

# ERM – Qualitative Implementation Guide for Insurers

George C. Orros, BA, MSc, MBA, FIA, FCII, C.Stat, Chartered Insurer and Jane Howell, BA, MBA

16<sup>th</sup> September 2009

---

## Abstract

This paper provides a practical ERM implementation guide for insurance companies, from a qualitative perspective. It has been designed to meet the broad requirements of relatively large insurers that would like to implement an ERM framework that is grounded in corporate governance principles and in qualitative aspects of strategic management. ERM implementation is achieved via a 6-stage, iterative process of Analysis, Risk Identification, Risk Assessment, Risk Evaluation, Risk Planning and Risk Management, each with feedback loops to ensure a robust and resilient iterative process. The authors show how these processes can be achieved efficiently and can result in a robust and resilient insurer that is well positioned to face the storms and shocks that may lie ahead.

## Availability

To discuss further, please contact the authors at [uhcg@cwgsy.net](mailto:uhcg@cwgsy.net)

## Keywords

Enterprise Risk Management; Risk Management; Stress and Scenario Tests; Risk and Uncertainty; Governance; Control Framework; Risk Modelling; Risk Appetite; Risk Maps; Risk Exposure

---

## Contents

1. Introduction
2. Executive Summary
3. Black Swans and Fat Tails - The Problem of Inductive Logic
4. ERM Framework for Corporate Governance
5. Implementation Stage 1 - Analysis
6. Implementation Stage 2 - Risk Identification
7. Implementation Stage 3 - Risk Assessment
8. Implementation Stage 4 - Risk Evaluation
9. Implementation Stage 5 - Risk Planning
10. Implementation Stage 6 - Risk Management

# ERM – Qualitative Implementation Guide for Insurers

George C. Orros, BA, MSc, MBA, FIA, FCII, C.Stat, Chartered Insurer and Jane Howell, BA, MBA

## 1. Introduction

This paper provides a practical ERM implementation guide for insurance companies, from a qualitative perspective. It has been designed to meet the broad requirements of relative large insurers that would like to implement an ERM framework that is well grounded in corporate governance principles and in qualitative aspects of strategic management.

ERM involves strategic business risk management – it enables management to critically and self-consciously set a strategic direction and take greater risk in order to improve business performance and gain competitive advantage. This implies a focus on risk and opportunity management. ERM exists to provide a culture, framework and process to achieve a balance between risk and opportunity.

There is a wealth of actuarial and other literature available on ERM and risk management practices in the insurance industry and in other industries and public/private sector organisations. The reader is encouraged to become familiar with ERM applications in the insurance sector, such as the healthcare insurance industry <sup>1</sup>, and with recent ERM literature reviews <sup>2</sup>. Some of these literature reviews outline the key features of ERM and provide some useful reference materials for practitioners <sup>3</sup>.

What is ERM from a qualitative viewpoint. Perhaps it can be encapsulated via the following graphic.



## 2. Executive Summary

ERM can be described as strategic business risk management in enabling organisations to set a strategic direction and take greater risk in order to improve business performance. The practical ERM framework and process issues discussed in this paper are designed to enable organisations to achieve a balance between risk and opportunity; where risk is seen as a restraint on action which needs to be controlled in order to allow the organisation to exploit its opportunities.

ERM is located within a corporate governance model which can be interpreted as having five elements <sup>4</sup>:

- (a.) Corporate governance (Board oversight)
- (b.) Internal control (sound system of internal control)
- (c.) Implementation (appointment of external support)
- (d.) Risk management process (incremental phases of a 6-stage iterative process.
- (e.) Sources of risk (internal and external).

The risk management process consists of a 6-stage process of Analysis; Risk Identification; Risk Assessment; Risk Evaluation; Risk Planning and Risk Management. The first iterative step in the 6-stage process is Analysis, whereby one gains an understanding of the business as a whole and the specific business activity, process or project, forming the subject of the ERM study. It provides the ERM foundation for everything that follows, so how well it is completed will determine the quality of the remainder of the risk management process as its outputs are the inputs to downstream processes and can underpin or undermine the efficacy and traction of the ERM implementation.

Rigorous implementation of the Analysis stage is a pre-requisite for a high quality ERM implementation. The outputs from this stage will provide an information underlay and clear picture of the business which will be essential to make the following stages meaningful and capable of creating a concrete and relevant ERM framework. The following stages of risk identification and risk assessment, in particular, rely on the outputs from this stage in order to produce a realistic and accurate risk register and judgement of the likelihood and impact of risks and opportunities identified for the business.

*“Risk appetite is the degree of risk, on a broad-based level, that a business is willing to accept in pursuit of its objectives. Management considers the business’s risk appetite first in evaluation of strategic alternatives, then in setting boundaries for downside risk”<sup>4</sup>*

The Board is primarily responsible for setting the organisation’s risk appetite and tolerances. Risk appetite is a critical output from the Analysis stage and should quantitatively and qualitatively define the organisation’s capacity to absorb risk, for example, via risk response strategies such as risk

transfer, risk organisation, risk origination and risk retention. It should be recognised that risk appetite is a preference, attitude, tolerance or capacity which will change over time responding to changes in organisational objectives, culture and the external environment (economic, political, social, technological, global/regional/local, industry).

Risk appetite is an input to the second iterative step in the ERM process, Risk Identification, a transformation process whereby one generates a series of risks and opportunities that are then recorded on the risk register. As it is a process within ERM, it is useful to adopt the philosophy of process mapping, whereby one process exists to make a contribution to one or more of the enterprise risk management goals.

Risk Assessment follows the Risk Identification stage and provides a judgement of the likelihood and impact of the risks and opportunities identified, should they materialise. This process provides an order of the potential ‘pain’ or ‘gain’ associated with risk and opportunity. Even when there is considerable uncertainty, quantitative techniques provide a useful framework.

The fourth iterative step is Risk Evaluation, which involves evaluation of the results of the risk assessment stage and includes an understanding of the inter-relationships between the individual risks and the opportunities. It provides an iterative process of challenge and refinement of the information captured during the risk assessment process.

Risk Planning follows, which combines the risks and opportunities together and considers their combined effect. It uses the preceding ERM processes to produce responses and specific action plans to address the risks and opportunities identified to secure the business objectives; it is essential that these plans are prepared, considered, refined and implemented.

The sixth and final iterative step is Risk Management, which consolidates all the previous steps. In fact, all of the six steps are iterative and it is frequently necessary to revisit earlier steps when more information becomes available or circumstances change, as each stage relies upon inputs from the earlier stages. All risk management process maps should state a need to ensure that the risk responses to identified risks are implemented and that the implementation is pro-actively managed.

Implementing and achieving benefits from ERM depends on people and team work, rather than on good ideas from the top management team. ERM needs to be embedded throughout the insurance organisation, with the underlying message that “*we are all risk managers here*”. Embedding ERM within the organisation and ensuring that it is part of the DNA of every strategic and operational decision hinges on the organisation’s success in managing its human resources and business culture.

## 4. Black Swans and Fat Tails – The Problem of Inductive Logic

In the authors view ERM is about realism and building resilience to a frequently complex and ‘messy’ world: a world where assumed events do not always cluster around an average and where we should appreciate the limitations of inductive logic. This almost philosophical view underpins the discussion of ERM within this paper and it can be illustrated by considering the famous case of the ‘black swan’<sup>5</sup>. A black swan can be defined as a highly improbable incident or event with three principal characteristics: (a) its unpredictability, (b) its massive impact; and, after it has happened, (c) our desire to make it appear less random and more predictable than it was. They underlie almost everything, from the rise of religions, to events in our personal lives. Examples include ‘Black Swans’, ‘9/11’ and the ‘Internet’.

People generally severely underestimate the possibility of unexpected events and the potential depth of the negative/positive outcomes. Non-Australians used to be convinced that all swans were white, an unassailable belief from empirical evidence. The sighting of the first black swan illustrated the fragility of our knowledge. One single observation of a black swan invalidated a general statement derived from millennia of confirmatory sightings of millions of white swans.<sup>5</sup>



Before the discovery of Australia, people in the Old World were convinced that all swans were white, an unassailable belief as it seemed to be completely confirmed by empirical evidence. The sighting of the first black swan illustrates a severe limitation to our learning from observations or experience and the fragility of our knowledge.

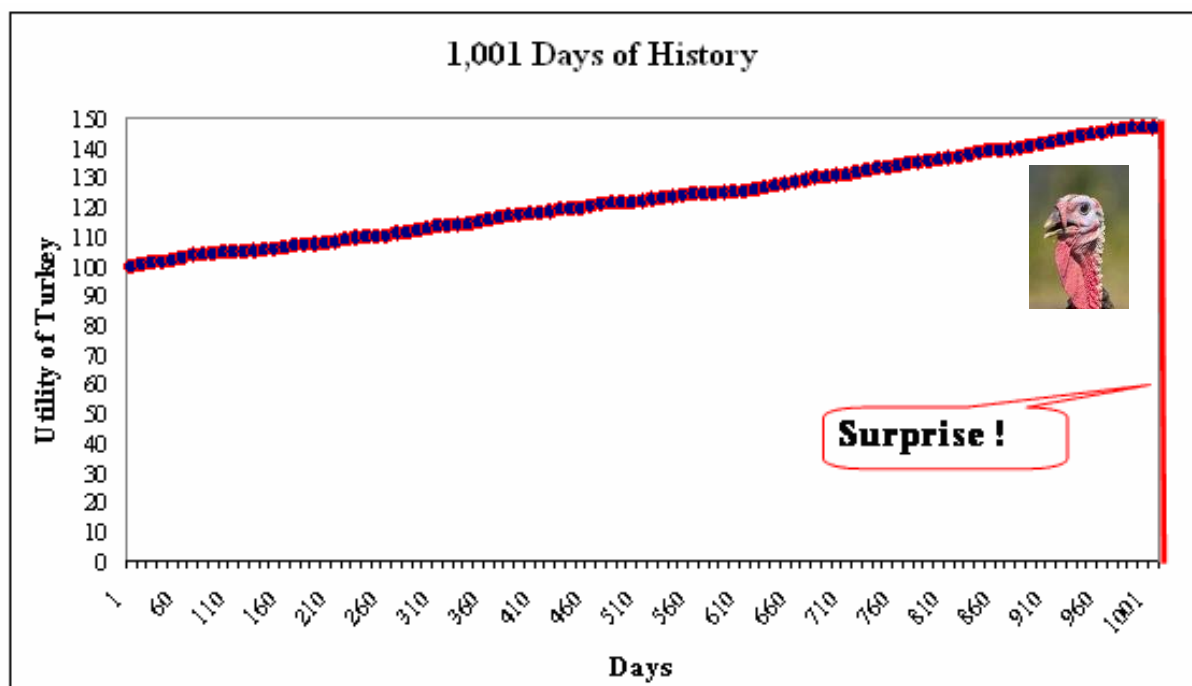
Black Swan logic makes what you don't know far more relevant than what you do know. Many black swans can be exacerbated by their being unexpected. For example, consider the terrorist attack of 11<sup>th</sup> September 2001. Had the risk been reasonably conceivable on 10<sup>th</sup> September 2001, it would not have happened. If such a possibility were deemed worthy of attention, fighter planes would have circled the sky above the twin towers and aeroplanes would have had locked and bullet-proof doors, and the attack would not have taken place.

In the ‘mediocristan’ world of Gaussian normality and equilibrium, one thinks of ordinary fluctuations as the dominant source of randomness, with jumps as an afterthought. Everything needs to fit some

general socio-economic model; people frown upon descriptive models. Mediocristan practitioners seek to be perfectly right in a narrow model, under precise assumptions. They use top-down models and rely on scientific papers and go from books to practice. They are inspired by physics and rely on abstract mathematics.

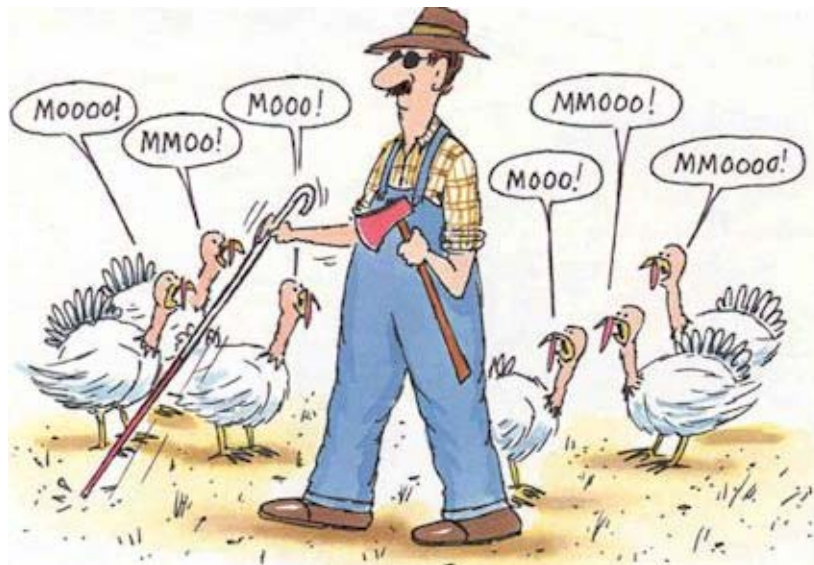
On the other hand, in the fat-tailed, 'extremistan' world of sceptical empiricists, one thinks of black swans as the dominant source of randomness. They use bottom-up models and minimal theory, believing that theorising is a disease that should be resisted. They do not believe that one can easily compute probabilities. They develop intuitions from practice and go from empirical observations to books. They are not inspired by any science and use messy mathematics and computational methods.

Consider the case of a turkey that is fed every day, an illustration of the 'problem of inductive knowledge'. Every single feeding will firm up the bird's belief that it is the general rule of life to be fed by friendly members of the human race "*looking out for its best interests*", as a politician might say. On the afternoon of the Wednesday before Thanksgiving, something unexpected will happen to the turkey. It will incur a revision of belief, as illustrated below.





The problem of inductive logic can be simply illustrated by the following graphic.



In the black swan world of extreme unexpected events, there is also the notion of ‘the known unknowns and the unknown unknowns’. This theory was expounded by Donald Rumsfeld at a ‘news briefing’ on 12<sup>th</sup> February 2002 <sup>6</sup>, shortly after the 9/11 events ...



*“Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.”*

## Case Study 1

### A Casino and its unexpected losses



Casinos operate extensive security, compliance and risk management programs. The casino focuses its attention upon the risk from a 'whale' i.e. a gambler who places large amounts of money and receives generous incentives from casinos to persuade them to play on the gambling floors, and its own staff. The four largest losses recorded in our case study were 'off-model' risks;

1. A \$100m loss when the white tiger attacked Roy Horn (of Siegfried and Roy). Roy had hand-reared the tiger and it had even slept in his bedroom. The casino management were concerned about the safety of the audience and not the risk that the tiger would turn against its master.
2. A disgruntled contractor, hurt during construction of the hotel annex to the casino, was so offended by the settlement offered to him that he attempted to dynamite the casino. The contractor's plan was discovered and the planned explosion did not happen.
3. The casino owner violated gambling laws by taking funds from the casino to pay a ransom in exchange for the return of his kidnapped daughter.
4. The casino was required to file a return with the Internal Revenue Service where a gambler's profit exceeded a certain amount. However, for some unknown reason an employee failed to file returns for some years. The casino management paid a large fine to retain their license.

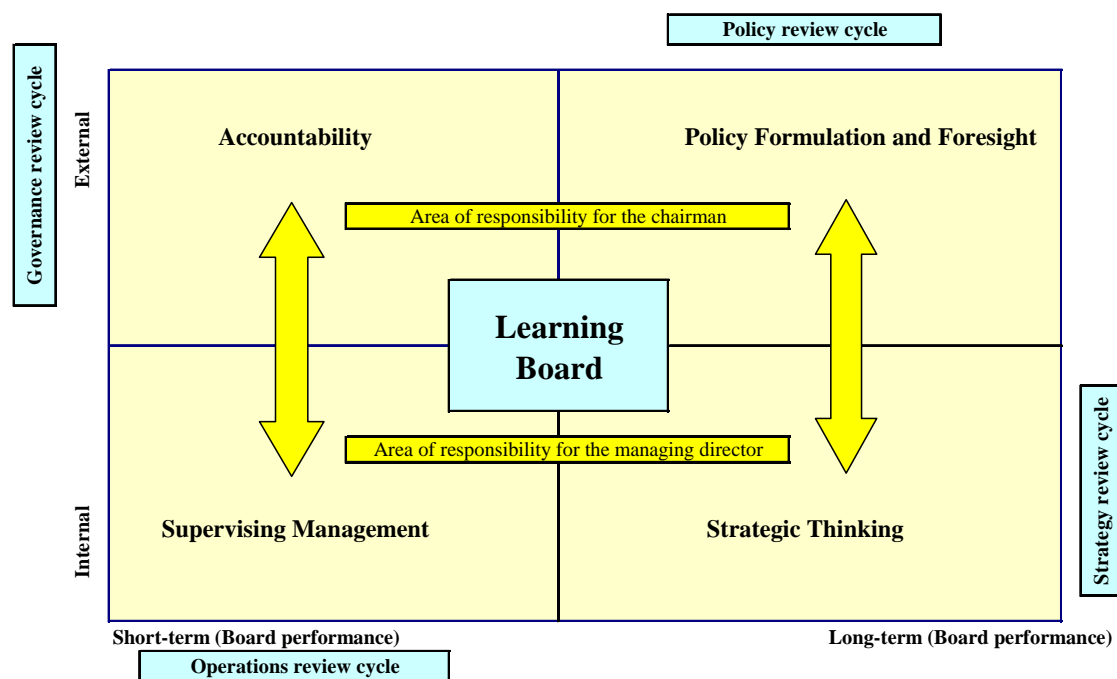


### 3. ERM Framework for Corporate Governance

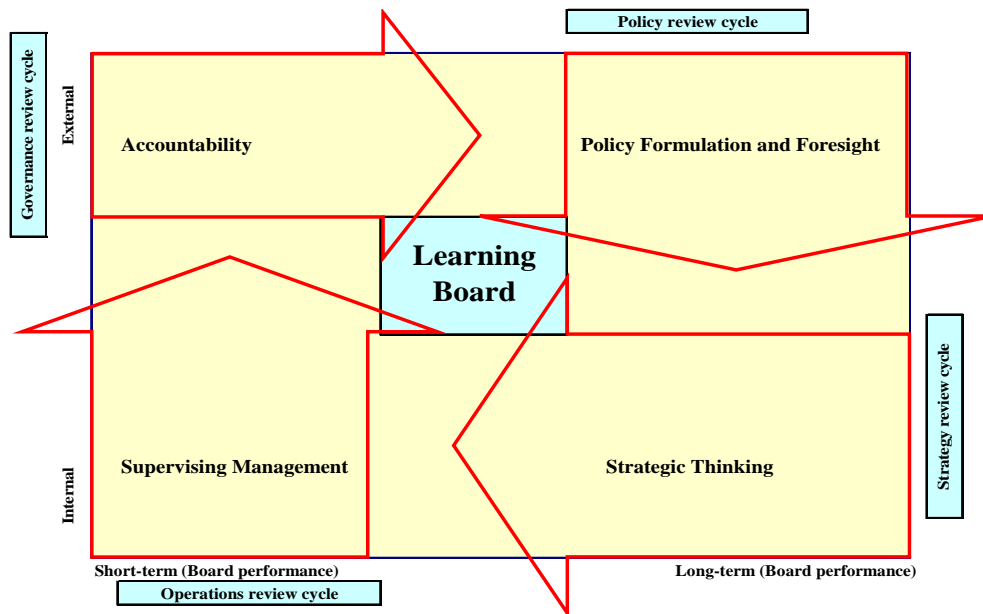
Corporate governance is concerned with improving the business performance, compliance in actions/behaviour of companies for the benefit of its stakeholders e.g. shareholders, policyholders and the wider economy. It involves the conduct of, and relationship between, the board of directors, managers and the insurer's owners:

*“Corporate governance generally refers to the processes by which organisations are directed, controlled and held to account. In a corporate governance context risk management is best described as an enabling process in the sense that it enables and facilitates the exercise of direction, control and accountability. In practice, the link between corporate governance and risk management is manifested in the form of a board committee and/or board charter responsibilities.”<sup>7</sup>*

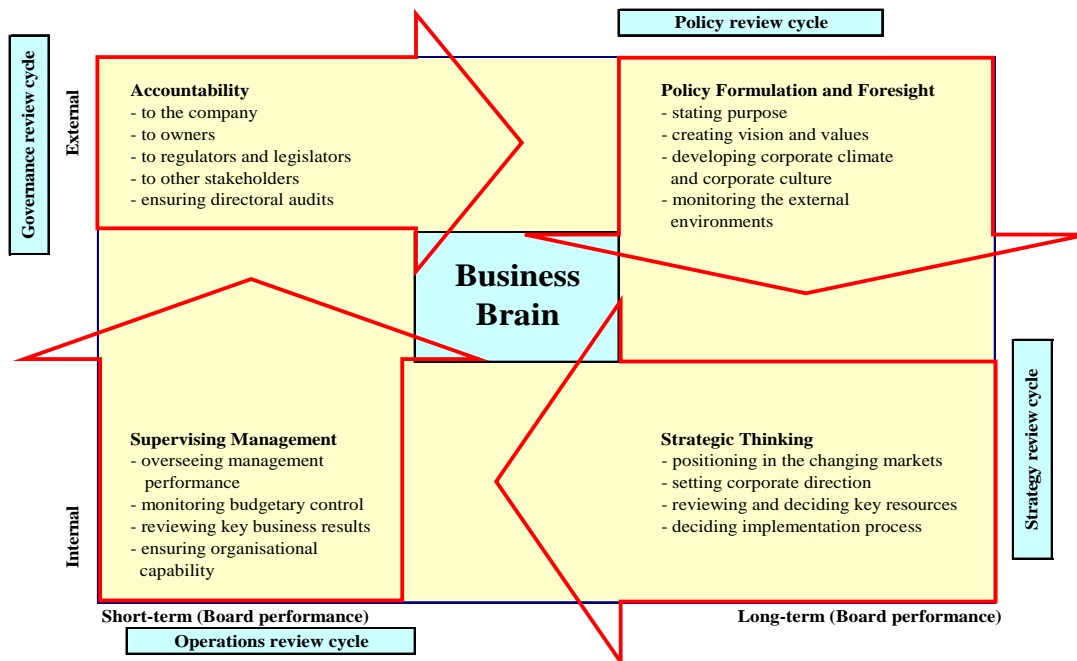
ERM as a philosophy should influence the conduct of, and relationship between, the board of directors, managers and the insurer's owners. ERM should inform all stages of the corporate governance cycle (policy, strategy, governance and operations)<sup>8</sup>. The Board should be the central processor for the organisation – the Learning Board – which drives the business forward.



The learning model for corporate governance can be illustrated in terms of the key functions at the learning cycle stages. These separate out the short-term and long-term issues from the internal and external focus of the organisation, as indicated below. Policy formulation and foresight is externally orientated, long-term thinking. Strategy follows as the configuration and deployment of the organisation's resources to achieve policy objectives. Supervision concerns the organisation's capability to deliver the strategy. Accountability is about synchronisation – is the Board legally, intellectually and emotionally in synchronisation with its stakeholders?<sup>8</sup>



A more detailed view of the duties and responsibilities contained with each of the major functional areas is shown below. The Learning Board is seen as the business brain of the organisation.



A practical interpretation of the 'business brain' model for the insurance industry is that it can represent the 'risk and opportunity management' capability. The insurance company board should instigate and direct ERM implementation and outcomes:

- Approving and directing the externally orientated, long-term ERM policy and strategy
- Appointing a CRO who has responsibility, autonomy and authority to act
- Setting the risk appetite for the organisation
- Monitoring key risks by ensuring the implementation of an ERM framework, effective feedback and control systems
- Embedding ERM in the fabric of organisational culture

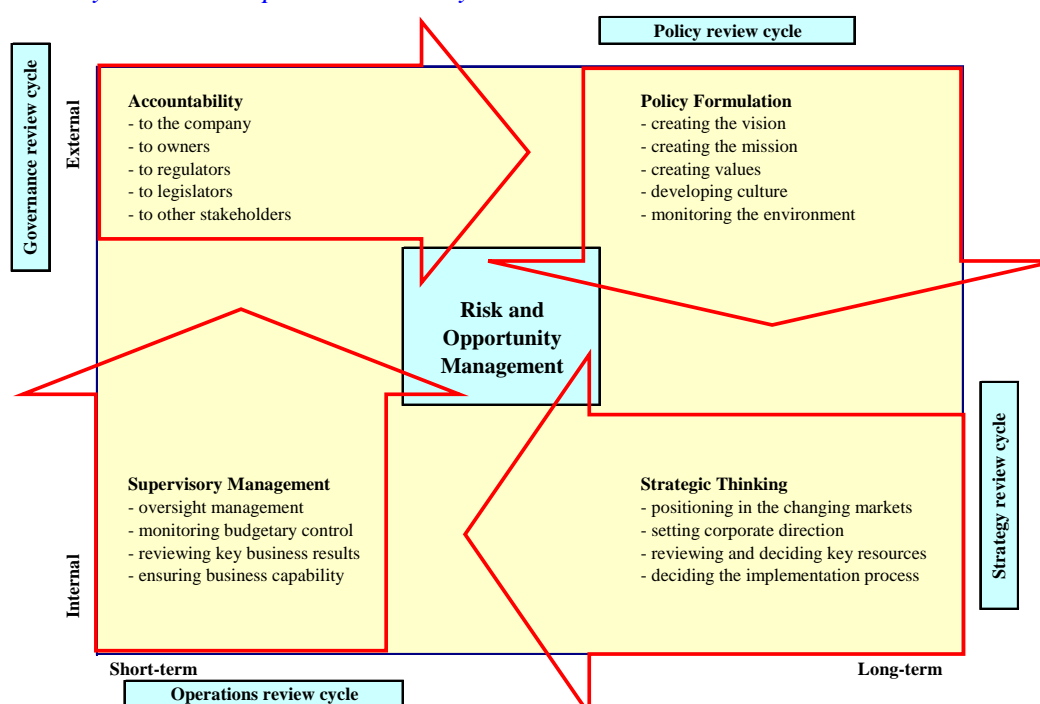
As a practical first step the Board should establish a committee to focus on long-term ERM policy and strategy. The Board should collaborate with the committee on a ‘Charter’ or mission statement for the ERM implementation and beyond. The committee should be multi-disciplinary and involve experienced, responsible and accountable staff from risk, audit, financial reporting but also from marketing, human resources and operational management disciplines. The involvement of independent, external experts with wider industry experience can serve to challenge internal perspectives and to introduce broader cross-industry and international experience.

The committee’s charter may include development of an ERM framework model, compliance with regulatory requirements, establishing a dedicated ERM implementation team and pursuing ERM implementation across the organisation.

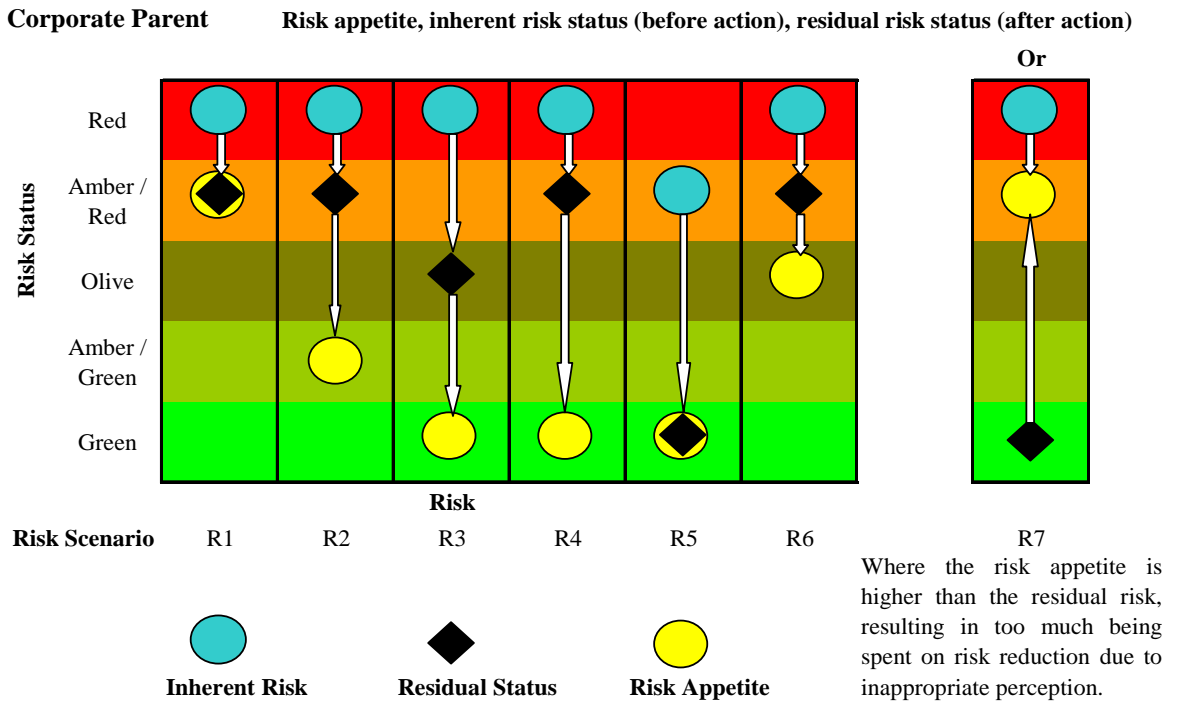
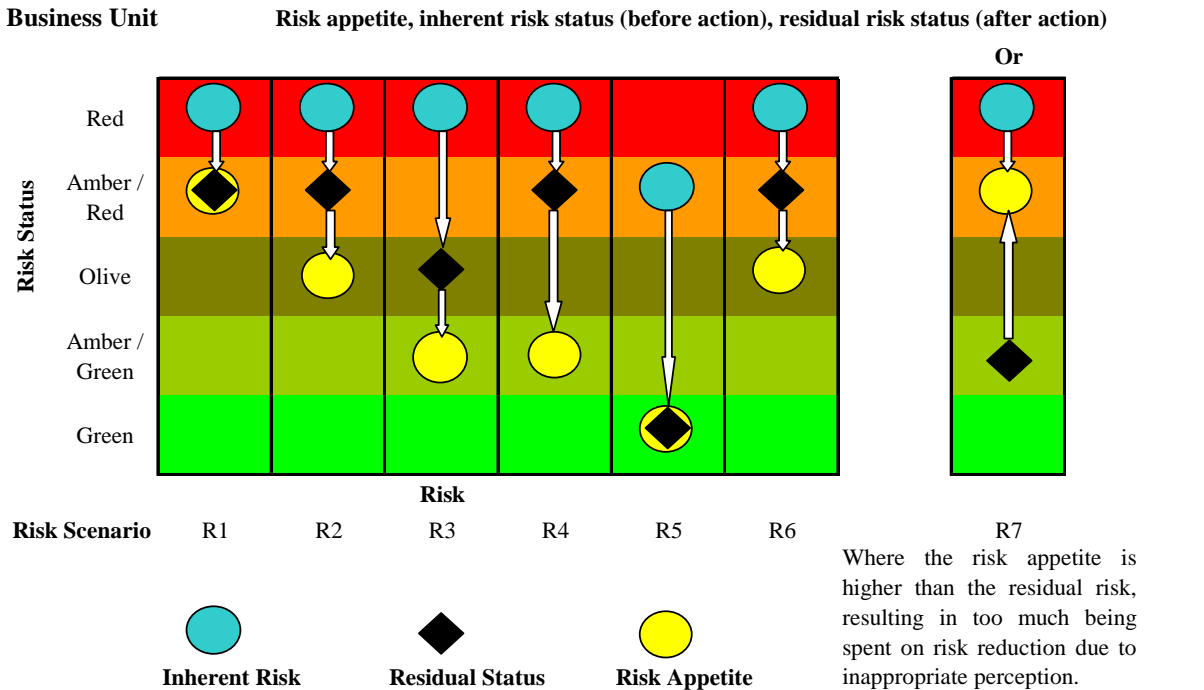
A practical ERM definition for insurance companies has been provided by Chapman <sup>4</sup>

*“ERM is a systematic process, embedded in a company’s system of internal control (spanning all business activity), to satisfy policies effected by its board of directors, aimed at fulfilling its business objectives and safeguarding both the shareholder’s investment and the company’s assets. The purpose of this process is to manage and effectively control risk appropriately (without stifling entrepreneurial endeavour) within the company’s overall risk appetite. The process reflects the nature of risk, which does not respect artificial departmental boundaries and manages the interdependencies between the risks. Additionally, the process is accomplished through regular reviews, which are modified when necessary to reflect the continually evolving business environment.”*

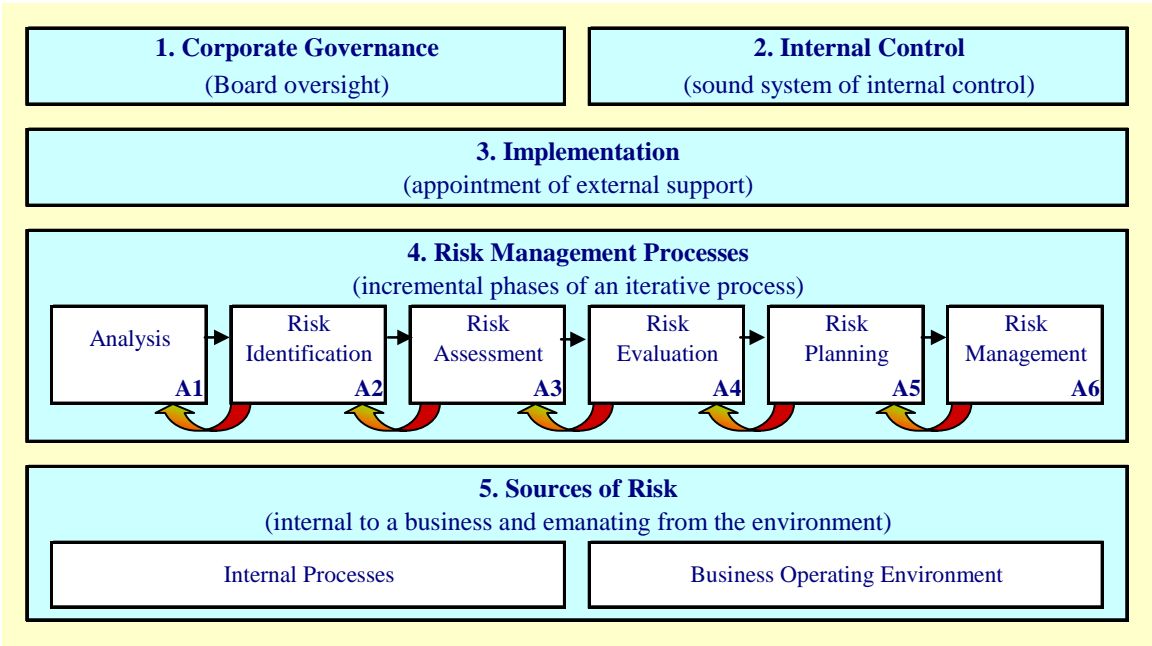
The ERM process is essentially one of risk and opportunity management, as impinging *“on the 4 main functions of Boards; policy formulation, strategic thinking, supervisory management and accountability and their respective control cycles”*



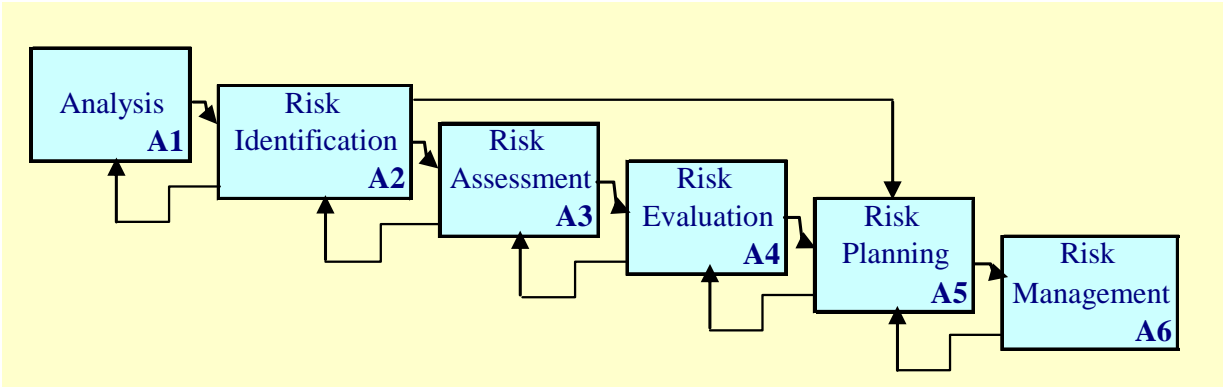
A prerequisite for an effective ERM implementation is a good understanding of risk tolerance and risk appetite. This needs to be framed with reference to the scale, complexity and diversity of the organisation. For example, a corporate parent with diverse regional business operations may have a high-level unifying statement of risk appetite which co-exists with regional ‘exits’ to support differential risk appetite across/within each region. Understanding risk appetite, inherent risk status and the residual risk status for the corporate HQ and the operational business units can be assisted by a risk ‘dashboard’, or a risk ‘heat map’, as illustrated below.



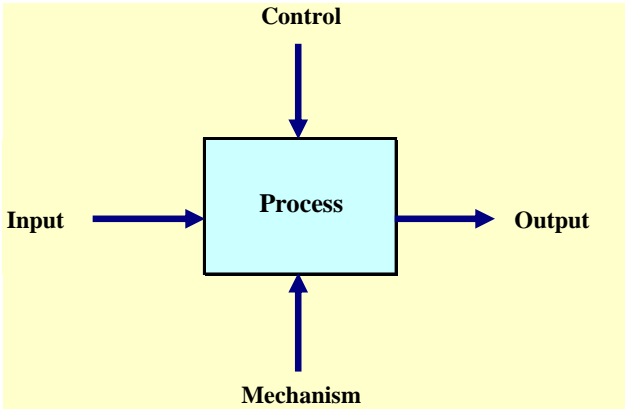
The ERM framework model which has five elements, as illustrated below. **Note:** The model has been adapted by the authors to provide the necessary feedback control loops that can facilitate the iterative development of a robust and resilient ERM process.



The risk management process is a 6-stage iterative process, with feedback control loops at each stage. These are necessary to develop a robust and resilient ERM framework that can be embedded within the organisation and serve to facilitate real-time risk response strategies.

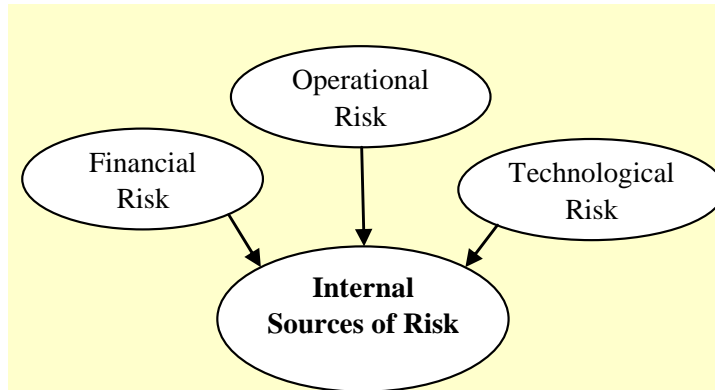


Each of the six risk management processes has inputs, outputs, control and mechanisms. The modes of data connectivity can be charted using the IDEFO (Integration Definition for Function Modelling) process mapping technique.



## Internal and external sources of risk

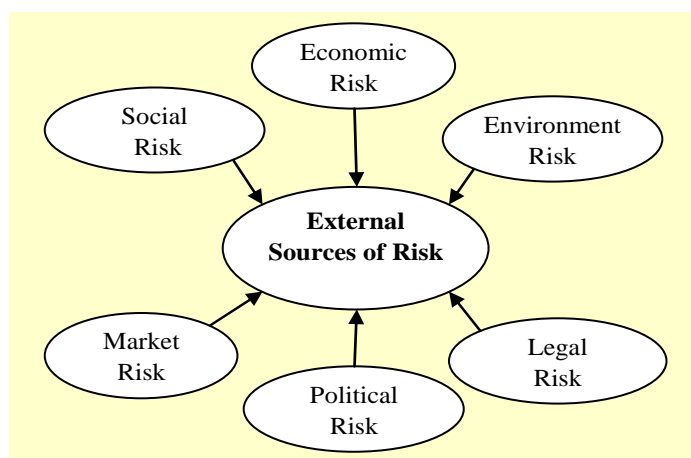
The risk management process needs to focus on the micro and macro influences which are sources of risk and opportunity and shape business performance (i.e. internal and external sources of risk). Internal / micro sources of risk are sourced and may (potentially) be controlled within an organisation. For example, financial risk, the exposure to adverse events which can adversely affect profitability and may trigger closure of a business e.g. liquidity risk may mean the firm cannot pay its suppliers.



The operational risk issues facing the general insurance industry were the subject of a recent paper.<sup>9</sup>

## External Sources of Risk

External, macro sources of risk occur at sub-national, national, regional and global/international levels. These sources of risk are largely exogenous to the insurer such as demographic trends however some factors may be influenced by the insurer or its peers (e.g. regulation which addresses market and consumer issues). External sources of risk include the economic, natural/physical, political, legal and regulatory environments, market structure and conditions, legislation and socio-demographic and cultural factors. These factors create sources of risk and opportunity; single factors can have relative pre-eminence or factors can interact and create a series of unpredictable and volatile shocks to the organisation which may contradict all past lessons learned by the organisation.<sup>44</sup>

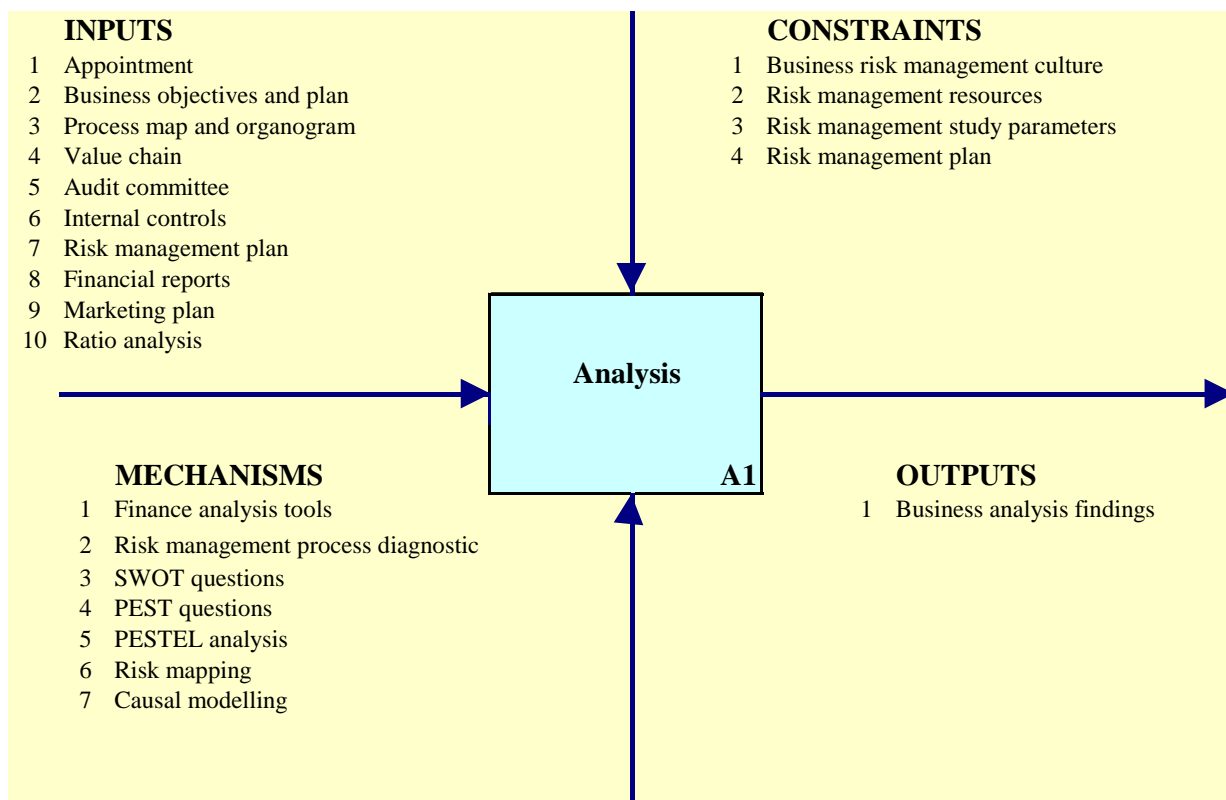


A discussion of the each of the above external sources of risk can be found in Chapman<sup>4</sup>

## 5. Implementation Stage 1 - Analysis

### 5.1 Analysis –Foundation of ERM process

The first iterative step is Analysis, whereby one gains an understanding of the business as a whole and the specific business activity, process or project, forming the subject of the ERM study. It provides the ERM foundation for everything that follows, so how well it is completed will determine the quality of the remainder of the risk management process.



### 5.2 Analysis – Active Team Involvement

It is important (for an effective ERM framework implementation) that the Analysis stages goals are met via active representation and involvement across all business units and departments. In practice, 'active representation' will need to involve the committed engagement of the individuals who have knowledge, experience, perspective and responsibility.

The 'active representation' process should also involve and engage the Non-Executive Directors and the senior management group. Without their full and committed support, it is unlikely that an effective ERM framework implementation can be achieved.



### 5.3 Analysis – Evaluation Criteria Checklist

In order to be judged sufficient this stage should be planned and evaluated using formal criteria. The use of evaluation criteria encourages more rigorous planning of the activities and an objective review (involving non-participants in the process stage). The criteria might include – at a minimum<sup>4</sup>:

1. Define and articulate the mission and business objectives
2. Review and issue a clear, current and accurate business structure document
3. Review and issue a high-level business process map or flow chart
4. Identify and review the existing internal control system
5. Identify and examine all primary business functions
6. Review the existing corporate risk management plan
7. Define, articulate and review the remit of the audit committee
8. Define, articulate and review the remit of the existing risk management committee
9. Profile the current ERM maturity level of the organisation
10. Define and articulate risk appetite – in qualitative and quantitative terms
11. Review the existing risk register
12. Canvas and engage knowledgeable and expert participants from across the organisation
13. Engage participants who can input to the project from a position of authority and expertise
14. Brief all participants and make them aware of their responsibilities
15. Consider and consult with non-executive directors where appropriate

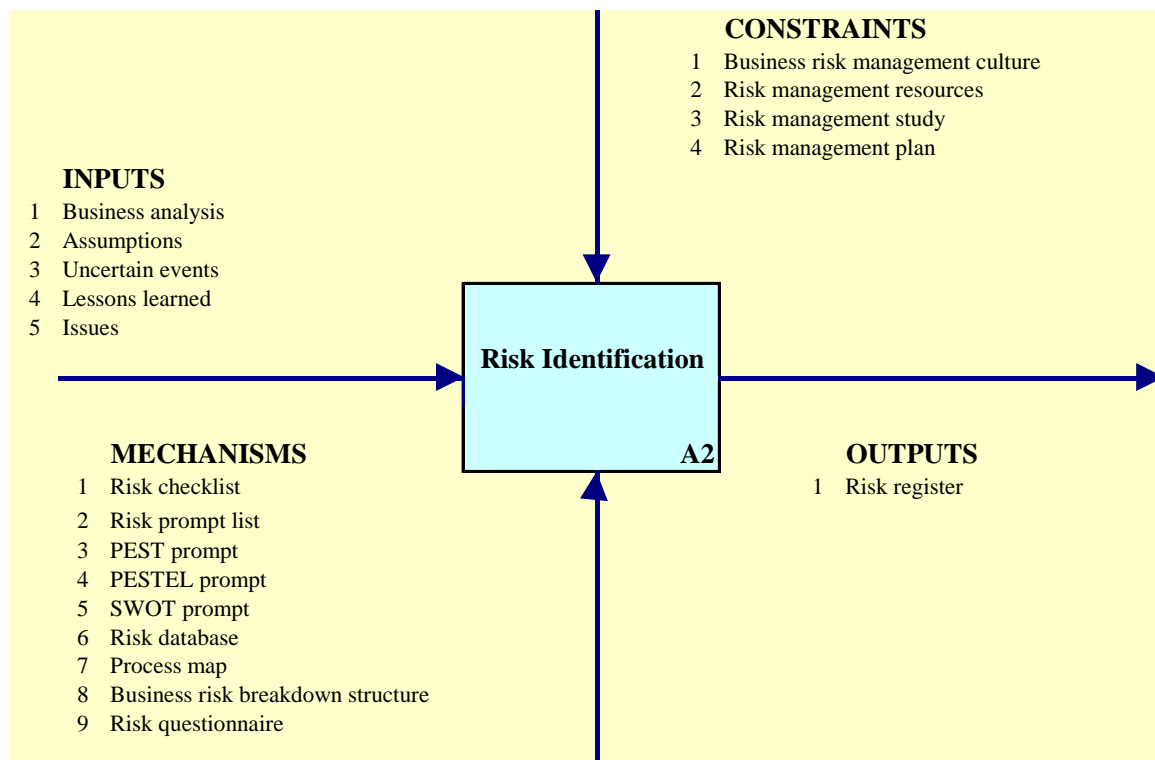
Inputs to the process include comprehensive high-level business process maps and value chain analysis. The value chain describes the activities within and around an organisation which combine to create a product or service offer. Value chain analysis enables managers to understand how and where value may be created within the organisation and whether the value chain is aligned to strategic objectives.

The optimal value chain should also inform risk identification by providing a model of business activities within and around the organisation which is cross-referenced to specific strategic objectives. The value chain is also an input to later assessment, evaluation and planning stages in the ERM implementation process. An ERM-enabled organisation can evaluate the risk/return economies associated with its existing value chain configuration and linkages and plan risk response strategies to re-configure its value chain.

## 6. Implementation Stage 2 - Risk Identification

### 6.1 Process

The second iterative step is Risk Identification, which is a transformation process whereby one generates a series of risks and opportunities that are then recorded on the risk register. As it is a process within ERM, it is useful to adopt the philosophy of process mapping, whereby one process exists to make a contribution to one of more of the ERM goals.



The Risk Identification process must be based on a clear understanding of the management and objectives of the overall business or the activities involved. This activity needs to identify risks to the business which would adversely affect the organisation's ability to achieve its objectives and the opportunities, which may be the upside to an identified risk. The output of this activity is a risk register of risks and opportunities.

External or internal risk facilitators can improve the quality of analysis by encouraging experienced staff to adopt a more critical, self-conscious and objective methodology to this activity.

The ERM process will generate a set of terminology which should be managed to ensure consistency of use and meaning amongst participants. The Risk Identification process stage will need to clarify the definitions of 'Risk' and 'Uncertainty'. Failure to create universally understood and accepted definitions will undermine the entire ERM process and create flawed outputs which cannot be implemented.

## 6.2 Risk Register

The output from the Risk Identification process is a risk register which should be mapped across business objectives, value chain activities and their components (people and processes). The risk register should provide a risk breakdown structure and risk taxonomy. The risk register will be developed, refined and revisited throughout the ERM process stages. There may be difficulties deciding where specific risks belong within the register but it is safest to ensure that all risks are recorded and identify any which may not be in the correct position in the register.

The risk register can further be validated via an independently prepared risk checklist based on 'lessons learned' and past experience. This should not prejudice or in any way replace the pre-eminence of the risk register but provides another perspective on the extent of risks which should be included in the register and their associations with business activities.

The risk register needs to be accessible to the ERM team but access needs to be underpinned by protocols to enter new information or make edits to the register. A simple database structure can provide a means of sharing information, controlling changes to the master and developing an information management platform for ERM implementation, communication across the organisation and future development.

Systematic risk and opportunity identification is a facilitated process which can use a combination of different techniques. Facilitation means that the process is controlled and led by individuals who use analytical, arbitration, guiding and influencing skills working with the ERM team to elicit and record the risks to the business activity or project under examination.

## 6.3 Business Risk Structure

A business risk structure can be described as: <sup>4</sup>

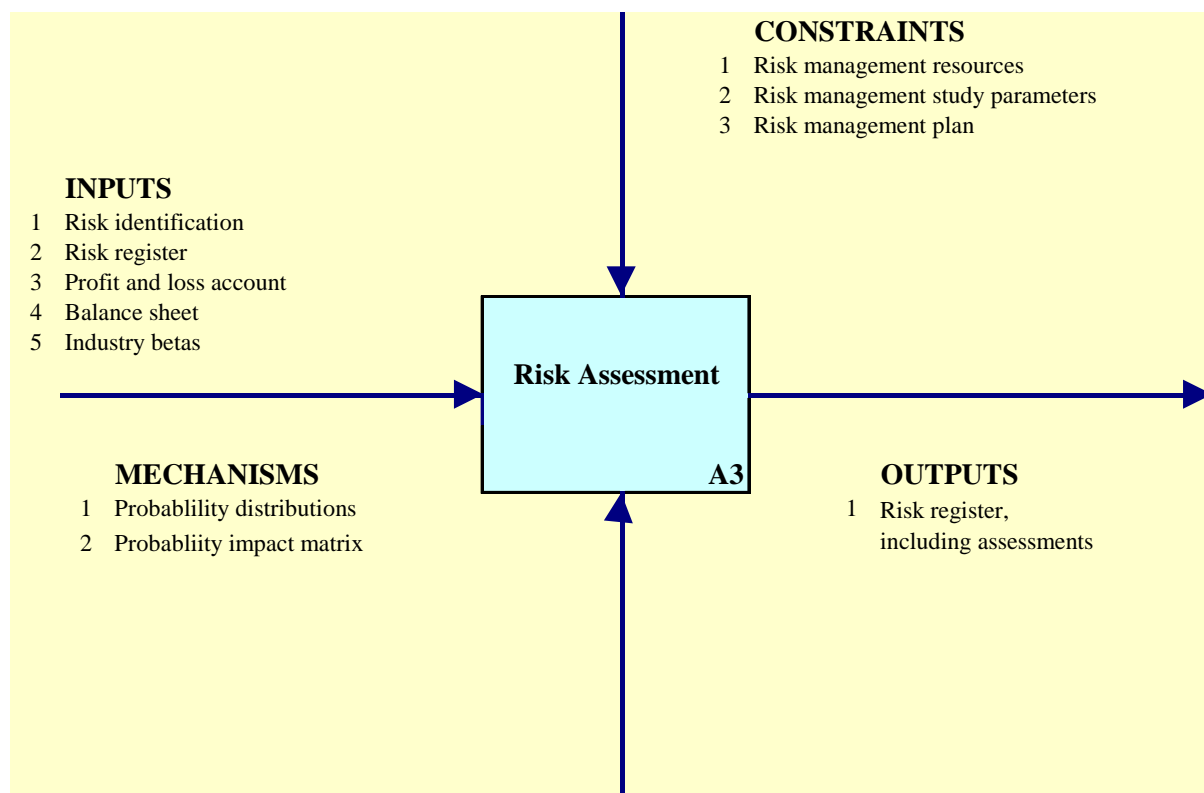
*“A hierarchical decomposition of the business environment through to business processes, assembled to illustrate potential sources of risk. It organises and defines the total extent of business operations established to accomplish the business objectives. Each descending level represents an increasingly detailed definition of sources of risk to the business”*

A risk taxonomy is a form of checklist that defines risks into high-level classes or types and decomposes these classes into elements, attributes and their features. For example, Operational Risk is a class that in turn might have several elements including Strategy, People, Processes and Systems, External Events, Outsourcing. Each element will have attributes, for example, Strategy can include objectives, business plan, new business development, resources, stakeholder interests, corporate experience and reputation. The features of Business Plan (an Element) might include assumptions, currency, and regulatory priorities.

## 7. Implementation Stage 3 - Risk Assessment

### 7.1 Risk Assessment Process

The third iterative step is Risk Assessment, which provides a judgement of the likelihood and impact of the risks and opportunities identified, should they materialise. This process provides an order of the potential ‘pain’ or ‘gain’ associated with risk and opportunity. Even when there is considerable uncertainty, quantitative techniques provide a useful framework.



### 7.2 Probability Distributions

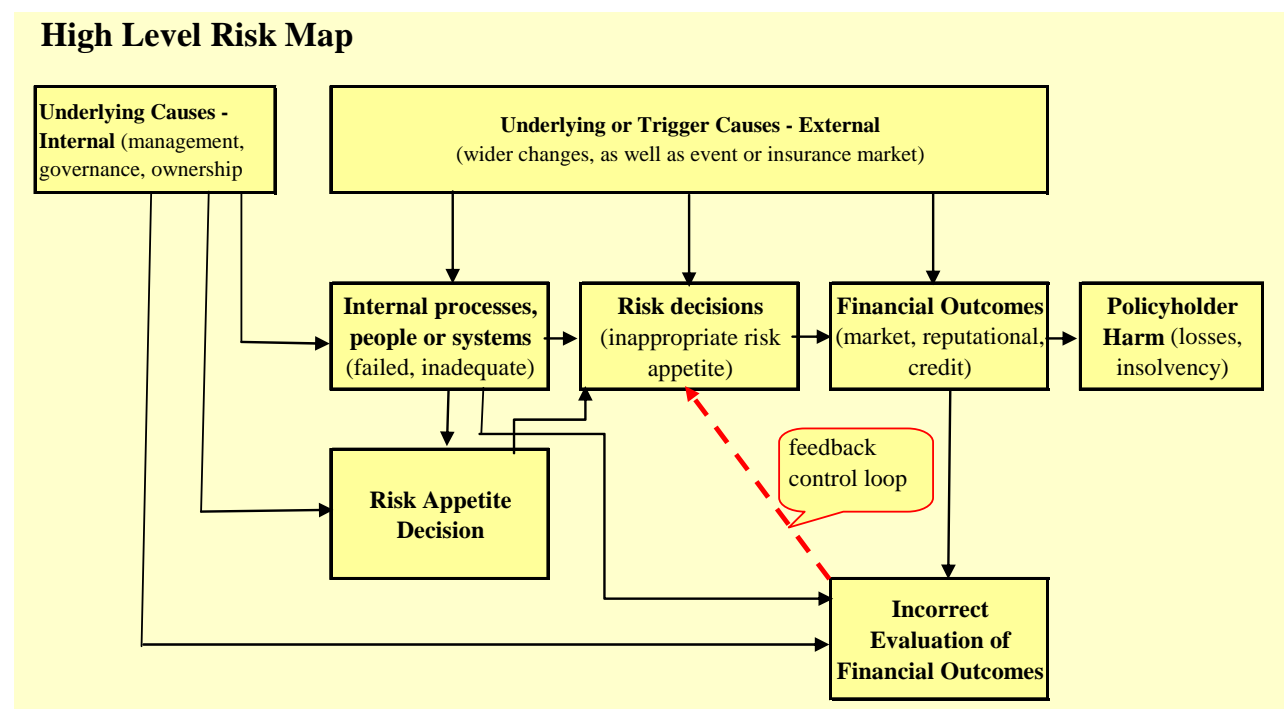
Probability distributions can still be useful even where there is little data (e.g. Normal, Binomial and/or Poisson distributions). The probability impact matrix aims to categorise risks according to the degree of impact they can have on business activities. The matrix needs to have sufficient granularity to reflect different levels of severity attached to different risks.

However, excessive granularity can increase the degree of subjectivity and scope for inconsistency when allocating severity levels. A practical degree of granularity may be to use ‘very high’, ‘high’, ‘medium’, ‘low’ and ‘very low’. This avoids loss of granularity but does not introduce excess granularity and additional subjectivity.

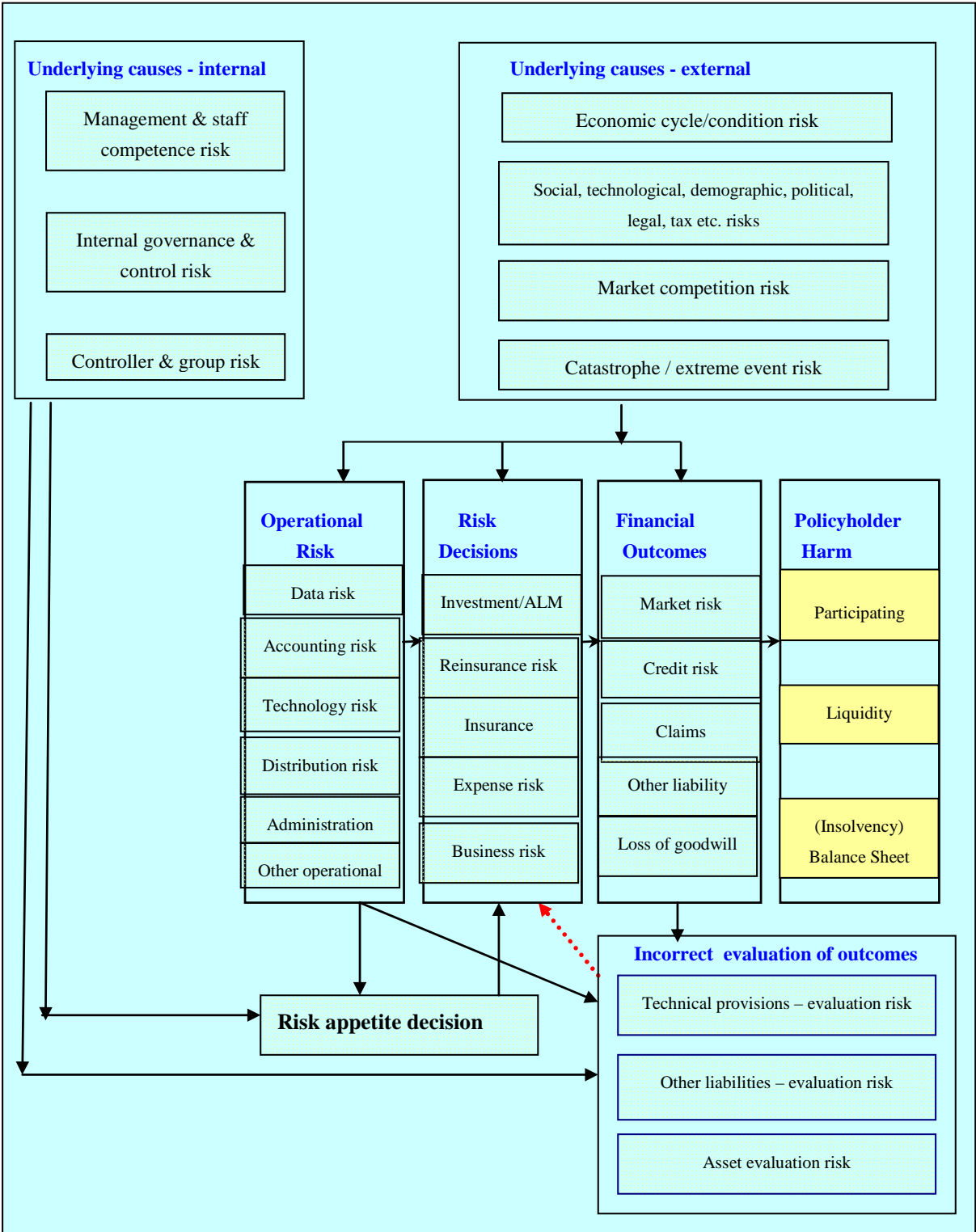
### 7.3 Risk Mapping via Causal Modelling

Causal modelling may be a useful tool to investigate the relations between an effect and its possible causes. A simple technique uses a cause-and-effect diagram. Where appropriate, more complex modelling approaches may be used to help analyse the risk data. However, in many cases risk identification has access to limited relevant data and it is unhelpful to shift attention towards the detail of a more complex modelling solution which is not appropriate to the data available.

Our high-level cause-effect risk map is shown below. It is noteworthy that it has an adaptive feedback control loop, from "incorrect evaluation of financial outcomes" back to "inappropriate risk decisions", which then leads on to "financial outcomes" and then cycles back to "incorrect evaluation of financial outcomes", and so on. The adaptive feedback control cycle loop is managed by examining the output from "incorrect evaluation of financial outcomes" to determine whether there is a continuing need to modify the inputs to "inappropriate risk decisions". In practice, this is a manual process requiring a sound interpretation of the model office outputs.<sup>10 11</sup>



We can drill down from the high-level cause-effect risk map to obtain granularity. Our detailed cause-effect risk map is shown below <sup>10 11</sup>.

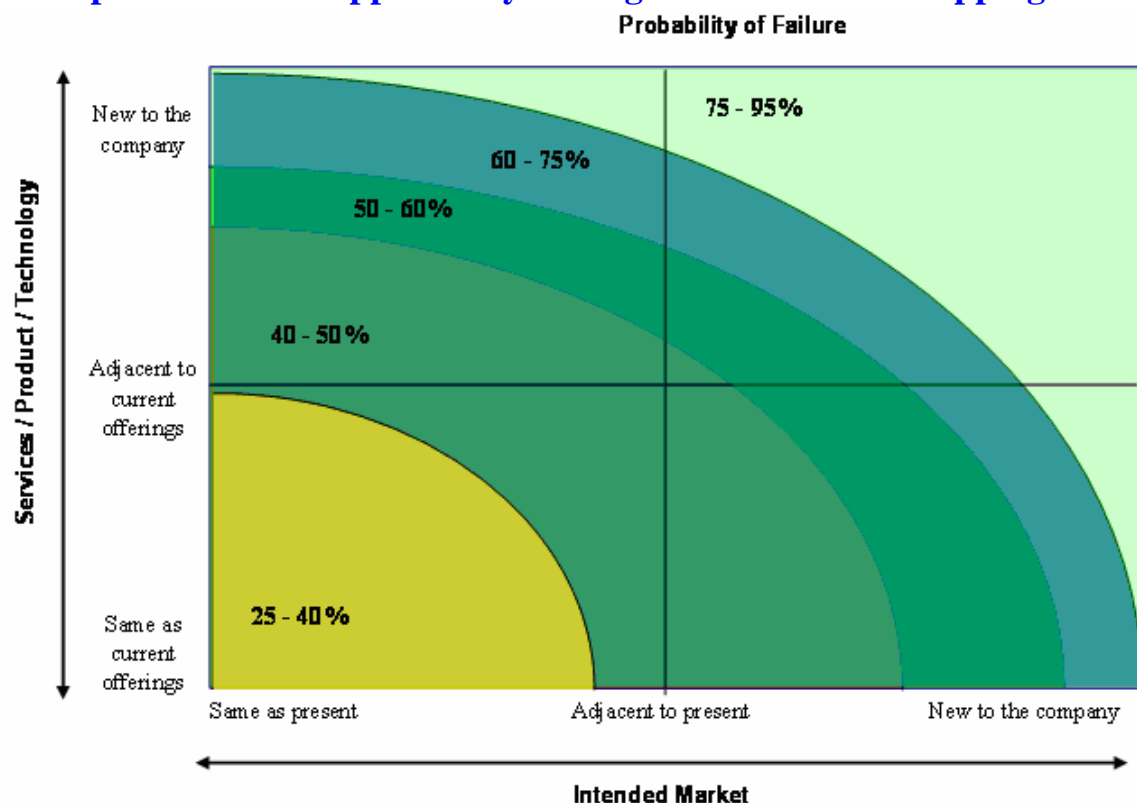


## 7.4 Risk Appetite

The CRO has adopted the Chapman model<sup>4</sup> (as this seemed to be more aligned with the agreed corporate strategy) and started to deal with the effective risk management of the innovation portfolio and the road towards the achievement of the corporate strategy. The balancing of the risks and rewards inherent in the innovation portfolio requires the adoption of a risk matrix<sup>12</sup>, in order to obtain a clearer picture of how its planned projects fall on the spectrum of risk.

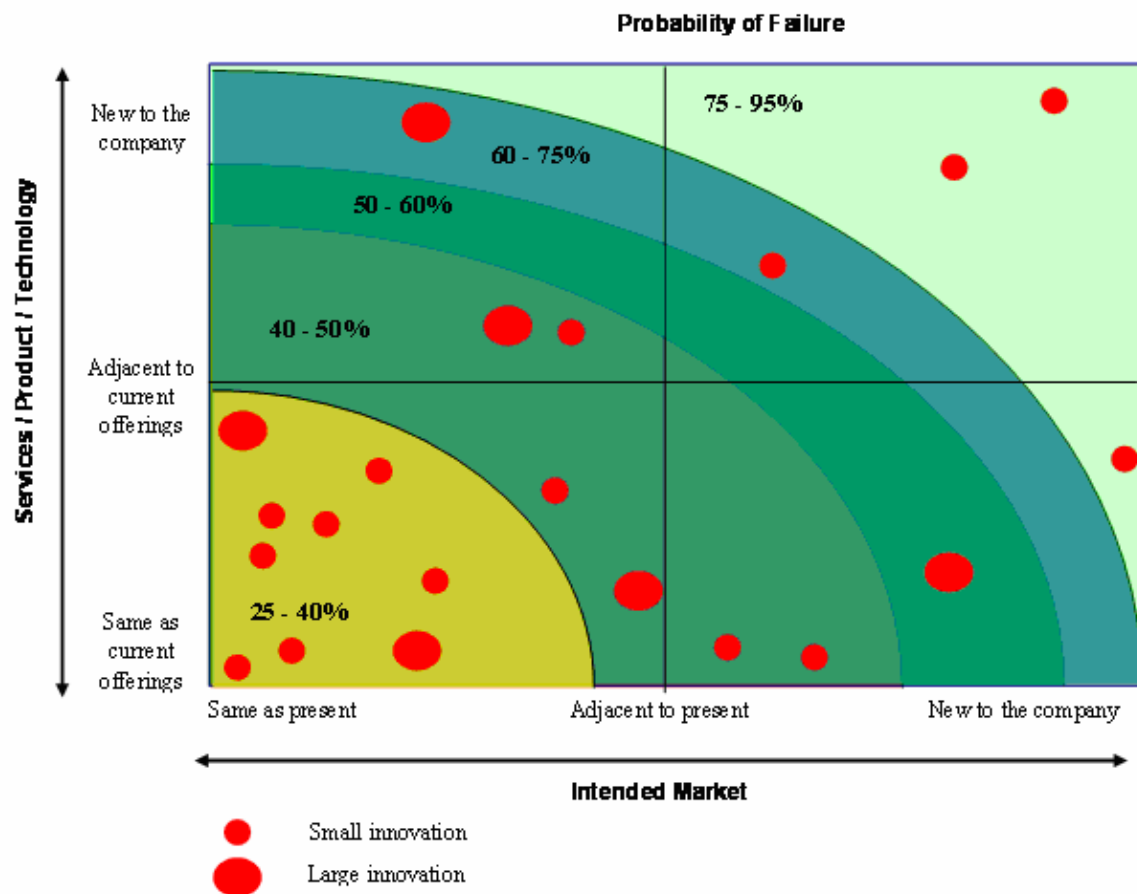
The risk matrix is the output from an experienced, multi-disciplinary team involving senior managers with a strategic focus and authority for financial resource allocation and the participation of team members delivering specific projects. Individual team members are required to position products on the matrix and to provide a rationale to support their risk matrix. Differences and divergences across the team are used to help initiate a continuous process of evaluating the company's mix of projects and their alignment with strategy and risk appetite. The risk matrix model, with probability bands indicating the probability of failure, is illustrated below.

### Example - Risk and Opportunity Management Portfolio Mapping





The innovation portfolio can then be plotted on the risk matrix, as illustrated below. Some of the product/service/technology innovations are categorised as relatively small innovations, whereas others are judged to be relatively large innovations.



The positioning of each innovation product/service on the risk matrix is based on a scoring system, generally using the ordinal scales 1 to 5. Score 1 represents “same as present” whereas 5 represents “entirely different from our present market, or is unknown”. In order to calculate the ‘x’ and ‘y’ coordinates of the product innovation in the risk matrix, one needs to score each of the attributes of the ‘Intended Market’ and ‘Product / Service / Technology’ matrices, and then accumulate the scores.

## 7.5 Risk Heat Maps

Risk heat maps can help management to review the significant risk facing the business. It is important to consider the likely impact as well as the likelihood. The following example provides a graphic based on a typical example <sup>13</sup>.

Impact	Likelihood				
	Rare $0.00 < p < 0.03$	Unlikely $0.03 < p < 0.10$	Moderate $0.10 < p < 0.50$	Likely $0.50 < p < 0.90$	Almost certain $0.90 > p > 1.00$
<b>Catastrophic</b> - the business survival at risk (eg £25M loss)	High	Extreme	Extreme	Extreme	Extreme
<b>Major</b> - operations severely damaged (e.g. £10M loss)	High	High	Extreme	Extreme	Extreme
<b>Moderate</b> - significant time & resources (e.g. £1M loss)	Moderate	Moderate	High	High	Extreme
<b>Minor</b> - some disruption is possible (e.g. £0.5M loss)	Low	Low	Moderate	High	High
<b>Insignificant</b> - minor problem, utilise normal daily processes	Low	Low	Low	Moderate	High

Another example is shown below, based on an insurance company model for a relatively large multinational insurance group.

	Rare $0.00 < p < 0.05$	Unlikely $0.05 < p < 0.30$	Likely $0.30 < p < 0.70$	Probable $0.70 < p < 0.95$	Almost certain $0.95 > p > 1.00$
impact > £300M	Extreme	Extreme	Extreme	Extreme	Extreme
£150M > impact > £300M	Severe	Extreme	Extreme	Extreme	Extreme
£60M > impact > £150M	High	Severe	Extreme	Extreme	Extreme
£30M > impact > £60M	High	Severe	Severe	Extreme	Extreme
£10M > impact > £30M	Moderate	High	Severe	Severe	Extreme
£1M > impact > £10M	Moderate	High	High	High	Severe
£0.5M > impact > £1M	Low	Moderate	High	High	High
£0 > impact > £0.5M	Low	Low	Moderate	High	High








## 7.6 Inherent Risk versus Residual Risk

Risk assessment of the ‘inherent risks’ and the ‘residual risks’ is an important business process and risk management control function for senior management and the ERM implementation team. Having completed the draft risk register, it can be instructive to give further and deeper consideration to the most significant risks that have been identified. In practice, a useful ERM implementation exercise is to review the ‘top 10’ risks and to tabulate the considered risk assessments in respect of the ‘inherent risk’, the ‘control effectiveness’ and the remaining ‘residual risk’. Questions can then be asked about the management control effectiveness measures and assessments.

**Figure 6.10** below provides a useful template for showing this analysis as part of the risk management dashboard approach to an effective ERM framework implementation.<sup>7</sup>

**Figure 6.10 - Top 10 Residual Risks**

Top 10 Residual Risks		Inherent Risk			Control Effectiveness	Residual Risk		
Risk ID	Risk Description	Impact	Likelihood	Risk Severity		Impact	Likelihood	Risk Severity
1	Inappropriate advice provided to clients	5	4	20	2	4	4	16
2	Incorrect payments	6	4	24	3	5	3	15
3	Incorrect limit or conditions being assigned to client	7	3	21	5	5	2	10
4	Key member of staff leaves or is on long term sick leave	5	2	10	5	4	2	8
5	Failure of external supplier	7	2	14	8	6	1	6
6	Business disruption (e.g. due to terrorism, natural disaster)	6	3	18	8	3	2	6
7	Systems failure	3	3	9	7	3	2	6
8	Health and Safety breach	3	2	6	6	2	2	4
9	Breach of regulatory requirements	4	3	12	8	3	1	3
10	External fraud	3	1	3	9	2	1	2

Risk Scoring Key			
<b>Risk severity = Impact = Likelihood</b>		<b>Control effectiveness = Design = Execution</b>	
	Risk rating extreme	score 16+	 score 7-9
	Risk rating high	score 8-15	 score 4-6
	Risk rating medium	score 5-8	 score 1-3
	Risk rating low	score 1-4	

## 7.7 Risk Profiling

Management needs to ensure that the risk profiling process does not become stale or be seen as an end in and of itself. The risk profile is unlikely to change significantly in the short term, unless the insurance business is rapidly changing or growing. A long term view is required, along with secular consistency. One needs to seek out opportunities that will increase the likelihood of the risk profile remaining relevant over time to the management decision making processes. The risk profile reports should provide ‘snapshot’ management information about the significant risks, as indicated in the executive summary report below.<sup>7</sup>

Impact on enterprise value	Likelihood				
	Rare $0.00 < p < 0.05$	Unlikely $0.05 < p < 0.30$	Likely $0.30 < p < 0.70$	Probable $0.70 < p < 0.95$	Almost certain $0.95 > p > 1.00$
impact > £300M	Extreme 11	Extreme	Extreme Risk 7	Extreme	Extreme
£150M > impact > £300M	Severe	Extreme 7	Extreme	Extreme 12	Extreme
£60M > impact > £150M	High	Severe	Extreme Risk 6	Extreme	Extreme
£30M > impact > £60M	High 1	Severe 6	Severe 10	Extreme	Extreme
£10M > impact > £30M	Moderate	High 8	Severe	Severe	Extreme
£1M > impact > £10M	Moderate	High	High 3	High 4	Severe
£0.5M > impact > £1M	Low 2	Moderate	High	High	High
£0 > impact > £0.5M	Low	Low	Moderate 5	High	High 9
Control effectiveness →	High ●	Medium ●	Low ●	Opportunity ●	

Inherent  
Residual Risk

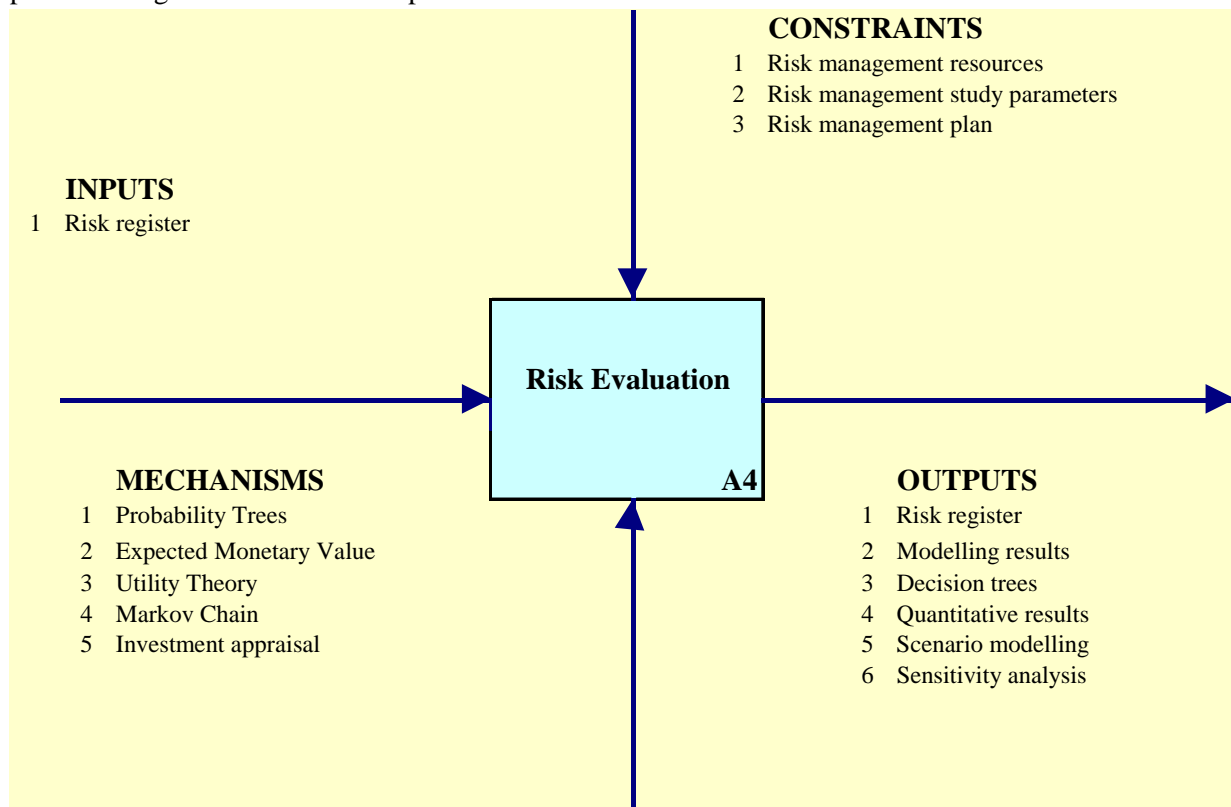
## 7.8 Risk Identification and Assessment Workshops

Organising regular and ad-hoc risk assessment exercises can help to create risk awareness in the organisation. Risk assessments can be conducted from different perspectives e.g. business unit, distribution channel, customer, product group to create comprehensive and rigorous discussion and prioritisation of risks. This process can help to change how managers and employees perceive risk assessment and risk, not as an adjunct to running the business but as an integral part of running the business. The aim is to build risk into all business decisions and activities rather than seeing risk management as the responsibility of a single, specialised line function

## 8. Implementation Stage 4 - Risk Evaluation

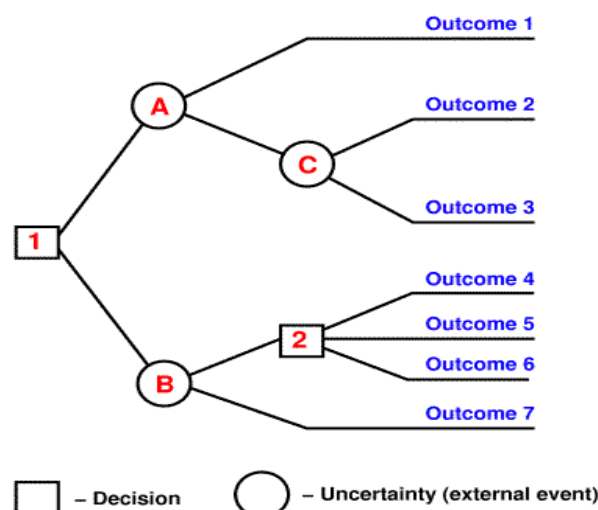
### 8.1 Risk Evaluation Process

The fourth iterative step is Risk Evaluation, which involves evaluation of the results of the risk assessment stage and includes an understanding of the inter-relationships between the individual risks and the opportunities. It provides an iterative process of challenge and refinement of the information captured during the risk assessment process.



### 8.2 Risk Evaluation Mechanisms

Decision analysis may also be helpful to gain insight into decisions in response to experienced problems, uncertain events and the values of outcomes. This information can then be used to apply to influence diagram techniques. The output from the influence diagram can be used to construct a decision tree.



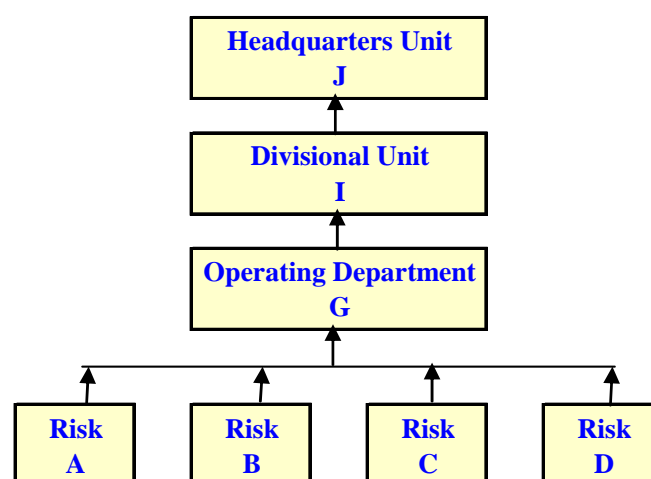
### 8.3 Decision Tree Analysis

The probability and impact of various combinations of multiple risks occurring is often a major concern. Decision tree analysis is a simple, and often graphical, technique to connect multiple risk combinations to come up with some estimates of the outcomes. A technique that historically was used in project planning critical path charts, it can be an effective technique for looking at probabilities covering a limited set of risks. The process is particularly useful for looking at related risks. That is, we may have one risk that may or may not occur, but there will be related risks with their own likelihood probabilities. Using decision tree analysis and the rules of joint probability, we can assess the likelihood of multiple risk events. The real strength of the decision tree graphical approach is to illustrate the impact that certain risks may have on subsequent risk-based matters. A risk event at a small unit may have an impact on other elements of operations when all of these risks are strung together. It can be a useful risk analysis tool.

### 8.4 Risk Interdependencies

Risk interdependencies will need to be considered. As illustrated below, activities **A, B, C,** and **D** all operating in parallel and reporting to activity or unit **G** and then to unit **I** and ending with unit **J**. One can think of this as separate operating entities in an overall enterprise or as operating departments with a single plant or facility. In an ERM sense, risks should be identified and assessed at each of these levels. Each of the **A, B, C,** and **D** risks would often be independent of each other, although some would often be common. That is, each of these units may share the same risks but with potentially different likelihoods and significances. However, operating department **G** must consider the impact of the separate risks at each of these units. These separate risks will impact **J**, but that unit must evaluate the nature of those individual unit risks.

Error! Bookmark not defined.



The concern here is that risk interdependencies must be considered and evaluated throughout the organisational structure. Any entity should be concerned about risks at all levels of the organisation but only really has control over the risks within its own sphere.

## 8.5 Risk Ranking

An organisation that carries out a risk ranking and assessment process might end up with a long list of potential risks. They will then need to consider the established significance and likelihood estimate, calculate risk rankings, and identify the most significant risks.

The likelihood and significance scores show where these risks would be plotted on a risk assessment analysis chart and the product of these two gives their relative risk ranking. Risks **C** and **G** have the highest risk rank scores and would be plotted in the upper-right-hand quadrant as the most significant risks in this sample. Risks **C** and **G** represent the ‘risk drivers’ or ‘primary risks’, which should then become the focus of management attention.<sup>14</sup>

Identified Risk	Significance Probability (P)	Likelihood Probability (L)	Risk Score (P x L)	Rank
A	0.55	0.30	0.17	8
B	0.88	0.24	0.21	7
C	0.79	0.66	0.52	1
D	0.77	0.45	0.35	4
E	0.35	0.88	0.31	5
F	0.54	0.49	0.26	6
G	0.62	0.72	0.45	2
H	0.66	0.20	0.13	9
I	0.90	0.45	0.41	3
J	0.12	0.88	0.11	10

It is important that the risk ranked schedules are organised on a business unit basis and adjusted to accommodate all related risks, including those above and below the business unit level.

For example, unit **A** may face a risk that a drop in its production quality will lower its unit's sales and profitability. Another unit **B** might have its own production quality risks but may lose business in its operations because of unit **A**'s production problems. The headquarters unit **C** may be subject to the production quality risks at its subsidiary units. Unit **C** will need to recognise this and identify the risks from unit **A** and unit **B**. Furthermore, there may be an escalation risk up to the headquarters unit **C** if adverse publicity arises from the risk incidents occurring at unit **A** or unit **B**. This could result in a reputational risk exposure that the headquarters unit **C** will need to address.

The ERM team will need to identify these unit-by-unit risk, and their risk interactions, in order to ensure that risks at all levels have been assessed and the likelihood and significance estimates are appropriate. In practice, risk events that have occurred far away from the headquarters unit have sometimes resulted in major problems for the whole enterprise.



## 8.6 Scenario Modelling Case Studies

Case studies from real life can provide a useful risk management tool to facilitate scenario modelling, scenario planning and stress testing.

## 8.7 Case Study 2

This case study illustrates how a small foreign subsidiary can severely damage a global enterprise.<sup>15</sup>

In December, 1984, over 40 tons of poisonous gases leaked from a pesticide factory in Bhopal, India, belonging to Union Carbide, killing more than 20,000 residents. After much corrective action and legal wrangling, Union Carbide, which built the plant in 1969, settled a civil suit brought by the Indian government in 1989 by agreeing to pay US\$470 million for damages suffered by the 500,000 people who were exposed to the gas. The company maintained that the payment was made out of a sense of 'moral' rather than 'legal' responsibility since the plant was operated by a separate Indian subsidiary, Union Carbide India Ltd.

The court proceedings revealed that management's cost cutting measures had effectively disabled safety procedures essential to prevent or alert employees of such disasters. Dow Chemical has since taken over Union Carbide and denies responsibility for this disaster. However, because of the large loss of life there and the fact that Dow Chemical is much larger than what was once Union Carbide and its Union Carbide India Ltd. subsidiary, ongoing litigation continues to haunt Dow Chemical. The Bhopal gas leak is an example of how a risk event at a distant and relatively small unit can have disastrous consequences on a firm.

This case study demonstrates the need for thorough 'risk identification' and 'risk assessment' processes that consider catastrophic incidents, such as one this magnitude. Each operational business unit needs to recognise the likelihood and consequences of the risks that they face. A risk event at a small foreign subsidiary can bring down the entire enterprise - risk management at all levels should recognise that catastrophes can happen. We can never predict risks of this major consequence, but an enterprise should always be aware that disasters can happen.

## 8.8 Case Study 3

This case study illustrates that an organisation is only as strong as its weakest link.<sup>15</sup>

For most of the 20<sup>th</sup> century, Andersen LLP was one of the world's leading independent accountancy firms. Its practices set the standard for the field and its corporate ethics were considered by many to be impeccable. However, in less than 12 months, its reputation was destroyed as a result of its dealings with Enron and the aftermath. The organisation imploded as a result of reputational damage caused a small number of staff in one of its offices.

The demise of Arthur Andersen LLP following the Enron collapse illustrates the need to consider risks throughout the enterprise. Although their local offices had risk assessment procedures and almost all followed firm wide standards, a risk event at one offices (Houston) and perhaps at the legal affairs department, caused the global firm to collapse. An operating office in another area, such as Toronto, might not have even fully anticipated such risks in faraway Houston. Each operating unit was responsible for managing its own risks but was also subject to the consequences of risk events on units above or below each in the organisational structure.

With the benefit of hindsight, it appears that the organisation had lost sight of its core business model, which was that of an independent auditing firm. That independence was compromised by its close relationship with the executive management team at Enron. The large fees that it collected from its auditing and consultancy activities resulted in professional conflicts of interest. Its endeavours at this rogue office to protect its consultancy fees had compromised its auditing standards. The public disclosure that it had shredded tons of documents (e.g. its Enron working papers and files) gave the appearance that it had something to hide. The public outrage and resulting damage to its reputation was particularly acute as so many innocent parties, such as employees and small investors, were irretrievably harmed and the firm imploded.

Although the firm had 'errors and omissions' liability insurance, this proved inadequate and the equity partners were called upon to meet the excess claims. This case study demonstrates reputational loss can be swift and that an organisation is only as strong as its weakest link. It is also underlines the need for corporate governance and a thorough consideration of reputational loss exposure. Had the senior executive team been wide awake, they would almost certainly have changed their business processes and controls to review and the act upon their reputational risk exposure.

## 8.9 Case Study 4

This case study illustrates how corporate culture can affect ERM outcomes.<sup>15</sup>

Ericsson, a major Swedish company, was a major global force in telecommunications and in the mobile telephone industry (with an almost 40% worldwide market share). However, its corporate culture was more conservative and less pro-active than Nokia and this contributed to its operational risk losses following a catastrophic incident at one of its major suppliers.

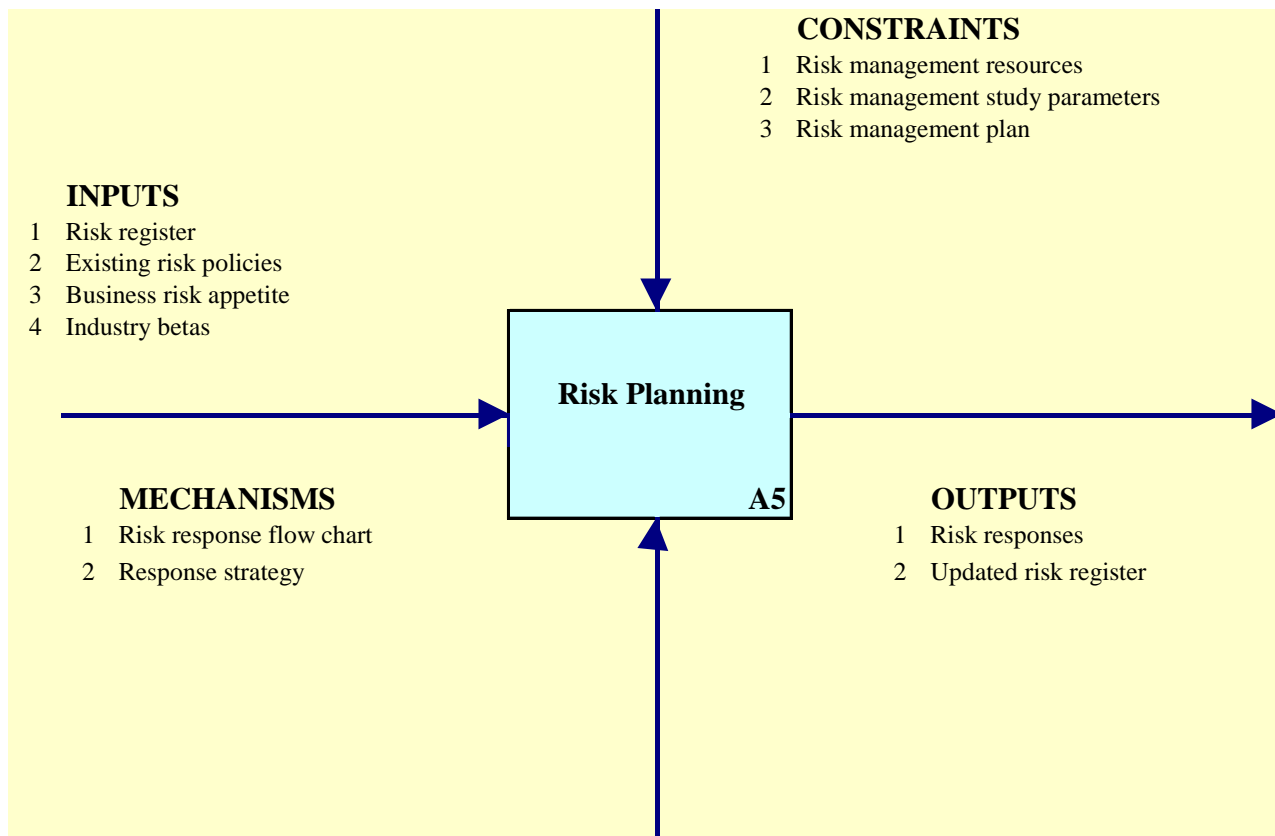
In March 2000, lightning started a small fire in the Phillips factory in New Mexico that manufactured silicon chips for its major mobile telephone customers, which included Ericsson and Nokia. The Ericsson local management team was slow to report the 'disruption of supply' and logistics problem to the senior management team at its global headquarters. They assumed that the disruption of supplies would not last long and so there was no need to escalate the disruption of supplies issue. Nokia, on the other hand, was pro-active and pressured Phillips to immediately locate substitute suppliers. The Nokia local management team quickly referred the disruption of supplies problem to its global headquarters, whereupon its senior management team pressured the Phillips senior executives to ensure that production (as far as silicon chip supplies to Nokia was concerned) was not materially interrupted.

With the benefit of hindsight, the difference in corporate culture (between Ericsson and Nokia) contributed to Ericsson's lack of focus on the supplies items over which it thought (at the local management level) that it had no control and made it vulnerable to any disruption. The aftermath was that Ericsson was unable to locate substitute suppliers and ended up reporting a financially significant global loss in its mobile telephone division for that year. It also lost its global industry leadership and has not yet recovered its former glory.

## 9. Implementation Stage 5 - Risk Planning

### 9.1 Risk Planning Process

The fifth iterative step is Risk Planning, which combines the risks and opportunities together and considers their combined effect. It uses the preceding ERM processes to produce responses and specific action plans to address the risks and opportunities identified to secure the business objectives; it is essential that these plans are prepared, considered, refined and implemented.



### 9.2 Risk Response Register

The Risk Planning activity generates a series of risk responses which document, at the most basic level, the 'risk ID', risk description, impact in terms of time and cost, the risk response strategy to respond to the risk or opportunity. Each 'risk ID' must be referenced to an owner, manager and personnel who are responsible for taking action, the date or timescale by which actions must be implemented, the cost of the risk response strategy and any secondary risks which may arise from the risk response strategy.

### 9.3 Risk Planning – Review Risk Evaluations

Having assessed and identified its more significant risks, the next step is to determine how to respond to these various identified risks. This is a management responsibility to perform a careful review of estimated risk likelihoods and potential impacts, and with consideration given to associated costs and benefits, to develop appropriate risk response strategies. These risk responses can be handled following any of four basic risk management approaches: <sup>14</sup>

1. **Avoidance.** This is a strategy of walking away from the risk. This might involve: (a) selling a business unit; (b) exiting from a geographic area of concern; (c) dropping a product line. The difficulty here is that organisations sometimes do not drop a product line or walk away until after the risk event has occurred. In practice, it is difficult to walk away from a business area or product line just on the basis of a potential future risk if all currently appears to be satisfactory. Avoidance is sometimes perceived to be a potentially costly strategy if significant investments were made, followed by a subsequent divestment to avoid the risk.
2. **Reduction.** A wide range of business decisions may be able to reduce certain risks. Product line diversification may reduce the risk of too strong a reliance on one product line. For example, dividing an IT operations centre into two geographically separate locations is likely to reduce the risk of operational losses from a catastrophic failure.
3. **Sharing.** Organisations routinely share some of their risks by purchasing insurance to hedge or share their risks. For example, financial transaction risks can be shared via hedging operations to protect from possible price fluctuations. Another example of risk sharing of potential business risks and rewards is via strategic alliance partners or joint venture agreements.
4. **Acceptance.** The ‘acceptance’ is essentially to retain the risk by actively deciding to take no further risk management action. An enterprise can self-insure rather than purchase an insurance policy. They might regularly put aside resources to cover or shield them from some event. Essentially, an organisation should look at a risk's likelihood and impact in light of its established risk tolerance and then decide whether or not to accept that risk. For the many and varied risks that approach an organisation, acceptance is often the appropriate strategy for some risks.

## 9.4 Risk planning - Risk Optimisation

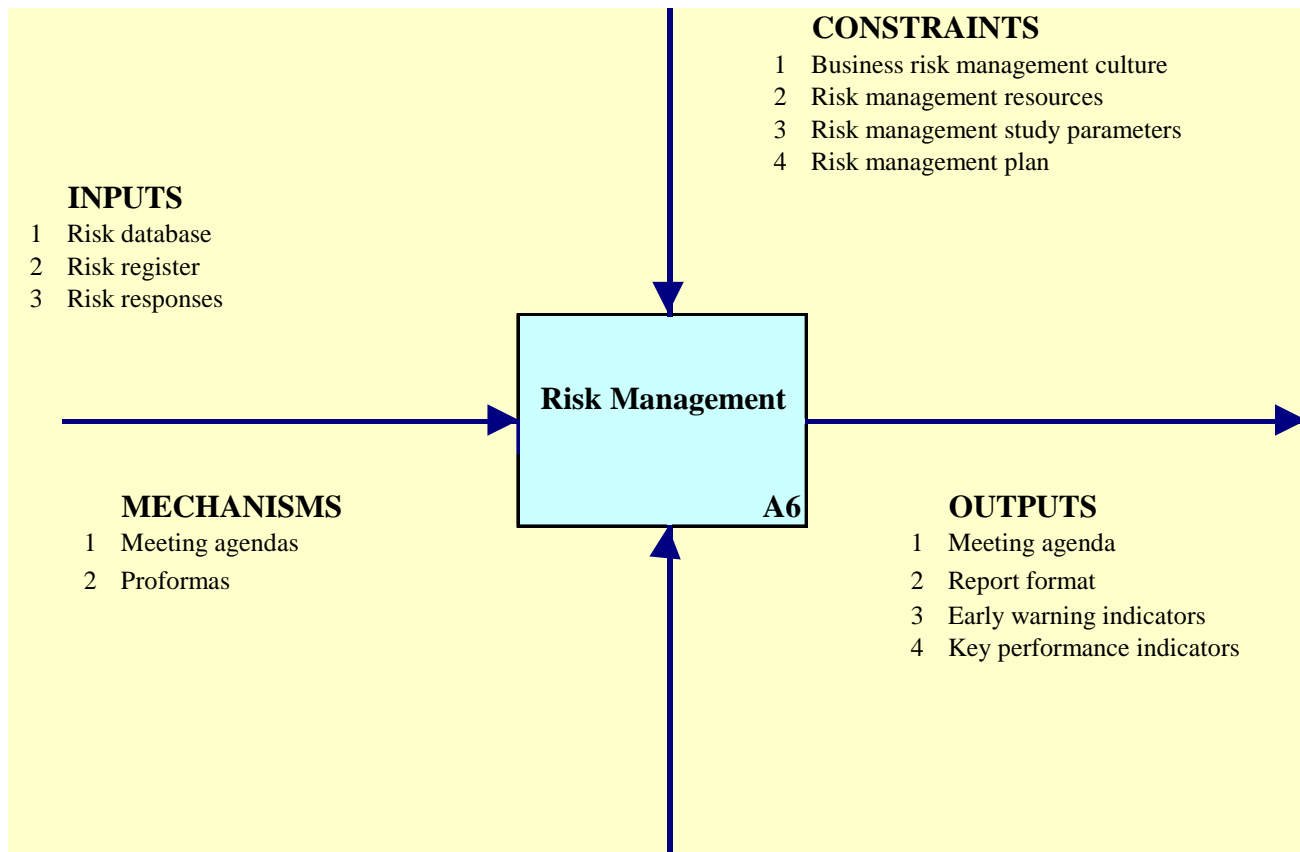
Risk planning should also be considered holistically in order to support a risk optimisation strategy. For example, Lam <sup>16</sup> provides an example of an insurer providing home owner cover against damages caused by natural catastrophes such as hurricanes. Purchasing reinsurance reduces the net expected return for the insurer but reduces the risk of insolvency due an extreme weather event (or series of events). Increasing volatility of loss is linked to increasing frequency of severe weather events. The reinsurance contract transfers the insurer's unpredictable hurricane risk to the reinsurer and, potentially, transforms the risk to a more predictable credit risk in the context of the reinsurer. Organisations also need to adopt a risk optimisation strategy which can be aligned to stakeholder expectations. For example, powerful customer segments may exist who are unwilling to accept any degree of risk transfer.

Lam <sup>16</sup> provides an example of a manufacturer who has powerful overseas customers who are unwilling to assume any foreign currency risk exposure and will only pay in their national currency. The manufacturer must also satisfy its shareholders expectations for steady growth in revenues and profits. In the example the manufacturer adopts a strategy based on seeking third-party protection against risk via forward contracts based on exchanging a fixed rate of currency at a predetermined exchange rate.

## 10. Implementation Stage 6 - Risk Management

### 10.1 Risk Management Process

The sixth iterative step is Risk Management, which consolidates all the previous steps. In fact, all of the six steps are iterative and it is frequently necessary to revisit earlier steps when more information becomes available or circumstances change, as each stage relies upon inputs from the earlier stages. All risk management process maps should state a need to ensure that the risk responses to identified risks are implemented and that the implementation is pro-actively managed.



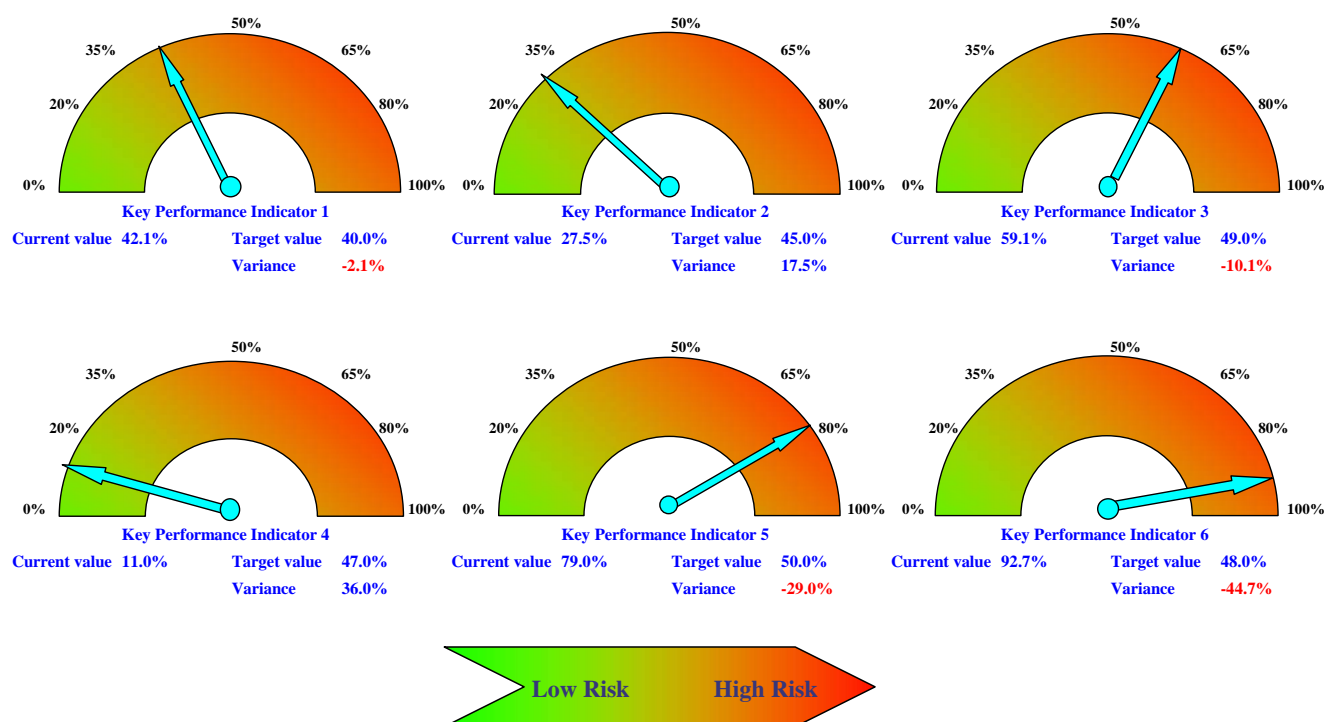
Risk management consists of executing, monitoring and controlling all risk management actions against the actions and parameters contained in the risk plan. Ensuring execution means compliance with the risk plan and identifying rationale for any deviation.

Monitoring should be a passive, neutral exercise which needs to assess how people and processes are working, that the ERM process is 'alive' and alert to emerging signals in the internal and external business environment e.g. are new risks and opportunities being identified and correctly cascaded through the ERM stages. It is important that any signals of change are fed backwards or forward to the appropriate ERM activity stage.



## 10.2 Using early warning indicators and key performance indicators

Changes arising from the business analysis need to be explored and fed forward into the risk identification stage and downstream to update the risk assessment, evaluation, planning and inform risk management. Early warning indicators and key performance indicators are outputs from this ERM process stage. The example KPI grid below indicates actual or current values for key indicators against a target value.



The construction of a 'watch list' or dashboard of priority information should underpin reporting activity. This approach would concentrate on KPI, residual risks, assess the severity of the emerging risk and the effectiveness of control mechanisms. The use of visuals to produce 'heat maps' indicating all substantial, quantifiable risks is also a useful tool. The dashboard needs to be underpinned by an information underlay which enables fast and flexible access to the underlying experience and data.

### **10.3 ERM Reporting Framework**

The ERM reporting framework needs to provide timely, accurate and focused analysis of:

- Emerging and known financial risks
- Efficacy of risk response strategies
- Implications for business analysis
- Identify emerging changes in risk profile and exposure
- Assess the outcome and effectiveness of controls

### **10.4 Risk Management Control Function**

The guidelines that should inform the control function are similar to those applied to the ERM reporting function. Controlling requires focused action to intervene and take remedial action where necessary. The control function needs to have sufficient flexibility to be 'fleet of foot' and make rapid changes in direction based on emerging experience. The controls applied need to be simple, focused and flexible to provide a rapid, first response to situations where risk response actions have not been implemented, implemented incorrectly or are proving inadequate.

### **10.5 Risk Management - Case Study 5**

Organisations such as Microsoft have attempted to embed risk management within project planning, processes and activities.<sup>17</sup>

Web-based knowledge tools have been developed in association with the risk management group. The Microsoft intranet includes risk checklists, best practices and factual, reference information for managers and staff. The core risk management group are evaluated on the amount of time they spend working 'hands-on' with managers on risk issues. The risk management group is engaged in building risk awareness in managers and leveraging wisdom from them. "The job of the risk management group is to learn from them and see how we can leverage the wisdom gained across the enterprise and share best practices. Further, perhaps we can add some incremental value by providing information they have not considered." (Microsoft Risk Group Manager).

The Risk Management stage consolidates all the previous steps by generating a watch-list of early warning indicators; ensures that managers and staff responsible for specific risk planning actions are responsive and alert; and maintains the risk register as a living, dynamic document which is updated to allow for emerging signals of risk and opportunity and the organisational learning experience.

## 10.7 Risk Management - Case Study 6

The public sector has developed practical guidance to assist governments and government agencies in developing ERM frameworks and risk response strategies to manage outcomes of policy implementation, extreme events (natural and man-made) and increasing consumer activism where the State is deemed to under-deliver or fail in delivering its legal responsibilities and duties.

The Strategy Unit of the UK Cabinet Office first published a report in 2002 that describes how handling risk and opportunity is increasingly perceived at the centre of good government<sup>18</sup>. Public sector ERM focus is driven by the public sector's need to do more to anticipate risks so that there are fewer unnecessary and costly crises (citing BSE and failed IT contracts as examples); to ensure that risk management is part of the delivery plans; get the right balance between innovation and change on the one hand and avoidance of shocks and crises on the other; and, finally, to improve the management of risk and its communication.

The report concludes that, at the strategic level, the risk appetite concerns are about where the organisation wants to go, how to get there and how to ensure survival. Any major risks at this level are likely to stop the organisation functioning. Risks at this level are typically concerned with commercial, financial, directional, environmental, cultural, acquisition, political and quality issues. The following graphic provides a public sector perspective on the separation required between strategic-level, programme-level and operational-level decisions.<sup>18</sup>



## References

- 
- <sup>1</sup> Orros, George and Howell, Jane. (2008). *Creating Value through Integrated ERM for Healthcare Insurers in Europe*. (2008), ERM Symposium 2008, sponsored by the Joint CAS/CIA/SOA Risk Management Section, The Actuarial Foundation, and the PRMIA, USA, published via <http://www.ermssymposium.org/pdf/papers/Orros.pdf>
- <sup>2</sup> Orros, George. (2007a). *ERM Literature Review*, GIRO 2007 Convention, Institute and Faculty of Actuaries, published via [http://www.actuaries.org.uk/files/proceedings/giro2007/BHPrize\\_Tripp\\_Appendices.zip](http://www.actuaries.org.uk/files/proceedings/giro2007/BHPrize_Tripp_Appendices.zip) and via [http://www.actuaries.asn.au/NR/rdonlyres/1C5D0157-1B4E-4059-B75E-32F751723D99/2811/ERM\\_LitRev\\_Main\\_180807.pdf](http://www.actuaries.asn.au/NR/rdonlyres/1C5D0157-1B4E-4059-B75E-32F751723D99/2811/ERM_LitRev_Main_180807.pdf)
- <sup>3</sup> Orros, George. (2007b). *ERM Bibliography and Literature Review*, GIRO 2007 Convention, Institute and Faculty of Actuaries, published via [http://www.actuaries.org.uk/files/proceedings/giro2007/BHPrize\\_Tripp\\_Appendices.zip](http://www.actuaries.org.uk/files/proceedings/giro2007/BHPrize_Tripp_Appendices.zip) and via [http://www.actuaries.asn.au/NR/rdonlyres/1C5D0157-1B4E-4059-B75E-32F751723D99/2812/ERM\\_LitRev\\_Annex\\_180807.pdf](http://www.actuaries.asn.au/NR/rdonlyres/1C5D0157-1B4E-4059-B75E-32F751723D99/2812/ERM_LitRev_Annex_180807.pdf)
- <sup>4</sup> Chapman, Robert J. (2006). *Simple Tools and Techniques for Enterprise Risk Management*. John Wiley & Sons, Inc., New Jersey, USA
- <sup>5</sup> Taleb, Nassim N. (2007). *The Black Swan: the Impact of the Highly Improbable*. Allen Lane, an imprint of Penguin Books, London England.
- <sup>6</sup> Rumsfeld, Donald. (2002). *Department of Defense news briefing*, February 12, 2002, published via <http://www.quotationspage.com/quote/30526.html>
- <sup>7</sup> International Actuarial Association. (2008). *Practice Note on Enterprise Risk Management for Capital and Solvency Purposes in the Insurance Industry*, Final 11 August 2008, International Actuarial Association. Published via [http://www.insurance.naic.org/documents/committees\\_e\\_isawg\\_IAA\\_ERM\\_draft.pdf](http://www.insurance.naic.org/documents/committees_e_isawg_IAA_ERM_draft.pdf)
- <sup>8</sup> Garratt, Robert. (2003). *The Fish Rots from the Head: The Crisis in Our Boardrooms - Developing the Crucial Skills of the Competent Director*, published by Profile Books Ltd., London, England.
- <sup>9</sup> Orros, George et al. (2008). *Enterprise Risk Management from the General Insurance Actuarial Perspective* (2008), Institute of Actuaries, London [http://www.actuaries.org.uk/\\_data/assets/pdf\\_file/0017/132038/sm20080428.pdf](http://www.actuaries.org.uk/_data/assets/pdf_file/0017/132038/sm20080428.pdf)
- <sup>10</sup> Orros, George et al. (2004). *Measurement or Bust*, Operational Risks Working Party, 2003 GIRO Convention, Institute of Actuaries, Oct 2003, <http://www.actuaries.org.uk/files/pdf/proceedings/giro2003/Tripp.pdf>.
- <sup>11</sup> Orros, George et al. (2004). *Quantifying Operational Risk in General Insurance Companies*, Institute of Actuaries, March 2004, published via <http://www.actuaries.org.uk/files/pdf/sessional/sm20040322.pdf>
- <sup>12</sup> Day, George S. (2007). *Is it Real? Can We Win? Is It Worth Doing? : Managing Risk and Reward in an Innovation Portfolio*, Harvard Business Review, December 2007.
- <sup>13</sup> International Actuarial Association. (2008). *Practice Note on Enterprise Risk Management for Capital and Solvency Purposes in the Insurance Industry*, Final 11 August 2008, International Actuarial Association. Published via [http://www.insurance.naic.org/documents/committees\\_e\\_isawg\\_IAA\\_ERM\\_draft.pdf](http://www.insurance.naic.org/documents/committees_e_isawg_IAA_ERM_draft.pdf)
- <sup>14</sup> Moeller, Robert R. (2007). *Enterprise Risk Management: Understanding the New Integrated ERM Framework*, John Wiley & Sons, Inc., New Jersey, US
- <sup>15</sup> Skipper, Harold D. and Kwon, W, Jean. (2007). *Risk Management and Insurance: Perspectives in a Global Economy*, Blackwell Publishing Ltd., Oxford, England.
- <sup>16</sup> Lam, James (2003). *Enterprise Risk Management - from Incentives to Controls*. John Wiley & Sons, Inc., New Jersey, USA.
- <sup>17</sup> Barton, Thomas L. et al. (2002). *Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management*, published by FT Press, Prentice Hall, Canada.
- <sup>18</sup> Cabinet Office (2002). *Risk Improving Government's Capability to Handle Risk and Uncertainty*, Strategy Unit, Cabinet Office, HM Government, London, UK.