2013

Quantifying operational IT risk

Improving Achmea IM&IT's risk management

Master Thesis
Industrial Engineering &
Management

Mart Stokkers

Management summary

Confidential

Preface

Everything comes to an end. This Master thesis marks the beginning of a new period in my life, as well as the closure of my student life. A time with a lot of fun, happiness, adventures and of course studying.

This Master thesis is written to obtain my Master's degree in Industrial Engineering and Management, with a specialisation in Financial Engineering and Management, at the University of Twente. The previous five months I have been given the opportunity to conduct my research at Achmea, for which I am very grateful. It has been a challenging experience for me to find the right balance between academics and practice. I can say that I am very content with the end result.

I would like to thank my colleagues from the operational risk management & compliance department at Achmea IM&IT, who have been of great support and really made me feel at ease at Achmea. I would like to thank Rik Voerman and Bert Witteveen for arranging my Master assignment as well as all other employees of Achmea that contributed to my research. I am especially grateful to my two supervisors from Achmea, Boudewijn Cremers and John Storms, for their great effort, time and patience in helping me to achieve my goal.

I would also like to thank my two supervisors from the University of Twente, Toon de Bakker and Berend Roorda, for challenging me and guiding me through the process. You both really made sure that I kept enthusiastic for my research, while at the same time reviewing me with useful criticism. I truly experienced your supervision as a delight.

Finally, I would like to thank my family and friends for their support. Dad, thanks for coffee drinking, driving me home and everything else. Mom and Talitha thanks for listening to my stories and your love.

Enschede, 16th of August, 2013,

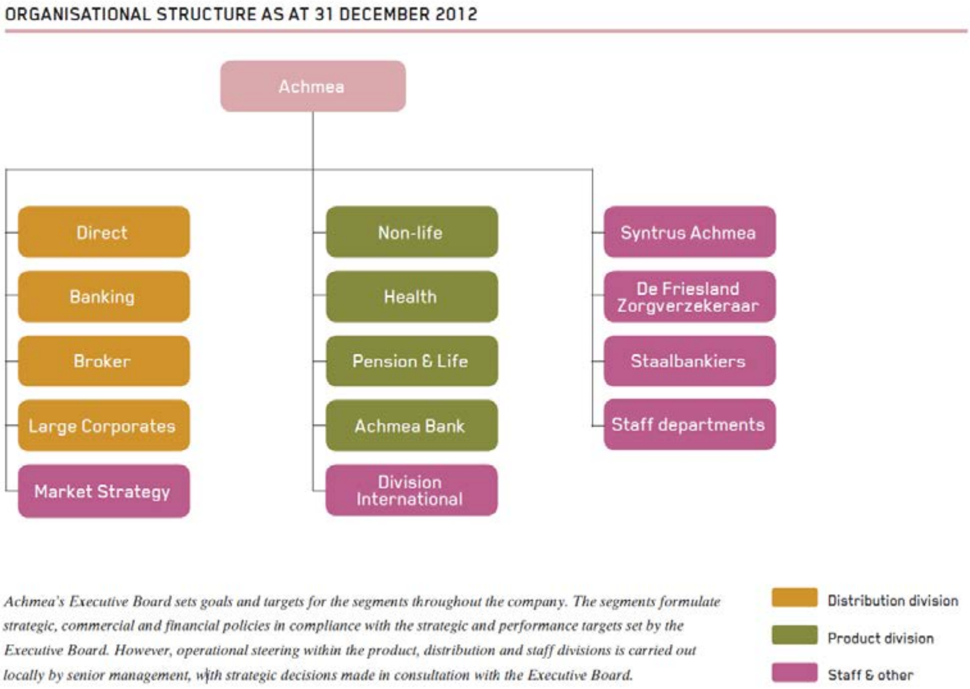
Mart Stokkers

Table of Contents

1 Introduction

1.1 Achmea

The Achmea group is the largest insurance company in the Netherlands with over 20.000 employees of which 16.000 in the Netherlands and 4.000 in its European subsidiaries. Next to the Dutch market it operates in Bulgaria, Greece, Ireland, Romania, Russia, Slovakia and Turkey. Achmea was founded by farmers who collectively wanted to insure their property against fire and is different from other insurers in that it has a cooperative structure. Achmea is primarily owned by the 'Vereniging Achmea' (65%, essentially Achmea's customers) and the Rabobank (30%, a large cooperative bank in the Netherlands). Over time the company grew rapidly due to mergers and acquisitions in the Dutch market and later European market. Achmea offers its products through a wide range of brands of which Interpolis, Zilveren Kruis Achmea, FBTO, Centraal Beheer Achmea and Avéro Achmea are biggest. Main motto is 'Achmea unburdens' and primary focus lies in meeting customer needs. It does so by applying core competences in main segments comprising non-life, life, health, income protection, term insurance and standard pension products. Apart from these segments Achmea offers the full spectrum of insurance and other financial products related to this. Achmea's group gross written premium (turnover) in 2012 was €20.4 billion and net profit €453 million. The company has a solid equity position of €10.4 billion leading to a solvency of 207% on a total assets position of over €90 billion (Achmea annual report, 2012). Achmea's organizational chart is depicted in figure 1. The organization is concentrated around the non-life, health and life divisions in the second column. Products/services are distributed through several distribution channels as can be seen in the first column of the organizational chart. Non-core segments and staff constitute the third column, these staff divisions support the non-life, health and life divisions in the second column.



Achmea's Executive Board sets goals and targets for the segments throughout the company. The segments formulate strategic, commercial and financial policies in compliance with the strategic and performance targets set by the Executive Board. However, operational steering within the product, distribution and staff divisions is carried out locally by senior management, with strategic decisions made in consultation with the Executive Board.

Figure 1: Organizational chart

The service division IM&IT is the central division responsible for maintaining and developing information technology at Achmea. It strives to support the organisation and especially the core business divisions (non-life, health and life) by taking control of the information technology and introducing generic information systems.

The Finance and Risk department (F&R) is one of the staff departments within Achmea IM&IT. It is responsible for assessing, controlling and measuring finance and risks for the service division IM&IT. Finance and Risk consists of five different departments, namely F&R reporting, corporate control, business control, quality management and ORM & compliance. The operational risk management (ORM) & compliance department identifies, measures and controls operational risks and advices on mitigating these risks within Achmea IM&IT. The Basel committee on banking supervision defines operational risk as:

"the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events" (BIS, 2001).

Achmea uses the three lines of defence model for risk management as illustrated figure 2.

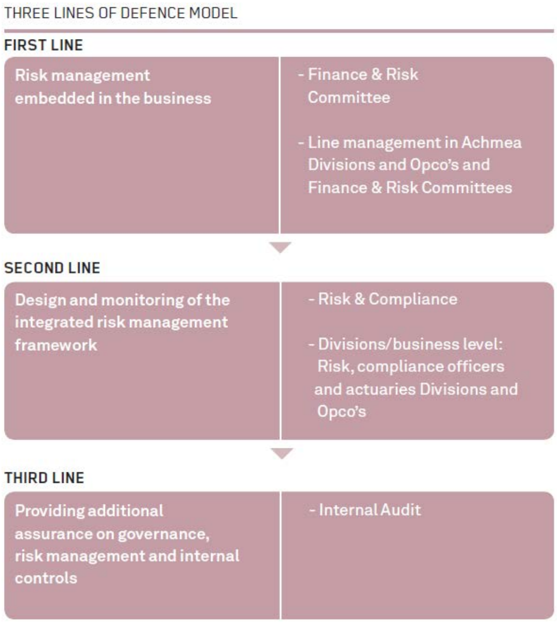

THREE LINES OF DEFENCE MODEL
FIRST LINE
Risk management embedded in the business
- Finance & Risk Committee
- Line management in Achmea Divisions and Opco's and Finance & Risk Committees
SECOND LINE
Design and monitoring of the integrated risk management framework
- Risk & Compliance
- Divisions/business level: Risk, compliance officers and actuaries Divisions and Opco's
THIRD LINE
Providing additional assurance on governance, risk management and internal controls
- Internal Audit

Figure 2: Three lines of defence model

With respect to operational risks for the IM&IT division line management is responsible for the first line of defence, where internal audit is responsible for the third line of defence. The operational risk management & compliance department is one of the departments that are responsible for the second line of defence concerning operational risk at Achmea's IM&IT division. The department comprises nine (senior) operational risk managers that actively identify and control operational IT risks. Main tasks of the department are supporting and advising line management on controlling risks, determining what these risks are and monitoring whether these risks are being mitigated (Achmea, 2013). In the next section challenges are being addressed that the operational risk management & compliance department face.

1.2 Background

Financial institutions, like banks and insurance companies, have categorized operational risk as residual risk compared to other risk types as credit and market risk (Power, 2003). However, recently with the upcoming new regulatory frameworks Basel III for banking industry and Solvency II for insurance industry the importance of operational risk as a crucial risk type is increasing. Yet still relatively little regulatory capital is allocated to operational risk, in general fifteen to twenty percent of total regulatory capital (Samad-Kahn, 2008). In 2012 required capital for operational risk at Achmea constituted eight percent of total required capital, reaching €700 million (Achmea annual report, 2012). Operational risk has always been present in financial institutions but in the last decade affluent attention is given to the definition, measurement and control of this risk type. Several incidents from the past stress the importance of measuring and controlling operational risk. Rogue trader Nick Leeson from Barings Bank caused the oldest investment bank in the United Kingdom to lose $1 billion because of fraudulent trading, resulting in the collapse of Barings Bank. Salomon Brothers lost $303 million because of business disruption and system failures and Bank of America lost $225 million from system integration failures and transactions processing failures (Hull, 2010).

Operational risk is often considered to be one of the most difficult risk types to measure, because relatively few data is collected over the last years. Nevertheless regulatory frameworks like Basel III and Solvency II provide methods to calculate required capital under these frameworks. Basel III proposes three methods to calculate operational risk capital. These include the basic indicator approach, the standardized approach and the advanced measurement approach. The first two methods are fairly simple and measure required capital for operational risk by multiplying a factor(s) with a volume parameter(s), e.g. annual gross income. The third method allows banks to use own internal models in measuring operational risk capital (BIS, 2011). Solvency II proposes two methods to calculate operational risk capital that show similarities with Basel III methods. These include the standardized approach and the use of internal models (EU, 2009). So although operational risk is hard to measure, regulatory frameworks at hand come up with methods that companies can use in calculating operational risk capital.

Achmea is a company with a long history of mergers and acquisitions carrying more legacy than the typical insurer. Since all these independent entities with their systems, people and culture have been merged into one company operational risk is of crucial importance to Achmea. Currently operational risk capital is calculated at group level using the standardized approach method from Solvency II. Given Achmea's nature of being a merged company and relative size in the Dutch market, supervisors expect Achmea to be able to come up with own internal models to calculate operational risk capital. These models should better capture the risk sensitiveness Achmea is exposed to. Although operational risk management is widely introduced in the company, emphasis has not been laid on measurement of operational risk via internal models. Primary emphasis is currently on identifying and controlling operational risk via expert judgement in order to mitigate and steer upon operational risk. Quantitative modelling of operational risk is in that perspective lagging other components of risk control.

Measurement is an integral part of risk control and a necessary condition for risk financing and risk mitigation (Doff, 2011; Samad-Kahn, 2005).

Since quantitative modelling of operational risk insufficiently takes place at Achmea IM&IT there is no insight into financial consequences of operational risk. This has implications for the validity of ranking of operational risks, the ability to control and steer upon these risks and clarity regarding costs and benefits of risk mitigating efforts. Besides internal motives to research the financial impact of operational risk there are external motives as well. Solvency II requires insurance companies to assess the financial consequences of their risk position. Operational risk is one of the risk components that make up solvency capital requirement (SCR), the minimum amount of regulatory capital an insurer must hold. As explained, Achmea currently uses the standardized approach to calculate operational risk capital at group level. Using own internal models has the advantages of better/justified ranking, risk awareness, improved steering and mitigation of operational risk and insight into costs and benefits of risk control. Next to that internal models create better risk control, changing the regulatory capital charge for operational risk Achmea must hold. Thus Achmea might need to hold less capital for buffer purposes and consequently is able to invest more of this capital into the market or hold more capital and is better able to absorb losses given their risk profile.

1.3 Problem overview

1.3.1 Problem statement & research questions

The challenges addressed in the background section and relations between them have been illustrated in figure 3. Core problem that operational risk management & compliance department of Achmea IM&IT face is that insufficient quantification of operational IT risk takes place. This has implications for meeting insurance regulation and leads to insufficient risk control at Achmea IM&IT. Since Achmea IM&IT is the central service division for information technology at Achmea, consequences of operational risk eventually lie within the business. For instance when a system is down for some time, Achmea business loses customers and is not able to function properly. Without yet touching the complexity concerning this topic one can see that the business incurs operational losses. In the context of this thesis ‘Achmea business’ comprises the three business divisions, non-life, health and life, as introduced in section 1.1. So insufficient quantification of operational IT risk leads to insufficient risk control and has financial consequences for Achmea business as well as implications meeting insurance regulation.

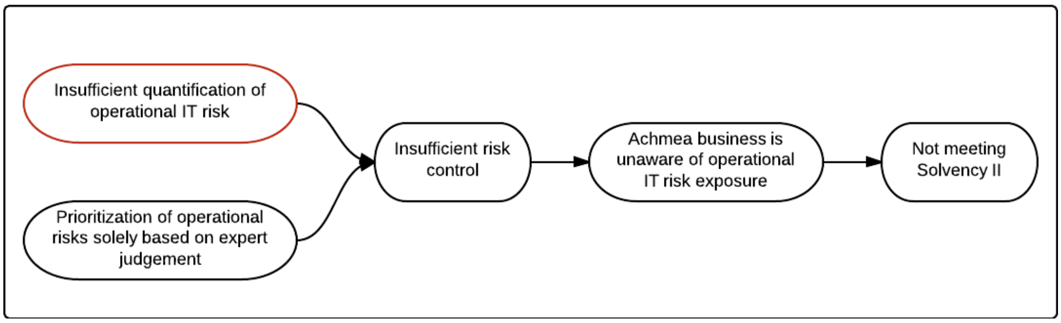

Insufficient quantification of operational IT risk
Prioritization of operational risks solely based on expert judgement
Insufficient risk control
Achmea business is unaware of operational IT risk exposure
Not meeting Solvency II

Figure 3: ‘Problem tangle’

Clearly there is an incentive to quantify or measure operational IT risk at Achmea's IM&IT division, because it is a crucial part of risk control. With the knowledge created Achmea IM&IT is better able to prioritize operational risks and communicate these risks throughout the organization. Quantifying operational IT risk eventually means coming up with an euro amount for operational risks. Central research question for this thesis in that perspective is formulated as:

What is the financial impact of operational IT risk at Achmea's IM&IT division?

An operational risk carries potential losses for Achmea. Operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events" (BIS, 2001). Since operational IT risk is a subset of operational risk this concept requires further specification in this thesis. From the definition of operational risk implicitly a definition of financial impact can be deducted. The 'risk of loss' can be considered as financial impact for Achmea.

The central research question encompasses several aspects that have to be researched in order to come up with an answer to the central research question. These aspects constitute the following research questions in this research:

1) What requirements does Solvency II impose in quantifying operational risk?

2) What models are being used in academic literature to quantify operational risk?

3) What are operational IT risks and how can it be classified?

4) What is the practical usefulness of operational risk models in quantifying operational IT risk for Achmea's IM&IT division?

1.3.2 Research goal

This research aims to set first steps in developing a methodology to quantify operational IT risk in order to assess the financial impact of these risks in conjunction with recent regulatory developments known as Solvency II. This knowledge is crucial because of regulatory pressure and to create better risk control at Achmea IM&IT and business divisions. Quantifying operational IT risk leads to better risk ranking, risk awareness and insight into costs and benefits of risk mitigating efforts. It can also add to lowering regulatory capital charges for operational risk Achmea is required to hold. The research problem is borne by the operational risk management & compliance department of Achmea IM&IT and this research aims to support the department by generating necessary knowledge and empirical evidence about quantification of operational IT risk.

1.4 Research outline

The remainder of this thesis is structured as follows. In chapter two the research design is discussed that will specify how research is conducted. To answer the research questions as proposed in section 1.3.1 different types of research are required and chapter two specifies what kind of types. Solvency II, the regulatory framework for insurance companies, is introduced in chapter three focusing on the aspect of quantifying operational risk. Chapter four gives an overview and review of academic literature related to operational risk modelling hereby answering the second research question of this thesis. In order to use operational risk models classification of operational risk is required and chapter five is centred around this topic, thus solving research question three. In chapter six operational risk models are empirically tested and analysed on practical usefulness for Achmea's IM&IT division. Given the answers of research question one to four, chapter seven focuses on both the central research question and conclusions and recommendations of this research. Finally scientific relevance and limitations of this research are presented in chapter eight as well as directions for further research. The research process implied by this structure is adopted from the book 'Business Research Methods' by Blumberg, Cooper & Schindler (2008) depicted in figure 4.

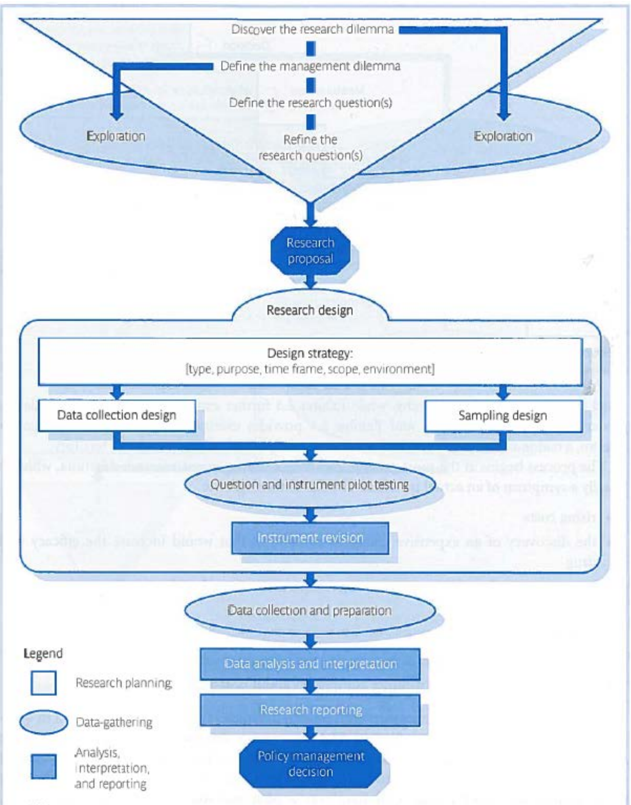

Discover the research dilemma
Define the management dilemma
Define the research question(s)
Exploration
Refine the research question(s)
Exploration
Research proposal
Research design
Design strategy: [type, purpose, time frame, scope, environment]
Data collection design
Sampling design
Question and instrument pilot testing
Instrument revision
Data collection and preparation
Legend
Research planning
Data-gathering
Analysis, interpretation, and reporting
Data analysis and interpretation
Research reporting
Policy management decision

Exhibit 2.1 The research process.

Figure 4: The research process

First part of the research process, up to and including research proposal, comprises of elements presented in chapter one. Remaining part of this thesis is structured as specified and illustrated above. One remark with respect to the research process of Blumberg, Cooper & Schindler is that this research is not executed in such a strict sequential order.

2 Research Design

Research design refers to the ways we can analyse empirical evidence using research methods in order to answer research questions (Gemenis, 2012). This means that research design consists of at least three elements which are research questions, research methods and empirical evidence. The research questions of this thesis have been formulated in chapter one and empirical evidence contributes to answering these questions in chapters three to six. Main focus of this chapter will lie on the way research is conducted, in essence the research methods. These methods form the basis in answering the four research questions defined in section 1.3.1. Since research questions differ in type, different research methods are required to collect empirical evidence. One of the essentials of research design is that design is always based on research questions (Blumberg, Cooper and Schindler, 2008). The next sections outline per research question what different research methods are used in this thesis.

2.1 Solvency II

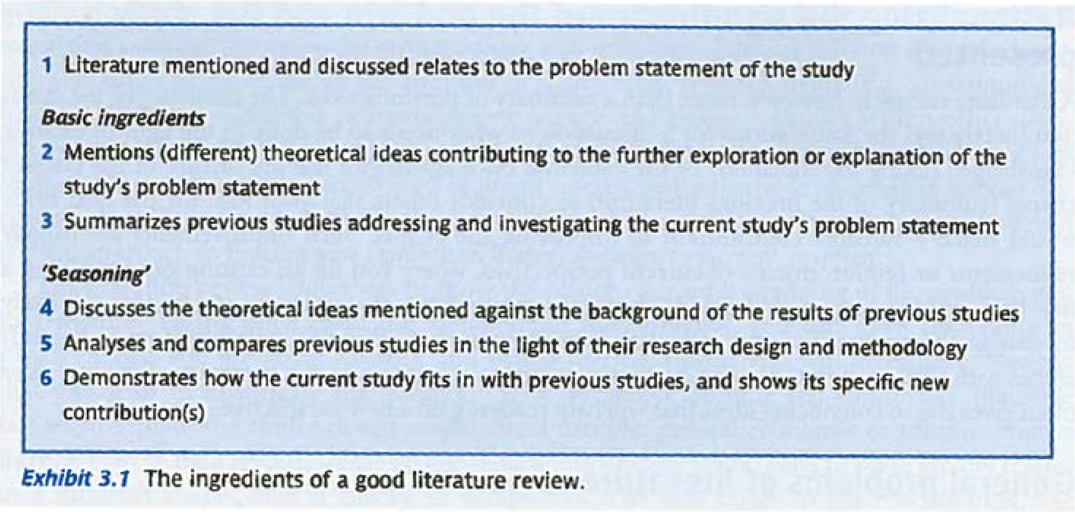
What requirements does Solvency II impose in quantifying operational risk?

Research question one concerns regulatory framework for insurance industry, Solvency II, and requirements in quantifying operational risk that this framework imposes. The method used here to answer the research question is a descriptive analysis of available literature about Solvency II. Guiding literature and unit of analysis is the framework itself, the 'Directive 2009/138/EC of the European parliament and of the council of 25 November 2009 on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II)' by the European Union. But also books, papers and articles related to Solvency II are analysed to complement the framework. The objective of answering this research question is introducing Solvency II and coming up with possible methods to quantify operational risk. The type of information necessary can be classified as qualitative secondary data and is publicly available. Therefore no problems with acquiring data are foreseen. Given its nature, data is analysed and processed in a qualitative manner. Concepts in this research question are clearly defined in Solvency II and throughout this thesis Solvency II can be used to define concepts. Because of that reason and the fact that Achmea should comply with Solvency II, the framework is extensively discussed in this thesis. In addition, Basel II/III is analysed to complement Solvency II where necessary. Given the descriptive research method no variables or concepts are influenced while conducting the research. Lastly time and money constraints play no role in answering research question one, consequently research is conducted on a stand-alone basis. Research question one is being answered in chapter three of this thesis.

2.2 Operational risk models

What models are being used in academic literature to quantify operational risk?

Second research question focuses on academic literature about operational risk modelling. Aim is to explain how operational risk is modelled and to provide a systematic overview of operational risk models and characteristics as prescribed in current and past academic literature. In order to acquire necessary information a literature review is performed. According to Blumberg, Cooper and Schindler (2008) a good literature review consists of elements as depicted in figure 5.



1 Literature mentioned and discussed relates to the problem statement of the study

Basic ingredients

2 Mentions (different) theoretical ideas contributing to the further exploration or explanation of the study's problem statement

3 Summarizes previous studies addressing and investigating the current study's problem statement

'Seasoning'

4 Discusses the theoretical ideas mentioned against the background of the results of previous studies

5 Analyses and compares previous studies in the light of their research design and methodology

6 Demonstrates how the current study fits in with previous studies, and shows its specific new contribution(s)

Exhibit 3.1 The ingredients of a good literature review.

Figure 5: Literature review elements

So a good literature review does not only mention and summarize literature, it critically reflects and evaluates the importance to own research. Therefore literature review in this thesis not only outlines current operational risk models but addresses their usefulness to quantify operational IT risk. A literature review is methodologically categorized as a descriptive, qualitative study and is relatively little time consuming.

One important aspect of a literature review is searching and obtaining information. However it is needless to fully specify how this is done. In general it comprises searching through online academic databases by using and combining different search terms. When data is abundant filters can be used to focus on most relevant papers. Papers can quickly be analysed on relevance by reading abstracts, titles and conclusions. Resulting selected information then forms the basis in writing the literature review. This literature review is expected to solve research question two. Furthermore it acts as a starting point for research question four. It is expected that the literature review comes up with operational risk models of which at least one is empirically tested in the field. Based on the information collected thus far most appropriate model(s) are selected. So goal of this literature review is to solve research question two, which is treated in chapter four, and lay foundation for research question four, which is treated in chapter six.

2.3 Operational IT risk and classification

What are operational IT risks and how can it be classified?

Research method for the third research question is twofold. Mainly existing risk classification schemes from Basel II, Achmea and other sources are used to answer this research question. However, additionally information related to operational IT risk is used. Nature of this part of research is best described as descriptive, because objective is to find out 'what' operational IT risks are and 'how' these risks can be classified. Expected outcomes are definitions of operational IT risk and assessment of risk classification schemes. Idea is that it is first important to know what operational IT risks are before operational risk modelling is applied, otherwise not risks but causes or effects are modelled. Research mainly takes place from behind the desk, not influencing variables or concepts at hand. Empirical evidence collected via the described research methods is processed and analysed in a qualitative manner. Time is not expected to constrain correctly answering research question three. Answering of the third research question is presented in chapter five of this thesis.

2.4 Operational risk model in practice

What is the practical usefulness of operational risk models in quantifying operational IT risk for Achmea's IM&IT division?

Fourth and final research question captures field research in this thesis. It is decided to write the research design of question four after answering research question one to three, because then there is better insight into most important concepts of operational risk modelling. This makes it easier to find a suitable study area for the field research. From clarity perspective the reader is advised to firstly read through chapter three to five of this thesis, before this section is treated.

Objective of this fourth research question is to test the practical usefulness of the operational risk models as proposed in chapter four. By doing so, it adds to reaching the goal of this research, namely to set first steps in developing an internal model to quantify operational IT risk. Central research question of this thesis encompasses assessing the financial impact of operational IT risk at Achmea's IM&IT division. Given time constraints it is not possible to fully assess financial impact of all operational IT risks. That is why it is decided to focus on a specific operational IT risk that is quantified in this research. The quantification of this specific operational IT risk acts as the basis for research question four. Meaning that an operational IT risk is quantified using the identified operational risk models in this research. Practical usefulness of these models can then be described as a result of the process followed. Research is best described as descriptive since aim is to observe and describe the financial impact of an operational IT risk and the practicability of operational risk models. The conceptual framework as proposed at the end of chapter four is guiding in this process of operational IT risk quantification.

Firstly the specific operational IT risk that is quantified is identified and described in detail. Identification of this specific operational IT risk is made in consultation with operational risk managers from Achmea IM&IT. Secondly, available data related to the operational IT risk is gathered and fitted to be suitable for operational risk modelling purposes. Any modelling/quantification/measurement of operational risk requires some form of data on which the model is based and the risk is measured. In order to acquire necessary data, a search is performed through Achmea's IT systems. Other relevant data is retrieved from experts related to the specific operational IT risk. After collection of available data, third step is to analyse the data using operational risk models. Data is processed in a quantitative manner, possibly using statistical software, with as an end result a measure for the financial impact of the specific operational IT risk. So at least one of the four identified operational risk models is empirically tested in the field. Constraints for correctly answering research question four mainly come from time aspects and available data. That is why only one specific operational IT risk is quantified and possibly not all operational risk models can be tested in the field.

Variables are not influenced while conducting research question four, although data is retrieved from experts related to the specific operational IT risk.

So concluding, the research method for research question four comprises the quantification of a specific operational IT risk using operational risk models based on available data. This way it adds to the central research question of this thesis by assessing the financial impact of one specific operational IT risk. Aim is to answer research question four, hereby evaluating the practical usefulness of operational risk models to quantify operational IT risk. The results of the field research and thus answering of research question four are presented in chapter six of this thesis.

3 Solvency II

As the successor to the European Union's existing solvency regime for insurers, Solvency II (SII) is a fundamental review of capital adequacy requirements (Achmea annual report 2012). Solvency II is the new regulatory framework for European insurance industry imposed by the European Union. The framework initially scheduled to be effective from 1 November 2012, though this has been postponed to 1 January 2014 and further delay is plausible. Solvency II sets standards for insurance companies with respect to their risk management practices and capital levels. This chapter digs deeper into fundamentals of Solvency II for broader understanding and possible methods for risk quantification relevant for this research.

3.1 Solvency II fundamentals

Early regulatory frameworks like Basel I and Solvency I focused only on a subset of available risk types and lacked risk sensitiveness. Because of globalization, the current crisis, differences in national rules, growing size of insurance companies and identification or existence of new risk types the need for a new regulatory framework became apparent. Solvency II is expected to solve these issues by introducing European insurance regulation that better captures risks faced by current insurance companies. The Solvency II framework is 155 pages long, consequently it is unnecessary to explain the framework in detail. Because of that reason this section treats the fundamentals of Solvency II. This is important for the research, since Solvency II requires assessing financial impact of operational risk. As with Basel II/III, Solvency II is structured around three pillars.

Pillar one treats capital requirements that insurance companies must follow up to, in order to absorb unexpected losses. It also covers the types of capital eligible to classify as capital. Three types are identified, which are tier one, tier two and tier three capital. Tier one capital comprises ordinary equity capital and retained earnings, tier two capital is made up of subordinated liabilities meeting certain availability criteria and tier three capital constitutes subordinated liabilities without these criteria. Together these three types form the available capital set aside by insurance companies to absorb unexpected losses. Rules are set out regarding composition of available capital, e.g. one third of available capital should be tier one capital. The capital requirements break down into a minimum capital requirement (MCR) and a solvency capital requirement (SCR). The minimum capital requirement is the absolute minimum capital an insurance company must hold to absorb losses. When capital falls below the MCR 'ultimate supervisory intervention' is triggered, meaning that the regulator is deciding on the course of action to take, possibly forcing the company to stop entering new business or liquidation of the business. In the Netherlands the Dutch national bank (DNB) is responsible for these tasks. When capital falls below the SCR an action plan is required setting out how to restore capital above the SCR. Supervision of the regulator intensifies as capital moves from SCR to MCR. How SCR is calculated is treated in the next section of this chapter, MCR can be calculated as a percentage of SCR.

Pillar two in solvency II deals with the supervisory review process. Insurance companies are required to implement risk management practices and processes and have sound risk management governance. Pillar two therefore focuses on internal control and risk management processes. Important element of pillar two is the own risk and solvency assessment (ORSA). In the ORSA the insurance company outlines its risk profile, the material impact of this profile and the risk management practices in place. Goal of pillar two is to ensure that insurance companies conduct proper risk management and that this is integrated throughout the company.

Pillar three is about disclosure of risk management information to the public and to the supervisor. It points out what information to disclose to the market and the required information transparency of an insurance company. On an annual basis, insurance companies should report their solvency and financial condition including information as articulated in article 51 of the Solvency II directive. This information also acts as verification for the regulator that the analysis underlying pillar one and two is dependable.

Within the context of this research pillar one of Solvency II is most important, since calculation of capital requirements is treated here. One of the reasons mentioned to quantify operational risk is that it is required in Solvency II, the framework therefore should provide guidelines on how to quantify these risks. This topic is treated in the next section, firstly different risk categories are identified. Throughout the years different types of risk have been identified that consequently were not included in Solvency I. In order to include all relevant risk types and create clear distinction between these types Solvency II uses the following categorization of risk based on inclusion in the solvency capital requirement as depicted in table 1.

Risk Type	**Definition**
Non-life underwriting risk	The risk of loss, or of adverse change in the value of non-life insurance obligations.
Life underwriting risk	The risk of loss, or of adverse change in the value of life insurance obligations.
Health underwriting risk	The risk of loss, or of adverse change in the value of health insurance obligations.
Market risk	The risk of loss or of adverse change in the financial situation resulting, directly or indirectly, from fluctuations in the level and in the volatility of market prices of assets, liabilities and financial instruments.
Credit risk	The risk of loss due to unexpected default, or deterioration in the credit standing, of the counterparties and debtors of insurance and reinsurance undertakings.
Operational risk	The risk of loss resulting from inadequate or failed internal processes, personnel or systems, or from external events.

Table 1: Solvency II risk types (EU, 2009)

Every risk type can be further subdivided but this goes beyond the scope of this research, except for operational risk which is treated in chapter five. Important is identification and existence of operational risk as a risk type in Solvency II and inclusion of operational risk capital in the solvency capital requirement. The calculation of solvency capital requirement therefore provides insight into how risks can be quantified. Since core problem is that operational IT risks are not quantified this information contributes to solving the core problem of this thesis.

3.2 Solvency II risk quantification

Pillar one of Solvency II concerns capital requirements that specify how much capital an insurance company must hold to absorb unexpected losses based on its risk position. As explained in the previous section these capital requirements are expressed in the solvency capital requirement and cover risk charges for non-life underwriting risks, life-underwriting risk, health underwriting risk, market risk, credit risk and operational risk and adjustments for the loss absorbing capacity of technical provisions and deferred taxes. First five risk types constitute the basic solvency capital requirement, whereas operational risk is treated independently and added to basic solvency capital requirement. Adjustments for the loss absorbing capacity of technical provisions and deferred taxes is subtracted from the latter. In formula terms this means $SCR = BSCR + SCR_{Op} - Adjustments$. So the solvency capital requirement (SCR) is made up of the basic solvency capital requirement (BSCR) and the operational risk capital charge (SCR_{Op}) minus the adjustments. This means that Solvency II prescribes how risks can be quantified, since capital charges for operational risk must be calculated. Solvency II states that:

"The Solvency Capital Requirement shall be calibrated so as to ensure that all quantifiable risks to which an insurance or reinsurance undertaking is exposed are taken into account. It shall cover existing business, as well as the new business expected to be written over the following 12 months. With respect to existing business, it shall cover only unexpected losses. It shall correspond to the Value-at-Risk of the basic own funds of an insurance or reinsurance undertaking subject to a confidence level of 99.5 % over a one-year period" (EU, 2009).

For broader understanding firstly concepts as Value-at-Risk (VaR) are explained. Value-at-Risk is a risk measure that tries to summarize total risk in one single number. VaR is calculated from a probability distribution and is the amount of loss not exceeded in time T given confidence level X (Hull, 2010). Within Solvency II the European Union has chosen to use a one-year period and a confidence level of 99.5%, corresponding to a one-in-200-year event. So an insurance company needs to hold capital in order to absorb losses of a loss event occurring once every 200 years, in other words has a probability of 99.5% that the loss does not exceed VaR amount in one year. VaR is graphically displayed in figure 6.

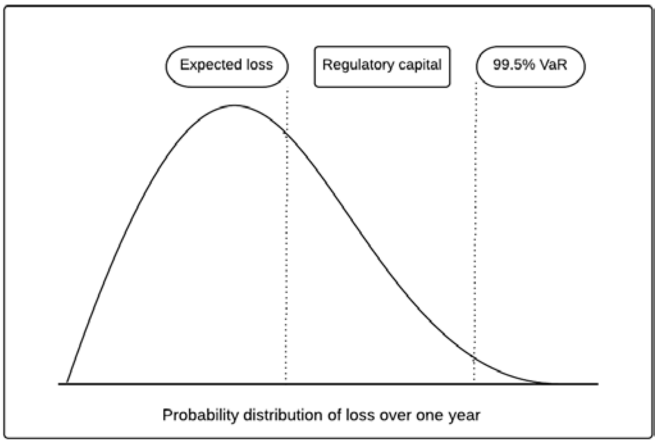


Figure 6: VaR

So VaR, in Solvency II, represents the amount of loss that is not exceeded in one year given a confidence interval of 99.5%. The difference between VaR and expected loss is capital that insurance companies must hold. This amount is called regulatory capital when insurance companies calibrate their internal models to the 99.5% confidence level. Economic capital is a financial institution's own internal estimate of the capital it needs for the risks it is taking (Hull, 2010). So regulatory capital is a specific level of economic capital. Appendix A provides figures for Achmea's Solvency II economic capital per segment and risk type in 2012.

Solvency II distinguishes two approaches to risk quantification or more specific to cover the solvency capital requirement. These approaches are the standardized approach and the internal models approach. With the standardized approach risks are quantified in individual risk modules derived from the risk types as illustrated in table 1. These risk modules, except operational risk, are aggregated to form basic solvency capital requirement using a standard correlation matrix. In order to calculate capital charges the balance sheet is stressed on the specific risk factor and simply change in available capital is observed. This change in or effect on available capital determines capital charges. Capital requirement for operational risk is treated as a separate module which is added to the basic solvency capital requirement. This operational risk charge may not exceed 30% of basic solvency capital requirement. Under the standardized approach, calculation ultimately comes down to a factor-based approach. Meaning that operational risk capital charge is calculated by multiplying factors with parameters, for instance the earned premiums on life insurance obligations over the last twelve months. Because of its complexity and readability of this thesis the exact method of calculation is explained in more detail in appendix B. The standardized approach from Solvency II shows similarities with the standardized approach and the basic indicator approach from Basel III, which are also factor-based approaches.

The internal models approach specifies that solvency capital requirement may be calculated using full or partial internal models as long as they are approved by the regulator. Partial internal models may be used for any module or sub-module of the basic solvency capital requirement, the operational risk charge or the adjustments. This means that operational risk can be quantified for Solvency II using own internal models. However, Solvency II does not specify what these models can be or provide some examples of internal models used in insurance industry to quantify operational risk. In that aspect it differs from Basel III, where the loss distribution approach (LDA) and other approaches are presented as methods under the advanced measurement approach (AMA), Basel III's internal modelling approach to quantifying operational risk. Since Solvency II does not provide such methods, only procedures for approval and policies are described. To acquire approval from the regulator internal models should meet three criteria as illustrated in table 2, adopted from Doff (2012).

Statistical quality test	Calibration test	Use test
Are the data and methodology that underlie both internal and regulatory applications sound and sufficiently reliable to support both satisfactorily?	Is the SCR calculated by the undertaking a fair, unbiased estimate of the risk as measured by the common SCR target criterion (=99.5% VaR)?	Is the risk model genuinely relevant to and used within risk management?

Table 2: Internal model approval criteria (Doff, 2012)

Two other important criteria are the level of documentation around the process of producing the figures and how the business validates externally sourced models and data as applicable for its own business (Ernst&Young, 2008). Even though Solvency II does not provide guidelines to internal modelling, it is expected that research question two enhances insight into possibilities of using internal models to quantify operational risk.

3.3 Conclusion

Goal of this chapter is to present Solvency II with respect to operational risk modelling, hereby answering the first research question.

What requirements does Solvency II impose in quantifying operational risk?

Solvency II is the European Union's legislative framework for insurance industry. It is structured around three pillars focusing on capital requirements, supervisory review process and disclosure of risk management information to the public/supervisor. Six different risk types are identified which are life/non-life/health underwriting risk, market/credit risk and operational risk. For each of these risk types capital should be held to absorb unexpected losses, together this capital forms the solvency capital requirement. Insurance companies should hold capital at least as high as the solvency capital requirement. Solvency capital requirement is part of pillar one and stipulates how risks can be quantified. Solvency II proposes two methods to quantify operational risk. Firstly the standardized approach can be used which quantifies operational risk by multiplying factors with parameters, it therefore is a factor-based approach. Secondly insurance companies can use own internal models to quantify operational risk, but Solvency II does not provide guidelines to internal modelling. These internal models should satisfy several criteria before the regulator can approve the use of internal models. Solvency II allows combining the two methods for different risk types, for instance operational risk can be quantified using the standardized approach whereas market risk is quantified using an internal model.

4 Operational risk models

This chapter describes the literature review that is performed to answer second research question of this thesis focusing on academic literature about operational risk models. The literature is collected from different online academic databases, of which Scopus and Business Source Premier. Papers are selected on appropriateness and are found by combining search terms, including 'operational risk modelling', 'quantifying operational risk', 'Solvency II' and 'measuring operational risk'. Papers are also acquired using forward and backward citation searching or cited reference searching. Goal of the literature review is to come up with core concepts of operational risk modelling to structure the theoretical framework. This knowledge is a supplement to Solvency II, which is treated in the previous chapter, because Solvency II does not provide guidelines on internal modelling of operational risk. Therefore academic literature is expected to provide several models applicable to the internal modelling approach of Solvency II. Firstly an overview of academic literature related to operational risk modelling is provided to illustrate the current state and challenges regarding this topic. Secondly operational risk models are introduced and explained in more detail as far as they can be treated distinctly. Thirdly in the conclusion a theoretical framework is proposed that incorporates most important concepts of operational risk modelling.

4.1 Literature review

Operational risk has received increased attention over the last two decades as a distinct risk type that can be calculated separately and for which capital needs to be hold. From the nineties on banks and insurance companies have started to focus on this specific risk type, allocating resources and management attention to deal with operational risk. Operational risk was first included in the Basel II accord for banking industry regulation, so most literature on operational risk originates from the last ten to fifteen years (Ergashev, 2011). Due to the fact that Basel regulation for banking industry as well as Solvency II regulation for insurance industry allow for internal modelling of operational risk, many papers tend to focus on the aspect of operational risk modelling.

An important aspect in operational risk modelling is the purpose of quantification. Peccia (2003) argues that "the only purpose of an operational risk model is to give business leaders a tool for making better operational decisions. This exclusive purpose should guide and constrain each decision along the model construction process. Focusing on the decisional output of the model also avoids introducing tangential elements, which may be mathematically rigorous but less managerially useful." Peccia therefore does not see a regulatory purpose in quantifying operational risk. It is important in this research to clarify the purpose of quantifying operational (IT) risk and relate it to modelling deficiencies.

Any modelling/quantification/measurement of operational risk requires some form of data on which the model is based and the risk is measured. This is where the first challenges arise. Given the short existence of operational risk as a risk type relatively few data is available on operational risk losses, implicating all kinds of limitations to statistically analysing the available data (Guillen, Gustafsson, Perch Nielsen & Pritchard, 2007; Plunus, Hübner & Peters, 2012; Politou & Giudici, 2008). That is why models often combine various types of data to more or less overcome this situation of lacking internal datasets. Four different types of data can be distinguished that are used on a stand-alone basis or in any combination. These types are internal data, external data, expert data and prior knowledge of parametric models (Bolancé, Guillen, Gustafsson & Perch Nielsen, 2012; Embrechts & Hofert, 2011).

1) Internal data comprises the financial institution's own historical loss data. By its nature internal data is backward looking and does not include real catastrophic events that endanger a firm's capital. Internal data tend to be underreported, meaning that not all operational losses are reported. It is observed that the probability of reporting increases with the size of the operational risk loss (Buch-Kromann, Englund, Gustafsson, Perch Nielsen & Thuring, 2007).
2) External data consists of historical loss data experienced by other financial institutions or third parties. It may cover operational losses not yet experienced by the firm itself in fields where it has potential risk. Therefore external data is of added value and used by firms to better capture an operational loss distribution. Consortia exist of banks and/or insurers where loss data is pooled that can be used for internal modelling purposes. Difficulties with using external data for operational risk modelling come down to scaling issues and representativeness (Guillen et al., 2007). However, Shih, Samad-Kahn & Medapa (2000) propose a solution to the scaling issue by introducing a scalar formula, $estimated\ loss\ for\ bank\ A = observed\ loss\ for\ bank\ B * \left(\frac{bank\ A\ revenue}{bank\ B\ revenue}\right)^{0.23}$, hereby extending the applicability of external loss data.
3) Expert data entails information derived from experts or professionals in the field of operational risk. This can be considered to be a more qualitative approach to acquire quantitative loss data. Shevchenko & Wütrich (2006) argue that these expert opinions should be taken into account when quantifying operational risk, since this data is forward looking and thus describes future behaviour.
4) Prior knowledge of parametric models is information from the experience of fitting parametric models to data sets. Quantifying operational risk eventually means coming up with a distribution of operational losses over one year. Many different distributions exist and "it is clear that if you have some good reason to assume some particular parametric model of your operational risk distribution, then this makes the estimation of this distribution a lot easier" (Bolancé et al., 2012).

So it must now be clear that operational risk models require at least one of the four data types to be present in a company in order to quantify operational risk. What type of data is used depends on the operational risk model. From the regulatory frameworks Basel III and Solvency II it is known that there are factor based approaches and internal modelling approaches to quantify operational risk. The factor based approaches do not reflect operational risk exposure of a large insurer and only come up with a single capital amount and thus are not applicable to quantify individual operational risks from specific events or in specific business lines. Therefore these factor based approaches are not consistent with the goal of this research, which is to set first steps in developing an internal model to quantify operational IT risk, and are subsequently taken out of consideration. The models that are taken into consideration are internal models, whether or not these models are applicable from a regulatory perspective depends on if they meet requirements as set out in chapter three. As explained in chapter three Solvency II does not provide guidelines for its internal modelling approach, however Basel III does under its AMA (advanced measurement approach) internal modelling approach. In order to quantify the operational risk capital charge under the current regulatory framework for banking supervision many banks adopt the loss distribution approach (Shevchenko, 2009). This loss distribution approach (LDA) is one model to quantify operational risk and characteristics of this method are explained in the next section. For more in-depth application and possibilities of this model see Dutta & Perry (2007), Lambrigger, Shevchenko & Wüthrich (2007), Samad-Khan (2008), Shevchenko (2009) or Embrechts & Hofert (2011).

Another widely used method in operational risk quantification is extreme value theory or EVT. Extreme value theory is often used in conjunction with the loss distribution approach or other actuarial approaches because EVT better describes the tail region of a distribution which is of particular importance in operational risk management (Embrechts, Furrer & Kaufmann, 2003). Since extreme value theory focuses on tail region it is useful when VaR calculations are necessary, as is the case in operational risk quantification. Many authors have studied the use of EVT in operational risk modelling. Embrechts et al. (2003) present a brief introduction into basics of extreme value theory and modelling assumptions underlying extreme value theory. Chavez-Demoulin, Embrechts & Nešlehová (2006) stress the importance of EVT but also the pitfalls when using this methodology on operational risk loss data. Liqin & Hongfeng (2007) used EVT to measure operational risk and researched the use of copulas to aggregate risks, though the aggregation problem is out of the scope of this research. Another extensive application of the usefulness of extreme value theory to fit operational risk data is the research of Gourier, Farkas & Abbate (2009). Extreme value theory can thus be used to quantify operational risk and it is explained in more detail in the next section.

Next to the loss distribution approach and extreme value theory an often distinguished method to quantify operational risk is scenario analysis. “Because financial institutions only began collecting operational risk data recently, information from historically observed data is often insufficient to model operational risk reliably. A need exists for additional sources of information such as scenarios-hypothetical realizations of an institution’s, and broadly speaking the financial industry’s, inherent risks” (Ergashev, 2011). Scenario analysis is almost never used on a stand-alone basis but in addition to other operational risk modelling techniques. Ergashev (2011), Rippel & Teplý (2011), Cope (2012) and Dutta & Babbel (2013) all treat this topic of combining scenario analysis data with other types of data in quantifying operational risk. More on scenario analysis can be found in the next section on quantification methods.

Lastly one of the more recent methods or models to quantify operational risk is via Bayesian inference or Bayesian networks. These mathematical models are mainly based on Bayes theorem and useful because they allow combining different sources of data. Shevchenko & Wütrich (2006) and Lambrigger et al. (2007) used Bayesian inference to quantify operational risk, combining internal data with external data and expert opinion. Their research has shown that Bayesian inference is a useful model, especially to model low-frequency risks. Bayesian inference hereby eliminates the problem that a model is purely backward or forward looking. Cowell, Verrall & Yoon (2007) use Bayesian networks to model operational risk and conclude that main advantage of this method is that it incorporates expert opinion. Another application of Bayesian network theory to quantify operational risk is treated by Politou & Giudici (2008) but this research also focuses on the aggregation problem and simultaneously quantifying operational risks and therefore is of less importance to this research. From the literature review on Bayesian models it can be concluded that Bayesian inference as well as Bayesian networks can be used in quantifying operational risk. Bayesian networks model multiple operational risks, hereby also treating the aggregation problem. Bayesian inference tends to focus on individual operational risks and therefore is found to be better suitable for this research. From now on the model to quantify operational risk based on Bayesian theory is considered to be Bayesian inference.

Main methods to quantify operational risk emerging from the literature review have now been identified. Given the increasing importance of operational risk, the modelling aspect is subject to regular change. The identified models therefore constitute current practices in operational risk modelling. Apart from the loss distribution approach model, extreme value theory, scenario analysis and Bayesian inference other less frequently used models exist to quantify operational risk. One of such models concerns the transformation of the credit risk model CreditRisk+ to an operational risk model, OpRisk+ (Plunus et al., 2012). From clarity, readability and goal alignment purposes it has been decided not to focus on such smaller models but on the four models identified. In the next section these models are explained in more detail.

4.2 Quantification methods

After an extensive search through available literature it has been concluded that there are four main models to quantify operational risk. These models are the loss distribution approach, extreme value theory, scenario analysis and Bayesian inference. This section describes the working of these models and their main advantages and disadvantages. Goal of this research is to set first steps in developing a methodology to quantify operational IT risks, therefore these models act as the basis for this methodology.

4.2.1 Loss distribution approach

The loss distribution approach originates out of the banking industry as a method under the advanced measurement approach, Basel II’s internal modelling approach. It treats modelling of operational risk losses where these losses are a combination of two distributions, namely the loss frequency and the loss severity. The loss frequency distribution defines distribution of number of losses in one year in a certain risk category. The loss severity distribution defines distribution of amount of losses given that a loss occurs. Together these two distributions form the annual loss distribution of a certain operational risk. Mathematically the approach can be structured as follows:

$$S = \sum_{i=1}^{N} X_i$$

The sum S is the total loss of a certain operational risk in a specified time interval, usually this is one year. N is a random variable corresponding to the loss frequency. The distribution of X_i represents the loss severity distribution. It is often assumed that $X_i{}'s$ are independent and identically distributed and that each individual X_i is independent from N. However this assumption of zero correlation is arguable and widely discussed in literature. In order to acquire a distribution of the total loss (S) in one year simulation techniques are applied. Monte Carlo simulation can be used to draw figures from the loss frequency and loss severity distributions that together merge into a total loss distribution. When this is done repetitively and with enough iterations, all these individual losses (S) together specify the total loss distribution. The 99.5% VaR can be derived from this total loss distribution as a measure/quantification of risk compliant with Solvency II regulations (Dutta & Perry, 2007). The loss distribution approach can be seen as a sequential process including the following steps:

1) Estimate the loss frequency and loss severity distributions and its parameters of a certain operational risk based on relevant data, this is mostly internal loss data.
2) Apply simulation techniques such as Monte Carlo to draw figures from the loss frequency and loss severity distributions generating the annual total loss distribution (distribution of S).
3) Calculate the 99.5% VaR from the annual loss distribution. This risk measure embodies the quantification of operational risk.

The loss distribution approach process is depicted in figure 7.

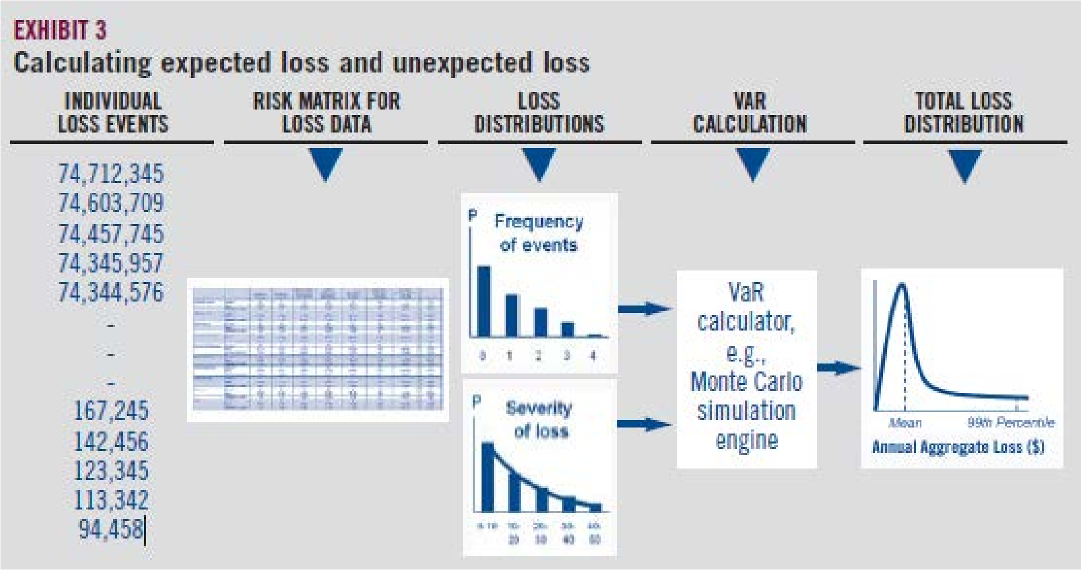
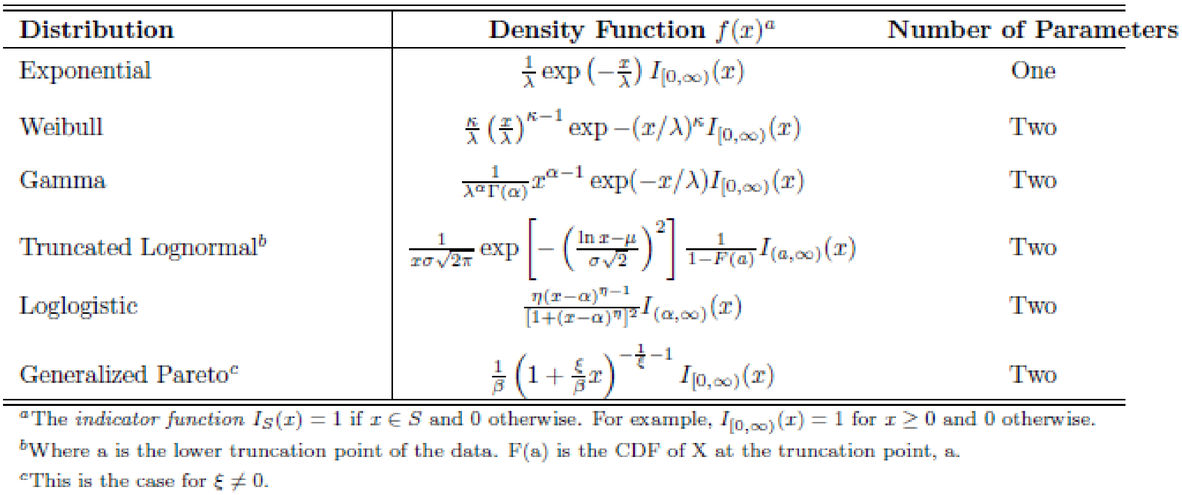


Figure 7: LDA (Samad-Kahn, 2008)

The loss distribution approach can be used to quantify single operational risks and to quantify multiple operational risks simultaneously. In the latter case challenges arise with respect to aggregation of operational risk. Since dependencies between operational risks fall outside the scope of this research no attention is given to the topic of aggregation/dependence/copulas within the loss distribution approach. Emphasis within literature lies on the aggregation problem and on the types of distributions that can be used to, or that best fit the loss frequency and loss severity distributions. Because the loss frequency distribution represents the number of times that a loss occurs in one year it is often characterized by a counting process such as the Poisson distribution, binomial distribution or the negative binomial distribution. The loss severity distribution can consist of several parametric distributions. Dutta & Perry (2007) fitted distributions as depicted in figure 8 on loss data from American financial institutions.



Distribution	Density Function $f(x)^a$	Number of Parameters
Exponential	$\frac{1}{\lambda} \exp\left(-\frac{x}{\lambda}\right) I_{[0,\infty)}(x)$	One
Weibull	$\frac{\kappa}{\lambda}\left(\frac{x}{\lambda}\right)^{\kappa-1} \exp -(x/\lambda)^{\kappa} I_{[0,\infty)}(x)$	Two
Gamma	$\frac{1}{\lambda^{\alpha}\Gamma(\alpha)} x^{\alpha-1} \exp(-x/\lambda) I_{[0,\infty)}(x)$	Two
Truncated Lognormal[b]	$\frac{1}{x\sigma\sqrt{2\pi}} \exp\left[-\left(\frac{\ln x-\mu}{\sigma\sqrt{2}}\right)^2\right] \frac{1}{1-F(a)} I_{(a,\infty)}(x)$	Two
Loglogistic	$\frac{\eta(x-\alpha)^{\eta-1}}{[1+(x-\alpha)^{\eta}]^2} I_{(\alpha,\infty)}(x)$	Two
Generalized Pareto[c]	$\frac{1}{\beta}\left(1+\frac{\xi}{\beta}x\right)^{-\frac{1}{\xi}-1} I_{[0,\infty)}(x)$	Two

[a] The *indicator function* $I_S(x) = 1$ if $x \in S$ and 0 otherwise. For example, $I_{[0,\infty)}(x) = 1$ for $x \geq 0$ and 0 otherwise.

[b] Where a is the lower truncation point of the data. F(a) is the CDF of X at the truncation point, a.

[c] This is the case for $\xi \neq 0$.

Figure 8: parametric distributions

These distributions do not capture the whole range of possible parametric distributions, as the g-and-h distribution and others were not included. Given the fact that operational loss data is mostly heavy tailed it is best fitted by heavy tailed distributions, for instance the Pareto distribution (Fontnouvelle, Rosengren & Jordan, 2007). So an important aspect of the loss distribution approach is what distribution to choose to model loss frequency and loss severity.

The loss distribution approach heavily relies on the use and thus existence of loss data and is therefore only applicable in situations where sufficient loss data is available. When this data is available the model proves to be useful to quantify operational risk in a time efficient way. It is important that distributions are chosen for loss frequency and loss severity that best fit available loss data. Aggregation of individual operational risks requires some form of dependency structure in the LDA framework. Main advantages and disadvantages of the loss distribution approach are presented in table 3.

Advantages	**Disadvantages**
time efficient	requires historical loss data
reliable	backward looking
consistent approach	i.i.d. modelling assumption

Table 3: LDA main advantages and disadvantages

4.2.2 Extreme value theory

Extreme value theory is a statistical technique dealing with maxima or high quantiles of probability distributions. It can be applied in various fields where random variables and probability distributions are used. Extreme value theory found its application in risk management because of the ability to model tail behavior of distributions. In risk management especially extreme deviations from what is expected are important and EVT is a technique that can be used to model these extreme deviations. With extreme value theory only extreme data points are used, so with respect to operational risk modelling only large losses are relevant. Because of its nature, EVT is especially useful to model rare events. In essence this comes down to modelling low frequency, high severity operational risks.

In extreme value theory a threshold value u needs to be defined over which excess losses are calculated. Say X_i's are historical losses, then $X_i - u$ corresponds to the excess loss over threshold value u. For sufficiently large u the unknown excess loss distribution $F_u(x) = P(X - u \leq x | X > u)$ approximately tends to follow a generalized Pareto distribution (GPD) given by $G_{\xi,\sigma}(x)$, where

$$G_{\xi,\sigma}(x) = \begin{cases} 1 - \left(\frac{1}{1 + \xi x/\sigma}\right)^{1/\xi} & if\ \xi \neq 0 \\ 1 - e^{\frac{-x}{\sigma}} & if\ \xi = 0 \end{cases}$$

σ and ξ are size and shape parameters and $\xi > 0, \xi = 0, \xi < 0$ represent the heavy tailed, medium tailed and light tailed case respectively. This distribution only models the tail of the loss distribution, in essence excess losses over threshold value u. However since risk management is especially about tail behavior of distributions and in general there is more data of a distribution's body, this is not considered to be a problem when applying EVT to quantify operational risk. From the excess loss distribution $F_u(x)$, that is assumed to follow the generalized Pareto distribution $G_{\xi,\sigma}(x)$, it is possible to calculate the 99.5% VaR. This 99.5% VaR estimate corresponds to Solvency II and is therefore useful to measure operational risk. In order to get the 99.5% VaR estimate the equation $F_u(x) = \propto = 0.995$ needs to be solved. Combining this equation with the generalized Pareto distribution fundamentals, VaR estimate with confidence level $\propto$ is given by:

$$\widehat{VaR}_\alpha = u - \frac{\hat{\sigma}}{\hat{\xi}}\left(1 - \left(\frac{N_u}{n(1-\propto)}\right)^{\hat{\xi}}\right)$$

In this notation u is the threshold value, N_u is the number of exceedances over the threshold value, n is the total sample size and $\hat{\sigma}, \hat{\xi}$ denote maximum likelihood estimators of ξ, σ. So applying EVT to quantify operational risk essentially comes down to following the next steps:

1) Define threshold value u over which excess losses follow a generalized Pareto distribution.
2) Estimate parameters of generalized Pareto distribution.
3) Calculate 99.5% VaR.

Pitfalls and discussion of extreme value theory relate to the choice of threshold value u and about applicability of EVT to operational loss data. Many authors have struggled over the appropriate choice of threshold value u and although the importance of this subject is realized, it goes beyond the scope of this research to further dig into it. Characteristics of operational loss data impose difficulties for reliability of standard EVT analysis, because of modelling assumptions. Extreme value theory assumes independent and identically distributed loss data, which is questionable given exploratory analysis of current available loss data in the market (Chavez-Demoulin et al., 2006; Embrechts et al., 2003). Main advantages and disadvantages of extreme value theory as an operational risk model are presented in table 4.

Advantages	**Disadvantages**
time efficient	choice of threshold value u
focuses on extremes (risk management)	backward looking
consistent approach	dependent on (enough) loss data
	i.i.d. modelling assumption

Table 4: EVT main advantages and disadvantages

4.2.3 Scenario analysis

Scenario analysis is a method that is widely used in various fields of business or science, including risk management. Over the last decade it has become an approach in operational risk modelling, mainly because of the lack of sufficient internal loss data and the forward looking feature of scenario analysis. “Scenarios are hypothetical realizations of an institution’s, or broadly speaking the financial industry’s, inherent risks” (Ergashev, 2011). Scenario analysis has the appealing feature that it describes future adverse advents that are not included in historical internal loss data, but plausible to impact the specific company. Data generated from scenario analysis is used to create more robust risk management and risk quantification. Scenario analysis can be used on a stand-alone basis to quantify operational risk, but most literature prescribes the use of scenario analysis as supplement to other approaches in operational risk quantification. That is why in literature especially incorporation of scenario analysis into risk quantification is discussed and not how scenario analysis should be conducted. In general it comprises using knowledge from experts or professionals in the company to assess and professionally judge possible future loss events. The identified scenarios can be derived from external historical loss data or tailored to fit the specific risk profile of the company, another advantage of scenario analysis. A specific structure for scenario analysis is not defined in this research, because there exist multiple ways to conduct scenario analysis in scientific literature. At Achmea, scenario analysis is already used and here experts judge the frequency, loss mode, ‘high’ loss and ‘high’ loss probability of certain loss events. This information is used to fit a Poisson distribution for loss frequency and a lognormal distribution for loss severity. Monte Carlo simulation is then applied to arrive at the total loss distribution on which VaR estimate can be calculated. An important aspect in scenario analysis is the unit of measure, in fact meaning what type of operational risk is quantified. Scenarios often do not fall precisely into risk categories of business lines and/or event types as proposed by Basel III framework. Cope (2012) extensively researched this subject of granularity, by introducing individual 'loss generating mechanism' on which scenario analysis is applied. For this research it is sufficient to state that it is crucial to critically define what type of operational risk is quantified or what the unit of measure is.

As explained, there exist multiple ways to conduct scenario analysis and the challenge remains what to do with the data. It can be treated on a stand-alone basis, but it can also be combined with other sources of data. It is believed that it is unnecessary to dig deeper into this subject and remain at the current level of abstraction. The process of scenario analysis is best described by the following chain of activities:

1) Select experts, determine unit of measure, and define scenarios.
2) Retrieve relevant data from experts about scenarios, for instance about loss frequency and loss severity.
3) Use scenario data to create annual loss distribution on a stand-alone basis or use scenario data as supplement to other operational modelling techniques.
4) Calculate 99.5% VaR from the annual loss distribution.

One of the difficulties of scenario analysis is that this method is resource intensive, especially with respect to time. Experts have to be chosen and workshops or meetings have to be arranged when performing scenario analysis. Also subjectivity and biases of human judgment negatively affect the reliability of scenario analysis. For instance, a business line manager responsible for a certain business process has a tendency to understate possible operational losses originating from that process, because he/she is evaluated on performance of that process. Main advantages and disadvantages of scenario analysis as an operational risk model are given in table 5.

Advantages	**Disadvantages**
focuses on extremes (risk management)	time intensive
forward looking	subjectivity and expert biases
company specific	unreliable when used on stand-alone basis

Table 5: Scenario analysis main advantages and disadvantages

4.2.4 Bayesian inference

Last identified model to quantify operational risk makes use of Bayesian theory and in the context of this research is described as Bayesian inference. Bayesian inference is preferred over Bayesian networks to model operational risk, because Bayesian inference is better able to model individual operational risks as already explained in section 4.1. Expert judgment used to form the basis in operational risk quantification, but treated on itself is considered to be too subjective. Historical internal loss data often lacks within companies as a basis for operational risk quantification and external loss data is hard to adapt to company specifics.

This situation creates a need for combining all or some of these types of data. Bayesian inference is an approach to combine various types of data that can be used for operational risk modelling purposes. Shevchenko & Wütrich (2006) propose a method based on Bayesian inference to combine expert data/external data with internal data, in essence two sources of data. Lambrigger et al. (2007) propose a method based on Bayesian inference to combine external data with internal data and expert data. Both studies are used in this research to clarify Bayesian inference and the research of Shevchenko & Wütrich is especially used for the operational risk model applicable to this research. This research is chosen instead of Lambrigger et al., because it is less complex and thus better aligns with this research's goal, to set first steps in developing an internal model for operational risk quantification. Also classical Bayesian inference is about combining two sources of data not three.

Every operational risk model is about modelling the annual loss distribution specific to the operational risk being modelled and then taking the 99.5% VaR as a measure of risk. This annual loss distribution can be considered to be a combination of two distributions, namely the loss frequency and loss severity distribution. Distribution types need to be chosen and specific parameters estimated. When these parameters are known, simulation techniques are used to calculate the annual loss distribution. Bayesian inference allows for estimation of loss frequency and loss severity parameters by combining various sources of data based on Bayes' theorem. Bayes' theorem, adopted from the work of Shevchenko & Wütrich (2006), is formulated as:

$$\hat{\pi}(\theta|X) = \frac{h(X|\theta)\pi(\theta)}{h(X)},$$

Where θ is a vector of parameters, X a random vector of observations, $\hat{\pi}(\theta|X)$ a posterior distribution of θ given X, $\pi(\theta)$ a prior distribution of θ, $h(X|\theta)$ a distribution of observations for given θ and $h(X)$ the marginal distribution of observations. Generally Bayes' theorem states that the posterior distribution, $\hat{\pi}(\theta|X)$, is the product of a prior distribution, $\pi(\theta)$, times a 'likelihood function' of observed data, $\frac{h(X|\theta)}{h(X)}$. The observed data acts as evidence against the prior belief of distribution of the 'true' parameters.

With respect to operational risk modelling the prior distribution can be estimated using expert data or external data. The posterior distribution is then calculated using Bayes' theorem, in essence weighting the prior distribution with the observed data, which is internal loss data. This posterior distribution can be used to calculate the predictive distribution of the next data point given observed data. For instance, the predictive distribution of the number of losses in the next year can be calculated. Using this distribution and the predictive loss severity distribution, via simulation, the 99.5% VaR estimate can be obtained from the annual loss distribution. In order to apply Bayes' theorem, distribution types for the prior and posterior distribution are assumed for which conjugate or alike distributions are useful. To illustrate the applicability of Bayesian inference to model operational risk an example is provided, again adopted from the work of Shevchenko & Wütrich (2006).

In order to estimate loss frequency distribution parameter of a certain operational risk the Poisson distribution is assumed with parameter λ. Prior distribution of λ is Gamma distribution with parameters α and β, which are specified by experts. N corresponds to the observed number of losses in year n. Since this research focuses on setting first steps in developing a model to pragmatically quantify operational IT risks, full mathematical justification is not provided here but referenced to the papers of Shevchenko & Wütrich (2006) or Lambrigger et al. (2007). The expected number of loss events in the next year, characterized by λ is defined as:

$$E[N_{n+1}|N] = E[\lambda|N] = \hat{\alpha} * \hat{\beta} = \beta * \frac{\alpha + \sum_{i=1}^{n} N_i}{1 + \beta * n} = w\bar{N} + (1-w)\lambda_0,$$

Where

$$\bar{N} = \frac{1}{n}\sum_{i=1}^{n} N_i = estimate\ of\ \lambda\ from\ observed\ loss\ data\ represented\ by\ N_i's,$$

$$\lambda_0 = \alpha * \beta = estimate\ of \lambda\ as\ specified\ by\ experts, the\ prior\ distribution,$$

$$w = \frac{n}{n + 1/\beta} = the\ weight\ used\ to\ combine\ \lambda_0\ and\ \bar{N}, prior\ and\ 'likelihood'.$$

Similar formulas can be mathematically derived using other conjugate distributions or when estimating loss severity parameters. Applying Bayesian inference to model operational risk consists of the following core activities:

1) Determine a prior distribution for parameters of loss frequency and loss severity and estimate parameters using expert data.
2) Update the prior distribution as specified by experts with the observed internal loss data using Bayes’ theorem and derived formulas tailored to the specific case. This should result in estimations of loss frequency and los severity parameters.
3) Use Monte Carlo simulation to construct the annual loss distribution.
4) Calculate 99.5% VaR from the annual loss distribution.

One of the limitations of using Bayesian inference models to quantify operational risk is its complexity. Especially when three sources of data are combined, calculations are extensive and not easily performed by someone who has limited skills in mathematics. The method also requires effort to gather the expert data and therefore is time intensive. Next to that, reliability of Bayesian inference is dependent on the modelling assumptions underlying this model. Main advantages and disadvantages of Bayesian inference as an operational risk model are given in table 6.

Advantages	Disadvantages
combines different sources of data	complexity
both backward and forward looking	time intensive
company specific	i.i.d. modelling assumption

Table 6: Bayesian inference main advantages and disadvantages

4.3 Conclusion

Goal of this chapter is to clarify the process of operational risk modelling and its most important concepts, especially focusing on operational risk models from academic literature. By doing so, research question two is answered.

What models are being used in academic literature to quantify operational risk?

In order to solve this research question an extensive literature review is performed of which main concepts are presented in the conceptual framework illustrated in figure 9.

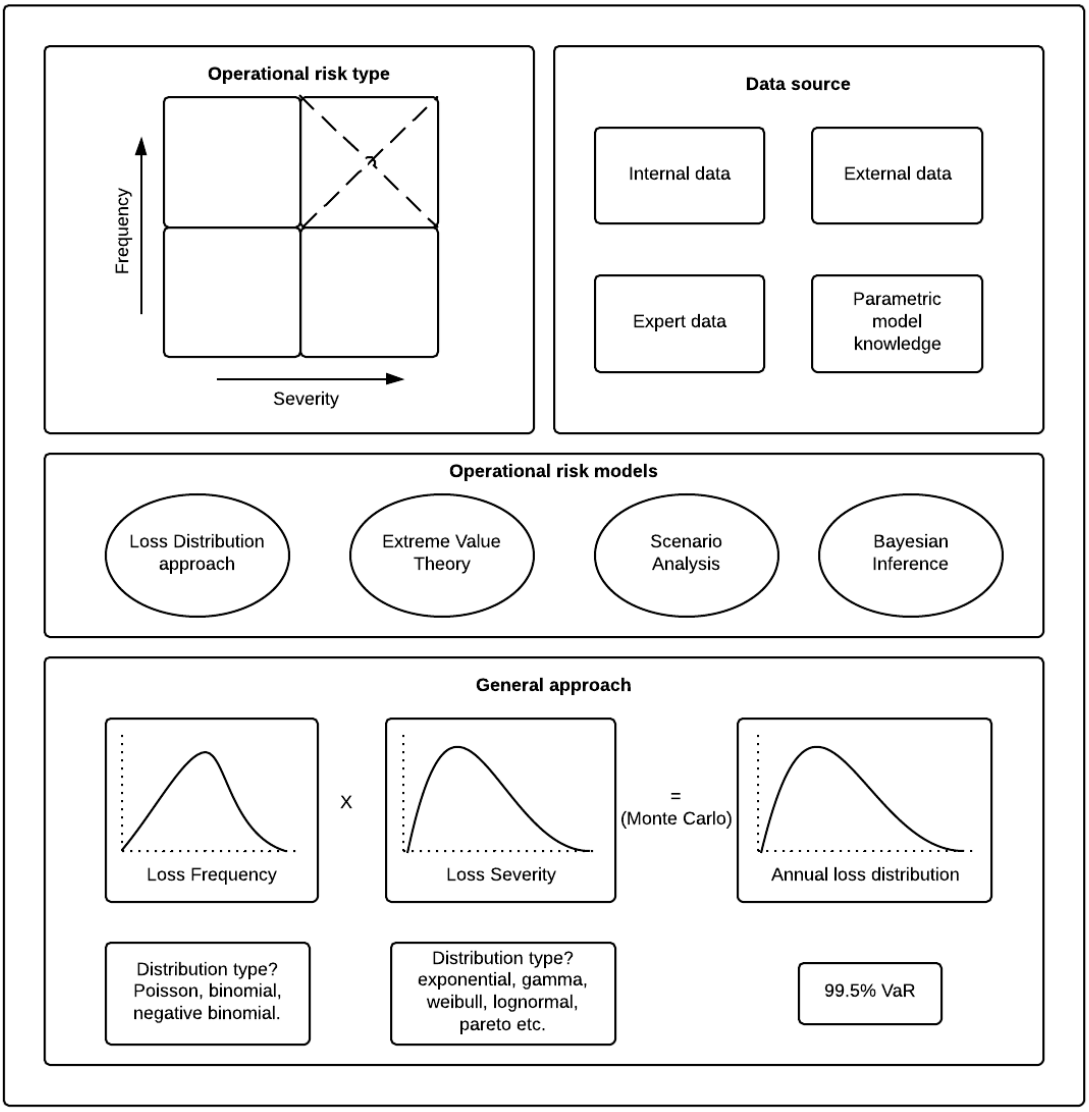


Figure 9: Conceptual framework

One of the main challenges in operational risk modelling is data or more specifically the lack of (loss) data. From the literature review four distinct data sources have been identified, namely internal data, external data, expert data and prior knowledge of parametric models. Any operational risk model is dependent on one or a combination of these data sources. Another important aspect of operational risk modelling is the operational risk type, in essence what operational risk type is being quantified. This aspect has not received full attention in this chapter, because it is covered in the next chapter where research question three is answered. However the importance is already stressed, since different operational risks are differentially distributed and thus might require an alternative approach.

The general approach in operational risk quantification is to determine the annual loss distribution of a specific operational risk from which the risk measure (99.5% VaR) can be derived. The annual loss distribution can be composed out of two specific distributions, namely the loss frequency distribution and the loss severity distribution. In literature discussion exists on what type of distribution best fits these loss frequency and loss severity distributions. The Monte Carlo simulation technique can be used to combine loss frequency and loss severity distributions to calculate the annual loss distribution.

Four main models have been identified that are used in academic literature to quantify operational risk:

- Loss Distribution Approach (LDA)
- Extreme Value Theory (EVT)
- Scenario Analysis (SA)
- Bayesian Inference (BI)

Each of these models has its advantages and disadvantages that are presented in section 4.2 and is thus best applicable to quantify a specific operational risk. However, available data might restrict the use of one of these four models to quantify operational risk. Lastly it is important to notice that reliability of any operational risk model is dependent on modelling assumptions and data characteristics.

5 Operational IT risk and operational risk classification

Emphasis has been laid on operational risk in general and how to quantify operational risk, whereas this research is about setting first steps in developing a model to quantify operational IT risk for Achmea's IM&IT division. The role of information technology systems is becoming increasingly important in the financial services industry. Operational IT risk is considered to be a subset of operational risk and a concept that is not yet clearly defined in this research. Classification of operational (IT) risk is required to adequately quantify operational risks. From the conceptual framework proposed in section 4.3 it can be seen that operational risk type is of importance in operational risk modelling. In essence this comes down to defining exactly what operational risk is being quantified. This chapter tries to overcome these issues by specifying what an operational IT risk is and by identifying and assessing operational risk classification schemes.

5.1 Operational IT risk

The concept of operational risk is clearly defined in the solvency II framework for insurance industry and formulated as:

"The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events" (BIS, 2001).

Operational IT risk is a subset of operational risk related to the information technology of a company. "IT risk is a potential damage to an organisation's value, resulting from inadequate managing of processes and technologies. IT risk includes the failure to respond to security and privacy requirements, as well as many other issues such as: human error, internal fraud through software manipulation, external fraud by intruders, obsolesce in applications and machines, reliability issues or mismanagement" (Savić, 2008). The definition of operational IT risk off course is strongly related to that of operational risk and it is questionable whether operational IT risk can be captured stand-alone and apart from other operational risks. This is especially the case in insurance companies that rely heavily on the use of information technology to support core operations. After discussion with operational risk managers from Achmea IM&IT the definition of Savić (2008) appeared to be most appropriate to explain what an operational IT risk is. But in a broader context and related to the Solvency II directive a general definition of an operational IT risk is composed.

"The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events related to the information technology of a company."

5.2 Classification

One of the important aspects of operational risk modelling is classification of operational risk. In essence this comes down to defining the level at which individual operational risks are quantified. The standardized approach method from Solvency II proposes one capital figure for operational risk for the whole company. Meaning that just one operational risk is identified and in fact no subdivision takes place. Since this does not capture the risk sensitiveness of large insurers, they often quantify several operational risks that together aggregate to total operational risk. In order to effectively aggregate these individual operational risks some form of classification is required. The degree to which individual operational risks are quantified is called granularity. “An operational risk category (ORC) is the level (e.g., organizational unit, operational event type, or risk category) at which the bank’s model generates a separate distribution for estimating potential losses” (Embrechts & Hofert, 2011). Granularity and classification therefore define what individual operational risks are for which separate loss distributions are estimated. The most widely used classification scheme stems from the Basel II framework of the banking industry and classifies operational risk according to several business lines and event types. These different business lines and event types are presented in table 7.

Business line	**Event type**
Corporate finance	Internal fraud
Trading and sales	External fraud
Retail banking	Employment practices and workplace safety
Commercial banking	Clients, products, and business practices
Payment and settlement	Damage to physical assets
Agency services	Business disruption and system failures
Asset management	Execution, delivery, and process management
Retail brokerage	

Table 7: Basel II operational risk classification (Hull, 2010)

Because this classification scheme originates from the banking industry it cannot be used one on one in the insurance industry. The fact that Solvency II did not adopt this classification scheme and did not propose an alternative also indicates that it cannot be readily used in the insurance industry. The idea is that there exist seven distinct operational risk events that can be present in all eight business lines of a bank. This leads to 7*8=56 operational risk categories for which data needs to be hold. “According to the 2008 LDCE, 45% of the banks have 20 or fewer ORCs, 74% have 100 or fewer, and 9% have over 100. For defining their ORCs, 21% use only business line designations, 29% use only event type designation, and 40% use a combination of both” (Embrechts & Hofert, 2011). Operational risk classification creates the need for aggregating operational risk categories to form operational risk capital. The way this should be done is out of the focus of this research, but widely discussed in literature. For more information about this aggregation problem, see Chavez-Demoulin et al. (2006) or Liqin & Hongfeng (2007).

At Achmea, classification of operational risk is related to that of the Basel II framework. Seven different event types are identified and operational risks should be defined according to a cause-event-effect scheme. Idea is that an operational risk event may have several causes leading to the occurrence of the event, which on itself has several effects. The different causes, events (Basel II) and effects identified at Achmea are presented in figure 10.

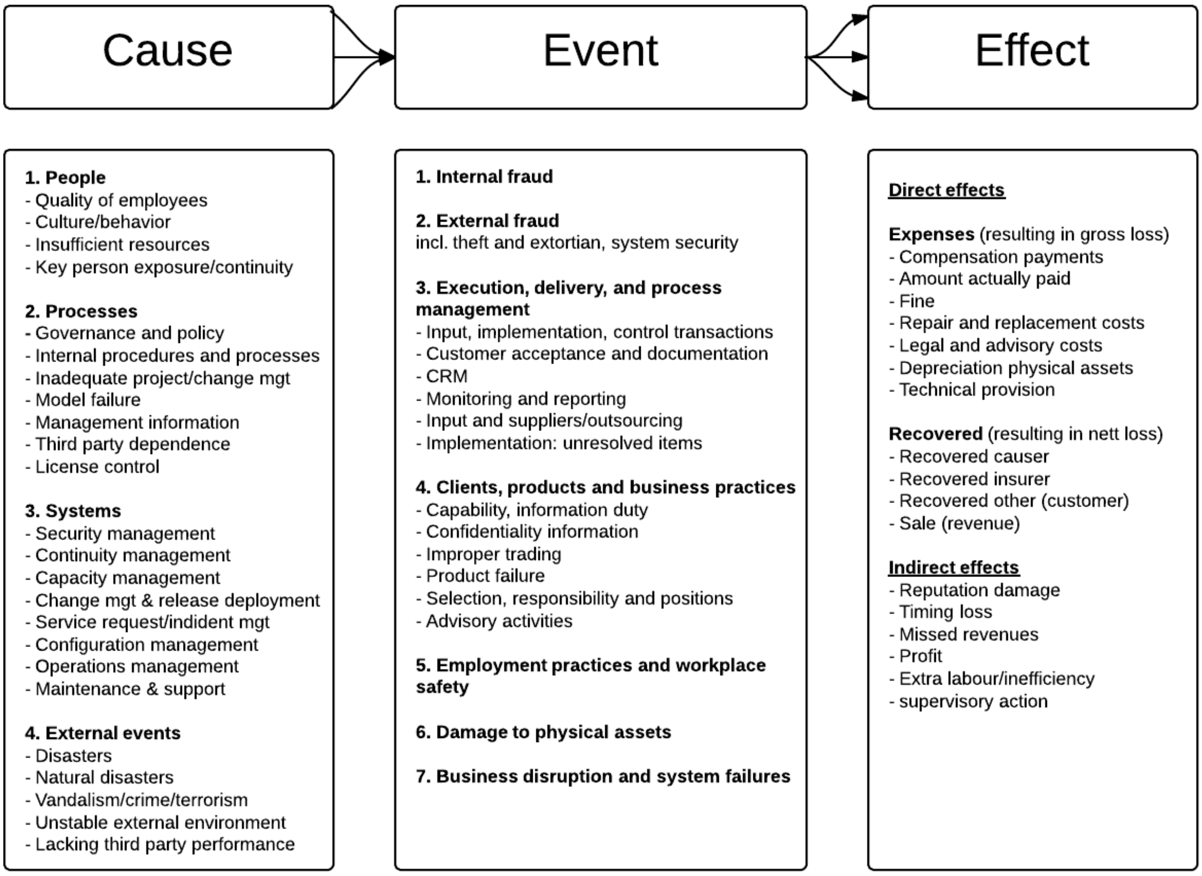

Cause
Event
Effect
1. People
- Quality of employees
- Culture/behavior
- Insufficient resources
- Key person exposure/continuity
2. Processes
- Governance and policy
- Internal procedures and processes
- Inadequate project/change mgt
- Model failure
- Management information
- Third party dependence
- License control
3. Systems
- Security management
- Continuity management
- Capacity management
- Change mgt & release deployment
- Service request/indident mgt
- Configuration management
- Operations management
- Maintenance & support
4. External events
- Disasters
- Natural disasters
- Vandalism/crime/terrorism
- Unstable external environment
- Lacking third party performance
1. Internal fraud
2. External fraud
incl. theft and extortian, system security
3. Execution, delivery, and process management
- Input, implementation, control transactions
- Customer acceptance and documentation
- CRM
- Monitoring and reporting
- Input and suppliers/outsourcing
- Implementation: unresolved items
4. Clients, products and business practices
- Capability, information duty
- Confidentiality information
- Improper trading
- Product failure
- Selection, responsibility and positions
- Advisory activities
5. Employment practices and workplace safety
6. Damage to physical assets
7. Business disruption and system failures
Direct effects
Expenses (resulting in gross loss)
- Compensation payments
- Amount actually paid
- Fine
- Repair and replacement costs
- Legal and advisory costs
- Depreciation physical assets
- Technical provision
Recovered (resulting in nett loss)
- Recovered causer
- Recovered insurer
- Recovered other (customer)
- Sale (revenue)
Indirect effects
- Reputation damage
- Timing loss
- Missed revenues
- Profit
- Extra labour/inefficiency
- supervisory action

Figure 10: Operational risk classification Achmea (Achmea, 2010)

When using this classification scheme it is clear that an operational risk event should be quantified and not a cause or an effect. Though it allows for inclusion of causes and effects of operational risk events. The scheme also introduces the complexity in operational risk classification, in that events may have several causes or that multiple events may be triggered by the same cause. In other words, there is a certain interrelation in operational risk modelling that makes distinct classification hard to achieve. This, combined with the fact that Solvency II proposes no operational risk classification scheme, creates room for discussion and indistinctness regarding operational risk modelling. Another consequence is that data collection and sharing becomes more difficult in the insurance industry when there is no industry wide consensus on operational risk classification. It is observed that insurers adopt the Basel classification in absence of specific regulatory (insurance industry) operational risk classification.

Last two classification schemes provide classification for operational risk as a whole. This research is about quantifying operational IT risk, which is a subset of operational risk. But operational IT risk is not an operational risk category compliant with the Basel II classification scheme and is thus intertwined with the business lines/event types scheme. Meaning that it is hard to squeeze operational IT risk into Basel's operational risk categories. Operational IT risk on itself can be further subdivided into different categories of operational

IT risk. Research of Savić (2008) has shown that operational IT risk can be classified into four different categories, which are:

1) Security risk
2) Availability risk
3) Performance risk
4) Compliance risk

Security risk corresponds to operational risk arising from unauthorised access to the information technology of a company, for instance through an external attack by hackers. Availability risk is the risk that certain systems or websites are not available for service for a specific period of time. When the payment system of Achmea is down, customers are not able to file their claims, posing an availability risk for Achmea. Performance risk is the risk that current information technology underperforms and does not fully contribute to organisational value. Compliance risk is the risk of potential losses arising from not meeting regulatory standards or business policy (Savić, 2008).

Any insurer can use its own classification scheme for operational risk and for operational IT risk. It is observed that operational risks are constructed without using proper risk classification or that operational risks cannot be fitted into business lines or event types. For instance availability risk, from the research of Savić, covers several business lines and relates to several event types. It is therefore a challenge to quantify availability risk when no data is collected specific to this risk category. From the analysis it must be clear that operational risk classification is a difficult but necessary part of operational risk modelling.

5.3 Conclusion

Aim of this chapter is to define what an operational IT risk is and to discuss operational risk classification, hereby answering the third research question of this thesis.

What are operational IT risks and how can it be classified?

Operational IT risk is a subset of operational risk and best defined as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events related to the information technology of a company." One of the important aspects of operational risk modelling is classification of operational risk. Solvency II does not propose an operational risk classification scheme and that is why many insurers adopt a modified version of Basel II's classification scheme of business lines and event types, including only the event types. It is observed that it is a challenge to properly classify operational risk, because of the complexity and interrelations of causes, events and effects. There should be industry wide classification of operational risk in the insurance industry. Operational risks should be fitted in this classification, only then data can be properly collected and shared. Although there is no such classification yet, it is proposed that the insurance industry can adapt the Basel classification scheme of business lines and event types. It has already been concluded that the event types are also applicable to the insurance industry, but the business lines are related to banking organizations. An alternative approach therefore is to create new business lines specific to insurance organizations, hereby creating a business lines and event types scheme for the insurance industry. Business lines include, among others, life, non-life, health, bank and IT. This approach is still a rough concept and it requires further concretisation, therefore it is advised that this topic is further researched.

From the literature review in the previous chapter it is concluded that internal data is crucial in operational risk modelling. When identified operational risks do not coincide with an operational risk category, modelling becomes difficult due to data issues. In those cases just expert data can be used to quantify operational risk. So operational risk quantification requires some form of classification, because then data can be collected corresponding to the specific operational risk. Operational IT risk can also be further classified into security risk, availability risk, performance risk and compliance risk. It is observed that operational IT risk relates to several business lines and event types, posing difficulties in using internal data from this classification scheme to quantify individual operational IT risk. This situation creates challenges for the practical usefulness of the described models in chapter four of this thesis, of which some rely heavily on the availability of internal loss data. In the next chapter these issues of operational risk modelling are further treated from a practical point of view.

6 Operational risk model in practice

Confidential

7 Conclusions & Recommendations

Main conclusions and recommendations of this research are presented in this chapter. Core problem of this research is that insufficient quantification of operational IT risk takes place at Achmea IM&IT. The corresponding central research question is formulated as:

What is the financial impact of operational IT risk at Achmea's IM&IT division?

Due to time constraints it is impossible to quantify all operational IT risks and thus to fully answer this question. Therefore this research aims to set first steps in developing an internal model to quantify operational IT risk. Most important concepts related to operational risk modelling are presented in this research and a first attempt is made to quantify the operational IT risk of DDoS cybercrime. By doing so, the practical usefulness of theoretical operational risk models can be evaluated and the central research question can be partially answered.

7.1 Conclusions

Main conclusions of this research are as follows:

Insufficient internal loss data available

Most operational risk models, like extreme value theory, loss distribution approach and to a lesser extent Bayesian inference, rely heavily on the availability of internal loss data. At Achmea, there is insufficient internal loss data available to act as a basis for these models, let alone at the Achmea IM&IT level. Collection of internal loss data requires proper operational risk classification, because operational losses need to be allocated to an operational risk category. Operational IT risks are often identified on an ad hoc basis, meaning that they do not fit into a specific operational risk category for which loss data is (will be) collected. This means that in the process of operational IT risk quantification, the absence of internal/external loss data is a recurring issue. Therefore operational risk models that are purely based on internal loss data, in fact extreme value theory and loss distribution approach, are not considered to be practically useful when quantifying operational IT risk. In practice, this means that a combination of models and data is required to quantify operational IT risk. Expert data is then the most important source of data in quantifying operational IT risk.

General approach in operational IT risk modelling

The four identified operational risk models in this research differ in detail, but all follow the same general approach. This general approach entails the estimation of a loss frequency and loss severity distribution of an operational IT risk. Several distribution types can be used to fit these distributions and in this research the Poisson and lognormal distributions are used. Four data sources can act as the basis for estimation of the parameter(s) of loss frequency and loss severity distribution. These sources are internal loss data, external loss data, expert data and prior knowledge of parametric models. From the loss frequency and loss severity distributions of an operational IT risk, the annual loss distribution can be constructed. The 99.5% VaR as well as the regulatory capital figure can be derived from the annual loss distribution as measures of the financial impact of the specific operational IT risk.

Uncertainty is part of operational (IT) risk quantification

The process of operational IT risk quantification is subject to uncertainty. On the one hand this uncertainty stems from the assumptions underlying operational risk modelling, like the assumption that loss frequency and loss severity are independent. On the other hand this uncertainty stems from the data and thus the input parameter(s) value(s). For instance expert data may be biased or internal loss data may be underreported. Limitations are simply a part of operational risk modelling and the resulting capital figure, in essence the measure for financial impact, should be seen in that perspective. Therefore the quantification of operational IT risk should mainly contribute to managerial decision making concerning operational IT risk ranking and control.

7.2 Recommendations

Main recommendations of this research are as follows:

Theoretical framework as guidance

Aim of this research is to set first steps in developing a methodology to quantify operational IT risk in order to assess the financial impact of these risks. It is concluded that most theoretical operational risk models are insufficiently or partly capable of quantifying operational IT risk. Therefore it is advised to use the theoretical framework of this research as guidance in every operational IT risk quantification process. This framework displays most important concepts related to operational risk quantification and thus helps in structuring the process. In essence this process comes down to identifying the operational IT risk that is quantified and assessing what data sources are available. Data availability determines what models or combination of models can be used to quantify the operational IT risk. The general approach, as described in the previous section, can be used to finish the process.

Quantifying malware cybercrime

In this research, due to time constraints, solely the operational IT risk of DDoS cybercrime is quantified. However, experts at Achmea judge that the expected contribution of DDoS cybercrime to the total risk of cybercrime is low. In order to get a better understanding of the total (strategic) operational IT risk of cybercrime it is advised to quantify the operational IT risk of malware cybercrime as well as other components of cybercrime. Apart from cybercrime, it is advised to further enhance the quantification of main operational IT risks at Achmea IM&IT. Since only then it is possible to assess the full financial impact of operational IT risk at Achmea IM&IT, in essence the central research question of this thesis. When main operational IT risks are quantified it adds to better managerial decision making concerning risk ranking, risk awareness, costs/benefits of risk mitigating efforts and thus ultimately to better operational risk control.

8 Discussion

In the first section of this chapter, findings from this research are critically reviewed on scientific relevance and on how this research contributes to the field of operational risk modelling. It is concluded that there are many limitations in operational risk modelling that impact the reliability of quantifying operational risk, these limitations are addressed in the second section of this chapter. Lastly recommendations for further research, with respect to operational risk quantification, are presented.

8.1 Scientific relevance

This research aims to set first steps in developing an internal model to quantify operational IT risk for Achmea IM&IT. In order to do so, an extensive search through available literature regarding operational risk modelling is performed as well as an analysis of regulatory requirements. Current and best practices in the field of operational risk quantification have been identified and a systematic overview is provided of main operational risk models and its advantages and disadvantages. Therefore this literature review has not resulted in significant new operational risk models, as this is not the goal of this research. It has however, resulted in a systematic and clear overview of most important concepts related to the process of operational risk quantification. Most literature tends to focus on the application of a particular operational risk model. This research adds to the literature in that it puts operational risk modelling in a broader perspective, before applying a particular model to quantify operational risk. The theoretical framework of this research can act as a starting point in every operational risk quantification process. Apart from theory, this research also analyses operational risk models in the field. An attempt is made to quantify the operational IT risk of DDoS cybercrime. In the literature, little information was found regarding the practical application of operational risk models. Often availability of internal loss data is assumed, where in practice there is regularly insufficient internal loss data to ‘feed’ the operational risk model. Or internal loss data relates to event types at high, abstract levels, where in practice a strong need exists to quantify more specific operational risks. So in order to apply theoretical operational risk models in the practical world, strong assumptions need to be made or combinations of models need to be used. In that perspective, this research adds to the literature by applying the theoretical operational risk models to a real practical situation instead of researching just an aspect of these theoretical operational risk models. This more pragmatic approach to operational risk modelling is believed to be a good addition to the current literature about operational risk quantification. Nevertheless, given the relative short time frame of this research several assumptions had to be made and the scope of this research remained limited. In the next section these limitations are presented that impact the reliability and validity of this thesis.

8.2 Limitations

The process of operational risk quantification is a complex and quite new field in risk management. Therefore limitations with respect to reliability and validity of operational risk modelling exist and assumptions need to be made to enhance usability of the process. Main limitations regarding operational risk modelling in general and of this research are as follows:

- **Underreporting**
  Internal loss data or external loss data tends to be underreported, meaning that not all losses related to the operational risk are reported. A threshold often exists in databases above which losses are reported. End result is that the loss data does not truly reflect the distribution of losses related to the operational risk that is quantified.
- **Loss reporting**
  Are losses reported in databases net losses, or gross losses? In other words do losses reflect the losses after mitigating efforts or do they reflect the losses without mitigating efforts. Again this impacts reliability, because historical loss data might not reflect the 'true' distribution of operational risk losses.
- **Combination of data**
  There exist several methods or ideas on how to combine various data sources in operational risk modelling. In this research it is assumed that Bayesian inference is appropriate for this purpose. However other methods might be useful and also other/more types of data can be combined.
- **Model risk**
  There is risk involved in using a specific model to quantify operational risk. Different models using the same data might lead to different result concerning the financial impact of operational risk.
- **Modelling assumptions**
  In operational risk modelling (loss) data is often believed to be independent and identically distributed. Also loss frequency and loss severity are assumed to be independent. These independence and i.i.d. assumptions are questioned in literature, however in this research taken as valid. Also stationarity and repetitiveness as well as time dependence of loss data are not researched. All of these elements impact the reliability of operational risk modelling.
- **Distribution type**
  In this research the Poisson distribution is used to model loss frequency and the lognormal distribution is used to model loss severity. These distributions are chosen because of best/current practices in the field and because of suitability. The whole discussion about what type of distribution best fits loss frequency and loss severity is left out of the scope of this research. This topic is extensively discussed in literature, see for instance Dutta & Perry (2007).
- **Aggregation**
  This research does not touch upon the aggregation problem of operational risk modelling. The quantification of individual operational risks creates a need to aggregate these risks to acquire a total operational risk capital. One of the ways to achieve this is by copulas. This research leaves the aggregation problem out of consideration, because single operational risk events form the basis for quantification. The purpose is not to come up with a total operational risk capital amount. It also means that diversification effects from aggregating operational risks are not examined in this research.

- **Granularity**
  Granularity is about the level at which individual operational risk events are quantified. The lower the level at which individual operational risks are modelled the more complex the aggregation issue becomes. On the other hand, the higher the level at which individual operational risks are modelled the worse loss data reflects the 'true' distribution. A choice has to be made concerning granularity in operational risk modelling, but this affects reliability.
- **Interdependence**
  The question is to what extent individual operational risk events can be treated independent or on itself. The complexity in operational risk modelling lies in the interrelation between causes, events and effects. This might make the allocation of losses to specific operational risks difficult and ambiguous. However most operational risk models rely on the use of internal loss data to measure the financial impact of that operational risk.
- **VaR**
  In this research the 99.5% VaR is used for single operational risk events as a measure of risk. The use of this risk measure for single events is arguable, since aggregation/correlation/diversification might lead to a different ranking of operational risk. When all individual operational risks are aggregated, the composition of total operational risk capital might be different than the composition of all individual operational risks treated alone.

8.3 Further research

One of the most important concepts in operational risk modelling is the classification of operational risk or the granularity in operational risk quantification. It is concluded that there does not exist a classification scheme specific to the insurance industry. What can be seen is that insurers adopt the event types/business lines classification from Basel regulations of the banking industry. Although banks and insurers are quite related, it is advised to further research what classification best fits to the insurance industry. This is of crucial importance in operational risk modelling, because the reporting of internal loss data is based on this classification. Most operational risk models rely heavily on the availability of proper internal loss data.

Another suggestion for further research relates to the sensitivity of operational risk quantification to the input parameters of loss frequency and loss severity distributions. In essence, quantification comes down to the estimation of parameters of loss frequency and loss severity distributions. These figures leave room for discussion and people might argue that using slightly different figures lead to very different results. It would be interesting to research this assumption by performing a sensitivity analysis with respect to the input parameters of the loss frequency and loss severity distributions. This analysis might take some of the skepticism towards operational risk modelling away.

Lastly, an interesting topic for further research is the subjectivity of experts. Given that internal or external loss data is often lacking at companies, they often fall back in using expert data as basis for operational risk quantification. The problem with expert data is that expert judgment has a subjectivity bias. The ability of experts to reliably judge risk is discussable. Research into reliability of expert judgment is useful, since most companies still rely on this source of data in the absence of other data sources. This issue has also been the case in this research, where the loss severity distribution was based upon expert data. One way to conduct such a research is to let experts judge the mode, 'high' loss and 'high' loss probability of a loss severity distribution of a certain operational risk. Implicitly, they have also estimated the mean and median of that distribution, which can be calculated analytically. But by letting experts also judge the mean and median themselves, these figures can be compared with the mean and median that was already analytically derived.

Bibliography

Achmea, (2010). *Eureko Achmea incidentenbeleid 1 0 0 0*. Obtained from https://achmeanet-divisie.hosting.corp/sites/08/beleid/Documents/Achmea%20Incidentenbeleid.pdf

Achmea, (2013). *Achmea annual report 2012*. Obtained from https://www.Achmea.nl/financieel/jaarverslagen/Paginas/default.aspx

Achmea, (2013). *About IM&IT*. Obtained from https://Achmeanet-divisie.hosting.corp/sites/10/overimit/Pages/default.aspx

Arbor, (2011). *Planning security budgets: quantify the financial risk of DDoS*. Obtained from: www.arbornetworks.com

Basel Committee on Banking Supervision, (2001). *Operational risk*. Obtained from http://www.bis.org/publ/bcbsca07.pdf

Basel Committee on Banking Supervision, (2011). *Basel III: A global regulatory framework for more resilient banks and banking systems*. Obtained from http://www.bis.org/bcbs/basel3.htm

Blumberg, B., Cooper, D.R. & Schindler, P.S. (2008). Business Research Methods. New York: McGraw-Hill Education.

Bolancé, C., Guillen, M., Gustafsson, J. & Perch Nielsen, J. (2012). Quantitative operational risk models. Boca Raton: Taylor & Francis group.

Buch-Kromann, T., Englund, M., Gustafsson, J., Perch Nielsen, J. & Thuring, F. (2007). Non-parametric estimation of operational risk losses adjusted for under-reporting. Scandinavian actuarial journal, 4, 293-304.

Chavez-Demoulin, V., Embrechts, P. & Nešlehová, J. (2006). Quantitative models for operational risk: extremes, dependence and aggregation. Journal of banking & finance, 30, 2635-2658.

Cope, E.W. (2012). Combining scenario analysis with loss data in operational risk quantification. The journal of operational risk, 7, 39-56.

Corero, (2012). *Protecting the enterprise against today's distributed denial of service attacks*. Obtained from http://www.corero.com/resources/files/white-papers/CNS_Protecting-the-Enterprise-Against-Todays-DDoS-Attacks_WP.pdf

Cowell, R.G., Verrall, R.J. & Yoon, Y.K. (2007). Modeling operational risk with Bayesian networks. The journal of risk and insurance, 74, 795-827.

Deloitte, (2010). Cyber crime: a clear and present danger. Obtained from http://www.deloitte.com/assets/DcomUnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf

Doff, R. (2011). Risicomanagement bij verzekeraars. Amsterdam: NIBE-SVV.

Doff, R. (2012). *College UT 4juni2012*. Obtained from https://blackboard.utwente.nl/webapps/portal/frameset.jsp

Dutta, K. & Perry, J. (2007). A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital. Federal Reserve Bank of Boston, 6, 1-93.

Dutta, K. & Babbel, D.F. (2013). Scenario analysis in the measurement of operational risk capital: a change of measure approach. Journal of risk and insurance, 1, 1-26.

Embrechts, P., Furrer, H. & Kaufmann, R. (2003). Quantifying regulatory capital for operational risk. Derivatives use, trading & regulation, 9, 217-233.

Embrechts, P. & Hofert, M. (2011). Practices and issues in operational risk modelling under Basel II. Lithuanian mathematical journal, 51, 180-193.

Ergashev, B.A. (2011). A theoretical framework for incorporating scenarios into operational risk modelling. Federal Reserve Bank of Richmond, 1, 1-21.

Ernst&Young, (2008). *Measuring operational risk*. Obtained from http://www.ey.com/Publication/vwLUAssets/Industry_Insurance_SolvencyII_Measuring_operational_risk/$file/Industry_Insurance_SolvencyII_Measuring_operational_risk.pdf

European Union, (2009). *Solvency II Directives*. Obtained from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:335:0001:0155:EN:PDF

Fontnouvelle de, P., Rosengren, E.S. & Jordan, J.S. (2007). Implications of alternative operational risk modeling techniques. The risks of financial institutions, 1, 475-511.

Gemenis, K. (2012). *Lecture 1: Asking questions in management research*. Obtained from https://blackboard.utwente.nl/webapps/portal/frameset.jsp

Gourier, E., Farkas, W. & Abbate, D. (2009). Operational risk quantification using extreme value theory and copulas: from theory to practice. The journal of operational risk, 4, 3-26.

Guillen, M., Gustafsson, J., Perch Nielsen, J. & Pritchard, P. (2007). Using external data in operational risk. The Geneva Papers, 32, 178-189.

Hull, J.C. (2010). Risk Management and Financial Institutions. Boston: Pearson Education.

Karam, E. & Planchet, F. (2012). Operational risk in financial sectors. Advances in decision sciences, 1, 1-57.

Lambrigger, D.D., Shevchenko, P.V. & Wütrich, M.V. (2007). The quantification of operational risk using internal data, relevant external data and expert opinion. Journal of operational risk, 2, 3-27.

Liqin, H. & Hongfeng, P. (2007). The application of EVT-copula in operational risk quantification. WiCom, 1, 4564-4567.

Neustar, (2012). *DDoS survey: Q1 2012, when businesses go dark.* Obtained from: http://www.neustar.biz/enterprise/docs/whitepapers/ddos-protection/neustar-insights-ddos-attack-survey-q1-2012.pdf

Peccia, A. (2003). Operational risk: Regulation, Analysis and Management. London: Prentice Hall.

Plunus, S., Hübner, G. & Peters, J.P. (2012). Measuring operational risk in financial institutions. Applied financial economics, 22, 1553-1569.

Politou, D. & Giudici, P. (2008). Modelling operational risk losses with graphical models and copula functions. Methodol Comput Appl Probab, 11, 65-93.

Ponemon, (2012). *Cyber security on the offense: A study of IT security experts*. Obtained from http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf

Power, M. (2003). The invention of operational risk. Centre for Analysis of Risk and Regulation, 16, 1-21.

Rippel, M. & Teplý, P. (2011). Operational risk - scenario analysis. Prague economic papers, 1, 23-39.

Samad-Khan, A. (2005). Why COSO is flawed. OpRisk Advisory, 1, 1-6.

Samad-Khan, A. (2008). Modern operational risk management. Emphasis, 2, 26-29.

Savić, A. (2008). Managing IT-related operational risks. Communications, 1, 88-109.

Shevchenko, P.V. & Wütrich, M.V. (2006). The structural modelling of operational risk via Bayesian inference: combining loss data with expert opinions. The journal of operational risk, 1, 3-26.

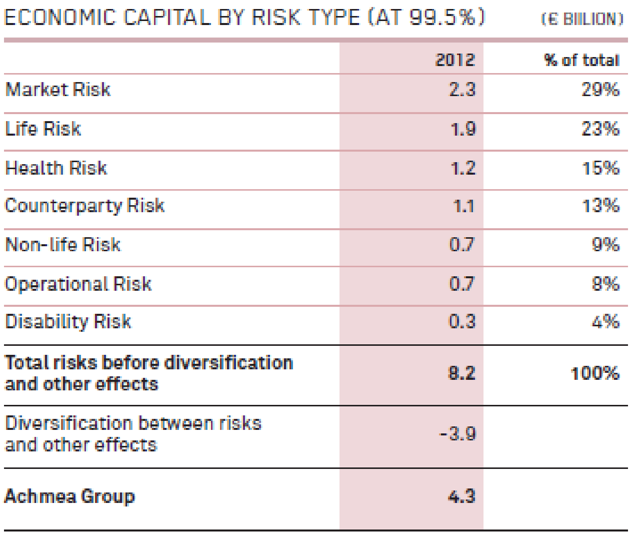
Shevchenko, P.V. (2009). Implementing loss distribution approach for operational risk. Applied stochastic models in business and industry, 26, 277-307.

Shih, J., Samad-Kahn, A. & Medapa, P. (2000). Is the size of an operational loss related to firm size? Operational risk magazine, 2, 21-22.

Appendices

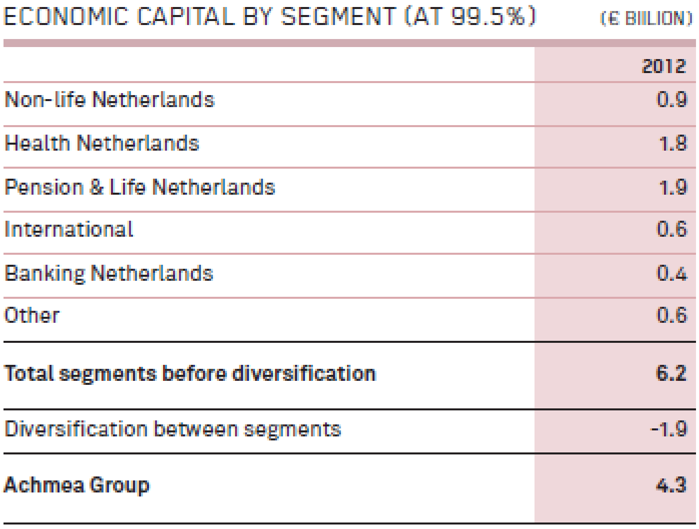
Appendix A Solvency II capital Achmea annual report 2012

These figures are taken from the Achmea annual report 2012 and represent economic capital per risk type and per segment. Within Achmea, business divisions carry the risks as we can see in the figures depicted below. Economic capital is the risk measure used in calculating required regulatory capital in Solvency II. Achmea uses the standardized method as well as internal methods to calculate economic capital. For operational risk the standardized method is applied and operational risk economic capital totals €700 million.



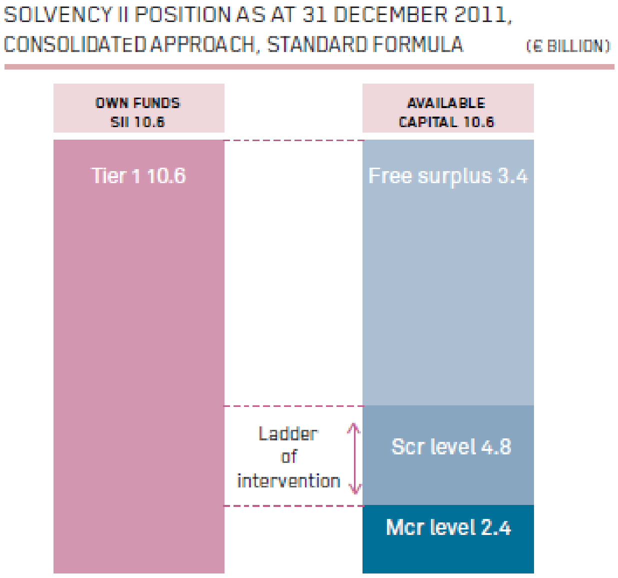
ECONOMIC CAPITAL BY RISK TYPE (AT 99.5%) (€ BILLION)

	2012	% of total
Market Risk	2.3	29%
Life Risk	1.9	23%
Health Risk	1.2	15%
Counterparty Risk	1.1	13%
Non-life Risk	0.7	9%
Operational Risk	0.7	8%
Disability Risk	0.3	4%
Total risks before diversification and other effects	**8.2**	**100%**
Diversification between risks and other effects	-3.9	
Achmea Group	**4.3**	



ECONOMIC CAPITAL BY SEGMENT (AT 99.5%) (€ BILLION)

	2012
Non-life Netherlands	0.9
Health Netherlands	1.8
Pension & Life Netherlands	1.9
International	0.6
Banking Netherlands	0.4
Other	0.6
Total segments before diversification	**6.2**
Diversification between segments	-1.9
Achmea Group	**4.3**



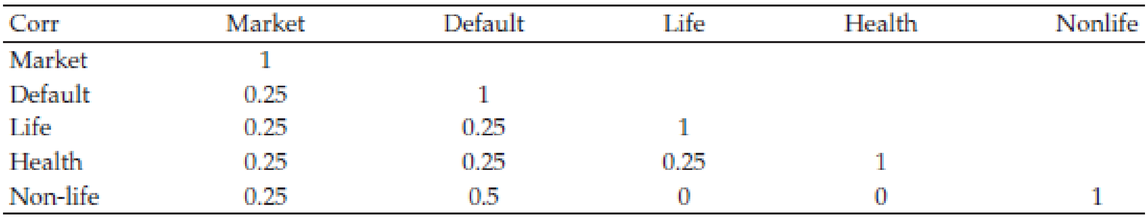
SOLVENCY II POSITION AS AT 31 DECEMBER 2011, CONSOLIDATED APPROACH, STANDARD FORMULA (€ BILLION)

Appendix B Solvency II operational risk charge standard formula

In this appendix the procedure to calculate operational risk charge using the standard formula approach from Solvency II is explained, adopted from the work of Karam & Planchet (2012) from the University of Lyon. The solvency capital requirement is the sum of the basic solvency capital requirement (life/non-life/health underwriting risk, market risk and credit risk), the risk charge for operational risk and the adjustments for the loss absorbing capacity of technical provisions and deferred taxes. Individual risk modules are aggregated using a standard correlation matrix to form the basic solvency requirement.

$$SCR = BSCR + SCR_{Op} - Adjustments$$

Table 8: Correlation matrix for the different risk modules in QIS5.



Corr	Market	Default	Life	Health	Nonlife
Market	1				
Default	0.25	1			
Life	0.25	0.25	1		
Health	0.25	0.25	0.25	1	
Non-life	0.25	0.5	0	0	1

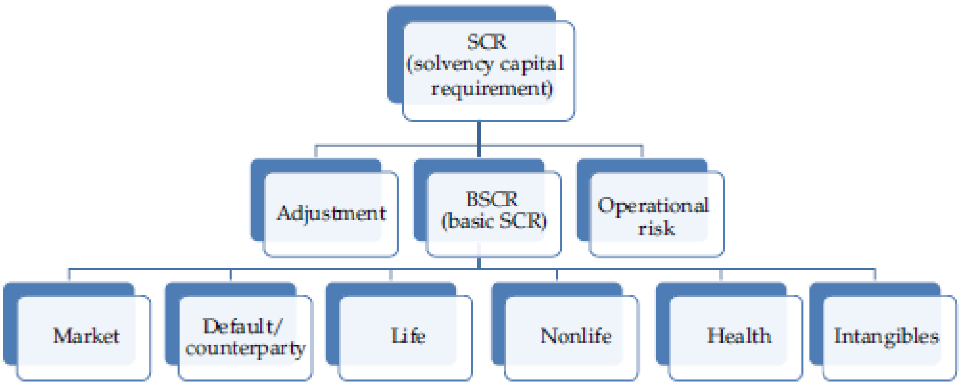


Figure 4: Solvency Capital Requirement (SCR).

$$\mathrm{BSCR} = \sqrt{\sum_{ij} \mathrm{Corr}_{ij} \times \mathrm{SCR}_i \times \mathrm{SCR}_j} + \mathrm{SCR}_{\mathrm{Intangibles}}.$$

Since this research focuses on quantifying operational risk especially the operational risk charge standard formula (SII) is important. That is why this part is explained in further detail whereas other risk modules are not further explained. The operational risk part of solvency capital requirement is calculated by multiplying factors with parameters and is capped at 30% of basic solvency capital requirement. Parameters include items such as earned premiums and insurance obligations. The full formula is depicted in the figure below.

$$\mathrm{SCR_{op}} = \min\left(0.3\mathrm{BSCR}, \mathrm{Op}_{\mathrm{all\ none\ ul}}\right) + 0.25\mathrm{Exp}_{\mathrm{ul}},$$

where $\mathrm{Op}_{\mathrm{all\ none\ ul}} = \max(\mathrm{Op}_{\mathrm{premiums}}, \mathrm{Op}_{\mathrm{provisions}})$,

$$\begin{aligned}\mathrm{Op}_{\mathrm{premiums}} &= 0.04 * (\mathrm{Earn}_{\mathrm{life}} - \mathrm{Earn}_{\mathrm{life\ ul}}) + 0.03 * (\mathrm{Earn}_{\mathrm{nonlife}}) \\ &\quad + \max\left(0, 0.04 * \left(\mathrm{Earn}_{\mathrm{life}} - 1.1\mathrm{pEarn}_{\mathrm{life}} - (\mathrm{Earn}_{\mathrm{life\ ul}} - 1.1\mathrm{pEarn}_{\mathrm{life\ ul}})\right)\right) \\ &\quad + \max\left(0, 0.03 * (\mathrm{Earn}_{\mathrm{nonlife}} - 1.1\mathrm{pEarn}_{\mathrm{nonlife}})\right), \\ \mathrm{Op}_{\mathrm{provisions}} &= 0.0045 * \max(0, \mathrm{TP}_{\mathrm{life}} - \mathrm{TP}_{\mathrm{life\ ul}}) + 0.03 * \max(0, \mathrm{TP}_{\mathrm{nonlife}}).\end{aligned}$$

(i) $\mathrm{TP}_{\mathrm{life}}$ is the life insurance obligations. For the purpose of this calculation, technical provisions should not include the risk margin and should be without deduction of recoverables from reinsurance contracts and special purpose vehicles.

(ii) $\mathrm{TP}_{\mathrm{nonlife}}$ is the total nonlife insurance obligations excluding obligations under nonlife contracts which are similar to life obligations, including annuities. For the purpose of this calculation, technical provisions should not include the risk margin and should be without deduction of recoverables from reinsurance contracts and special purpose vehicles.

(iii) $\mathrm{TP}_{\mathrm{life\ ul}}$ is the life insurance obligations for life insurance obligations where the investment risk is borne by the policyholders. For the purpose of this calculation, technical provisions should not include the risk margin and should be without deduction of recoverables from reinsurance contracts and special purpose vehicle.

(iv) $\mathrm{pEarn}_{\mathrm{life}}$ is the earned premium during the 12 months prior to the previous 12 months for life insurance obligations, without deducting premium ceded to reinsurance.

(v) $\mathrm{pEarn}_{\mathrm{life\ ul}}$ is the earned premium during the 12 months prior to the previous 12 months for life insurance obligations where the investment risk is borne by the policyholders, without deducting premium ceded to reinsurance.

(vi) $\mathrm{Earn}_{\mathrm{life\ ul}}$ is the earned premium during the previous 12 months for life insurance obligations where the investment risk is borne by the policyholders without deducting premium ceded to reinsurance.

(vii) $\mathrm{Earn}_{\mathrm{life}}$ is the earned premium during the previous 12 months for life insurance obligations, without deducting premium ceded to reinsurance.

(viii) $\mathrm{Earn}_{\mathrm{nonlife}}$ is the earned premium during the previous 12 months for nonlife insurance obligations, without deducting premiums ceded to reinsurance.

(ix) $\mathrm{Exp}_{\mathrm{ul}}$ is the amount of annual expenses incurred during the previous 12 months in respect to life insurance where the investment risk is borne by the policyholders.

(x) BSCR is the basic SCR.

Appendix C workshop expert judgment loss frequency

Confidential

Appendix D workshop expert judgment loss severity

Confidential

Appendix E annual loss distributions

Confidential