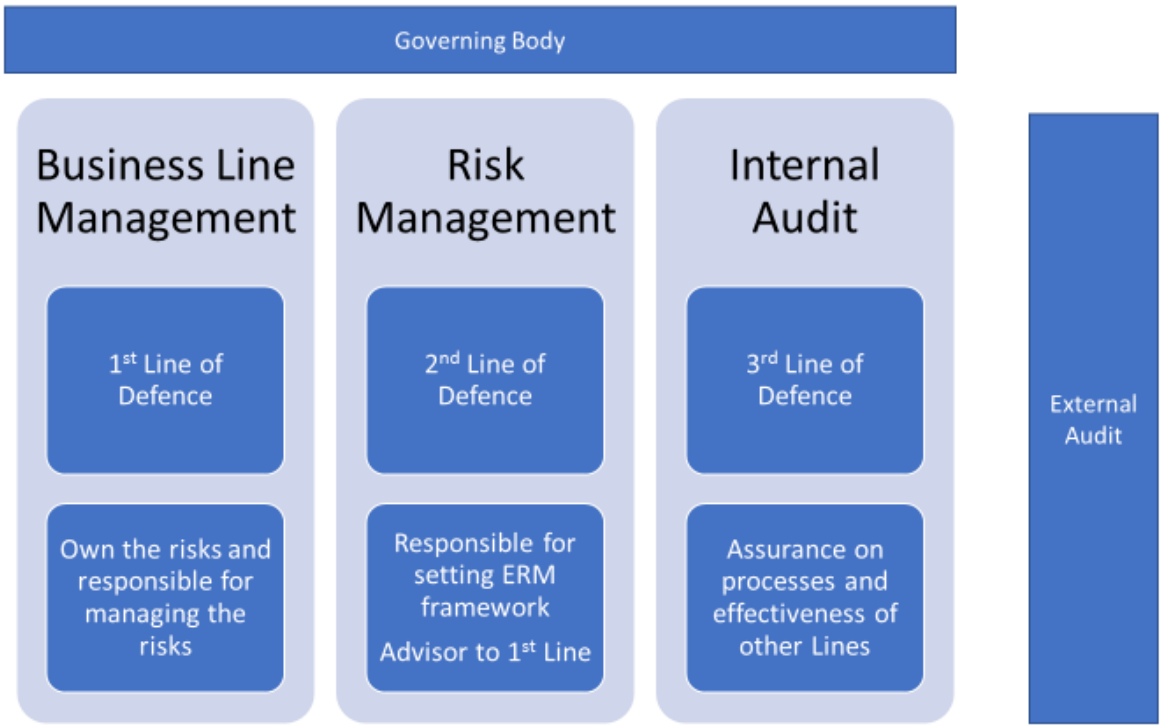
The main issue with this model relates to the level of interaction between the first two lines of defence.

A critical component of the three lines of defence model is the ability to separate duties. In particular, the risk reporting function needs to be independent of any business unit that is the subject of a risk report. Achieving this type of independence in practice can be costly. In the past, some smaller companies and funds have depended to a large extent on self-assessment, with intermittent independent internal or external audits.

It is also important that the leader of each line of defence has direct access to the governing body. It is not effective if the chief risk manager and internal auditor report only to the chief financial officer who has accountability for business line management. as the CFO can selectively report to the governing body. The chief risk manager and internal auditor should be able to report directly to the audit and risk committee or board or the independent directors, as may be appropriate.

The three lines of defence model is shown graphically in Figure 13.3, followed by a description of the various roles and responsibilities under this model.

Figure 13.3: Three lines of defence model



Governing Body

An insurance company's board or a retirement fund's trustees are responsible for "driving from the top" the need for risk management. They hold management accountable for having clear risk management processes and reporting, and for building a risk-aware culture. This is strongly reinforced by regulation, both locally and internationally.

The governing body is ultimately responsible for the risk management framework and for ensuring:

- it defines the institution's risk appetite and establishes a risk management strategy;
- a sound risk management culture is established and maintained throughout the institution;
- senior management take the steps necessary to monitor and manage all material risks consistent with the strategic objectives, risk appetite statement and policies approved by the governing body;
- the operational structure of the institution facilitates effective risk management;
- policies and processes are developed for risk-taking that are consistent with the risk management strategy and the established risk appetite;
- sufficient resources are dedicated to risk management;
- uncertainties attached to risk measurement are recognised and the limitations and assumptions relating to any models used to measure components of risk are well understood; and
- appropriate controls are established that are consistent with the institution's risk appetite, risk profile and capital strength, and are understood by, and regularly communicated to, relevant staff.

In addition, it is usual for local laws to dictate that a life insurance board director's duty is to give priority to the interests of current and prospective policy owners over the interests of shareholders. Any risk that can impact policy owners is therefore of concern to the board.

Similarly, a trustee of a retirement fund is usually required to give priority to the interests of the members of the fund.

Business Line Management

Business line management (business owners) are responsible for day-to-day decision making involving risk identification, assessment, mitigation, monitoring and management. A key responsibility is, therefore, to operationalise the risk management framework into actions, limits and expectations for all employees.

At a cultural level, management needs to ensure that the right messages, with respect to risk tolerance and management, are sent down the organisation. This is an important but difficult area to get right, with a careful balance required between a number of opposing needs. Considerations include:

- business owners need to ensure bad news gets passed up the chain, in a timely fashion, to both senior management and to the risk management function. Where the news is significant, it should be reported to the board or trustees so the problems can be dealt with before they grow in size;
- business growth should not be stifled through excessive risk avoidance;
- frontline staff should be clear about which risks are acceptable and which are not (consistent with the organisation's risk appetite);
- there should be no perception that "risk management is someone else's job";
- remuneration should not provide the wrong incentives and appropriate rewards should exist for "good" risk-taking.

Exercise 13.8

Suppose a life insurance firm operates using a three lines of defence model. Is the Appointed Actuary in the first line of defence, the second line of defence, in both, or something else? Hint: Thinks about the roles undertaken by the AA and consider in which line each role lies.

Risk management

A designated risk management function could be set up that:

- is responsible for assisting the governing body, governing body committees and senior management to develop and maintain the risk management framework;
- is appropriate to the size, business mix and complexity of the institution;
- is operationally independent of business line management;
- has the necessary authority and direct reporting lines to the governing body, committees and senior management to conduct its risk management activities in an effective and independent manner;

- is resourced with staff who have clearly defined roles and responsibilities and who possess appropriate experience and qualifications to exercise those responsibilities;
- has access to all aspects of the institution that have the potential to generate material risk, including information technology systems and systems development resources; and
- is required to notify the governing body of any significant breach of, or material deviation from, the risk management framework.

Further, an institution might appoint a Chief Risk Officer (CRO) who is responsible for the risk management function. The CRO's role is usually quite broad, but a key function is co-ordination of risk management activity within the company. Again, it is critical that there is no perception that "the CRO is managing risk, so I do not need to".

A related point is that the key risk management jobs must be resourced appropriately in terms of both quantity and quality, with sufficient numbers of people who understand the business and are not afraid to speak up where needed.

Internal and external audit

The objective of auditing is to provide independent assurance that the risk management framework is working effectively and is being complied with. Typically, legislation requires annual external audit for listed companies. Prudential regulators may require audits for non-listed entities, including retirement funds.

In addition to regular audits, some prudential regulators also require entities to undertake a comprehensive review every three years. The objective of this review is to provide an assessment and recommendations as to the ongoing appropriateness, effectiveness and adequacy of the risk management framework. The audience for this report is the governing body's risk or compliance committee. Operational independence is critical for completing this review, to ensure it is performed in an objective manner. The report may contain a comparison between current and best practice. External audit firms are often well placed to make this assessment as they are independent and have exposure to a range of different risk management frameworks.

Exercise 13.9

A medium-sized proprietary life insurance company has only sold risk business, namely, yearly renewable term assurance, critical illness and income protection business to domestic customers. The board is considering diversifying into post-retirement products by offering annuities.

The concept of enterprise risk management is currently not practiced in the domestic market.

(i) How would you advise the board on setting up a risk appetite statement?
(ii) Briefly demonstrate how the board may use the statement resulting from question (i) to judge the strategy of introducing post-retirement products.

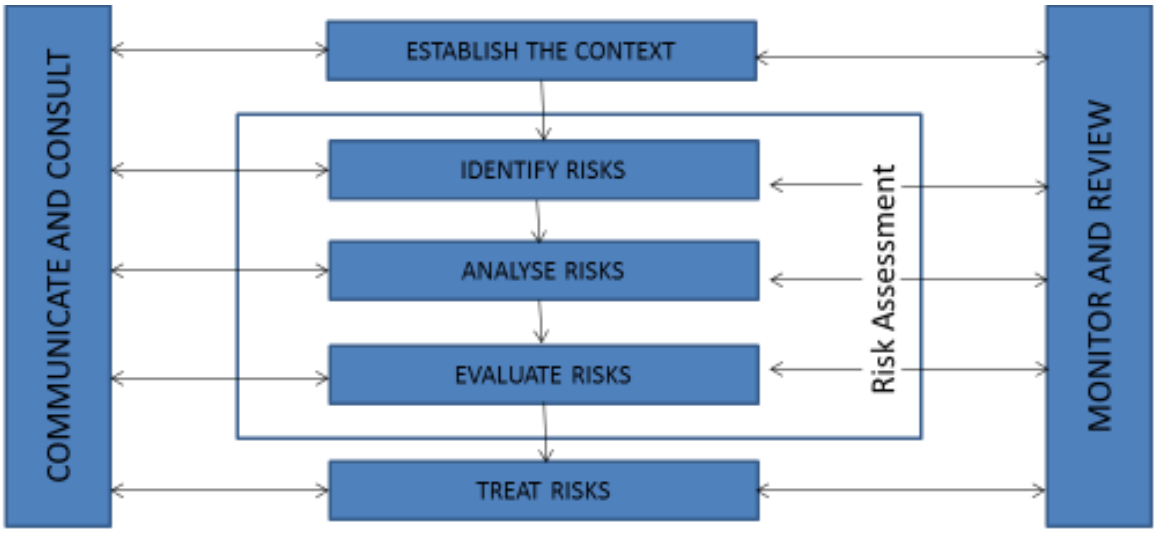
13.4. Risk Management Process

As stated previously, a risk management process informs decision makers of an entity's risks, how the entity intends to mitigate those risks and how much current and future capital is necessary in respect of those risks.

Risk management models, such as the AS/NZS ISO 31000 risk management process, can be used by companies or funds seeking an established process to aid the implementation of a risk management framework.

The AS/NZS process is based on the seven elements shown in Figure 13.4.

Figure 13.4: Seven elements of the risk management process



- **Establish the context** for strategic, organisational and risk management, and the criteria against which business risks will be evaluated.
- **Identify risks** which could prevent, reduce, delay or improve the achievement of an organisation's business and strategic objectives.
- **Analyse risks:** Consider the range of potential consequences and the likelihood of their occurrence.
- **Evaluate risks:** Compare risks against the entity's strategic objectives and risk appetite and consider the balance between potential benefits and adverse outcomes.
- **Treat risks:** Some risks may not need to be "treated". For others, this step includes developing and implementing plans for increasing the potential benefits and reducing the potential costs of those risks. In many ways, this is the key step that considers the risk and reward trade-off in the treatment of each risk. The process so far will identify some risks that deliver commensurate returns and some that do not. Dealing appropriately with risks in order to optimise value is core to the ERM process.
- **Monitor and review** the performance and cost-effectiveness of the entire risk management system and the progress of the risk treatment plans. Focus should be on continuous improvement through learning from performance failures and deficiencies.
- **Communicate and consult** with internal and external stakeholders at each stage of the risk management process.

The risk assessment stage (identify, analyse and evaluate) together with "establishing the context" is discussed briefly in Section 13.4.1. The treatment of risks is summarised in Section 13.4.2. An example of monitoring and reviewing is the focus of Section 13.4.3. Embedding the framework into the culture of an organisation is discussed in Section 13.4.4. The final section, Section 13.4.5, provides an overview of the types of stakeholders and their roles and interests in the governance process.

13.4.1. Risk assessment

Insurers and funds vary in size and complexity and use different risk assessment processes, although their processes have common themes. A typical process may include:

- **understanding the core business objectives** (e.g. meeting member and policy owner obligations, providing a return to shareholders) as well as its strategy for growth (e.g. new distribution channels, new administration systems, new markets). Prudential regulators often require life insurers to have a business plan that describes these objectives;
- **identifying risks in meeting these objectives**: These risks arise from both changes in the external environment as well as internal operations. Often, risk identification can be done in conjunction with a regular strategic review in a process known as *horizon scanning*. Commonly-used tools include PEST analysis (incorporating changes arising from politics, the environment and economy, society and technology) and SWOT analysis (review of an organisation's strengths, weaknesses, opportunities and threats); and
- **assessing the quality of the existing controls environment:** An insurer has controls in place for managing existing risks. The assessment process should determine whether these are operating effectively. If not, the underlying risk controls need to be redesigned. Senior management should be engaged in this process to reach an agreed view of the risks faced by the organisation under the existing control environment as well as any changes to the planned control environment.

Risk assessment may use financial models to quantify the size of the risk. Common tools include Value at Risk (VaR) for investment risks and Tail Value at Risk (TVaR) for extreme-event or catastrophe risks and economic capital measures. For risks that are more difficult to model (e.g. some operational risks), risk assessment may use a simple matrix of likelihood and severity. Figure 13.5 provides an example of such a risk assessment matrix.

Figure 13.5: Risk assessment matrix

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Risks are allocated to a cell in the matrix based on management's view of the likelihood and severity of each risk.

There will generally be an existing register or listing of risks that can be used as a baseline for the assessment. Risk registers include fields such as the risk name, the category of risk, a description of the risk, who owns the risk, a rating of the inherent risk before controls, a listing of key controls and a rating of the residual risk with controls in place.

The output of the risk assessment is the updating of this register.

As risk assessment is inherently uncertain (in fact, the risk of a flawed risk management process is a risk in itself), other tools can be applied to check the risk ratings. These include check lists, data on historic risk events (various agencies compile these databases such as the Australian Bureau of Statistics and the Australian Prudential Regulation Authority) and scenario modelling (see below).

Residual risk is defined as the risk remaining under the existing control environment. In some cases, residual risk allows for control improvements. This is less satisfactory, as such control improvements should be tested before being relied on. The next section discusses the process of reducing residual risk through risk management (sometimes referred to as *risk treatment*).

Inherent risk is harder to define. In principle, it is the risk existing prior to any controls being in place; however, this results in an unrealistic rating (e.g. imagine a life insurer with no underwriting function and no pre-existing condition exclusions). A practical definition is the risk in an environment where some controls are missing or others are only partly effective (e.g. a life insurer with an understaffed and deficient underwriting function that is still effective at identifying lives in very poor health).

When risk analysis is being undertaken, it can be difficult to think through the risks that could occur. It is also sometimes difficult to envisage how the mitigation/management strategies that have been put in place will work in practice. One method used by practitioners to assist with both of these aspects is *scenario modelling*.

Scenario modelling involves identifying a set of possible circumstances that could occur and working through all the aspects of the business, risk management or strategic plan to identify the business impact if the scenario came to pass. An important issue to consider in this context is that of *management action*. For example, consider a scenario which models a drop in asset values. The action taken by management (which could be anything from reducing participating policy surrender values or buying put options against the ASX) and the timing of this action is critical to understanding the likely impact. In the scenario of deteriorating claims experience on a trauma insurance product, the amount by which premium rates will increase, in addition to when this increase will occur, are both important to consider (as is the consequential impact on lapse rates). In addition, scenario modelling will include identifying what capital actions (if any) are relevant in the scenario, taking into account the stressed situation being considered (e.g. a company with poor claims experience may find it difficult to raise capital or find reinsurance at reasonable prices).

A challenge in scenario modelling is to think of plausible future scenarios. An example from recent history is the 2008/09 global financial crisis. When assessing and analysing the organisation's risk profile, if a risk manager had considered the possibility that such a crisis might occur, risk management or mitigation strategies could have been put in place (e.g. reducing exposure to equities or credit) to allow the organisation to cope with as little disruption to business as possible during the global financial crisis.

A variant of scenario modelling known as *reverse stress testing* can also be very useful, where a scenario is selected that causes the entity to fail to meet its objectives. The likelihood of this scenario is then considered.

13.4.2. Risk treatment

At a high level, there are four main responses to risk: reduce, remove, transfer or accept. These are defined in Table 13.2.

Table 13.2 Risk treatment

Reduce	Also known as *risk treatment* or *mitigation*. It can either involve reducing the likelihood of a risk occurring or reducing the impact if it does occur, or both. Reducing such risk can include, for example, changing product design or adding new controls to detect risks early (e.g. up-to-date experience studies).
Remove	This applies to situations where it is possible to get rid of a risk entirely; for example, by not proceeding with a new product during the initial planning phase.
Transfer	This is where the risk is passed to another organisation; for example, as is the case with reinsurance or derivatives. Some commentators refer to this as *risk transformation* as such transfers create other risks. For example, reinsurance can lead to *counterparty risk* (e.g. failure of the reinsurer) as well as *contract risk* (e.g. disagreement over what claims are covered).
Accept	Also known as *absorbing* or *tolerating* the risk. In some circumstances, an insurer may have no cost-effective alternative (e.g. pandemic risk). For any management approach there will be residual risk that will need to be accepted as it is no longer cost-effective to manage. Capital will need to be held for this residual risk.

Practical applications of these risk treatments will be considered in the LI&R Product Development subject.

13.4.3. Risk reporting

Effective risk management requires decision makers to be informed regularly, succinctly and meaningfully about the assessment of actual risks relative to the institution's risk appetite and the operation and effectiveness of risk controls.

At the board or trustee level, the objectives of risk reporting include:

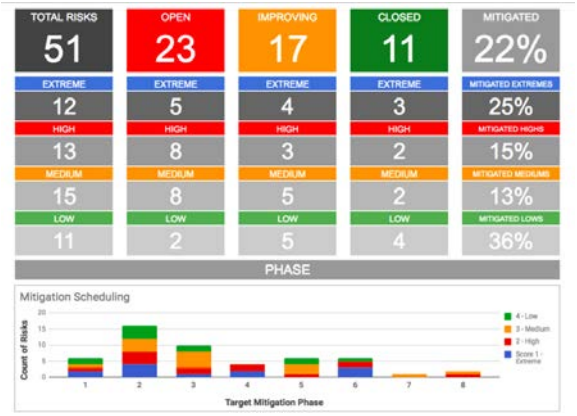
- making the governing body aware of changes to the entity's risk profile that may breach tolerances set out in its risk appetite statement. These significant risks may include significant consequences from recent events, key control failures (even if no significant consequences arose), recent or current events of concern that are worrying and are still playing out, and poor behaviours within the company that are evidence of a poor risk culture; and
- ensuring the governing body is aware of how senior management are managing risk and providing updates to the governing body on risk management progress.

Regular assessment of the effectiveness and adequacy of the reporting process (including breaches and incidents) is critical. Whilst too many breaches and incidents are bad news, too low a reported number may also be bad. In fact, it may be more comforting for a board or trustees to receive regular updates of control failures and troublesome events than to receive a run of "clean" reports, which might suggest ineffective identification of risk events. An important consideration for the board is the speed at which the company acts on breaches and how they are closed-off.

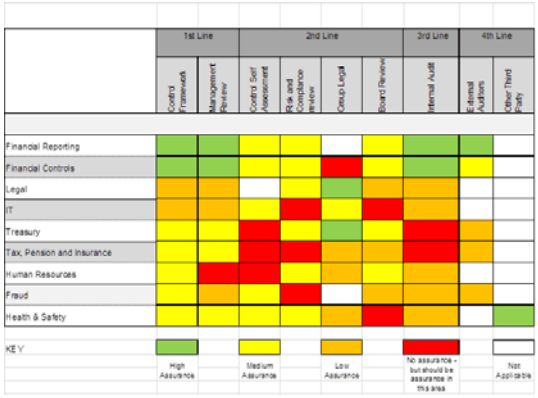
The format of risk reporting will depend on the size and complexity of the retirement fund or life insurer and may include the types of information presented in Figure 13.6.

Figure 13.6: Risk reporting

- Risk dashboards showing key risk indicators



- Risk heat maps showing risk ratings for different areas of the business



- A list of recent risk events or incidents
- Updates on risk management actions and commentary from the Chief Risk Officer (CRO)

In practice, the risk management function of each business unit may produce risk reports based on changes to risk registers, exception reports (in relation to risk appetite, tolerance and limits) and risk heat maps. Key messages from these reports then cascade up to the CRO's report to the board or trustees. Each senior manager is expected to have a risk reporting process that identifies and responds to risks before they become significant.

Management risk reporting may include the short- and long-term impacts of risks (such as on profit or surplus), segmented by product, product features, policy duration and underwriting conditions. The report may include an assessment of the uncertainty of these impact measures and a judgement about the underlying performance of the portfolio. It could also include an assessment of product complexity, product resiliency in the face of changes to market conditions, underwriting and claims management capabilities, data quality and risk culture.

13.4.4. Risk culture

Successful risk management frameworks are embedded into the culture of an organisation. Culture can be described as "the way we do things around here". While culture is the outcome of behaviours of all people in an organisation, its direction can be influenced by considering what behaviours the board/trustees and senior management want people to follow, particularly in managing risk. Importantly, the risk management framework and associated policies and procedures need to be implemented effectively in order to promote the desired risk culture and behaviours.

All organisations have a risk culture. However, the key is whether the risk culture supports and is aligned with the objectives of the risk management framework and the organisation's risk appetite.

The governing body sets the "tone at the top" for "the way we do things around here" through their actions. If the board or trustees show little interest in the risks and the way they are managed, chances are that risks will be managed poorly. Conversely, if there is keen interest in and understanding of risks and their management, supported by tight and clear risk management processes and regular monitoring by a dedicated committee, and senior management rewards are linked to effective risk management, risks are much more likely to be managed well.

To obtain buy-in to a desired culture, demonstration through everyday practices is often more successful than taking a "big launch" approach, which may be perceived as a passing fad and not taken seriously. A successful change in risk culture requires ongoing change in behaviours.

A sound risk culture:

- supports transparency and openness of risks, events and issues and facilitates effective internal controls and risk reporting (a culture which promotes "shooting the messenger" takes away an employee's feeling of empowerment to speak up and be protected from adverse consequences when they do so);
- encourages awareness of risks and responsibility for managing those risks;

- ensures appropriate actions are taken in a timely manner for issues and risks identified that are outside risk tolerances. For example, risk indicators that remain red for extended periods of time can indicate complacency or a lack of funding in the overall management of risk; and
- rewards staff for appropriate risk management behaviours. Typically, this is achieved by incorporating risk management as a core responsibility within individual roles and responsibilities.

Remuneration can be used to influence risk culture. Incorporating risk management into criteria for awarding bonuses can be an effective tool for influencing risk-taking behaviour.

13.4.5. Role of other stakeholders

Several other stakeholders play an important role in ERM governance. These are described below.

Appointed Actuary

The Appointed Actuary is the expert in the management of financial risks (in particular, insurance risk) for the organisation. If the Appointed Actuary is a member of the senior management team, he or she will have the same responsibility as other managers for embedding a risk management culture. In addition, the Appointed Actuary may perform an assessment of the suitability and adequacy of the risk management framework as part of a financial condition report, as well as providing advice prior to the launch of new products. These ideas are developed further in the Life Insurance Application subject.

Prudential regulators

Regulators need to balance two key (sometimes competing) objectives:

- ensuring standards are in place and enforced in order to support the active development of a stable and fair market; and
- allowing the development of competition, innovation and good service.

There are clearly risks of either under or over-regulating.

Prudential regulators have an obligation to members and policy owners to establish a regulatory regime which provides a high degree of confidence that contractual promises will be met. To this extent, the regulator's interests are aligned with those of members and policy owners.

For example, APRA's mission is:

> *"to establish and enforce prudential standards and practices designed to ensure that, under all reasonable circumstances, financial promises made by institutions we supervise are met within a stable, efficient and competitive financial system".*

This mission balances the importance of meeting promises while not over-regulating, which may have implications for an efficient and competitive system.

APRA sets standards to be met by the entities that it licences. These standards include general risk management obligations as well as a number of standards related to specific risks, including capital adequacy.

Market conduct regulators

Market conduct regulators have an obligation to protect individuals from inappropriate practices by financial services providers. They reduce fraud and unfair practice in financial markets and financial products, protect and enhance market integrity and provide consumer protection. This includes ensuring proper and timely disclosure of information, fair treatment of individuals and adequate redress for complaints. Here again, there is considerable alignment with members' and policy owners' interests.

The Australian Security and Investment Commission's mission is:

> *"To contribute to Australia's economic reputation and wellbeing by ensuring that Australia's financial markets are fair and transparent, supported by confident and informed investors and consumers".*

Members and Policy owners

The roles of members and policy owners will differ somewhat from those of other key stakeholders. They do not provide direct input to governance but are the beneficiaries of good governance processes.

The key concern for an insurance policy owner or retirement fund member is that the organisation fulfils its contract and makes claim or benefit payments when due. A secondary concern is that the specific product meets their needs, is fairly priced and is adaptable, as needs change over the life of a policy or fund.

For retirement fund members and investment policy owners, the key concern is that returns on investment are at or above expectations. This may be impacted by penalties on withdrawal, or poor investment returns.

13.5. Key learning points

- Risk can be described as uncertainty about the likelihood of achieving an objective. There is the risk of both exceeding or underperforming against objectives.
- ERM is concerned with the identification, management and monitoring of risk. A key objective is to integrate risk management into business processes to influence day-to-day operations and strategic decision making. It is critical that there is no perception that "the CRO is managing risk, so I don't need to".
- A sound risk culture supports transparency and openness of risks, encourages awareness of risks, ensures appropriate actions are taken in a timely manner and rewards staff for appropriate risk management behaviour.
- ERM needs to consider a range of quantitative and qualitative risks, including insurance, credit, market, liquidity, operational, strategic and application risks.
- At a high level, there are four main responses to risk: reduce, remove, transfer or accept.
- Effective ERM requires a clear and consistent risk management framework applied to all identified risks. The risk management framework incorporates systems, structures, policies, processes and people.

- Regulators have implemented standards and guidelines to ensure all financial institutions have robust operational risk management frameworks in place.
- Risk governance is the formal structure used to support risk decision making and oversight. The *three lines of defence* governance model incorporates day-to-day management (1st line), the risk management function (2nd line) and internal and external audit (3rd line).
- The objective of audit is to provide independent assurance that the risk management framework is working effectively and is being complied with.
- A typical risk assessment process includes: understanding objectives, identifying risks in meeting those objectives and assessing the quality of existing controls.
- Risk assessment tools used to quantify or classify the size of risks include VaR and TVaR, likelihood/severity matrices and scenario modelling.

13.6. Answers to exercises

Exercise 13.1:

Consider how news of the sales volumes in the scenario outlined above would be received within various departments within a mutual life insurance organisation. How would the news be reported to the board?

Answer:

This would be good for many departments. It may result in overtime payments for administration staff in new business processing and sales / marketing staff may receive bonuses for exceeding targets.

Actuarial / finance may be concerned about the impact on capital. In a mutual company, the only sources of capital are retained profits.

The use of capital for single premium endowment may result in inadequate capital for other planned purposes, such as funding new business for other product lines (this would be a concern if other products were more profitable). Other possible planned uses of capital may include business or system improvements, declaring bonuses or even improving the level of free capital to support solvency.

Exercise 13.2:

Explain why asking each department to calculate its required amount of capital is not adopted in practice.

Answer:

Assessment of the capital required for the various risks is a process that is generally co-ordinated and managed by a central risk function. To allow each department to do this separately would likely lead to following issues:

- Lack of uniformity in definitions of risks;
- Lack of clarity as to how to calculate capital and over what timescale;
- Most staff are not adequately trained to identify and quantitative risks and calculate the capital required to be held;

- While all staff are generally involved in helping to identify both risks and risk mitigation strategies for their departments, the risk function should not detract too much from their completing core business activities; and
- Departments may be rewarded for reducing risks and the capital required for their areas of operation. Therefore, a conflict may be created where a department could be accused of deliberately understating the capital required for their operations.

The impacts of combinations of risk factors and diversification across departments and operational areas may not be adequately considered

Exercise 13.3:

Think about how you would adapt the IAA recommendation for the following organisation types:

a) A medium-sized manufacturing company that offered a defined benefit scheme for employees until closing to new entrants three years ago.

b) A captive insurer for a worldwide oil and gas company.

c) A new life insurer set up to sell post-retirement annuities to retirees. The minimum purchase price per policy is $1m.

Answer:

From the IAA - *A sound ERM framework is appropriate to the nature, scale and complexity of its business and risks, integrated with the insurer's business operations and risk management policy.*

The ERM framework, including its policies, and required activities by business departments would be adapted by recognising key risks and the policies and processes for monitoring and managing these risks

The size of company and complexity of its operations will influence a company's risk management framework, including the sophistication of risk functions and processes.

a)

- The main business risks relate to supply, production and sales
- Also, all companies have a finance function, responsible for statutory reporting and financial functions of the company. The risks of the finance function include fraud and misstatement of the financial position or performance of the company
- DB schemes can represent a significant risk as employer provides explicit or implicit guarantees in respect of future benefits. The valuation of those benefits can impact the solvency and profitability of the company well in advance of those benefits becoming payable

b) A captive insurer would be responsible for quantifying, insuring and reinsuring a range of company risks. The business risks of the company would cover a range of operations in the production, transportation and sale of products and the investment in infrastructure to support operations over future years. Business risks include political risks, costs of production, safety, and market price volatility of oil and gas related products.

Not all risks of the company would be insurable and the captive insurer will be involved in assessing and insuring only a subset of the total company risks. However, the complexity of the company causes significant interdependencies of risks between departments. Examples are numerous such as the profitability of supply contracts may impact the budgets for implementing safety initiatives, which impact risks associated with production levels.

The captive insurer would require an RMF to cover its operations as a separate entity and would likely also be included in the broader company RMF.

c) Key risks specific to this company are in respect of any guarantees; longevity and investment risks. The risks relate to both the security of member benefits and ensuring that the costs of providing guarantees are within acceptable bounds. Other risks will relate to the financing of capital requirements, statutory and otherwise, to support the business, and political risks (legislation and policy on tax and savings incentives) affecting with the continuing viability of the products.

Some of the key departments or functions to be addressed in the RMF and processes includes sales (risks associated with achieving business targets and use of appropriate selling practices), actuarial (monitoring of risk capital, pricing terms and security of member benefits) and investment management (risks associated with possibly implementing a range of dynamic hedging strategies and ensuring that assets are managed in accordance with any commitments to policyholders.)

Exercise 13.4:

Can you think of other risks facing a life insurer or retirement fund that are not covered in the above lists? Which of the above risks do you think are hardest to quantify or measure? Why is this the case?

Answer:

Other risks:

- terrorism (although may be covered under extreme events);
- conduct risk may be considered a sub-category of "entity culture and empowerment" or "reputation". To what extent are the values implicit in the conduct of business consistent across the company and consistent with community expectations? This issue is central to the Royal Commission into misconduct in the financial sector. Many of the issues before the commission relate not just to breaches of regulatory and other codes. The commission has also been concerned with companies, not strictly in breach, but basing decisions on too narrow a financial objective and displaying poor values and judgements.;
- fraud (e.g. staff member stealing from the company or customer engaging in fraud)
- other risks that will emerge in the future that we haven't thought of (ego would cyber risk have been considered 50 years ago?);
- political risk; changing political attitudes relating to tax rules or retirement savings incentives may influence decisions well ahead of actual legislative changes.

Hardest to quantify/measure:

- entity culture – this is hard to observe directly, although may be addressed through surveys;

- regulation and/or politics – some aspects of politics are unseen by the public and can be hard to gauge, especially in times of political change such as around election time; and
- reputation is also hard to observe directly, and would need to be assessed through surveys (e.g. sentiment surveys), that may not always produce meaningful and reliable information, provide a snapshot in time and may not be conducted with sufficient regularity; and
- environment change – there is currently a lot of debate about the long term impact of climate change. This issue is a good example of the difficulty in identifying long term changes, versus observations of established statistical trends. It is also a good example of the range of debate and interpretations that can exist, and the influence of vested interests on the "objective" analysis of data.

Exercise 13.5:

Review and discuss recent commercial and financial services history and find examples of significant impacts, such as entities failing, for each of the types of operational risk specified.

Answer:

The examples below from the banking royal commission show some serious operational failures. Many of these lead to breaches of regulatory requirements. damaged company reputations and negatively impacted customers. Some of the key themes s are failure to identify risks, failure to adequately monitor customer facing operations, misalignment of reward incentives, failure to establish strong cultures of risk awareness and management throughout the company.

https://www.abc.net.au/news/2018-09-14/banking-royal-commission-life-insurance-live-blog/10246418

The royal commission hears how some, mainly young and low-income, workers are missing out on insurance through their super fund due to poorly advertised exclusions

https://www.theguardian.com/australia-news/2018/apr/20/banking-royal-commission-all-you-need-to-know-so-far

In August 2017, the Australian Transaction Reports and Analysis Centre (Austrac) announced it was suing the Commonwealth Bank for 53,700 breaches of money laundering and counter-terrorism financing laws after the bank failed to report properly on $77m worth of suspicious transactions through its intelligent deposit ATMs over a number of years.

In November, the federal court imposed pecuniary penalties of $10m each, and another $40m in other payments, on ANZ and NAB for attempting to manipulate the bank bill swap rate.

AMP executive Anthony Regan admitted that AMP had lied repeatedly to the corporate regulator

The NAB scandal involved falsified paperwork as staff raced to sign new loan customers, just one example of a litany of misconduct to emerge on first day of hearings

The banking royal commission has heard extraordinary evidence of National Australia Bank staff being involved in an alleged bribery ring covering multiple branches, forged documents, fake payslips and Medicare cards, with bribes being paid in cash to secure loans as staff responded to an incentive program to sign up new customers.

Senior counsel assisting Rowena Orr QC said a whistle-blower had been recorded as saying that "money exchanges hands in cash in envelopes, white envelopes, usually over the counter. The money is deposited at CBA so NAB can't detect the deposits. Happening on a daily or weekly basis and has been happening for a number of years."

Exercise 13.6:

What other risks from the lists provided in the previous section might be interrelated? Explain how they are interrelated.

Answer:

Changing social attitudes, judicial process and insurance risk: if enough policyholders complain about certain policy exclusions (e.g. coverage of mental health illness as a disability), claim decisions may be overturned more often when legally challenged (i.e. changing precedents set in court), which may flow through to higher claims costs than expected.

Technological change can cause operational and reputational risks (e.g. a new member servicing software platform is introduced for a retirement fund, which results in member privacy leaks due to inadequate testing of the software, damaging the reputation of the fund and resulting in large numbers of members leaving the fund and low numbers of new members joining the fund).

Competitive pressures result in policy exclusions to reduce the cost of providing cover or to simplify the sales process. An example is the introduction of policy exclusion for pre-existing conditions. This may impact reputational risk as customers may not appreciate the implications of exclusions when choosing or replacing cover; It may also impact legislative and judicial risks as the provisions and their interpretation under law may not be tested.

Exercise 13.7:

Search the internet to find examples of risk appetite statements for several life insurers and retirement schemes. How do the examples differ from one another? How might risk appetite statements for life insurers differ from those for retirement schemes?

Answer:

The answer will depend on the companies that are researched. Likely differences include: business objectives may differ, reflecting profits required for life insurance shareholders. The types of products sold will influence a company or fund's risk appetite. (e.g. a life insurer with only risk products might have a very different appetite to a life insurer selling mostly unit linked business, or a DC fund). The size of company/fund will likely influence the sophistication of its risk functions and processes. This factor is often evident when observing the risk appetite statement.

Exercise 13.8:

Suppose a life insurance firm operates using a three lines of defence model. Is the Appointed Actuary in the first line of defence, the second line of defence, in both, or something else? Hint: Thinks about the roles undertaken by the AA and consider in which line each role lies.

Note:

Answer for this should make it clear that this is a common point of discussion and there is not necessarily a right or wrong answer.

Hard question as we haven't studied some concepts.

Source: Actuaries Digital, Brett Riley, 2017

Answer:

- Policy liability valuation – 1st line since liability estimates are used by board;
- Other valuations such as for statutory capital and embedded value - 1st line;
- Financial Condition Report – all three as report is primarily an independent review but does consider commentary on liability valuations;
- Actuarial advice regarding policies, pricing, and reinsurance. 2nd or 3rd if others make decision based on the advice. 1st line if input drives decision. Often the AA co-ordinates and manages separate parties involved in both pricing and review of pricing advice;
- Assess uncertainty in capital stress testing - 2nd or 3rd line as the work in an independent review that does not directly affect the risk profile of the underlying business.

Exercise 13.9:

A medium-sized proprietary life insurance company has only sold risk business, namely, yearly renewable term assurance, critical illness and income protection business to domestic customers. The board is considering diversifying into post-retirement products by offering annuities.

The concept of enterprise risk management is currently not practiced in the domestic market.

(i) How would you advise the board on setting up a risk appetite statement?

(ii) Briefly demonstrate how the board may use the statement resulting from question (i) to judge the strategy of introducing post-retirement products.

Answer:

(i) The board should be advised of the purpose the risk management statement and what the statement might contain. Risk appetite is the amount and type of risk an organisation is willing (and able) to take on in pursuit of its business goals. A risk appetite statement summarises the company's risk appetite. The table below summarises key issues how these need to be addressed in completing a risk appetite statement. This can be used to guide by the company in the process of completing its risk management statement. (considerations before expansion to post retirement products).

See the details in the table overleaf.

Matters for RMS	Considerations when addressing these
the nature and size of the risks that the institution is prepared to accept in pursuit of its strategic objectives and business plan, giving consideration to the interests of policyholders and members; key stakeholder expectations	• This part requires the company to establish strategic objectives such as profitability or growth over a given timeframe and to establish the company's tolerance for accepting risks in order to meet those objectives. • The company is will be experienced in accepting insurance risk and business risks of development cycles for products and related business systems. • The RMS will involve identifying the various risks that company is expects to be exposed to • Security of policyholder benefits is key and is a focus of the regulator. • Risk appetite can be qualitative, for example "the fund has a low appetite for reputational risk exposure", or quantitative, for example "available capital will not drop below 120% of the regulatory capital requirements
the current competitive environment (including regulations, competitors, economy, technology)	• Understanding the current economic and competitive environment are key to assessing the level of risks associated with meeting targets for profitable sales and other business objectives
the company's risk capacity (including capital, liquidity, knowledge / skills, market influence	• The company will need to assess factors such as the amount of current available capital to absorb risk, the likely ease of access to capital in the future, the impact of volatility in profit results and the tolerance for possible financial losses • The company's skill set will include sales, underwriting, claims assessment and management of insurance risk, plus investment of assets backing policy benefits, capital and other liabilities

Matters for RMS	Considerations when addressing these
Establish the company's risk tolerance; for each material risk, the maximum level of risk that the institution is willing to operate within. The use of risk tolerance levels, risk targets and risk limits will assist business units assess business decisions relative to the risk appetite	• Modelling will be required to assess the probability of losses exceeding various thresholds, and the flow on impacts to profitability and capital requirements. These will form a basis for establishing risk targets. Stress testing may be used to assess the impact of specific adverse scenarios. Consideration need to be given to risk dependencies across functions and departments. • The company will have a reinsurance program to ensure that insurance risks are managed within acceptable bounds. The risk management statement defines those bounds, although the reinsurance program itself may be useful in communicating the companies risk tolerance
the process for monitoring compliance with each risk tolerance and for taking appropriate action in the event that it is breached	• The company will have strategies to mitigate risks. For insurance, underwriting and policy limits will ensure that individual risks are within acceptable bounds. as part of the RMS, the company will need to establish the processes to monitor compliance and ensure that appropriate action is taken in the event of breach.
the timing and process for review of the risk appetite and risk tolerance	• Business environments and the company's needs change over time. The pace of change is accelerating. Defining the process and timing of ongoing monitoring and review of the risk management statement is itself an important part of the statement

(ii) Many of the steps used to assess, monitor and mitigate risks in the current business can be adapted and applied to the acceptance of risks under post retirement products. The board would need to be aware of the following differences and their impact on the risk and return objectives of the company:

- cash flows under post retirement products generally involve receipt of a large initial premium and draw down of an income stream or a series of lump sum payments in the future. Additional investment processes, and mandates, and the need for competitive returns will create additional risks. This may not be a core skill area for the company;
- retirement products often have payment guarantees. The company may be subject to investment and longevity risks. For insurance products, there are often opportunities for the company to reprice future cover as experience emerges. For guaranteed retirement products, repricing is unlikely to be available to the company;
- there may be a considerable period of time before the company is able to establish a viable operation with its move into post retirement products. This brings risks associated with development costs, systems development and the ability of the company to diversify risks across its retirement portfolio;
- A larger, more diverse business provides some risk mitigation.

About the Actuaries Institute

The Actuaries Institute is the sole professional body for actuaries in Australia. The Institute provides expert comment on public policy issues where there is uncertainty of future financial outcomes. Actuaries have a reputation for a high level of technical financial skills and integrity. They apply their risk management expertise to allocate capital efficiently, identify and mitigate emerging risks and to help maintain system integrity across multiple segments of the financial and other sectors. This expertise enables the profession to comment on a wide range of issues including life insurance, health insurance, general insurance, climate change, retirement income policy, enterprise risk and prudential regulation, finance and investment and health financing.

Published December 2019

Institute of Actuaries of Australia

ABN 69 000 423 656
Level 2, 50 Carrington Street,
Sydney NSW 2000, Australia
t +61 (0) 2 9239 6100
f +61 (0) 2 9239 6170
actuaries@actuaries.asn.au
www.actuaries.asn.au