

# Chapter 1

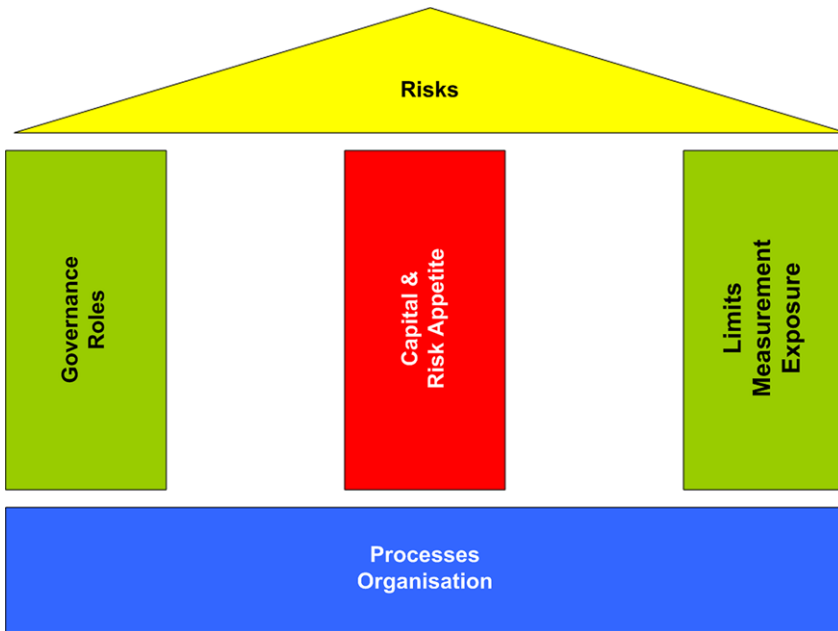
## What is Risk Management



### 1.1 Introduction

#### *1.1.1 Raison D'être of Risk Management*

In order to understand the need for risk management it is necessary to look at the different building blocks of a holistic risk management. Figure 1.1 tries to decompose the risk management into its generic components. The overall aim is to manage the risks a company is facing. All employees in the company are expected to some larger or smaller extent to manage risks in order to limit a potentially adverse out-



**Fig. 1.1** Overview

come and to generate profit and stability for the stakeholders of the company. The corresponding risk culture is of paramount importance. An open communication and a clear and unbiased view in respect of the risks are essential in order to become a professional risk-taker.

In order to control these risks it is first necessary to analyse and categorise the risks into its components. This decomposition is described in section 1.2.1.

After understanding the risks and their impact on the stakeholders, it is essential to understand what are the foundations and the pillars which allow us to operate in such a way that we manage risks in an optimal manner.

The foundations of each company are its organisation and its processes. Therefore it is necessary to define the relationship between these foundations and the risks. The second foundation of each organisation are its processes. Here the escalation processes (section 15.1.3) are particularly important, since they define how to behave in the case a risk “gets out of control” and “needs to be fixed”. The generic risk management process, in chapter 5, helps to better analyse the risks in a consistent way and hence ensures better communication, understanding and analysis within the insurance company.

The three pillars which ensure that risks are taken in a conscious and value enhancing way are:

- Governance and roles,

- Capital and risk appetite, and
- Measurement, limits and exposure.

Each of the pillars has a particular purpose:

**Governance and Roles:** In order to ensure a “fit and proper” management it is essential to have adequate governance in place. A common understanding of the various parts within the organisation is of paramount importance. The corresponding definitions, that cover part of the roles and responsibilities are documented in section 15.1.1. Together with the generic governance principles (section 15.1.2) they form the corner stones of the company’s governance structures. The governance structures are further detailed in section 15.10.

**Capital and Risk Appetite:** Risk can be defined as a potential adverse outcome, and it can normally be measured in monetary terms. The capital resources available to the company serve as a buffer in order to limit the need for fresh capital to prevent bankruptcy. Hence it is of utmost importance to know the available resources (which can serve as buffer) and to ensure that the risk appetite is commensurate with the company’s strategic aims (e.g. rating, capital level, etc.) and the limits imposed by its stakeholders (Board of Directors, regulators, etc.). This relationship is documented in chapters 2, 4 and 10.

**Measurement, Limits and Exposure:** The last pillar defines how to measure risk. This is particularly important in order to have reliable information for knowing the actual risk profile. To ensure that the company operates within its risk appetite, some of the risks are limited by a *limit system*. An example could be, that the company does not want to invest more than 10% of its assets in shares. How this is done, is documented in chapters 6 and 7.

Having all the before mentioned parts in place, means that the insurance company is a professional risk taker, which aims to outperform the market and its peers. This can *only* be achieved if everybody is responsible for risk management. The risk management function acts as an enabler and consolidator.

### ***1.1.2 The Role of Risk Management***

The role of risk management can be summarised as follows:

- To ensure risk appetite is clearly articulated for all risk categories.
- To ensure the businesses operates within the established risk appetite through monitoring and controls.
- To ensure the level of capital held in the balance sheets is compatible with the risks taken.

- To ensure efficient capital structures operate within the business.
- To ensure compliance with risk policies.
- To ensure an efficient process is in place to identify emerging issues and risks.
- To help mitigate the risks which are outside the risk appetite.
- To define methods and processes to measure the available and required risk capital.

### ***1.1.3 Three Lines of Defence in Risk Management***

Finally, it needs to be stressed that risk management is not only carried out by the risk management function, but by the whole organisation.

The organisation can be split into the so called three lines of defence.

**First line of defence:** The *line management* as first line of defence is of paramount importance in risk management, because this function is essentially responsible for ensuring that all processes in the business adhere to the *risk management policies* and that the company operates within the *limits* as agreed upon by the Board of Directors and the executive.

**Second line of defence:** The *risk management function* lead by the Chief Risk Officer is the second line of defence. It has the duty to provide a reliable challenge to the first line of defence and it measures the necessary risk capitals and independently monitors the adherence to limits and appetite. In case of limit breaches it initiates together with the first line of defence mitigating actions. The *risk management function* is also responsible for the various risk committees and risk reporting.

**Third line of defence:** *Internal audit* is the third line of defence. Its main task in respect to risk management is to provide independent assurance to the Board of Directors and the senior executive that the risk management processes are adequately working within the first and second lines of defence.

## **1.2 Principles**

The aim of this section is to define the generally applicable operating principles which are used within the company to ensure adequate and efficient risk management. These principles define on a high level the main risk categories and risk management principles and it is expected that the whole organisation adheres to them.

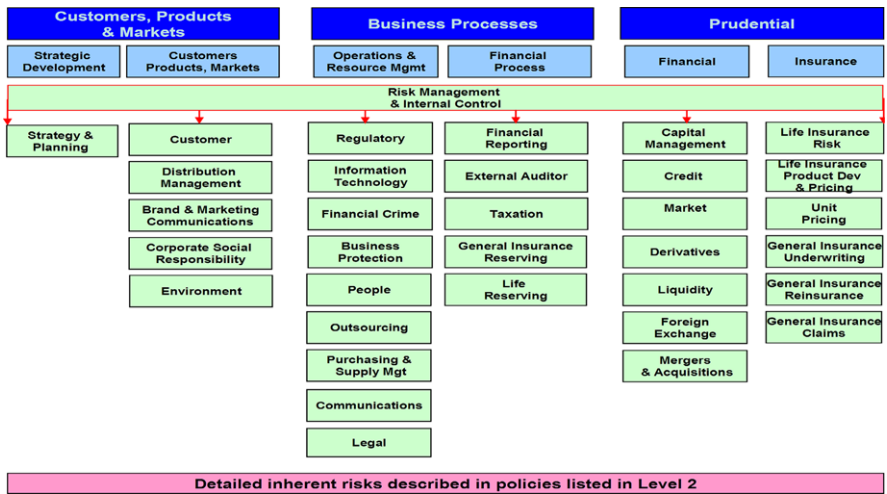


Fig. 1.2 Risk Map

1.2.1 Risk Categories

In order to have a systematic approach to measure, limit and to mitigate the risks the insurer is facing, a so called risk landscape has to be created. The main aim is to have a structured and uniform approach towards risks. Such a landscape normally takes the form of a tree where risks become more and more granular. The depth of the branches corresponds to the level of the model.

Each risk can be characterised by its impact (*severity*) and its probability (*frequency*). Furthermore we speak of *inherent risk* if we look at it before any dedicated controls or mitigating actions are put in place. We speak of a *residual risk* if we measure it taking into account the existence and effectiveness of controls.

Distinguishing *inherent risks* and *residual risks* is necessary in order to know whether a certain control is efficient or sufficient in order to limit a risk to an adequate level. Obviously the full elimination of a risk by using a lot of mitigating actions might not be optimal in the sense that the corresponding costs for the mitigating actions could outweigh the potential loss. Hence it is essential to have a commensurate risk appetite which takes this into consideration.

Risk is defined as the potential danger that an actual result will deviate (adversely) from the expected result. Risk is measured according to probabilities and the extent of negative deviations. Risk is defined as:

**The magnitude of a risk** expressed in terms of impact and probability before any dedicated controls or mitigating actions are put in place or assessed on the basis that the dedicated controls and mitigating actions in place fail.

**The impact and probability** of an *inherent risk* taking into account the existence and effectiveness of controls.

Risks are measured and assessed in financial terms, provided that this is both possible and appropriate. To weigh up and compare various risks, risk management ratios will be defined, providing consistent information on the probabilities and extent of negative deviations. Risks which cannot be directly quantified (especially operational and strategic risks) are also to be systematically recorded and represented in an appropriate form.

In order to identify, measure and limit certain risks, a systematic approach is needed. In a first step risks are categorised according to a risk map (figure 1.2). Examples of specific risks within the individual categories are:

<b>Market risks</b>	ALM or gap risk, interest rate risk, equity risk, currency risk, real estate risk, commodity risk, etc.
<b>Liquidity risks</b>	Market liquidity risk, funding risk.
<b>Credit risks</b>	Counter-party risk, country risk, concentration risk, risk of rating changes, etc.
<b>Insurance risks</b>	Death, disability, longevity, illness, etc.
<b>Operational risks</b>	Distribution risk, financial crime, legal risk, reputation risk, business protection risk, HR risk, loss of expertise, etc.
<b>Strategic risks</b>	Risk of pursuing the wrong strategy or of being unable to implement the strategy (e.g., market access).

### 1.3 Risk Management Process

Figure 1.3 defines the generic risk management and controlling process:

**Strategy and plans:** This is the first step of this generic and cyclic process where, based on risk and reward, a strategy is determined in order to optimise return to shareholders on a risk adjusted basis. Implicit to this task is the high level risk measurement and capital consumption of a certain strategy. This part of the process is owned by the *risk owners*. Risk management information should be used to provide insight, inform the operational planning process and influence resource allocation including capital. Businesses must ensure that changes to their risk profile including control effectiveness are explicitly considered within strategy setting, business planning, objective setting and performance monitoring.

**Risk appetite:** Based on the plans and the high level risk and capital allocation, the risk appetite is defined and risk limits are set. This process is governed by the risk committee and the owner of this process step is the *risk owner*. Risk

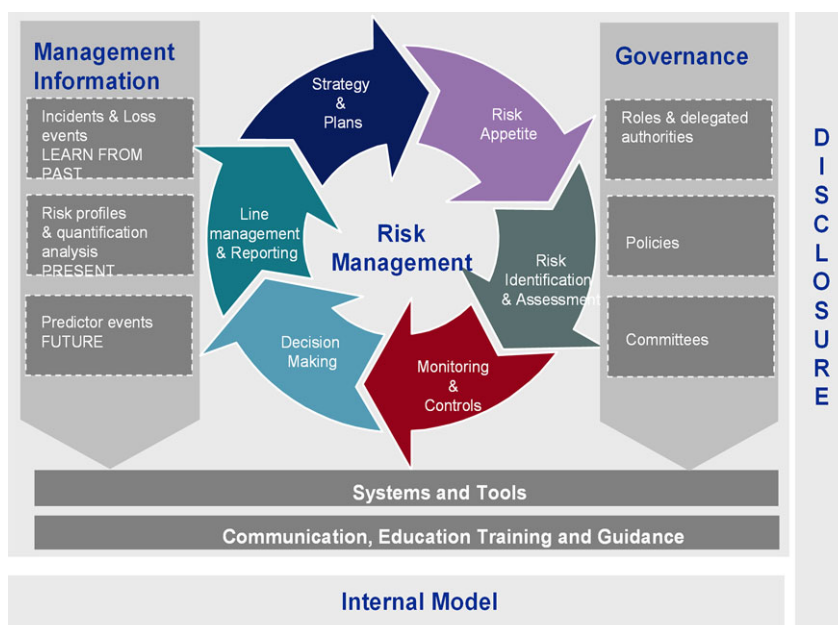


Fig. 1.3 Risk Management Process

appetite statements and tolerances should be clearly defined and refreshed on a regular basis and as an integral part of the planning process. Risk appetite should be defined for a business as usual situation within an established business and also needs to be sufficiently flexible to deal with a variety of situations (e.g. rapid market expansion, managing significant change) and should support rather than constrain sensible risk taking to deliver business objectives.

**Risk Identification and Assessment:** As next step there is a detailed risk analysis comprising risk identification and assessment. This step, owned by the different *risk experts* and the *risk function* ensures that all risks are properly captured within the systems and processes of the company. Furthermore it ensures that material risks can be quantified adequately with high quality. All material inherent risks must be identified, assessed and recorded. Controls to mitigate each material inherent risk must be documented and assessed for their adequacy and effectiveness in risk mitigation in order to produce a residual risk assessment which is within appetite. The risk model must be used as the basis for considering all types of risk.

**Monitoring and Controls:** The agreed risk limits are entered into the models monitoring the risk and controls in order to ensure a timely detection of limit and control breaks. This part of the process is owned by the *risk function*.

**Decision Making:** During the year risks are taken according to the policies defined by the company. *Line management* is responsible for adherence to the risk

policies and ensures the management control of them. By doing business *line management* ensures the embedding of the *risk management policies* and adherence to the limits granted. In case of limit breaks, the corresponding processes are initialised. During this task *line management* optimises the risk return profile and hereby generates value for the company and its shareholders. *Risk management* supports the *line management* by regular risk reporting and reports limit consumption and limit breaches to the *risk owners*.

**Line Management and Reporting:** This last step of the process ensures a proper feed-back over the cycle, by assessing the performance on a risk adjusted base. Risk adjusted returns and limit breaches are prepared by the *risk function* and are reported to the *line management* and the *risk owners*. This information serves as input to management remuneration and the strategy and planning process.

Risk is measured in two dimensions: frequency (likelihood) and severity (impact). The impact can be one of the following in decreasing order: catastrophic, critical, significant and important. Each level of impact corresponds to a monetary amount, which depends on the entity. The bigger the entity the higher the corresponding threshold. The probabilities in decreasing order of likelihood are: likely to happen, possible, remote and extremely remote. Based on the assessment of frequency vs severity the overall risk can be expressed in a more holistic way. The figure 1.4 shows a such an overview:

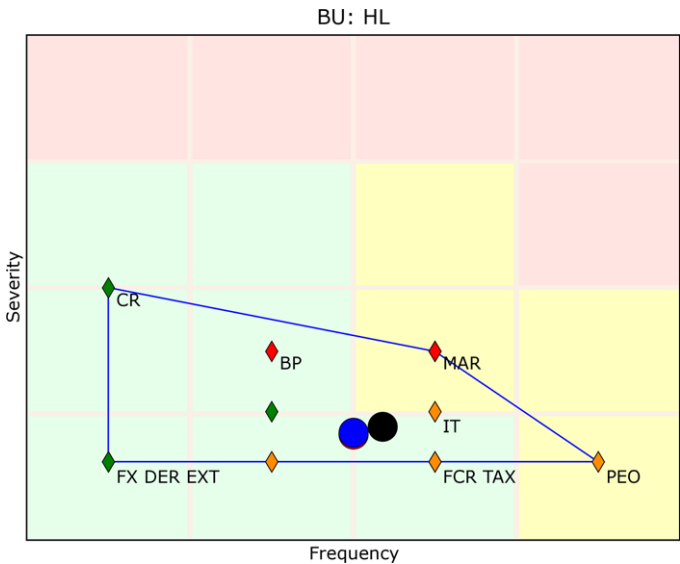


Fig. 1.4 Frequency vs. Severity



In figure 1.4, the frequency of the emergence of a risk is plotted and each of the four categories has a specified probability. Similarly the potential impact is classified into one of four categories. Depending on frequency and severity each of the 16 squares is allocated to one of the three colour codings: green, amber and red. In a next step all policies are mapped against this grid and plotted. The label “PEO” refers for example to people risk, which has in this example a high probability of materialisation with a rather low impact. This policy has been evaluated as amber and hence the marker is amber. In the same sense one can see the market policy (“MAR”), the credit policy (“CR”) etc. In order to have an overall picture the circles represent the barycentre of the assessments, in black for the past reporting period, and in blue for the current. From this it can be seen that the over all risk moved slightly south-east, hence has reduced a little.

## 1.4 Risk Management Policies and Risk Landscape

In order to define minimal standards on how different risks have to be treated and define minimal governance standard, insurance companies codify the corresponding rules and responsibilities in terms of risk management policies which cover risks, which belong together. The following list provides a quite complete list of risk management policies. Obviously there are different ways on how one can arrange these policies.

**Brand & Marketing Communications:** This risk management guideline describes the risk which is intrinsic in the brand and marketing communication process. Here the main aim is to safeguard the company’s reputation and to ensure that the communication is aligned with the core values of the company.

**Business Protection:** Business protection aims to protect the orderly running of the business and is therefore concerned with things such as physical security, IT security, data recovery, business continuity in case of a damage of a property or in case of a pandemic etc. Hence the aim of the policy is to define the limits of acceptable risk with respect to these topics.

**Capital Management:** The aim of this guideline is to define the processes and the risk appetite the company has in respect to capital management, hence in respect of levels and quality of capital. Here also the process of raising capital, paying dividends and the risk appetite of becoming insolvent is anchored. One could for example state: “There is no risk appetite that the statutory capital level falls below 120%.”

**Communications:** Communications cover both internal and external communication. Here it is defined how information is treated and who is allowed to communicate internally and externally. The corresponding risks are unhappy employ-

ees because of bad internal communication, or externally: reputational issues and communication leaks.

**Credit:** This is the financial credit risk, where credit migration, credit spread and default risk is addressed. Furthermore guidance is given in respect to concentration limits and the processes used in order to ensure the company operates within a given risk appetite. Hence some of the requirements limit financial risks and others aim to address operational (risk) issues.

**Customer:** One of the big reputational and regulatory risks of each insurance company is the relationship vis-a-vis the customers. Here it is important to define what “treating customers fairly” means and how the corresponding risk appetite is defined. In consequence governance rules are established in order that the company operates within these boundaries.

**Derivatives:** Since derivatives imply a much higher (operational and financial) risk than “normal” assets, it is important to define the corresponding governance processes in a stringent and efficient way. Hence this guideline addresses, besides the pure financial risk, also the important operational procedures and hence aims to limit also the operational risk.

**Distribution Management:** The distribution management policy aims to limit the risks which are induced by the insurer’s distribution network. Here risk appetite and processes are set in respect to the quality of people acting as distributors, turnover of distribution managers, remuneration schemes etc.

**Environment:** Here the company states its risk appetite with respect to environmental issues, such as energy consumption etc.

**External Auditor:** As a consequence of Enron and Worldcom, the attitude vis-a-vis accounting has become much more stringent and most companies have no appetite to make accounting errors and a lot of them have also implemented quality standards such as SoX 404. This guideline defines the relationship towards the auditors and states which behaviours are not acceptable and which services may not be taken from the own external auditor.

**Financial Crime:** The financial crime policy states the required behaviour in respect to financial crime, such as fraud, money laundry etc. Most companies do not have the slightest appetite for financial crime and hence these guidelines are normally very prescriptive and restrictive.

**Financial Reporting:** The financial reporting guideline needs to be viewed as a companion of the external auditor guideline with the aim to reduce errors and omissions with respect to financial reporting down to an acceptable (low) level.

**Foreign Exchange:** The FX guideline is also one of the financial risk guidelines and it has the same aim as all of these guidelines, namely that the company operates within a well defined risk appetite. In consequence the limit setting, monitoring and reporting processes are of utmost importance.

**GI Claims:** This guideline governs the GI claim processes and defines which measures have to be taken, to prevent fraud and to treat customers fairly. Obviously the claim settlement process for GI claims is of utmost importance, because there is a narrow margin between being too onerous and being too strict. As a consequence we speak here about operational risk, which has a direct financial impact.

**GI Reinsurance:** Since a lot of GI lines of business are heavily re-insured (say some 25% of the total GI premiums), it is important to have a clear guidance which level of risk is still acceptable and which risks need to be reinsured. Besides the insurance risk (such as windstorm, earthquake, . . .), it is important to recognise there is also credit risk involved, since reinsurers also might default. Hence a balanced reinsurance portfolio is important in order to avoid severe problems in case of a reinsurer default. In the reinsurance risk guideline the risk appetite is not only relevant for lines of business but also for counterparties.

**GI Reserving:** Looking at the balance sheet of a GI insurer it becomes obvious that a large part of the balance sheet consists of claim reserves. Hence it is important to have a clear risk appetite in order to ensure on one hand adequate reserves, which are on the other hand, not too onerous. Furthermore the GI reserving process involves, besides actuarial techniques, also considerable judgement. Hence in the light of financial reporting risk it is important to have rigid and robust processes in place.

**GI Underwriting:** The GI Underwriting guideline can be considered as a companion guideline to the GI claims guideline covering the underwriting process. A stringent process is needed in order to ensure an adequate portfolio quality. Let's assume for the moment that a company would attract all "bad" risks. In this case the company would obviously suffer because of an inadequate pricing. Hence also the GI pricing is anchored in this guideline.

**Information Technology:** Information technique per se is a vast topic and the corresponding intrinsic risks are big. This guideline steers the risk appetite in respect to IT risks, such as infrastructure, IT projects etc.

**Legal:** The legal risk policy speaks about the company's attitude in respect of legal issues, litigation etc. Here it is important to allocate the responsibilities and duties accordingly. This is in particular relevant when entering into a litigation or a settlement of a claim. The legal risk policy does not only cover the risks the corporate faces, but also risks which are consequences of disputed life and in particular GI claims.

**Life Insurance Product Development & Pricing:** As we will see in chapter 12 the product development and product pricing process for life insurance policies is a difficult one. As a consequence of the typically big volumes and long contract terms (20 years and more) and the fact that issues become costly quite easily. It is of paramount importance to have a clearly defined risk appetite in respect of product development and pricing, and corresponding robust governance processes. It is also important to recognise that besides the pure financial risks there

are also significant operational risks which can materialise in ill-designed products.

**Life Insurance Risk:** This guideline covers the risk appetite of the pure technical insurance risks which are, for example, mortality, disability, surrender etc. In order to operate within a well defined risk appetite these technical risks are to be limited with a limit system.

**Life Reserving:** This is the companion guideline of the “GI Reserving”.

**Liquidity:** Liquidity risk guideline governs the process to monitor liquidity and to ensure that the company has always enough liquidity to fulfil its obligations. This guideline is also one of the financial risk guidelines.

**Market:** From all the financial risk guidelines, this is the most important, covering the market risk of all financial assets (such as equities, bonds, hedge funds etc.) and the corresponding ALM risk if also taking the liabilities into consideration. In consequence governance, limit systems, escalation processes, risk mitigation and risk measurement play an important role in this guideline. Only if these building blocks are robust and accurate is it possible to operate in a well defined environment, taking risks in a conscious manner.

**Mergers & Acquisitions:** This guideline sets the risk appetite and standards for M&A processes. It is known that these processes are difficult and can lead to substantial problems if done in an inappropriate manner. Hence it is important to have a stringent guideline describing processes, governance arrangements and risk appetite.

**Outsourcing:** The Outsourcing guideline defines the risk appetite and the protocols to follow in case of outsourcing arrangements. Obviously it is the aim of such a guideline to limit the corresponding operational and counter-party risks.

**People:** For all financial institutions there are two main resources needed: capital and people (human capital). It is very important to clearly articulate the risk appetite in respect to people to ensure the attractiveness to key performers and to ensure an adequate turnover to get new talent on board.

**Purchasing & Supply Management:** See “Outsourcing”.

**Regulatory:** This guideline can be compared with the “External Auditor” guideline since it defines the risk appetite in respect to the different regulators of the company.

**Risk Management & Internal Control:** This guideline defines how risk management works in the corporate environment and covers many issues and questions of this book.

**Strategy & Planning:** Looking at the main processes of an insurance company, the strategy and planning process is particular, since it defines what the company will do in the following year. It is also known that ill-behaved strategies are one of the root causes for corporate failures. Hence it is important to also control this process and strategic planning in a environment with a well defined risk appetite.

**Taxation:** This is the companion guideline of “Regulatory” vis-a-vis the tax authorities.

Whereas the risk management policy view is efficient for managing the company another view is needed in order to decompose the risks in their generic risk factors. Assume, for example, credit risk. This risk factor influences more than one risk covered in one of the risk management policies, such as “Credit Risk”, “Reinsurance”, “Customer”, “Outsourcing” etc. Whereas the link is clear for “Credit Risk”, the relationship is not always as straight forward. The following table summarises these relationships:

Policy	Relationship
Credit	Via the credit default and credit mitigation risk of bonds and mortgages.
Reinsurance	Via the counter-party credit risk of the reinsurance treaties and insurance linked securities.
Customer	The reputational issue if the customer suffers in case of a credit default independently on whether the insurance company bears the risk or not.
Outsourcing	Via the operational risk, which is induced by the default of an outsourcing partner.

As a consequence it is necessary to decompose the risk-universe into its drives. This map is called *risk landscape*. Also here it is possible to have a coarser or finer view on the risk landscape. Figure 1.5 shows a quite high level risk landscape.

These risk factors form, from a mathematical point of view, the base for the risk capital calculations and represent a multi-dimensional random variable or stochastic process. All random fluctuation within a economic capital model are derived from these risk factors. The financial instrument sub-model of the Swiss solvency test uses for example about 80 different risk factors, which are modelled as a multi-dimensional normally distributed random variable ( $X \sim \mathcal{N}(\mu, \Sigma)$ ).

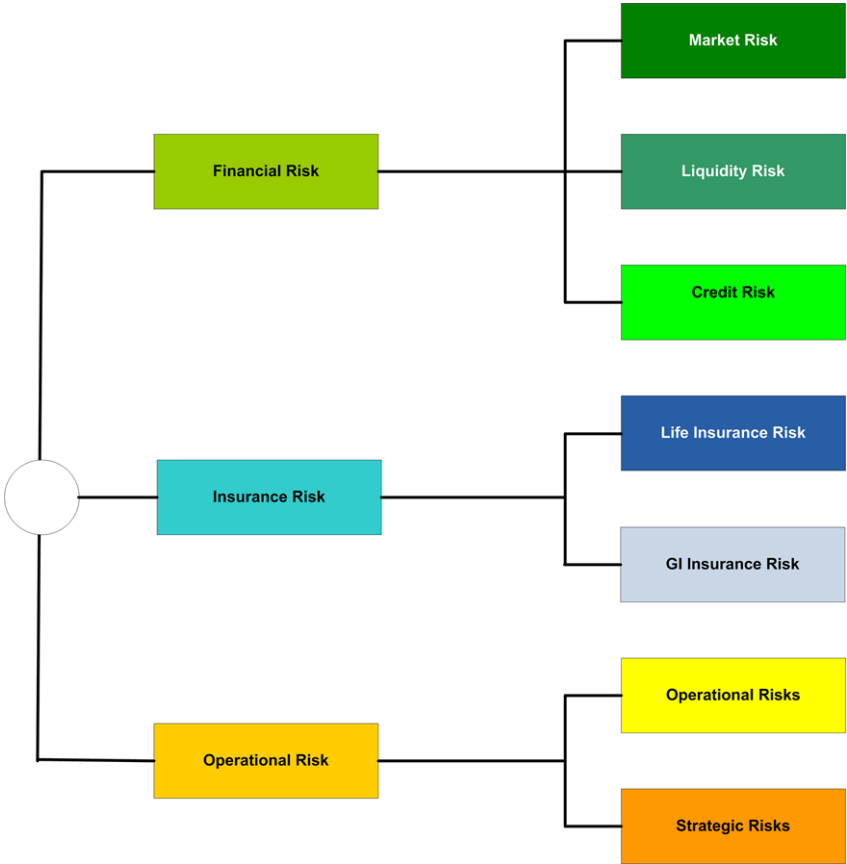


Fig. 1.5 Risk Landscape

<http://www.springer.com/978-3-642-20720-4>

Life Insurance Risk Management Essentials

Koller, M.

2011, XVIII, 360 p. 70 illus., 60 illus. in color., Softcover

ISBN: 978-3-642-20720-4