Improving Operational Risk Management using Business Performance Management technologies

Thesis by

A.J. Pieket Weeserik

for the degree of Master of Business Informatics

Department of Information and Computing sciences, Faculty of Science
Utrecht University, Princetonplein 5, 3584CC, Utrecht, The Netherlands

Supervisors

Dr. M. Spruit (Utrecht University)

Dr. F. Dalpiaz (Utrecht University)

Drs. S. Koelemeijer (Celcus B.V.)

masters of
business informatics
utrecht university.

July, 2017

Universiteit Utrecht

Name	A.J. Pieket Weeserik
Student number	5568226
Email address	a.j.pieketweeserik@students.uu.nl

MSc Program	Business Informatics
Title of the thesis	Improving Operational Risk Management using Business Performance Management Technologies

University & Department	Utrecht University, Department of Information and Computing Sciences
Address	Buys Ballot Laboratory, Princetonplein 5 3584CC, Utrecht, The Netherlands
Telephone	+31 30 253 1 454

Academic Supervisors	*From Utrecht University*
1st supervisor	Dr. M.R. Spruit
1st supervisor email	m.r.spruit@uu.nl
2nd supervisor	Dr. F. Dalpiaz
2nd supervisor email	f.dalpiaz@uu.nl

External supervisor	*From Celcus B.V.*
External supervisor	Drs. S. Koelemeijer
External supervisor email	steven.koelemeijer@celcus.nl

Summary

Operational Risk Management (ORM) comprises the (continuous) management of all risks resulting from: Human actions, (failed) internal processes, systems and external events. Business Performance Management (BPM) technologies are believed to provide a solution for effective Operational Risk Management. BPM developed from Business Intelligence (BI), which supports data collection, analysis and presentation of information. Business Performance Management extends BI with workflow and data entry. However, it is unclear whether the full spectrum of Business Performance Management technologies is suitable for improving operational risk management processes and whether the same set of Business Performance Management technologies are applicable for all types of organizations.

Central in this research is the development and practical validation of a maturity model. The maturity model consists of a process part, related to operational risk management implementation and the technologies part, relating to BPM technologies used. The maturity model and automated assessment were conceived by most (75%) of the participating organizations as accurate.

There appears to be no strong relationship (0.78) with ORM process maturity and a specific supporting BPM technologies. This means sets of BPM technologies nor individual software features appear to influence the full extent of organizations - in any industry - to manage their operational risks. From interviews and the assessments, it appears ORM is for a large part still a manual job. Software is mainly used for reasons regarding automation and efficiency.

However, there are some relations with specific sets of BPM technologies found to influence the maturity of Operational Risk Management. Therefore, the maturity model as developed in this research could provide some useful guidelines on the applicability of certain technologies, especially for non-mature industries. The maturity model as developed in this research provides a suitable path with six stages for organization seeking to improve their ORM processes. The six stages provide an instrument to match appropriate technologies to the current stage of maturity and enables organizations to grow in maturity towards enterprise integration and continuous improvement.

Table of Contents

Index of figures and tables

1 Introduction

Risk is often expressed as the product of the (predicted) probability of an event occurring, times the (estimated) impact of the event (chance * impact = risk). The English term "*risk*" is derived from the French word "*risqué*" that first appeared in literature around the 1600s. In that time the word "*risqué"* meant "*to run into danger*". The word "*risqué*" was adapted in England and around 1655 (re)defined as "*risk*", meaning "*a situation involving exposure to danger*" (Oxford English Dictionary, 2017).

Within an organizational context the term "*risk"* is defined by the International Organization for Standardization Risk Management Vocabulary as **"***the effect of uncertainty on objectives"* (ISO, 2009b, p. 1). This definition explicitly does not assign a value to "*risk"*, because exposure to an uncertainty can result in either negative or positive consequences. The exposure to risk could change over time, therefore organizations should perform a recurring risk management process.

Risk management frameworks provide guidelines or best practices for implementing risk management processes within organizations. A standardized process to manage risks is preferred and aids in governance and compliance of the risk management process. A risk management process can be performed in different ways, however ISO 31000 describes the following generic structure:

1. describe the organization, its internal and external relations and objectives;
2. identify risks, followed by analysis and assessment of these risks;
3. risk evaluation leads to a decision on how to handle or treat the risk;
4. decided treatments or mitigating measures should be implemented and executed properly;
5. the entire risk management process and related activities should be monitored;
6. Communication and consultation leads to continuous risk management improvement.

This report describes how these risk management processes can be supported using a specific set of information technologies, called Business Performance Management (BPM) technologies. These technologies are an extension of Business Intelligence and are intended for improvement of business performance using data integration, analysis, dashboarding & reporting, planning and workflow. The objective of this research is to study how these technologies can be used for risk environment, risk assessments, monitoring and aid communication & collaboration between people. That can be used to improve quality of risk management processes and reporting, resulting organizational performance.

1.1 A brief context on risk management in organizations over the last decades

Risk management within a business context is closely related to the financial services industry. In 1970s the Geneva Association was the first organization to link the domains: risk, insurance and economics together as a combination to manage and mitigate risks (Fraser & Simkins, 2008). In the 1970s the first supervisory requirements for insurance were introduced in Europe, called Solvency Directives (now known as Solvency I). They included the first regulatory requirements for risk management within the financial services industry, focused on insurance organizations (BaFin, 2016).

The major first forms of risk recognized within businesses were: credit risk and market risk. Credit risk involves the uncertainty that a buyer or borrower will (not) be able to pay the provided products or services. Market risk is the uncertainty an investment will be affected due to (volatile) market factors (Chernobai, Rachev, & Fabozzi, 2008). Monday October 19 1987, also known as "Black Monday", showed the high risks involved in credit and market investments. Stock trading markets around the

world suffered losses up to more than 20% in just one day, one of the fastest and biggest declines of stocks in history (Schwert, 1990).

In the 1980s the Basel Committee from the Bank for International Settlements introduced financial requirements for banks, called the Basel Accord in 1988 (Basel Committee, 2015). The Basel committee is an authority prescribing best practices and included central banking institutions from the G10 countries at that time. The Basel committee introduced the accord to help banking related organizations measure credit & market risks and set capital (reserves) accordingly.

From the early 1990s to the early 2000s internet connectivity experienced a tremendous growth in the Organization for Economic Co-operation and Development (OECD) member countries (Crenshaw, Robinson, Ding, Kumar, & Sha, 2006). Worldwide commerce and trading increased concurrently with the growth of internet connectivity. Globalization was leading to a vast increase in business transactions. At the end of the 1990s and the early 2000s this lead to an explosive growth of (technology) business (over) valuations, known as the dot-com bubble (Ofek & Richardson, 2003).

In the early 2000s the dot-com bubble and financial scandals such as Enron and WorldCom, showed that the laws and regulations of that time were not able to prescribe sufficient measures against malicious activities, such as fraud (Fraser & Simkins, 2008). Furthermore, many organizations failed to allocate decent financial buffers, to withstand the risks involved in trading on volatile markets.

In 2002 the Sarbanes–Oxley Act (also known as SOX) was introduced for all corporations operating in the United States of America. This act was aimed at improving corporate governance and preventing fraudulent transactions that caused the early 2000s financial failures. The Sarbanes–Oxley Act (2002) requires all organizations to prove they are taking measures against fraud and explain how they do it. Publicly traded corporations are required to publish their findings and validate them by an external independent party (auditor). Some countries followed Sarbanes-Oxley by developing their own variation. For example, in the Netherlands the governance code Tabaksblat (2003) was introduced.

In the early 2000s the Basel Committee from the Bank for International Settlements introduced the second Basel accord (also known as Basel II) including new financial requirements for banking. In this second accord the Basel committee recognized the need for managing types of risks other than credit and market risks (Power, 2005). In the second Basel accord 'operational risks' were explicitly defined to account for risks that find their source in: humans, processes, systems and external events.

The improved laws and regulations (such as SOX) did not stand against all risks. In 2007 mortgage holders in the United States of America defaulted on their payments and several banks, such as Lehman Brothers collapsed because large scale fraud became visible. Following into 2008, the mortgage crisis in the USA appeared to have a global impact on economies around the world (McNeil, Frey, & Embrechts, 2015). This lead to revisions of the second Basel accord, increasing requirements and paved the way for development of Basel III.

The first parts of Basel III were published in 2011. Basel III describes changes for operational risk management practices. The third Basel accord is scheduled to be completed and in full effect at the end of March 2019 (Basel Committee, 2013). In 2016 Solvency II was introduced for insurance organizations in the European Union, containing requirements similar to Basel II, including requirements for operational risks.

1.2 Problem statement

Operational risks are the root cause for many of the (large scale) financial failures in the past decades (Hoffman, 2002; Alexander, 2003; Power, 2005; Moosa, 2007; Chernobai, Rachev, & Fabozzi, 2008). The aforementioned studies note that operational risks are not new: human mistakes, fraud, theft, process failures, system errors and external hazards, such as fires and floods, have been around for many years. However, the impact of operational risks was most often insignificant. Several trends over the last decades made operational risks more significant than ever before.

Information Technologies enabled many countries in the western world to advance, although this advance concurrently boosted the impact of operational risks (Chernobai, Rachev, & Fabozzi, 2008). Globalization lead to a consequential increase in volume of financial transactions (McNeil, Frey, & Embrechts, 2015). Global networks were deployed and worldwide (value) chain dependencies added to corporate complexity (Mentzer, et al., 2001). Growing organization complexity made operational risks, such as fraud, system errors, process failures and other events impact entire global value chains.

An increasing number of organizations, mainly in the financial sector, are required by regulatory authorities or by law to manage their operational risks. Fontnouvelle, DeJesus-Rueff, Jordan and Rosengren (2003) found that in the early 2000s most international banks were already allocating more financial reserves to account for operational risks than for market risks. Operational risks tend to become more relevant in different types of organizations (Panjer, 2006; Kenett & Raanan, 2011). For example, operational risks have been studied for years in the healthcare sector (Kavakr & Spiegel, 2004; Moseley III, 2013). Additionally, operational risks are becoming increasingly important in the energy sector (Coca, et al., 2014).

Mitra et al. (2015) describe the importance of operational risks varies, depending on industry and markets an organization operates in. They found financial organizations have the lowest expected returns on operational risk, basic material producers have the highest return. Operational risk is different from other risks, such as credit risk or market risk, because operational risk is usually not taken to retrieve an expected return. Operational risk exists in every organizational activity. Inappropriate management of operational risks can result in significant losses.

With increasing requirements, complexity and volume of risks, information systems provide benefits for integrating risk management activities and optimizing risk management performance. Information systems and technologies can support the improvement of operational risk management processes (Tarantino, 2008; Malik & Holt, 2013; Arnold, Benford, Canada, & Sutton, 2015; Breden, 2006).

Lam (2014), Arnold, Benford, Canada and Sutton (2015) describe performance management systems as a set of technologies from the information systems domain suitable for application to support the operational risk management process. In recent years, this recognition is supported from practice by consulting firms, PwC (2012) and Deloitte (2015) who state Business Performance Management and its supporting technologies could provide effective support for risk management processes.

Nyenrode Business University (2014) performed a large scale study about the state of risk management practices in the Netherlands. Nyenrode writes risk management should be part of the Planning and Control cycle, aligned with strategic goals of the organization. Integrated risk management and better collaboration lead to a more mature risk management. These benefits could only effectively achieved by using appropriate software. However, Nyenrode concludes many organizations do not appear to know what software features to use for effectively improving risk management.

Sharda, Delen and Turban (2014, p. 150) describe Business Performance Management (BPM) as: "*The business processes, methodologies, metrics and technologies used by enterprises to measure, monitor and manage business performance*." Business Performance Management can be seen as a further development of Decision Support Systems and Business Intelligence; however, BPM is specifically developed towards the improvement of organizational performance to meet its strategic objectives. Concepts are Balanced Scorecards, KPIs and collaboration via (automated) workflow systems.

Beasley, Chen, Nunez & Wright (2006) indicate Balanced Scorecards including Key Performance Indicators could be used for improving risk management practices. Additionally, Fraser, Simkins and Narvaez (2014) indicate that the same principles and technologies of Key Performance Indicators are applicable for Operational Risk Management, known as Key Risk Indicators and Key Control Indicators. Azvine, Cui, Majeed and Spott (2007) describe real-time Business Intelligence is suitable for supporting Operational Risk Management processes by providing an effective system for high velocity risks.

At this moment, it remains unclear whether the full spectrum of Business Performance Management technologies is suitable for improving operational risk management processes and whether the same set of Business Performance Management technologies are applicable for all types of organizations. Additionally, there appears to be no existing maturity model guiding an organization to improve their operational risk management processes using Business Performance Management Technologies.

1.3 Next chapters

This research follows the Design Science approach using the methodology as described by Hevner, et al. (2004). Chapter two describes the research approach, research objective & target audience, research questions, research methods and motivates the design based on additional literature.

Chapter three describes important background information about the context and the domains of Operational Risk Management and Business Performance Management Technologies. Risk Management will be explained from its different perspectives on risk management into the scope of this research, Operational Risk Management. Chapter three is concluded with a description of Business Performance Management Technologies from its positioning related to performance management.

The Design Science approach describes an artefact to be studied and validated. Chapter four describes the development of the maturity model artefact that is central in this research. Maturity models are used to guide improvements of certain processes using capabilities or technologies, corresponding to levels of maturity. In this research a maturity model is created for Operational Risk Management as process to improve using Business Performance Management Technologies.

The maturity model was evaluated in practice trough assessment of sixteen different organizations. The results regarding contextual factors are described in chapter five. The results of the actual implementation level of software and specifically Business Performance Management Technologies is described in chapter six. Differences between different industries are described in chapter seven.

This thesis is concluded with conclusions regarding the research questions in chapter eight. The scientific contribution, some remarks, implications regarding quality and potential future research are the points of discussion in the ninth and final chapter of this thesis.

2 Research Design

This chapter describes the research approach, research objective & audience, research questions, selected research methods and motivates the research design based on additional literature.

2.1 Research approach

McCormack et al. (2009) write business processes including risk management are nowadays seen as important strategic assets essential for the achievement of business goals. Shtub and Karni (2010) describe business processes are essential to provide:

- enhanced functionality towards the achievement of business goals;
- increased quality, including conformance and reliability;
- increased flexibility to adapt to variability, compliance and future needs;
- reduced operational (cycle) times, including queue times, service times and waiting times;
- reduced operating costs and failures.

According to McCormack et al. (2009) process maturity is increasingly important. Since the 1980s maturity models are developed to guide an organization through the process of improving maturity that leads to competitive advantage. De Bruin and Rosemann (2005) write maturity is used to measure and evaluate the capabilities of an organization. Maturity assessments became popular since the Software Engineering Institute at Carnegie Mellon introduced the Capability Maturity Model (CMM).

The original CMM developed in the 1980s had a specific focus on the evaluation of software development processes. The maturity model development approach extended to other domains of application. McCormack et al. (2009) write maturity models help organizations where they should focus and where effort is wasted. Additionally, maturity models can be used to describe the current maturity stage and offer a specific guide on what is needed to improve a process. The improvement of processes and maturity are of vital importance and requires investments to mature.

A maturity model should be developed to provide a solution to a practical problem. Wendler (2012) writes a maturity model is often developed through the design science approach. The design science approach is described by Hevner, March, Park and Ram (2004) from a design-oriented paradigm with seven clear guidelines to evaluate the quality of the research:

1. design science should lead to an artefact in the form of a construct, model, method, or instantiation;
2. design science is intended to develop technology related solutions to important and relevant business problems;
3. the designed artefact should be evaluated in practice for quality and effectiveness;
4. the artefact should be a verifiable contribution to the research domain;
5. for construction and evaluation of the artefact rigorous methods should be applied;
6. the development of an artefact requires utilization of available means to reach desired ends while satisfying laws in the problem environment;
7. design science research needs to be presented effectively both to technological oriented audiences as well as management oriented audiences.

This research project follows the design science approach and the related design science guidelines as described by Hevner, March, Park and Ram (2004). Additionally, this research follows and the design science processes as described by Hevner (2007) that is further detailed on the following page.

Hevner (2007) clarified the design science process as an iterative process of continuously building knowledge base used for developing an artefact to be evaluated and tested for relevance in practice.

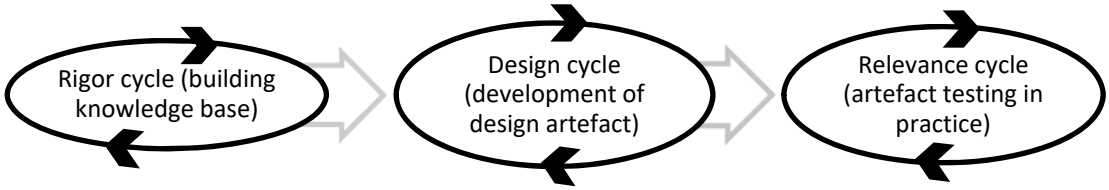


Figure 1: The Design Science cycles, adapted from Hevner (2007).

The rigor cycle as described by Hevner (2007) includes important foundations of the research project. The goal of this cycle is to ground the research project with sound scientific theories and methods. The researcher should gather experience and expertise into a knowledge base to develop an artefact. The cycle remains important throughout the project by additions to the knowledge base.

Hevner (2007) describes the design cycle components as to build design artefacts & processes. The maturity model artefact will be composed of two parts: a process part and a technologies part. The process part will be based on a description regarding the Operational Risk Management process. The technology part will be based on Business Performance Management technologies.

The artefact is derived from hypothetical components and should be tested in the field for practical relevance (Hevner A. R., 2007). The practical relevance should show how the artefact can be applied regarding people, organizational systems and technical systems. Within this environment problems and opportunities could be identified. These problems and opportunities could be resolved by adjusting the artefact's design or lead to new research directions.

2.2 Research objective & target audience

Information systems are found to provide benefits for integrating risk management activities and optimizing operational risk management performance. Business Performance Management technologies are a specific subset of information system technologies, designed to support processes towards decision making and steering the achievement of organization objectives and could be used to improve operational risk management performance. Therefore, this research aims to:

- Describe the importance of Operational Risks for organizations in different fields;
- Identify Business Performance Management technologies that are used or usable for operational risk management practices;
- Measure the extent to which an organization utilizes Business Performance Management technologies that are related to different maturity stages of the organization's Operational Risk Management process performance.

The expected results of this research are presumed to be of interest to:

- risk management professionals looking for ways to improve their operational risk management processes;
- service organizations providing consultancy services about (improving) operational risk management processes;
- software product development organizations aiming to develop a product for operational risk management processes.

2.3 Research questions

According to literature discussed in the previous section a maturity model artefact, developed through the Design Science approach would be suitable for this research project. To meet the research objective, the main research question is formulated as follows:

> *" How can organizations incrementally improve their Operational Risk Management processes using Business Performance Management technologies? "*

In this research two different domains (Operational Risk Management and Business Performance Management technologies) will be related to each other in the form of a maturity model artefact. This research follows three distinctive phases similar as described by Hevner (2007):

1. Collecting domain knowledge (rigor cycle);
2. Maturity model development (design cycle);
3. Maturity model relevance evaluation (relevance cycle);

Collecting domain knowledge (rigor cycle)

The first research questions are designed to provide important background information about the domains of Operational Risk Management and the domain of Business Performance Management Technologies. The following research questions were developed:

> *RQ1: " What is defined as the domain of Operational Risk Management? "*
> *RQ2: " What is the definition of Business Performance Management technologies? "*

Maturity model development (design cycle)

In this research a maturity model artefact will be developed. The maturity model artefact should be composed of a process part, in this research concerning the activities to manage operational risk. Additionally, the second part of the maturity model artefact will be composed of business performance management technologies that could support the operational risk management process.

The extent to which operational risk management activities are performed in practice play a vital role before linking them to an assessment with different BPM technologies. Therefore, it is important to know to what extent the operational risk management processes are implemented. The Risk Management Society (2017) provides a maturity assessment for measuring enterprise wide risk management implementation and corresponding maturity levels by using key characteristics. These key characteristics are used as a quick way to measure process implementation. In this research a similar structure is expected for use in the maturity model artefact.

This research, does not intend to gather a complete insight of the Operational Risk Management implementation level. Therefore, this research aims to identify some key characteristics usable to measure the level of operational risk management implementation. Galesic and Bosnjak (2009) studied lengthy lists of questions and found that long questionnaires result in degrading quality. This research aims to achieve an indication of the operational risk management implementation level within a relatively short timeframe. This construct will be referred to as 'quick scan' in this research:

> *RQ3: " How to develop a quick scan for assessing the implementation level of the Operational Risk Management process within an organization? "*

The following question serves as a sub question of developing the ORM implementation quick scan:

> *Sub RQ 3.1: " Which factors can be identified as key indicators for Operational Risk Management process implementation? "*

Next to the operational risk management process maturity quick scan, a set of business performance management technologies should be described for use in the maturity model artefact:

> *RQ4: " Which set of functionality is required from Business Performance Management technology in order to accommodate the Operational Risk Management process? "*

The Business Performance Management technologies derived from theory will be compared to existing risk management software products and is further specified into two sub research questions that should answer research question 4. In the first place the maturity model artefact should be related to practice, therefore a study of existing software products and features for risk management would provide an overview of the initial requirements of such a solution:

> *Sub RQ 4.1: " What functionality provided is by existing risk management software products?"*

Not all software technologies are related to business performance management technologies. Therefore, the gathered software technologies should be related back to business performance management technologies:

> *Sub RQ 4.2: " Which functionality from Business Performance Management technology is relevant for use in Operational Risk Management software systems? "*

Research question 4.1 is added in this proposal to support the maturity model artefact development with existing software functionality provided from practice. Another sub question to answer this research question was described in the short proposal: *SUB RQ 4.3: "Which factors are identified as key indicators for BPM technology maturity?"* This sub question will be sufficiently answered by sub question 4.2 about relevant BPM technologies. Therefore, this sub question will be omitted from further stages in this research.

Maturity model relevance evaluation (relevance cycle)

The conceptual maturity model developed via the previous steps only reflects theoretical and hypothetical findings from literature and expert opinions. Following the design science approach, the maturity model artifact should be evaluated for potential use in practice. The relevance evaluation phase is intended to find a fit for the artefact and describe its potential use for different sectors. To gather some contextual information the following research question is designed:

> *RQ5: " How important is Operational Risk Management in practice? "*

As one of the objectives is to describe the importance of Operational Risks for organizations in different fields; this objective is further specified to investigate some assumptions. One of the assumptions is that an organization has an Operational Risk Management Process implemented:

> *Sub RQ 5.1: " To what extent do organizations in practice have implemented an Operational Risk Management process? "*

Olson, Slater and Hult (2005) studied overall firm performance and concluded organization performance is strongly influenced by how well a strategy is matched to business processes. When research question 5.1 results to an implemented operational risk Management process, it is still unclear how important this process is compared to the strategic goals of the organization. Therefore, the perception of the participant will be compared to investments into operational risk management on the use of resources in financial sense and human resources FTE's. The perceived implementation should lead to a qualitative explanation of importance of the participating organizations. Where actual investments in operational risk management places the explanation in quantitative context of performance. Importance of the operational risk management process in this research is based on perception and investment of resources:

> *Sub RQ 5.2: " What is the perceived Operational Risk Management process implementation level by organizations in practice? "*
>
> *Sub RQ 5.3: " What are the estimated investments in Operational Risk Management by organizations in the field? "*

The previous questions are mainly intended to study the business process perspective of this research. The maturity model artefact is also composed of a technological component supporting the operational risk management processes, therefore the following questions are designed to provide insights into the supporting role of technology now and the expected future:

> *Sub RQ 5.4: " What is the perceived importance of the current use of software supporting the Operational Risk Management process by organizations in the field? "*
>
> *Sub RQ 5.5 : " What is the perceived importance of expected future use of software supporting the Operational Risk Management process by organizations in the field? "*

Question 5.4 provides the perception of importance of the supporting technologies. While the developed maturity model artefact will be used to quantify the actual current use of technologies. Question 5.5 is intended to provide qualitative insights into potential future use of the maturity model artefact that is created. This should provide information about the applicability of the maturity model artefact in the future and could provide future research directions for artefact improvements.

To conclude this research and answer the main research question the following research questions are developed to evaluate the main concepts of maturity model artefact:

> *RQ6: " What is the relation between the implementation level of Operational Risk Management and the supporting Business Performance Management technologies? "*

Research question 6 should provide an answer to what extent there is a relation between the Operational Risk Management processes and Business Performance Management technologies in general. Where research question 7 should provide an answer to what technologies are used:

> *RQ7: " Which set of Business Performance Management technologies is utilized to support Operational Risk Management processes in different fields? "*

2.4 Research methods

The Design Science approach requires a selection of scientifically sound techniques, depending on the artefact that is being developed. This section research follows the Design Sciences cycle approach as described by Hevner (2007). This section maps research methods that will be applied in each phase.

Collecting domain knowledge (Rigor cycle)

As described by Hevner (2007) experience and expertise are required to build a knowledge base to develop an artefact. The rigor cycle remains important throughout the project by additions to the knowledge base. Therefore, literature will be collected using snowballing technique, as described by Vogt (1990) as incremental technique suitable for building an in-depth body of knowledge.

The snowballing technique is used initially to write a theoretical context for this research, that is improved iteratively by adding literature throughout the development and evaluation processes. Starting from most recent literature back to underlying concepts. The snowballing technique will be applied continuously, however in the first stage of the research project it will be mainly used for answering the following questions and their sub questions:

- *RQ1: " What is defined as the domain of Operational Risk Management? "*
- *RQ2: " What is the definition of Business Performance Management technologies? "*
- *RQ3: " How to develop a quick scan for assessing the implementation level of the Operational Risk Management process within an organization? "*

Maturity model development (Design cycle)

The maturity model artefact will be composed of two parts: a process part and a technologies part. The process part will be based on a theoretical description of key indicators regarding the Operational Risk Management process. The technology part will be based on the theoretical description of Business Performance Management technologies. Additionally, the technological part of the artefact will be complemented by a risk management software market analysis. This market analysis is intended to gather a list of software features relevant to risk management practices.

The literature study and market analysis should result in a list of possible software features often used for risk management practices. However, a feature often provided does not necessarily provide any relevance and importance for operational risk management.

To validate relevance, importance and completeness a panel of operational risk experts will be consulted to provide feedback on the developed quick scan regarding the operational risk management process implementation level. Additionally, the expert panel should provide a ranking on the features suitable for operational risk management based on the features found through the market scan of risk management software systems.

In this research the Score voting technique will be applied for the expert panel. Ashton (1986) writes combining expert judgements is a very effective way of increasing validity of the research. Score voting or range voting is a voting method that originates from electoral voting. Each voter gives every proposed candidate (software feature) a score. Then each score is averaged or summed. The proposed candidate (software feature) with the highest mean or total summed score is selected.

According to Ashton (1986) the mean of score voting results in a 90% reliable measure with at least 3 experts in the group until a maximum of 95% with 8 experts. That is because then the mean does not significantly increase the reliability anymore and from 8 experts the variability remains flat. A 90% reliability is considered enough, therefore at least 3 experts should be part of the expert panel.

The Delphi method was also considered in an earlier stage of this research project, however (Linstone & Turoff, 2002) and (Hsu & Sandford, 2007) write an expert panel using the Delphi method could take months to complete because expert agreement is required. Although the Delphi method provides full anonymity to participants, the Delphi method is conceived less suitable for this research project.

The market analysis and expert panel will be mainly used for evaluation regarding completeness and preliminary design of the maturity assessment artefact. Therefore, their main purpose in this research is intended for answering the following questions and their sub questions:

> *RQ3: " How to develop a quick scan for assessing the implementation level of the Operational Risk Management process within an organization? "*
>
> *RQ4: " Which set of functionality is required from Business Performance Management technology in order to accommodate the Operational Risk Management process? "*

Maturity model relevance evaluation (relevance cycle)

A maturity assessment instrument is developed, based on the results from the literature study, software market study and the expert panel. This artefact is derived from hypothetical components and should be tested in the field for practical relevance (Hevner A. R., 2007). Problems and opportunities could be identified from applications in practice. These problems and opportunities could be resolved by adjusting the artefact's design or lead to new research directions.

The maturity assessment artefact created in this research will be evaluated using field study to examine the use of practical application regarding the artefact. According to Hevner, March, Park and Ram (2004) the field study falls within the observational category of Design Evaluation Methods.

The field study will be composed of open interview questions for determining contextual information and perceptions that might influence the maturity model application and use. The interviews will be analyzed trough coding and ranking. Additionally, structured assessments are performed to instantiate the designed maturity model artefact for evaluation in practice. The field study will be used for answering the following questions and their sub questions:

> *RQ5: " How important is Operational Risk Management in practice? "*
>
> *RQ6: " What is the relation between the implementation level of Operational Risk Management and the supporting Business Performance Management technologies? "*
>
> *RQ7: " Which set of Business Performance Management technologies is utilized to support Operational Risk Management processes in different fields? "*

2.5 Selection criteria

In this research project the design science approach is applied with a different method. For each method, different criteria apply, therefore this section will describe how the population will be selected and what criteria will be used to include or exclude certain parts of populations.

Selection criteria market scan risk management software products

Identification of possible risk management software products is performed via Market analysts, search engines or when referenced to by risk experts and only included when:

- The product is a software sold as an individual product, not (only) as part of a service provided by a (consultancy) organization, composed of multiple products;
- The product is referred to as a complete software product for:
    - Risk Management;
    - (e)GRC or Governance, Risk & Compliance;
    - ERM or Enterprise Risk Management;
    - ORM or Operational Risk Management;
- The vendor provides a complete product catalogue, screenshots or a demonstration about the software product;

Selection criteria expert panel

The aim for the expert panel is to get at least three operational risk experts involved, however at least six experts receive an invitation. Each expert is required to have:

- At least 5 years of experience with operational risk management or a person with a valid certification;
- Involved in day-to-day practices of managing, consulting or researching Operational Risk (Management) and its activities;
- A basic understanding of software features;
- Work in the Semi-public or private sector;

Selection criteria open interviews and maturity assessments

The evaluation of the maturity model will be performed by open interviews and taking assessments for testing the maturity model artefact. The mail goal of this stage is to find applicability within different fields, therefore this research aims to evaluate the maturity assessment artefact with at least one or more organizations within the following fields:

- Energy;
- Financial Services (Banking & Insurance);
- Healthcare (Hospitals);
- Production & Trade;
- Retail & consumer goods;
- Transport & Infrastructure.

Meeting the following additional criteria:

- Operating in the semi-public or private sector;
- At least 250 Full Time Equivalents (FTE) working in the organization.

3 Theoretical background

This chapter describes important background information about the context and the domains of Operational Risk Management and Business Performance Management Technologies. Risk Management will be explained from its different perspectives on risk management into the scope of this research, Operational Risk Management. This chapter is concluded with a description of Business Performance Management Technologies from its positioning related to performance management and performance measurement practices towards the performance management supporting technologies.

3.1 Different perspectives on the concepts of risk

An approach to the management of risks varies depending on the perspective and application. Differences in perspectives are leading to difficulties in misunderstandings between people, shortcomings in classifications of risk, analysis problems, and integration issues between different domains. A fair amount of research into the concept risk is available from psychology, sociology, management sciences and finance. This section describes some of the different perspectives.

Changing perspectives on the concept of risk

Sadgrove (2016) describes three ages, with changing perspectives on the concept of *risk*:

1. The first age spans before the 1970s, back to approximately 4000 years ago, when the concept of risk was only seen as a hazard or danger. Risks were treated reactively. They could be insured in some way, for example cargo insurance was often if guaranteed deliveries to a buyer or offered a compensation for non-delivered or broken products.
2. The second age spans from the 1970s to the 1990s when organizations started to treat risks in a more proactive and preventive manner. Over these years' product quality, workplace safety and the environment became a concern. Risks were proactively mitigated by quality management processes, such as ISO 9000. In the early 1990s corporate governance failures showed a need for improved laws and new financial regulations to improve pro-active risk management practices.
3. In the third age from 1995 onwards until now, risks are not only seen as hazard, but as an opportunity as well. Risks were redefined as an uncertainty rather than a danger. Changed laws and regulations determine boundaries within organizations can exploit this uncertainty.

Power (2004) writes in his book "*The risk management of everything: Rethinking the politics of uncertainty*" that there is an increasing tendency within organizations of trying to manage every type of uncertainty. Power describes a shift over the past decades of risk management as uncertainty management from the quantification of risk in the financial services industry and risk analysis from (technical) engineering domains now finds its way into other types of organizations.

Kloman (1990) describes that risk is seen differently from different fields of application. Analysts, politics, academics often view risk as a hazard. More specifically: technology related risks that threaten our existence, such as nuclear or environmental issues. From finance and accounting risk is uncertainty that can be exploited, however needs to be insured or reduced by building sufficient financial buffers and spreading the financial investments over multiple different sources. Within healthcare risk is integral part of quality assurance. Patient safety by professionals preventing injuries and reducing damage from accidents.

Personal factors and perspectives in a risk management environment

Lopes (1987) studied the personal factors of gains and losses in decision making. Lopes described two distinctive views in risk research. First is the mathematical experimental view, calculating risk based on probabilities and amounts, comparing a statistical chance to lose money versus the potential to gain more money. The second view is from personality psychology where differences in human behavior are studied, often based on chance and skill. For example, throwing a basketball into the ring from a self-chosen distance. Short distances increase the probability of success, but longer distances are more rewarding, however increases the chance to fail.

Lopes (1987) found two different variables that affect risk behavior. The first variable is the motivation to take a certain risk, comparing security versus potential gains. Risk averse people avoid risks to prevent bad outcomes, risk seekers are willing to take a risk to achieve a good outcome. This motivation is influenced by a second variable called: aspiration. Aspiration is situational and varies depending on immediate needs and opportunities of an individual. Therefore, risk taking behavior is influenced by other concepts, such as emotion, disappointment, regret, aesthetics, et cetera.

Several researchers studied the influence of personal factors and decision making on risks within organizations. Baird and Thomas (1985) described how decisions from a single individual affect the impact of strategic risks for corporations and potentially can turn into a disaster. MacCrimmon and Wehrung (1990) studied characteristics of risk taking behavior under 500 executives and found the most successful executives are big risk takers and mature executives are most risk averse.

Koller (2005) writes that there are differences in perspectives on the concept of risks between departments of the same company. People in the health and safety department tend to view risks as a hazard and something that can go wrong. They calculate risk based on probability times impact. On the other hand, people in the financial department view risk as an opportunity as well. They evaluate risk with a loss vs. return calculation to gain a profit, within certain limits they regard as safe.

Classifications of risk in an organizational context

Business and organization researchers exerted to further classify the concepts of organization risks into distinct types. Mowbray and Blanchard (1961) divided business risks in two broad types: pure risks and speculative risks. Pure risks are described as a potential source of incidental loss, resulting from mistakes or hazards, such as fire. Speculative risks involved both positive and negative (financial) potential on the business. Examples are financial investments and stock markets.

Renn studied risk management approaches from different disciplines in the 1990s and described seven distinctive approaches to the conception and the assessment of risk (Renn, 1992). For each of the concepts Renn described a different base unit for expressing the risk, method(s) for determining the risk, scope, problem area, application domain, and instruments that apply. The approaches to risk following the classification from Renn (1992) can be summarized as:

1. Actuarial approach (from accounting) using statistical models to calculate risks;
2. Toxicologic and epidemic approaches, contamination, infections and spread models;
3. (safety) Engineering approaches, applying probabilistic risk analysis (PRA) techniques;
4. Economics approach, calculating risk-benefit trade-offs for investments;
5. Psychological approach, analysis of psychometric views;
6. Social theoretical approach, (human) perceptions to the risk concept;
7. Cultural approach on theories regarding risk using group analysis.

A typology of organization related risks

Within the actuarial approach Chernobai, Rachev and Fabozzi (2008) describe a comprehensive topology of business related risks and their relation among each other. Financial risks are seen as the most important and are presented at the top level, followed by other risks. The topology can be summarized as follows:

Financial risks, including:

- **Credit risk**: the possibility that a borrower will not be able to pay back a loan within the agreed terms;
- **Market risk**: potential influence of market stock prices, exchange rates, interest rates and movements from the underlying market prices and their volatilities;
- **Operational risk**: possible exposure to loss because of inadequate or failed internal processes, human actions, system behavior or external events;
- **Liquidity risk**: potential inability to meet short term financial demands and the failure to lend money on the lending markets or raise capital.

Other risks, including:

- **Business & Strategic risk:** adapting to changes in the organization environment. These risks require good timing of strategic decisions, otherwise they could result in a loss or competitive disadvantage. For example, changing economic conditions, such as increasing material prices or technological innovations, such as internet shopping;
- **Reputational risk:** possibility that negative publicity about the organization results in a loss of customers, reduced revenue and/or (expensive) lawsuits;
- **Political risk:** country or region related changes in political policies or economic pressures that might influence the organization's ability to trade with foreign parties;
- **General legal risk**: Changes in a country's legal system and/or laws, that require an organization to be compliant or otherwise can result in penalties and/or lawsuits;
- **Other risks**: potential other risks that might influence the organization, outside of the risks discussed before.

Quantifying and expressing risks within an organizational context

Alongside the studies about the perception or risks, there are differences in expressing the exposure to risk within organizations. Different mathematical approaches are applied within organizations to quantify risk. Probably the best known and simplified quantification of risk is often expressed as the product of the likelihood of an event occurring, times the (estimated) impact of the event. The results are often expressed in a risk matrix, showing likelihood on one axis and impact on the other.

McNeil, Frey and Embrechts (2015) describe the evolvement of quantitative risk management (QRM) that focusses on statistical models to express risks. Throughout the 1990s Value at Risk was developed to quantitatively express financial buffers for certain risks. Value at risk is used primarily in risk management, calculating regulatory required capital, financial control and financial reporting. Furthermore, McNeil, Frey and Embrechts write that Value at Risk is applied in some instances for non-financial purposes as well. In the second Basel accord Value at Risk was adopted as primary measure for market risk and proposed variants based on Value at Risk for other types of risks.

3.2 Different perspectives on integrating risk management practices

Several studies describe risk management approaches throughout the 1980s and 1990s had grown into different silos of risk management practices, each type of risk was managed independently (Miller, 1992; Hoffman, 2002; Meulbroek, 2002; Rosenberg & Schuermann, 2006; Simkins & Ramirez, 2007; Power, 2009). Different silos of risk management practices lacked an organization wide overview and insights. This lead to concepts of integrating organization wide risk management practices with the objective to eliminate redundancies in double activities and other inefficiencies.

Enterprise wide risk management

According to (Olson & Wu, 2015) the concept of Enterprise Risk Management (ERM) developed from the 1990's into a discipline around the 2000's. In this period the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed an internal control framework that was aimed to counter fraud. The first internal control framework was published in 1992, but gained wide acceptance following financial failures of the early 2000's, such as the Enron and WorldCom scandals. Nowadays COSO ERM is a de facto standard framework used within many larger organizations.

In 2004 the Committee of Sponsoring Organizations of the Treadway Commission (COSO) introduced an integrated framework for Enterprise Risk Management. COSO defined ERM as: **"**Enterprise *risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*" (COSO, 2004, p. 2).

COSO is aimed at corporate wide governance including enterprise wide risk management. Gordon, Loeb and Tseng (2009) state Enterprise Risk Management is a subset of an organization's management internal control system. Enterprise Risk Management is the domain that provides a holistic approach on risk management practices throughout an entire organization and is related to the organization's objectives. ERM combines different risk management practices into a holistic discipline.

The Risk Management Society (2016, p. 1) states that "*Enterprise Risk Management ("ERM") is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.*"

More detailed the Risk Management society (2016) describes the main goals and activities of Enterprise Risk Management, they can be summarized as:

- Managing the exposure to different types of risk in all areas of organization related risks (financial, operational, reporting, compliance, governance, strategic, reputational, etc.);
- Considering the Internal and external environment, systems, circumstances, and relevant stakeholders as context factors influencing organization wide risk;
- Manage all types of risk, quantitative or qualitative in nature, in a structured process;
- Provide insights into individual risks across the organization, however risks are often interrelated and can create a combined exposure that differs from the sum of individual risks;
- Effective risk management can be utilized as a competitive advantage, therefore risk management should be embedded in all critical decisions within the organization.

Integrating Corporate Governance, Risk Management and Compliance

Another perspective on enterprise wide integration of risk management practices, comes from a technology perspective. The Open Compliance and Ethics Group (OCEG) is a nonprofit organization with roots in the IT services industry. The OCEG developed standards and guidance on integrating Corporate Governance, Risk Management and Compliance (GRC) practices.

According to the OCEG the three domains of Corporate Governance, Risk Management and Compliance share common objectives and complementing reporting requirements. The OCEG defined GRC as: *"GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives while addressing uncertainty and acting with integrity"* (OCEG, 2017, p. 1).

According to Racz, Weippl and Seufert (2010) there is little scientific research on Governance, Risk & Compliance (GRC). The authors found that much research was done on the separate domains of Governance, Risk and Compliance, however integration concepts are mainly present in practice. Therefore, the authors created a definition based on an extensive literature study and validation in practice, leading to a definition for GRC: "*GRC is an integrated, holistic approach to organisation-wide GRC ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness.*" (Racz, Weippl, & Seufert, 2010, p. 113)

Integrated Governance, Risk Management and Compliance consists of four holistic and organization wide components: strategy, people, processes and technology. Correctly managing and supporting operations with integrated GRC results in ethically correct behavior, improvements of efficiency and effectiveness (Racz, Weippl, & Seufert, 2010).

Concepts of Corporate Governance, Risk Management and Corporate Compliance

Gillan and Starks (1998, p. 4) defined corporate governance as "*the system of laws, rules, and factors that control operations at a company*". In practice a policy including the internal rules is created by the executive management team of the organization. The executive management team directs and controls the entire organization. This is done devising the organization management hierarchy, providing instructions on strategic objectives. Governance activities support effective decision making by systematically reporting corporate performance on time with complete and accurate information.

Risk Management is defined by the International Organization for Standardization (ISO, 2009b, p. 3) as "*coordinated activities to direct and control an organization with regard to risk*". Risk management is intended to identify, analyze and respond appropriately to risks in a continuous process. Properly executing, monitoring and communicating (about) the risk management performance ensures that important decisions are within the acceptable risk tolerance required for achieving the strategic objectives of an organization.

Tarantino (2008, p. 21) describes corporate compliance as "*acting in accordance with established laws, regulations, protocols, standards, and specifications*". Internal compliance is achieved by the executive management by developing and monitoring the adherence to policies, requirements, directives or procedures set by the executive management within the organization. External compliance means the organizations conforms to laws, contractual agreements, regulations or standards that are required in the countries or industries where the organization is operating.

Common grounds and differences between ERM and GRC

Considering the ERM and GRC definitions there appears to be shared objectives, or at least some overlap between both concepts. In literature and from practice, it appears there are many perspectives on how ERM and GRC would relate to each other. Therefore, this section provides a summary of the main commonalities and differences.

Racz, Weippl and Seufert (2011) researched the relationships between Enterprise Risk Management (ERM) and Governance, Risk & Compliance (GRC). The authors describe two distinctive perspectives:

1. ERM is a full subset of GRC, where GRC is the umbrella concept, overreaching ERM;
2. ERM and GRC overlap. Both share common objectives, processes and technologies, however both domains have their own specific processes as well.

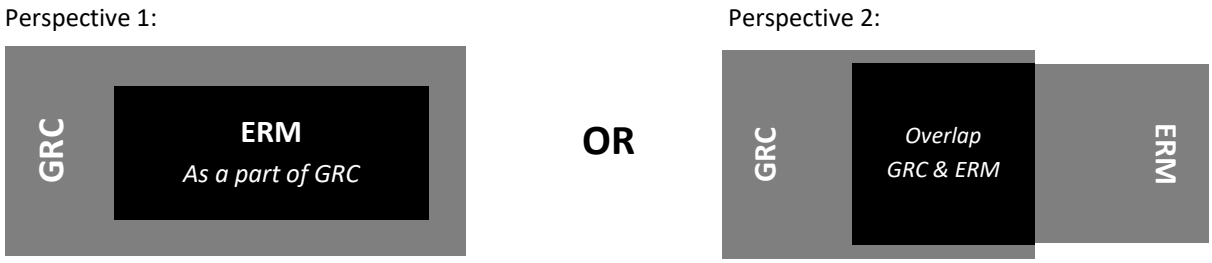


Figure 2: Different perspectives on ERM and GRC, adapted from Racz, Weippl and Seufert (2011).

Additionally, Peter (2010) described two perspectives on the relationship between GRC and ERM. In the first perspective ERM is part of GRC as the risk management component, similar to Racz, Weippl and Seufert (2011). In the second view ERM is an umbrella concept containing all aspects of GRC.

The Risk Management Society (2016) states that Enterprise Risk Management is different from GRC, because GRC is often aimed at one or a few areas of exposure to risk, while ERM considers all areas of exposure to risk, such as: financial, operational, reporting, strategic, reputation, et cetera.

The following table aims to provide an overview of the differences between both domains:

	Enterprise Risk Management	**Governance, Risk & Compliance**
Root Domain	Accounting	Information Technologies
Goal	Reasonable assurance regarding the achievement of entity objectives (COSO, 2004).	Ethically correct improving efficiency and effectiveness trough GRC (Racz, Weippl, & Seufert, 2010).
Type	ERM is a continuous **process** across the enterprise (COSO, 2004).	GRC is an integrated, holistic **approach** (Racz, Weippl, & Seufert, 2010).
Approach on integration	Integrating silos of different types of risk management (Simkins & Ramirez, 2007; Power, 2009).	Silos of duplicating efforts in the different areas of governance, risk and compliance (OCEG, 2015).
Role of Information Technology	Information Technology as enabler of firm agility and flexibility (Arnold, Benford, Canada, & Sutton, 2015).	Information technologies as an enabler for GRC to increase compliance procedures and concurrently reducing costs (Nissen & Marekfia, 2013).

Table 1: Different perspectives on ERM and GRC (composed from literature by the author).

3.3 Risk Management as a process

Risk management as a continuous process developed over time into a common understanding of risk management objectives and activities. Organizations struggled with implementation and application of a decent risk management process. This section will describe the historical developments of risk management as a process into standardized approaches as available today.

Historical perspective on risk management as a process

In 1974 Gustav Hamilton developed the "risk management circle" that shows risk management as a continuous process. Hamilton's publication is described as the first to depict risk management types and activities as applied in an organizational risk management context (Fraser & Simkins, A brief history of risk management, 2008).

Over the following years from several different domains in engineering, accounting and more disciplines developed their own risk management best practices. For example, Carr, Konda, Monarch, Ulrich and Walker (1993) from Carnegie-Mellon university created a risk management process for use in software engineering. The proposed process shows communication at the core. The process steps Identify, Analyze, Plan, Track and Control are executed as a continuous process including communication as essential core component in all steps.

In 1995 Standards Australia and Standards New Zealand published the first official Risk Management Standard. Purdy (2010) writes the AS/NZS 4360:1995 standard was created by a team from multiple disciplines working together to create a common frame of reference for risk management.

In 2004 COSO ERM was published, providing an internal control including enterprise wide risk management within a framework from an accounting perspective. COSO ERM aimed to provide a framework including risk management activities as essential part in steering organization objectives.

In 2005 The International Organization for Standardization (ISO) identified a need for resolving inconsistencies and ambiguous practices from different disciplines. The ISO created a working group including hundreds of experts from 28 different countries to write a global standard providing a definition, generic application practices, and one language of risk management. Four years later the ISO Committee for risk management published ISO 31000. Purdy (2010) describes the plan, do, check, act cycle by Deming and structure from the Australian and New Zealand standards are used as an important source by the ISO committee to develop the ISO 31000 standard for risk management. However most of the content was completely rewritten.

In 2015 the International Organization for Standardization stated that the ISO 31000 standard has been adopted by more than 50 different countries as their national standard for risk management. Resulting in a coverage of over 70% of the world-wide population (Tranchard, 2015).

Risk Management as a process from a business perspective

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) represented the Integrated Enterprise Risk Management (ERM) framework as a three-dimensional cube (2004). The top plane shows the different categories of organization objectives COSO ERM aims to support: strategic, operations, reporting and compliance. The front face of the cube represents the eight interrelated risk management activities. The side shows the activities apply at all organization levels: entity-level, division, business unit, subsidiary. Figure 3 shows the COSO ERM cube.

Figure 3: Integrated Enterprise Risk Management Framework cube, as published by COSO (2004).

Internal Environment

The internal environment should cover the organization philosophy regarding its risk appetite, ethics and environment at the organization board level.

Objective Setting

In this step organization objectives need to be identified, defined and prioritized to ensure the risk management activities align with the organization's overall mission and goals.

Event Identification

The organization should create a risk inventory, containing internal and external events that may influence the organization's objectives.

Risk Assessment

This step covers the analysis and rationalization of risks by determining the likelihood and (financial) impact. Assessment results in a risk profile, as inherent (gross) risk without mitigating measures (controls) or a residual (net) risk including mitigating measures (controls).

Risk Response

Covers the response to risks with the options: accept, avoid, reduce or share the risk. This is followed by determining (a set of) actions to align the risks with the organization risk appetite.

Control Activities

To ensure risk responses are carried out effectively. This step involves registration throughout the entire risk management process. Indicators and reports are used to manage the process performance. Additionally, these outputs can be used for internal and external audit purposes.

Information & Communication

How relevant information is identified, captured and communicated. Effective communication should occur across, top-down and bottom-up throughout the entire organization.

Monitoring

Covers how the entire enterprise risk management framework and process are monitored and adjusted when needed. This could include: ongoing management, evaluations, meetings, et cetera.

The ISO 31000 Standard for Risk Management

The Standards Australia approach provided a description how risk should be managed in a process. ISO 31000 goes further by standardizing an entire risk management system including guidelines on implementation. The International Organization for Standardization states that ISO 31000 is not intended for certification purposes. ISO 31000 states the standard is intended to support any type of organization implementing risk management for any purpose required.

ISO 31000 consists of a base document describing a generic framework for a risk management system, called *Principles and guidelines*. Additionally, the ISO 31000 standard is further detailed into:

- ISO Guide 73:2009, containing a vocabulary for risk management terms, to be used on every level/department in an organization, using the same unified language for risk;
- ISO 31010:2009, a description of methods and techniques for risk assessment;
- ISO 31004:2013, an implementation guide for organizations that want to use ISO 31000.

The ISO 31000 Principles and guidelines document advices to appoint a risk owner who is required to take ownership of the risk management process and extensively describes the process. Risk management is defined by ISO 31000 as: “process systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk” (ISO, 2009b, p. 3).

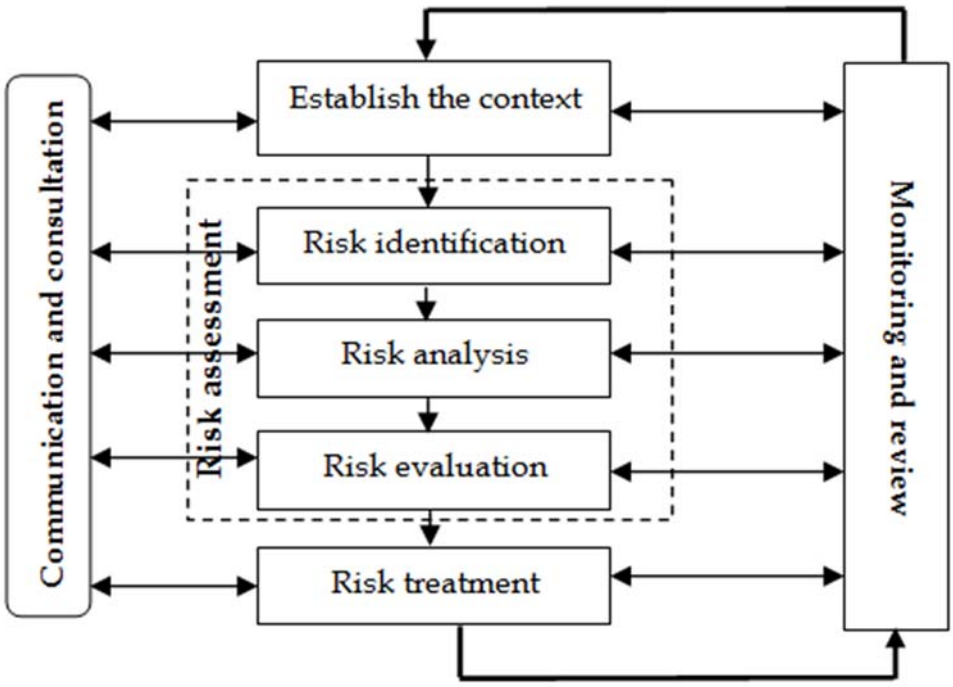


Figure 4: Standardized risk management process activities according to ISO 31000 (2009a).

ISO 31000 provides a generic risk management process to be applied in any situation and type of organization where risks need to be managed. ISO 31000 states it does not replace existing standards, but complements them by providing a common approach to risk. Therefore, the first step in the risk management process is to establish or investigate the context of the application.

Establish the context

Risk management is defined as "the effect of uncertainty on objectives" (ISO, 2009b, p. 1). ISO 31000 describes that any risk management process starts by identifying and describing the objectives, the internal and external environment where it will be applied. Furthermore, stakeholder requirements, policies and legislation should be considered before proceeding the risk management process.

Risk Assessment

Systematic assessment of risks aims to provide an understanding about causes and the impact of risks. Risk Assessment is split into three steps: risk identification, risk analysis and risk evaluation.

1. **Risk Identification**

   The first step in risk assessment is to gain recognition about what can happen. This should be done by identifying key or core sources of risks of the in the form of essential processes, people and tasks. This is followed by defining and categorizing the risks.

2. **Risk Analysis**

   The goal of risk analysis is to divide the identified risks into major and minor risks. Risk analysis is performed by identifying current controls, determining the likelihood of a risk occurring and estimating the consequence/impact to determine the level of risk.

3. **Risk Evaluation**

   Determine acceptable and unacceptable risks by comparing the level of risk from the previous step against the identified risk criteria, then prioritize risks that require treatment.

Risk treatment

All risks that fall outside the risk evaluation criteria should be considered a form of treatment. The risk treatment process starts by selection of a treatment option, followed by planning and implementing the selected treatment. ISO 31000 describes the following treatment options:

- **Accept or retain** the risk. This is based on documented procedures, policies or judgement;
- **Transfer or share** the risk by outsourcing certain activities or insurance;
- **Reduce the likelihood,** for example, by implementing mitigating measures, improving process (quality) providing training and education, communication about internal policies and performing internal audits;
- **Reduce the consequences,** by contractual arrangements, implementing business continuity plans and public relations;
- As a last resort, **avoiding the risk** by discontinuing an activity.

When implementing one of the treatment options an implementation plan should be created, including: responsibilities, schedule, expected results, available budget, performance measures and the review process.

Communication and consultation

During the entire risk management process performance, can be improved by informing internal and external stakeholders, not avoiding conflicts or concerns, but discuss them to reach mutual decisions.

Monitoring and review

Risk management is a continuous process, the exposure to risks may change over time. Therefore, the entire risk management process performance, all underlying process activities, mitigating measures and risk should be continuously monitored and reviewed by internal and external stakeholders.

Comparing COSO and ISO 31000

Although COSO ERM and ISO 31000 use a different language, both risk management processes appear to have a similar structure. Therefore, this section aims to provide a comparison from both processes and an overview of the main differences between both frameworks.

COSO ERM (2004)	**ISO 31000** (2009a)
Internal Environment	Establish the context - internal and external environment - identifying and describing objectives
Objective setting	
Risk Assessment: 1. Event Identification 2. Risk Assessment 3. Risk Response	Risk Assessment: 1. Risk Identification 2. Risk Analysis 3. Risk Evaluation
Control activities	Risk Treatment
Information and communication	Communication and consultation
Monitoring activities	Monitoring and review

Table 2: Comparing process activities between COSO ERM and ISO 31000 (composed by the author).

The main differences between both frameworks are mainly based on their approach and background. Table 3 provides a summary including some main differences between the frameworks.

	COSO ERM (2004)	**ISO 31000** (2009a)
Created by	A committee including international accountants and auditors	An international experienced team of risk management specialists and advisors
Scope	Offer an extension for the internal control framework of the 1990s to counter fraudulent practices	Manage any kind of risk, regardless of size and complexity. Provide a structured and integrated approach
Approach	Support (large) organizations on control and compliance (mainly for compliance with Sarbanes-Oxley)	Standardization of risk management, however not intended for certification or auditing purposes
Responsibility	Board of directors and management, CEO is overall responsible for all risks	All risk owners, appointment of a risk owner who is ultimately responsible
Terminology	Geared towards businesses, with clear roots in accounting and finance	Generic, applicable for anything involving risks that require a form of management
Risk definition	Only negative consequences as risk, may end up managing and focusing on controls instead of risks controls-based approach to risk management	Negative and positive consequences as risk, discussion can focus on managing the risk to achieve objectives
Focused on	Prevention of (financial) losses when an event occurs, adversely affecting the achievement of objectives	Adding value while managing the effects of uncertainty on objectives
Risk response	Four distinctive risk responses	Six distinctive risk responses
Risk profile	Inherent/gross risk included, as well as residual risks	No inherent or gross risk, only residual risk
Likelihood analysis	Likelihood analysis at the event level, high level	Likelihood analysis as the consequence level, deeper level of analysis

Table 3: Major differences between COSO ERM (2004) and ISO 31000 (2009a) (composed by the author).

3.4 Operational Risk Management (ORM)

Power (2005) writes that the term "*operations risk*" first appeared in the early 1990's. When the Committee of Sponsoring Organizations of the Treadway Commission (COSO) officially introduced its first version of the integrated internal control framework in 1991. According to Power, the term "*operations risk"* did not gain full attention until 1999 when the Basel Committee introduced Basel II.

Around the 2000s the Basel committee identified a need for a new type of risk appearing from fraud and human misbehaviors such as theft. Mistakes or fraudulent actions were not covered by any other type of risk management, therefore the committee defined operational risk as: "*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.*" (Basel Committee, 2001, p. 2). The committee states organizations can adapt or modify the definition to their own specific context.

Operational Risks within Enterprise Risk Management

Within the domain of Enterprise Risk Management, Operational risks falls within the category of financial risks, because the main goal is to calculate a financial reserve for operational losses.

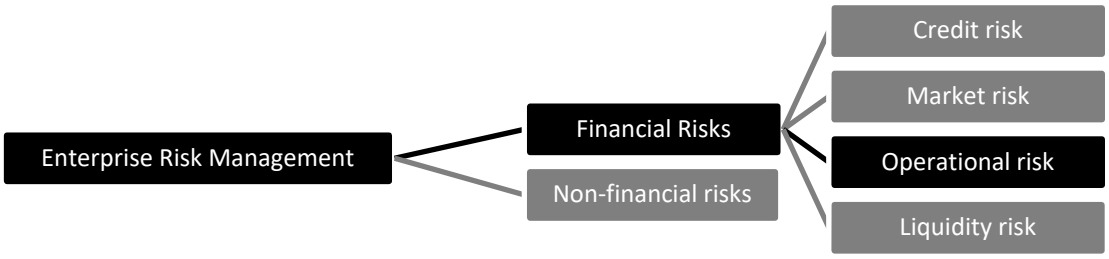


Figure 5: Operational risks within ERM, based on Chernobai, Rachev and Fabozzi (2008).

3.4.1 Sources of operational risk

Chernobai, Rachev and Fabozzi (2008) and Loader (2011) further conceptualized sources of operational risks. Exposure to risk could be a **hazard** (risk type), a risk type includes one or multiple factors influencing the probability of an event occurring. An event is an incident that leads to an effect, for example a **loss** (event type). Losses represent an amount of **damage** (loss type) resulting from an event.

Operational risk event type categories

The Basel committee (2003) detailed operational risks further into specific event type categories:

1. **Internal fraud**, losses related to intentional or inappropriate acts. Circumventing laws, regulations or organization policy, involving at least one internal stakeholder;
2. **External fraud**, losses related to intentional or inappropriate acts regarding misappropriate property, information breaches or acts that circumvent the law by a third party;
3. **Employment practices and workplace safety**, losses related to acts inconsistent with health, safety or employment laws or agreements;
4. **Clients, products and business practices**, losses arising from a failure to meet professional obligations to clients or from the nature or design of a product;
5. **Damage to physical assets,** losses or damage related to natural disasters or other events;
6. **Business disruptions and system failures**, loss from business disruptions and system failures;
7. **Execution, Delivery & Process Management,** losses resulting from process management, transaction processing or external relations, such as trade counterparties and vendors.

Examples of operational risks

Operational risks are further explained by the Basel committee with specific categories and examples:

Event-Type Category *(Level 1)*	**Categories** *(Level 2)*	**Activity Examples** *(Level 3)*
Internal fraud	Unauthorized Activity	Non-reported or unauthorized transactions or (intentional) mismarking of position.
	Theft and Fraud	Fraud, credit fraud, worthless deposits, theft, extortion, embezzlement, robbery, misappropriation or destruction of assets.
External fraud	Theft and Fraud	Theft, robbery, forgery, check kiting.
	(information) Systems Security	Hacking damage, information theft.
Employment Practices and Workplace Safety	Employee Relations	Compensation, missed benefit, termination issues or organized labor activity.
	Safe Environment	General liabilities (slip and fall, etc.), compensation, health & safety rules.
	Diversity & Discrimination	All discrimination types.
Clients, Products & Business Practices	Suitability, Disclosure & Fiduciary	Fiduciary breaches, (sales) guideline violations, disclosure issues, privacy issues, misuse of confidential information.
	Improper Business or Market Practices	Antitrust, improper trade, manipulation, unlicensed activity, money laundering.
	Product Flaws	Product defects, model errors.
	Selection, Sponsorship & Exposure	Failure to investigate client per guidelines, exceeding client exposure limits
	Advisory Activities	Disputes over quality of advisory activities.
Damage to Physical Assets	Disasters and other events	Natural disaster losses, human losses from external sources (terrorism, vandalism).
Business disruption and system failures	Systems	Hardware, software, telecommunications, utility outage or disruptions.
Execution, Delivery & Process Management	Transaction Capture, Execution & Maintenance	Miscommunication, data entry, maintenance or loading error, missed deadline or responsibility, system failures, accounting error, delivery failure, collateral management failure, reference data maintenance
	Monitoring and Reporting	Failed mandatory reporting obligation or inaccurate external report (loss incurred).
	Customer Intake and documentation	Client permissions, disclaimers missing, legal documents missing or incomplete.
	Customer / Client Account management	Unapproved access given to accounts, incorrect client records (loss incurred), negligent loss or damage of client assets.
	Trade Counterparties	Non-client counterparty misperformance, misc. non-client counterparty disputes.
	Vendors & Suppliers	Outsourcing, vendor disputes.

Table 4: Operational risk categories and examples, Basel committee (2002) (examples shortened by author).

3.4.2 Terminology related to operational risk, a cross industry perspective

Operational risk as defined by the Basel Committee is a term from a financial perspective, meaning the term operational risk is well known and understood by banking and insurance organizations. Within the financial services industry operational risks are often part of enterprise risk management activities and related to corporate governance activities.

Outside the financial services industry operational risks are also present, however not always managed from an integrated enterprise or corporate governance perspective. Additionally different terminology is used for the same types or categories of operational risks. This section aims to provide a summary of different terminology used in different industries.

Operational risk in the Energy industry

Panjer (2006) writes operational risk is a term that is well known in banking and insurance, however operational risk is adopted as a term in the energy industry as well. Additionally, Enterprise Risk Management and the COSO ERM framework are recognized in the energy industry.

Operational risk from a quality management perspective

Hoffman (2002) writes quality management practices, such as six sigma influenced the perspective of performance improvement, similarly as intended with operational risk management. Quality management follow a continuous improvement cycle using the Plan-Do-Check-Act cycle, similar to the risk management improvement cycle.

The International Organization for Standardization (ISO) started to standardize a Quality Management System (QMS), known as ISO 9000 in the late 1980s. Since ISO 9001:2008, versions of ISO 9000 describe risk assessment should also be considered an integral part of quality management. Although there are similarities between quality management and risk management, quality management is focused primarily on business processes. Risk management, especially operational risk management is also considering other factors, such as humans and systems.

Rahimi (1995) writes quality management and a safety management system combined integrates organizational processes, people and technological elements towards a common performance objective. Integrated safety and quality management lead to proactive mitigation of (operational) risks.

Integrating Quality, Safety, Health and Environment

Grote (2012) describes safety management is applied in high risk domains and have many similarities between different domains. From the safety management perspective there is also a recent movement towards integrating silos of safety and risk, often referred to as Health, Safety, Environment & Quality.

Abbreviation	Term	Focus/goal
QMS (ISO 9000)	Quality management system	Improving quality of a product and customer satisfaction.
SMS or ISMS (Grote, 2012)	(Integrated) Safety management System	Manage safety of people.
SHE or HSE (Rahimi, 1995)	Safety, Health, Environment	Integrate safety management, health of people and environment.
QHSE or QEHS or HSEQ (Väyrynen, Jounila, & Latva-Ranta, 2014)	Health, Safety, Environment & Quality	Integrate Quality management with safety, health and environment.

Table 5: Abbreviations & terminology used to Quality, Safety, Health, Environment.

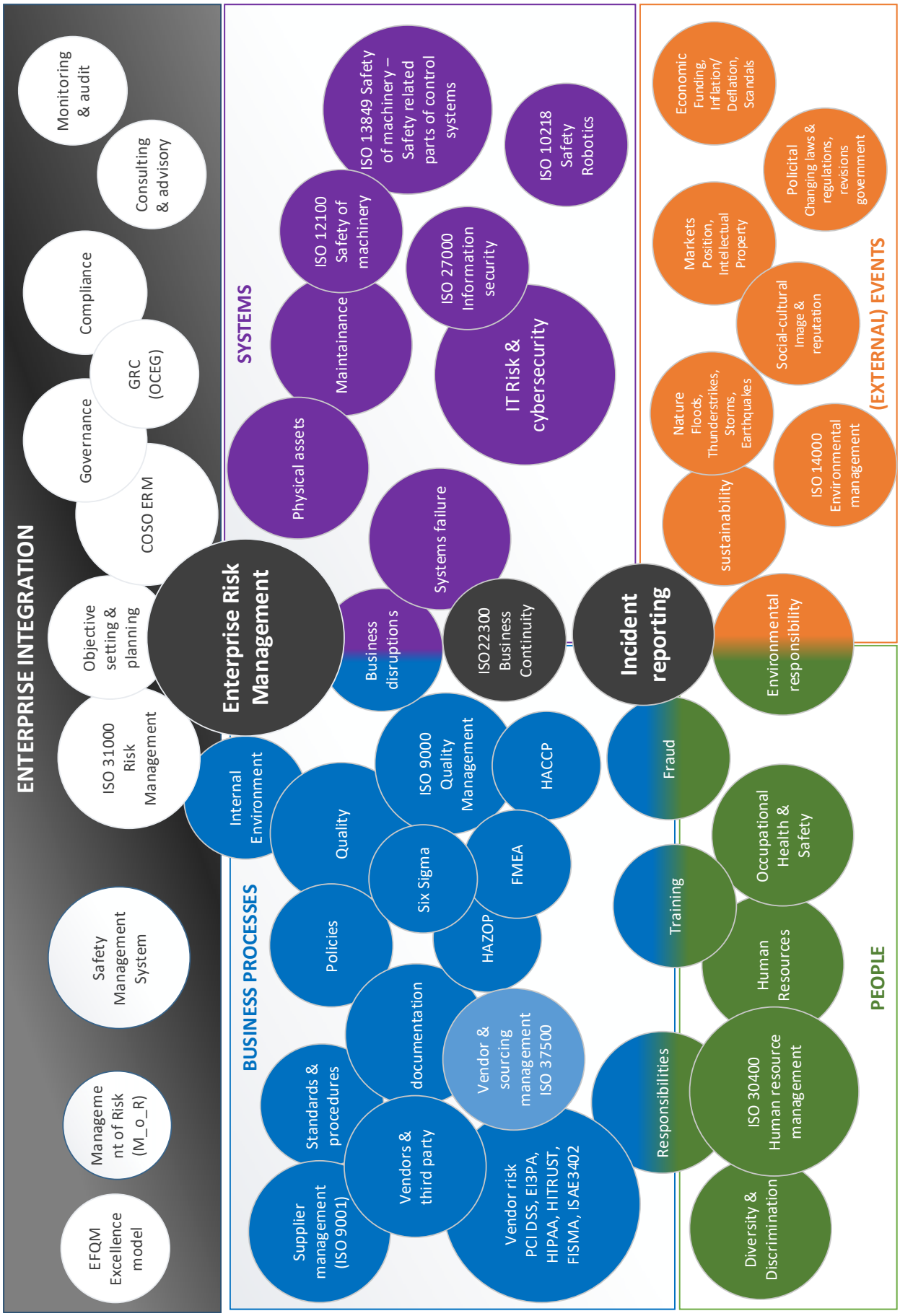


Figure 6: Different terms and practices, grouped and mapped to Operational Risk Management (own work).

Quality, Safety, Health & Environment in other industries

In many service providing or product producing organizations the terms Quality and Safety are often used in relation with quality management. Kauppila, Härkönen and Väyrynen (2015) write Health Safety, Environment and Quality (HSEQ) is often used as group for Integrated Safety Management Systems (IMS). More mature HSEQ processes result in organizational excellence.

Abbaspour, Toutounchian, Roayaei and Nassiri (2012) describe production and manufacturing organizations combine quality management with health, safety and environment on a strategic level in order to achieve a competitive advantage.

Morrison and Winston (2010) write safety was not a concern in the aviation industry until severe accidents happened because of low budget airlines who compromised on safety and maintenance for a profit. Therefore strict regulations in past decades required airline companies to have a more integrated safety management system (ISMS). Van der Schaaf, Lucas and Hale (2013) describe the railways look at the advanced aviation industry and try to use near miss information for railway safety as a component to reduce risks.

Jones, Kirchsteiger and Bjerke (1999) and Doucette (2006) write hospital utilize safety and quality management practices as used in the airline industry can be used to provide patients a high quality healthcare. They specifically describe how near miss data could be used to learn from risks and improve the quality of Health & Safety processes.

Mensah and Julien (2011) describe HSEQ in the retail and consumer goods sector. Safety & Quality management practices are used especially for reducing risk and ensuring reliable food products.

Quality, Safety, Health & Environment in relation to Operational Risk

This section describes the relationships with Quality, Safety, Health & Environment, based on each of the components that can be related to Basel's (2001) broad definition of Operational Risk.

Internal Processes

Abbaspour, Toutounchian, Roayaei and Nassiri (2012) describe vendor & third party risks, environmental management and occupational health and safety could best be managed combined. These risks often result from improperly executing internal organizational processes.

Human health & safety

Fernández-Muñiz, Montes-Peón and Vázquez-Ordás (2009) write safety management has a positive influence on safety performance, resulting in lower accidents and better employee health. Additionally they describe HSEQ increases, competitiveness and economic-financial performance.

Systems

Yuan, Mahdavi and Paul (2011) describe HSEQ also need to be concerned about IT Risks (cyber security). They describe effective safety management also should include management of IT risks.

External Events & Environment

According to Dentchev, Heene and Gosselin (2005) HSE is about sustainable and safe environment. External events could endanger these aspects and therefore risk management is necessary.

3.4.3 Stakeholders & lines of defense

Operational risks vary in importance and are present throughout every function within an organization. Most operational risk events occur in day to day operations of an organization. Small operational risks do not apply to senior management and therefore they should not be bothered with such risks, unless the risk evolves into a significant risk that effects the organization's achievement of objectives.

Properly managing operational risks is described as a *'three lines of defense'* model by Kennet and Raanan (2011), Tattam (2011) and Sadgrove (2016). Operational risk events and its consequences should be handled at the organization function it occurs, however severe consequences should be reported to the board and other stakeholders. Proper execution of the operational risk actions on the first lines should be monitored and managed by an independent function within the organization, called a second line of defense. A third line of defense is formed by an (independent) audit committee assessing the complete operational risk management structure, process and implementation on a regular basis. The audit committee can be internal, external or both internal and external.

Kennet and Raanan (2011), Tattam (2011) and Sadgrove (2016) write the concept of three lines of defense, consists of:

1. Business operations as first line of defense, this includes the front office and day-to-day operations, business line management owns the operational risks;
2. Risk and compliance as second line of defense, monitoring and oversight of the business operations, independent enterprise wide operational risk management function;
3. Audit as third line of defense, periodical reviews of risk management and compliance by independent internal or external auditors, independent reviews to provide assurance. Sadgrove (2016) writes the three lines of defense can also be four lines, when internal and external audit are split into separate lines, where internal audit is the third line and external audit the fourth line of defense.

The organization's board of directors is ultimately accountable for all operational risks within the organization. The CEO is responsible for all operational risks, however could dedicate some of its responsibilities to a Chief Risk Officer (CRO) who will be responsible for implementation and maintenance of all risk functions across the organization, including operational risk management. A CRO can be assigned to a risk committee and/or operational risk committee, supporting the responsibilities, implementation and management activities.

The first line of defense consists of people on the job. For example, a person responsible for the power backup generation unit, typically this person does not have a risk controller/owner title, however in this case manages the power supply. Managers of a department or team are responsible for managing operational risks on a day-to-day basis. Heads of a business division or senior executives are held accountable for the operational risks and provide a budget for operational risk (management).

The second line of defense is managed by a head of operational risk management, who should report to the chief risk officer. The second line of defense does not manage day-to-day risks, but is concerned with defining the operational risk framework and processes. The second line of defense usually includes specialist risk managers, providing specialized expertise on certain operational risks e.g. cyber security expert. The specialist risk managers are operating within specific functions such as information security, legal or insurance, reporting to the head of operational risk management.

The third line of defense is formed by audit teams. Those teams should act as independent function to provide assurance to risk committees and the board regarding operational risk management. Audit teams evaluate the performance and effectiveness of the operational risk management framework and process. Audit teams perform independent tests of controls (mitigating measures) and report their findings and suggestions for improvement to the board or operational risk committee. Audits should be performed by internal control testers or internal auditors. Although, several large organizations are required by regulators to have an external party perform an additional audit.

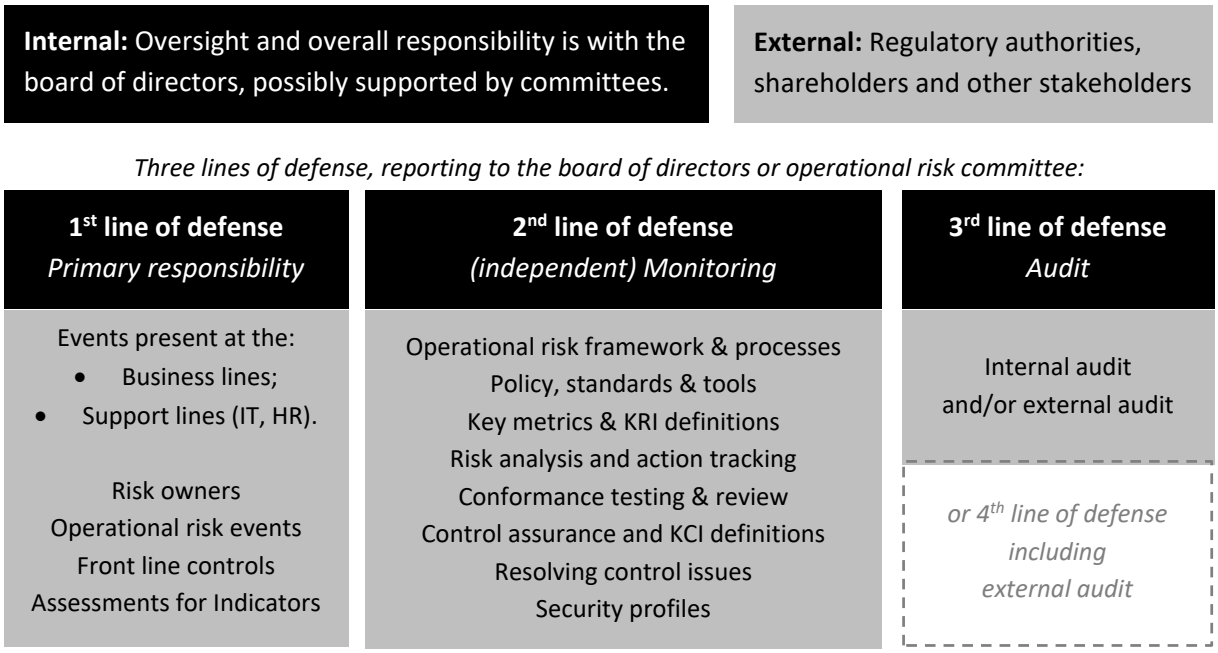


Figure 7: three or four lines of defense, based on Kennet and Raanan (2011), Tattam (2011) and Sadgrove (2016).

Role	Description
Board of Directors	Accountable for all risks related to the organization.
Operational Risk Committee	Selected people from the board of directors, primary concerned with operational risk management and its performance.
External stakeholders	Challenge and review operational risk management performance.
Chief Risk Officer (CRO)	Part of the board of directors (CxO level) responsible for coordinating and managing all risk teams, including operational risk.
Head of Operational Risk	Reports to the CRO and/or Operational Risk Committee, managing the operational risk function.
Operational Risk Management Function	Group within the organization responsible for the operational risk governance, framework and performance monitoring.
Regular employee	Involved in day-to-day operations of the organization, performing process activities and could introduce operational risks or key to identification and mitigation of operational risks.
Domain expert	Employee or manager within a department who has a deep understanding of the performed activities and risks. Often consulted during the risk assessment phase.
Internal auditor	Independent validations and consulting on operational risk management performance and compliance with internal standards.
External auditor	Objectively validating and advising operational risk management performance and compliance with law and regulations.

Table 6: Operational risk roles within the three lines of defense.

3.4.4 Operational Risk Management Objectives

Performing a decent operational risk management process should follow a risk management process as described in 2.3. However, managing operational risks should yield specific objectives. Tattam (2011) and Girling (2013) describe the objectives of operational risk management differ between different types of organizations. Major objectives include, but are not limited to:

- Identification of operational risk related opportunities;
- Improve the control culture, awareness, objectives, transparency and accountability of risk;
- Reduction of avoidable losses and insurance costs;
- Protection and enhancement of reputation or credit ratings;
- Increasing the effectiveness and efficiency of controls and the risk management process;
- Calculating and allocating capital for operational risk losses.

A systematic assessment of operational risks aims to provide an understanding about causes and the impact of risks to properly address the consequences and approach mitigating measures. Operational risk assessment follows ISO 31000 (2009a) and COSO's (2004) risk assessment process and is split into three steps: risk identification, risk analysis and risk evaluation.

3.4.5 Identification of Operational risks

Risk identification is the process of finding, recognizing and recording operational risks. Failure to identify operational risks means no action is taken to manage that risk. Making operational risks visible means they are made manageable. Identification of operational risks starts with risk awareness. The international organization for standardization describes three different approaches for risk identification within ISO 31010 (2009c):

- Evidence based methods, based on historical facts or legislation. Examples are checklists, incident & loss data and (physical) inspections;
- Systematic team approaches, group sessions to explore potential risk events. Examples are brainstorming sessions, workshops and interviews;
- Inductive reasoning techniques, identify events based on an iterative process of logical reasoning. Examples are scenario analysis, process and (work)flows analysis, Hazard and operability studies (HAZOP) and Failure Mode Effect Analysis (FMEA).

After the identification process, all identified risks should be collected in a Risk Register as a basis for further analysis (Sadgrove, 2016).

3.4.6 Operational Risk Analysis

The goal of operational risk analysis is to further assess the identified operational risks by placing them into categories and gain an understanding of the level of risk (also known as risk profile). Risk analysis is usually performed by determining the likelihood of a risk occurring and estimating the consequence to determine the level of risk. During the risk analysis process, existing mitigating measures (controls) are considered and their effectiveness can be deducted from the level of risk.

ISO 31010 (2009c) states that multiple approaches, techniques and methods can be used depending on the application and the quality of analysis an organization requires. Within some industries methods or techniques are prescribed by law or regulation authorities. Table 6 shows the main differences between qualitative, semi-quantitative or quantitative approaches.

Approach	Qualitative	Semi-quantitative	Quantitative
Goal	Categorizing and prioritizing based on (expert) ranking.	Weighted categorizing and prioritizing based on calculated values.	Prioritizing, based on calculated estimates of losses or predict financial reserves that would be required.
Results	Subjective, based on interpretation.	Subjective, might be complemented by facts.	Objective, Analytical facts.
Detail of Analysis	Categorical consequence, likelihood and level of risk, pre-determined significance levels such as: “high”, “medium” and “low”.	Numerical rating scales used for expressing consequence and likelihood. Then combining them to produce a level of risk using a formula.	Estimates practical values for consequences and their probabilities, based on numeric input and produces values of the level of risk in specific quantified units.
Scales of measure	Scales are ordinal.	Scales may be linear or logarithmic, or have some other relationship.	Scales are based on a mathematical function or formula.

Table 7: A comparison of risk analysis approaches based on ISO31010 (2009c) (composed by the author).

According to ISO 31010 choosing methods or techniques from the three approaches described in table 6 should be used based on the level of detail required. Qualitative approaches provide the least detail about the actual impact of risks, however quantitative approaches can become complex and quantitative models might fail to account certain factors and could cause quantitative models to become unreliable. Multiple approaches can be used to complement each other.

Within the domain of operational risk management, several methods and techniques are often applied in practice and some are required by regulatory authorities. Therefore, the following sections aims to demonstrate some examples, specifically used for operational risk management.

Qualitative and semi-qualitative operational risk analysis

The goal of qualitative and semi-qualitative operational risk analysis is to create categories that describe risk levels and then rank those based om their importance. Both approaches have much in common, however the main difference between both approaches is that qualitative assessments are usually solely based on (expert) opinions and semi-qualitative assessments are also related to data based on historical events. Additionally, the semi-qualitative approach relies on ratio or interval scales.

Historical data can show a pattern that can be used by an expert to extrapolate an estimate for future operational loss events. Low frequencies of historical events naturally lead to a low prediction in the future. An expert should follow a systematic and structured process to consider specific factors that influence the exposure to operational risks in the future. Table 7 shows different factors to account for within qualitative and semi-qualitative approaches. According to ISO 31010 (2009c) it is very important when applying these approaches:

- Scales and criteria that are used for analysis should be pre-defined, before the analysis starts;
- A pre-defined timeframe should be set for analysis and estimation of current and future operational risk events, e.g. one month or one quarter or one year or two years, etc.;
- All participants in the risk analysis process should be fully aware of the possible limitations a method or technique conveys and combining methods and/or techniques is more reliable.

Factor	Description	Qualitative	Semi-qualitative
Risk velocity	*Timeframe in which one operational risk event can occur.*	Fixed time scales, e.g.: Short (< month), Long (month - quarter), Very long (> year)	Ratio scale, time for example: minutes, hours, days, months
Impact	*Any disruptive event related to objectives or processes, (disruptive) impact during the next timeframe.*	Fixed time scales, e.g.: Short (< week), Long (week - month), Very long (> month)	Ratio scale, time for example: minutes, hours, days, months
Financial Impact	*Potential level of financial impact during the next timeframe.*	Fixed ranges, e.g.: Minor (€10k), Major (€10K – €100K), Severe (€100K+)	Ratio scale, numbers expressing currency
Likelihood	*How likely the risk is to occur during the next timeframe.*	Fixed ranges, e.g.: Unlikely (< 30%) Likely (30 % - 70%) Very likely (>70%)	Ratio scale, Probabilities or percentages
Frequency	*How many times could the risk occur during the next timeframe.*	Fixed ranges, e.g.: Low (< 5 times) Medium (5- 10) High (10+)	Ratio number scale, exact amounts / counts

Table 8: Differences between qualitative and semi-qualitative risk factors, composed by the author, based on: Tarantino (2008) and ISO 31010 (2009c) (composed by the author).

Based on table 7 we can conclude that qualitative factors mostly rely on fixed ranges and semi-qualitative factors allow for more precision because of their 'gliding' (ratio and interval) scales.

One of the most popular and well known visualizations of qualitative and semi-qualitative risks is the consequence and likelihood matrix (also known as: risk matrix or risk heatmap). One of the impact factors is set against one of the factors of occurrence. Scores can be combined by multiplying the consequence and likelihood, resulting in a risk score that indicates the risk profile. All operational risks from a scenario should be plotted in this matrix, showing the relative positioning for further evaluation.

← IMPACT →					
Catastrophic	5	10	15	20	25
Critical	4	8	12	16	20
Significant	3	6	9	12	15
Important	2	4	6	8	10
Minor	1	2	3	4	5
	Very unlikely	Unlikely	Probable	Likely	Very Likely

← LIKELIHOOD →

Figure 8: Example of a likelihood and consequence matrix, created by the author based on: Samad-Khan (2005) Blunden and Thirlwell (2012) and Sadgrove (2016).

Samad-Khan (2005) writes that a risk probability and consequence matrix should at least be composed of a matrix from 3 x 3. A matrix composed of less combinations is not suitable for operational risks, while more combinations, such as the 5 x 5 matrix (as shown in figure 5) provides more detail.

Quantification of operational risks

The likelihood/consequence matrix works well for qualitative-based ranking, but not for quantification of (predicted) losses and financial reserves for operational risks. Linear correlations of risk as likelihood times consequence function lead to critique in statistics, economics and finance, because the simple *likelihood x consequence* expression omits additional factors that influence risk.

Breden (2006) describes for credit and market risk an organization appoints a fixed financial portfolio and therefore it is clear how to estimate a maximum loss of a portfolio. When considering operational risks it is very hard to determine how much a fraudulent transaction or a mistake in a process will cost.

Samad-Khan (2005) and Haimes (2015) state it is virtually impossible to calculate the exact risk because the construct of the simple expression likelihood times impact omits the impact of catastrophic events with a very small likelihood. Therefore, uncertainties of unlikely catastrophic events, for example actions leading to corporate failure or an event causing many deaths could end up untreated.

Therefore, several methods are developed to quantify operational risks. Cornalba and Giudici (2004) describe that the goal of all operational risk quantification models is to estimate a loss distribution for operational risks. They describe two distinctive approaches:

1. Top down methods: Operational risk capital for losses is calculated at the central entity level of the organization, then distributed down over individual business units.
2. Bottom up methods: risk exposures and losses are broken into smaller sets of risk exposure on the level of business units (also called: business lines) and then aggregated up to entity level.

The Basel Committee (2014; 2016) proposed a number of approaches to quantify operational risks:

Approach	Introduction	Method	Data required
Basic Indicator Approach (BIA)	2004 (withdrawn in 2014)	Percentage of positive Gross Annual Income over 3 years	Financial statement
Standardized Approach (SA)	2004 (revised in 2014)	Percentage for each business line, then summed-up to top-level	Financial statement per Business Line
Business Indicator (BI)	2014 (replaced BIA)	Operational loss capital based on nature of business, related margins, income and expenses	Detailed financial statement
Advanced Measurement Approach (AMA)	2004 (withdrawn in 2016)	Empirical Internal Risk Modeling and development process, using historical and hypothetical statistics to predict loss values	Combinations of internal data, external data, scenario analysis
Standardized Measurement Approach (SMA)	2016 (replaced AMA)	Combination of Business Indicator and organization related (historical) loss data	Detailed financial statement and loss data

Table 9: Different operational risk capital approaches proposed by the Basel Committee from 2004 to 2016.

The simplest quantification for a risk capital reserve is the Basic Indicator Approach (BIA). In this approach an organization needs to calculate its reserve for operational risks based on a percentage (alpha) of its Gross Annual Income (usually 15 %) over the last 3 years. This operational risk quantification method is not very precise and was mainly advised for non-international banks.

The Standardized Approach (SA) is a more detailed calculation method for operational risk capital reserves. For each business line (or business unit) a different percentage is used to calculate operational risk reserves, then the calculations per business line are all aggregated to a risk capital reserve on entity level. For banking the Basel Committee defined 8 distinctive business lines, each with their own pre-defined capital charge. Before a bank is allowed to use this method the board and operational risk management oversight should be involved, the organization should have implemented a sound operational risk management framework and sufficient resources in use in each business line.

The Business Indicator (BI) approach was introduced by the Basel Committee in 2014, because the Basic Indicator Approach (BIA) was too simple and Gross Income did not reflect the operational risk properly. The Basel Committee has therefore withdrawn the BIA and suggested the Business Indicator approach. The business indicator approach considers factors for the nature of business and its related margins based on income and expenses. The Business indicator is sensitive to items with a higher operational risk, such as operational activities, services and net results. For larger banks, there are multiplication factors to scale the operational risk reserve increasing corresponding with the BI value.

The Advanced Measurement Approach (AMA) is the most advanced form of operational risk calculation. This approach expresses operational risk in much more detail. The AMA method was advised by the Basel Committee (2014) for use in larger and international banks. This method required a continuous and empirical model development cycle, where a model is built combining four distinctive sets of data to predict operational loss values. There is no standard technique for applying this method.

The most applied technique for AMA is the Loss Distribution Approach (LDA). In this technique, internal and external data are used to create a frequency distribution and a severity distribution as a lognormal function. Then a Monte Carlo Simulation engine is used to take many (usually more than ten thousand) random samples of both distributions, simulating scenarios of operational loss events. The simulation results in a new aggregated operational loss distribution. For this distribution, a confidence interval and timeframe should be determined to calculate the Operational Value-at-Risk (VaR). The Basel Committee suggests a confidence interval of 99% and a timeframe of a year. The Value-at-Risk then predicts with 99% certainty within year there will not be an operational loss of more than *x*.

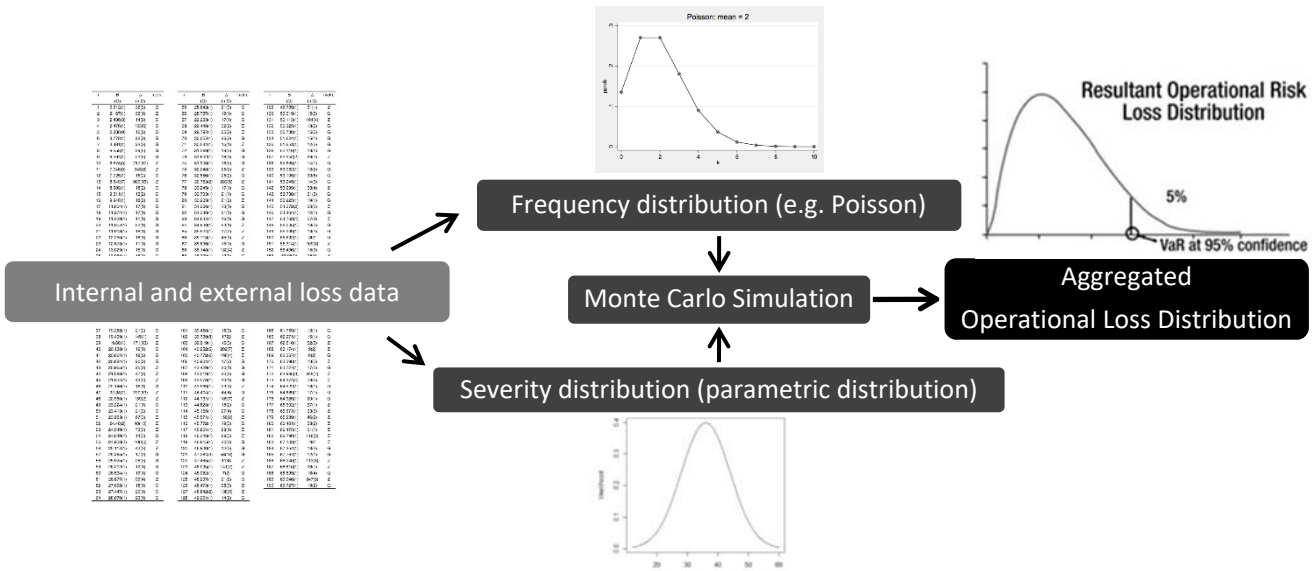


Figure 9: The Advanced Measurement Approach (AMA) and Value-at-Risk (Var), composed by the author.

The Basel Committee expected the financial sector to develop a best practice for AMA. However, in the Basel Committee concluded (2016) that the AMA method lead to a huge fragmentation of different techniques and models, leading to a high workload on both the organizations and regulators to validate all the different models. To solve this problem, the Basel Committee has withdrawn the AMA method in 2016 and replaced it with the Standardized Measurement Approach (SMA).

The Standardized Measurement Approach (SMA) is the new method for quantifying operational risk. This standardized approach makes it easier for organizations and regulators to execute and compare. SMA uses the Business Indicator (BI) approach and then complements this with operational loss data related to the activities of the organization. SMA uses the Internal Loss Multiplier (ILM) as a loss component to combine with the Business Indicator component and increases the operational loss capital requirement based on the size of the organization. An important component of ILM is that this formula weighs tail events (above the 99% confidence interval) heavier than other events and thus provide a better buffer for severe operational risk events within large organizations.

All operational risk quantification approaches have in common that they all try to identify the worst expected loss based on a certain confidence level. However, it needs to be recognized that even full quantification of the operational risk losses are just hypothetical loss estimates and not facts. An important note is that changes to the organization structure might influence the risk exposure in such way it is not comparable to the past. A combination of qualitative expert input and quantification methods are recommended. Expert input serves as a in depth understanding of the risk while simulation and scenario quantification provide a more objective measure, combining both would yield the most reliable results (Doerig, 2000; ISO, 2009c; McNeil, Frey, & Embrechts, 2015; Haimes, 2015).

3.4.7 Operational Risk Evaluation

After a detailed analysis follows a short evaluation stage. In the operational risk evaluation stage the significance of operational risks resulting from the analysis is compared a judged based on predefined thresholds and criteria. The goal is to prioritize major and minor operational risks that require a form of further treatment. This step is also intended for filtering small risks with low likelihood and little impact, such operational risks require no additional attention at this moment.

Quantified risks can be ranked based on exact threshold values and then split into groups that require treatment based on predefined thresholds. Within organizations the bands and corresponding thresholds are usually related to the organization's risk appetite. ISO 31010 (2009c) describes thresholds are often divides into three bands:

- The upper band with major risks, that require treatment at all cost;
- The middle band with minor risks, risks where the costs and benefits should be balanced;
- The lower band with negligible risks, that require no treatment.

The thresholds for each of the bounds can be related to qualitative semi-qualitative or quantified criteria, similar to the results of the analysis.

3.4.8 Operational Risk treatment activities

All operational risks that fall outside the tolerable risk criteria should be considered a form of treatment. The risk treatment process starts by selection of a treatment option as described by ISO 31000 (2009a), followed by planning and implementing the selected treatment. Figure 7 visualizes how the risk treatment options impact the total risk exposure.

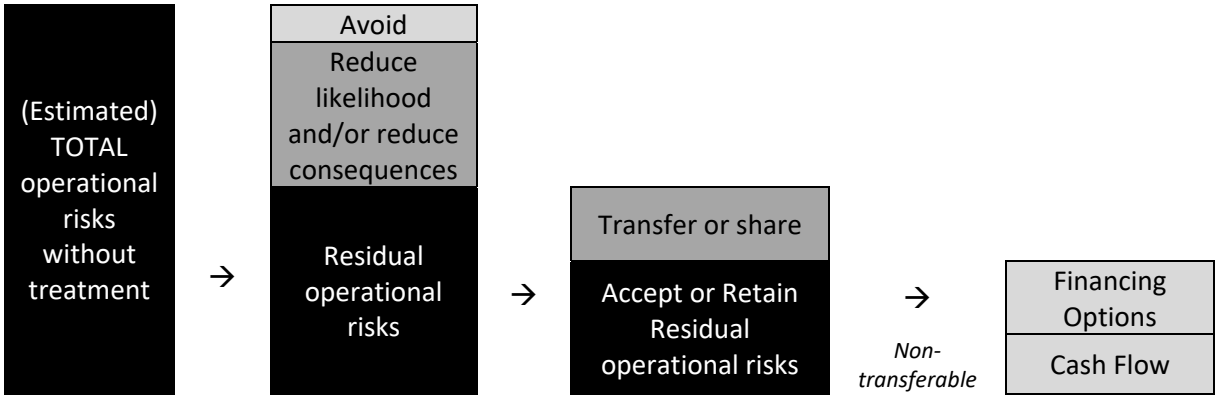


Figure 10: Visualization of risk treatment strategies, to reduce the total exposure to operational risks, created by the author, adapted from Doerig (2000).

Certain operational risks can only be mitigated by completely avoiding certain activities, especially those activities with high risks and little returns. Furthermore, a reduction of likelihood and consequences can be achieved using controls (mitigating measures). Examples of controls are divided into two groups of controls; controls can be from either group or both:

Reduce likelihood	**Reduce impact / consequences**
Additional process activities for validations and checks or redesigned processes for improving process quality, guarding core activities;	Installing physical controls, e.g. (zones with) different access levels, segregations of duties and authorizations, fire extinguishers, et. cetera.
Awareness and communication about internal policies and procedures. Additionally, providing training and education.	Implementing business continuity plans, including actions to quickly resume essential or core processes of organization and public relations.

Table 10: Examples of internal controls for reducing likelihood or impact.

Some risks have very small likelihood, but could have a big impact, those risks could be transferred to an insurance organization or outsourced when they are not a core part of the organization's operations. The residual risks should be accepted, because they are non-transferable. This is based on documented procedures, policies or (expert) judgement. When accepted, risks occur they should be financed using available cash or financing options.

When implementing one of the treatment options, an implementation plan should be created including: responsibilities, schedule, expected results, available budget, performance measures and the review process. The Basel Committee (2011) describes internal controls (mitigating measures) should be embedded in day-to-day operations and designed to ensure that:

- Activities are efficient and effective;
- Information is reliable, timely and complete;
- The organization is compliant with applicable laws and regulation.

3.4.9 Monitoring and review

The operational risk management function within the organization is responsible for continuously monitoring operational risk management, internal and external environment, risks and mitigating measures (controls) for its performance and possible changes. These should be within operational risk profile criteria, related to an organization's risk appetite. Risk Appetite is defined by the International Organization for Standardization Risk Management Vocabulary (ISO, 2009b) as: "Amount and type of risk that an organization is prepared to pursue or retain".

Operational risks and controls should be continuously monitored over time and kept within the set limits of the risk appetite. The operational risk management function should coordinate action when an operational risk threatens to go beyond the risk appetite boundaries and when necessary escalate to the board or operational risk committee. Scandizzo (2005), Davies, Finlay, McLenaghen and Wilson (2006) Chernobai, Rachev and Fabozzi (2008), Girling (2013), describe that the operational risk management function could do this by developing a set of operational Risk Exposure Indicators, Key Risk Indicators and Key Control Indicators:

- Key risk indicators (KRIs) describe how the risk profile is changing and whether it is within desired tolerance levels;
- Key Control Indicators (KCIs) describe the effectiveness of controls (mitigating measures) within the organization.

Chernobai, Rachev and Fabozzi (2008) describe some examples of operational risk exposure indicators. These indicators explain some of the significance of operational risk and organization is exposed to. In summary Risk Exposure Indicators, can be derived from:

- Organization's gross income, capital structure, debt-to-equity balance;
- Value of the organization's assets;
- Volume of sales and trades;
- Value of transactions and number of transactions with internal and external parties;
- Number of employees and their experience;
- Historical operational losses.

Alongside Key Risk Indicators the effectiveness of controls should be monitored on a regular basis. For example, a fire extinguisher should not only be present, but also in working condition when an event occurs. Therefore, controls should be frequently assessed to be in place and their effectiveness should be validated. In practice control testing is done on a regular basis, set periods and frequencies in a pre-defined test plan. When an organization has many controls or controls that require frequent testing, a (random) sampling strategy can be applied for control testing. When a risk or control is not properly managed, then an issue or action should be created to resolve the issue.

The actual results from control testing can be used to supply data for Key Control Indicators for use in monitoring. ISO 31010 (2009c) states that monitoring and reviews should verify:

- Assumptions regarding (operational) risks and risk assessment practices are valid;
- Treatments, used techniques and results are properly applied;
- Results of assessments are aligned with expectations and actual circumstances;

Monitoring activities, including performed and unperformed interventions, resolved issues and possible escalations should be reviewed by internal and external audit functions.

3.4.10 Components of a framework & communication lines

All operational risk management activities come together in an operational risk management framework. An operational risk management framework is an instrument to support and improve the complete integration of the operational risk management governance and communication flows. The design of an Operational Risk Management framework is a key component for implementing, embedding practices and communication within the organization (Blunden & Thirlwell, 2012).

The (operational) risk function of the organization is responsible for creating, implementing and maintaining the operational risk management framework. There is no blueprint or standard how organizations should design and implement their framework, however Blunden and Thirlwell (2012), Girling (2013) and Lancaster (2015) describe a similar frameworks consisting of the same components. An operational risk management framework for operational risk should:

- Provide transparency in the entire organization;
- Fit to the organization's objectives and operational risk management maturity;
- Awareness and understanding of operational risks at all levels of the organization;
- Facilitate a continuous structured process instead of a one-time exercise.

Blunden and Thirlwell (2012), Girling (2013) and Lancaster (2015) describe an oversight or governance layer that should be closely related with the organization's culture. Good operational risk governance practices have a close relation with policies, procedures, internal standards, process design and utilized instruments. Furthermore, culture and awareness should determine the tone at the board level and address every level of the organization, leading to a dialog about operational risks. A risk aware culture leads to informed and supported decisions about risk appetite and corresponding thresholds that are the limits of the amount of risk tolerated related to the achievement of the organization's objectives.

Framework components	Governance - culture, policies, risk appetite, responsibilities
	Management & Execution - risk events, assessments, indicators, modelling, resolving issues
	Reporting - indicaor performance, timeliness, frequency, quality

Figure 11: Global Operational risk framework components, based on Blunden and Thirlwell (2012), Girling (2013) and Lancaster (2015).

The top layer includes the organization objectives and risk appetite, leading to risk policies. This layer structures the day to day practices and operational risk management execution by expressing risk culture. This includes risk appetite and corresponding boundaries, responsibilities and procedures.

The middle layer contains components of day-to-day management and operational risk process execution. This includes operational risk events & operational risk losses, risk assessment practices, risk and control indicators, scenarios & modelling and resolving issues by further actions.

The board uses the operational risk management information to base decisions on. The information to base their decision on should be reported on time, of sufficient quality and appropriate to base their decision on. Therefore, the board level should understand and challenge the reported information. The bottom layer contains reporting components including the reporting structure, quality aspects, frequency of reporting and what should be reported to whom.

3.5 Business Performance Management (BPM)

The term Performance Management is used differently from different perspectives. This section is intended to clarify the terms Performance Management, Performance Measurement and Business Performance Management. This section is devoted to describe its supporting concepts, concluded by explaining Business Performance Management Technologies.

3.5.1 Concepts of Performance Management

Performance management is an abstract term that can be confusing because of its broad nature and the meaning of the words 'performance' and 'management'. It all depends on what kind of performance is intended to be managed. In this research Performance Management is viewed from an organizational and management accounting sciences perspective.

Hoffmann (2002, p. 8) defined performance as "valued contribution to reach the goals of an organization". In general Performance Management, can be seen as a way for organizations to become more successful and make sure they are delivering against their strategic priorities.

The process of performance management starts at the highest level of the organization by translating a mission and vision statement into a strategy, composed of objectives and priorities. These objectives and priorities should then be translated to high level measures and then by middle management into measures on operational levels. These high-level measures and operational measures express organizational performance. The performance should then be communicated by reporting the measured performance and managed to align people and culture with strategic goals. Figure 9 visualizes processes of performance management from the strategic level to the operational level, like the organizational Planning & Control cycle (Melchert, Winter, & Klesse, Aligning process automation and business intelligence to support corporate performance management, 2004).

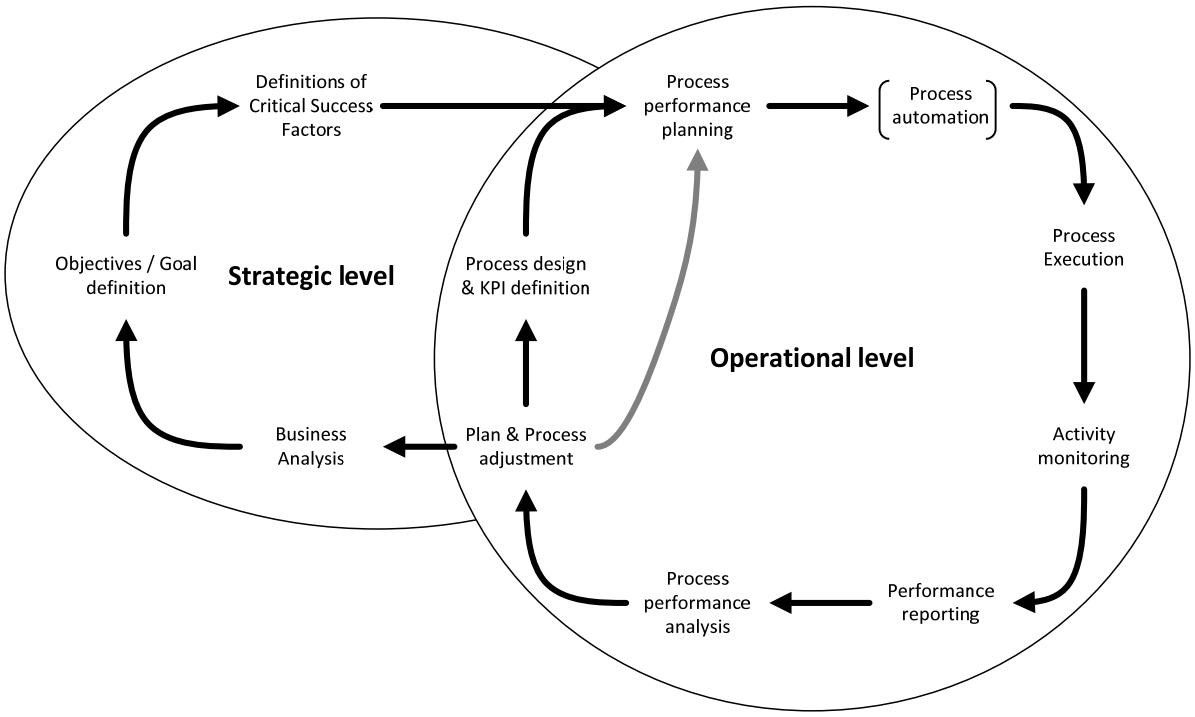


Figure 12: Performance management processes, adapted from Melchert, Winter and Klesse (2004).

According to Sharda, Delen and Turban (2014) most organizations use a performance management method based on the Balanced Scorecard, that was developed by Kaplan and Norton (1992). In the Balanced Scorecard, vision and strategy are shown in the center, leading to objectives within the four distinctive perspectives. From each perspective, the strategic objectives should then be translated to operational objectives, targets, measures, and initiatives.

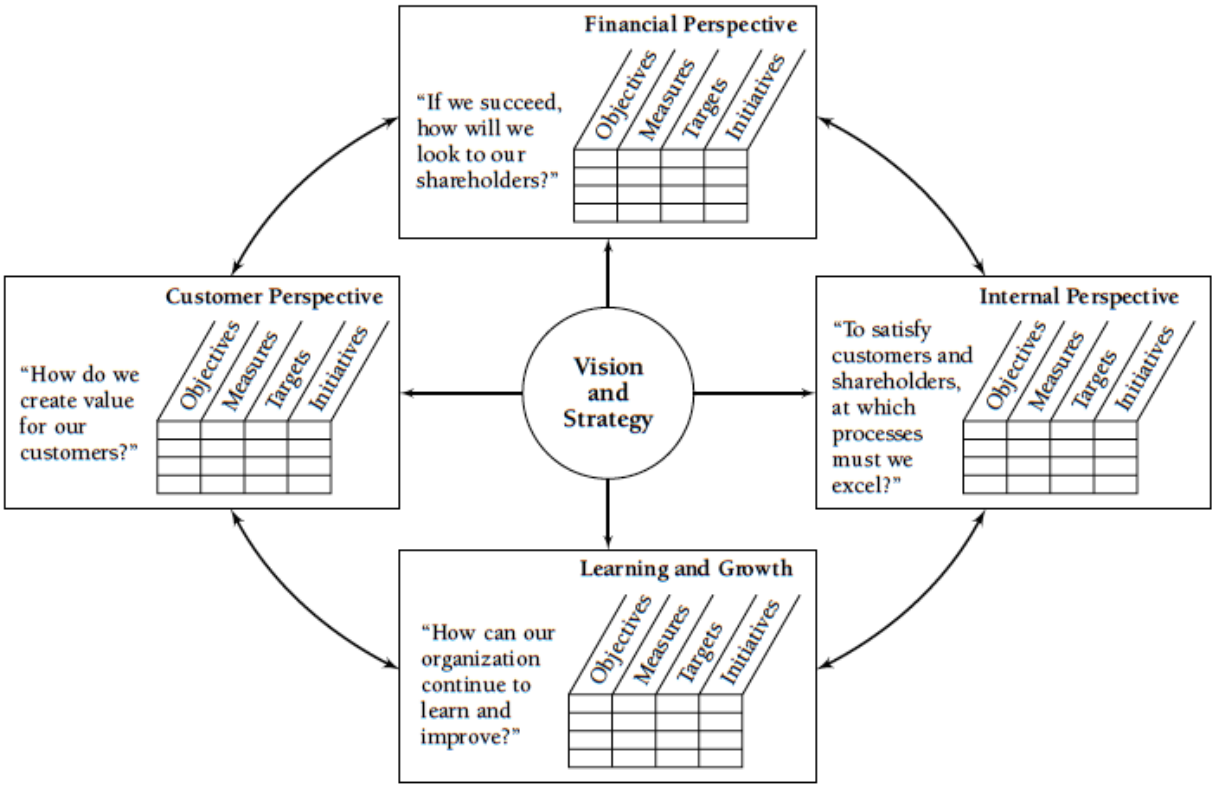


Figure 13: The Balanced Scorecard as developed by Kaplan and Norton (1992).

The word 'Balanced' comes from the causual relationships or dependencies on the four perspectives:

1) Financial; 2) Customer; 3) Internal Processes; 4) Learning and growth.

The Financial perspective is about increasing shareholder value. The Customer perspective is about increasing value for customers that drives the financial perspective. The internal process perspective is about process excellence in order to deliver added value to the customers and/or shareholders. The learning an growth perspective is about improving internal processes and employee skills. All perspectives are required to complement each other in order to effectivly and efficiently achieve the organization's strategic objectives.

Several organizations built their own variation of a scorecard methodology based on the Balanced Scorecard. These custom viariations of the balanced scorecard usually include the perspectives as proposed by Kaplan and Norton, however in most cases are extended based on specific context for that organization. Marr (2004) studied different perspectives used for custom scorecards and found almost all variants included a financial, customer and processes perspective. Complemented by perspectives including industry benchmarking, health & safety, innovation and other stakeholders.

3.5.2 Performance Measurement

Performance can only be managed when the actual performance is known. Performance Measurement is the method of developing performance indicators and relating them to contextual factors to enable measurement of performance. Performance could then be actively improved by management. According to Lebas (1995) Performance Measurement is a critical and inseparable component of performance management.

Lebas (1995) describes Performance Management and Performance Measurement are often confused, but are closely related to each other. Management is the process of coordinating and steering on performance. Measurement is expressing and quantifying measures to be managed. Therefore, performance measurement can be seen as subset of performance management.

Simons (2002) describes performance measurement systems: "Assist managers in tracking the implementations of business strategy by comparing actual results against strategic goals and objectives. A performance measurement system typically comprises systematic methods of setting business goals together with periodic feedback reports that indicate progress against goals".

What needs to be measured is determined by organization's strategy and derived strategic objectives. These objectives are then translated into performance measures and developed into performance indicators on an operational level. The critical Success Factors are related to corresponding performance indicators, called Key Performance indicators.

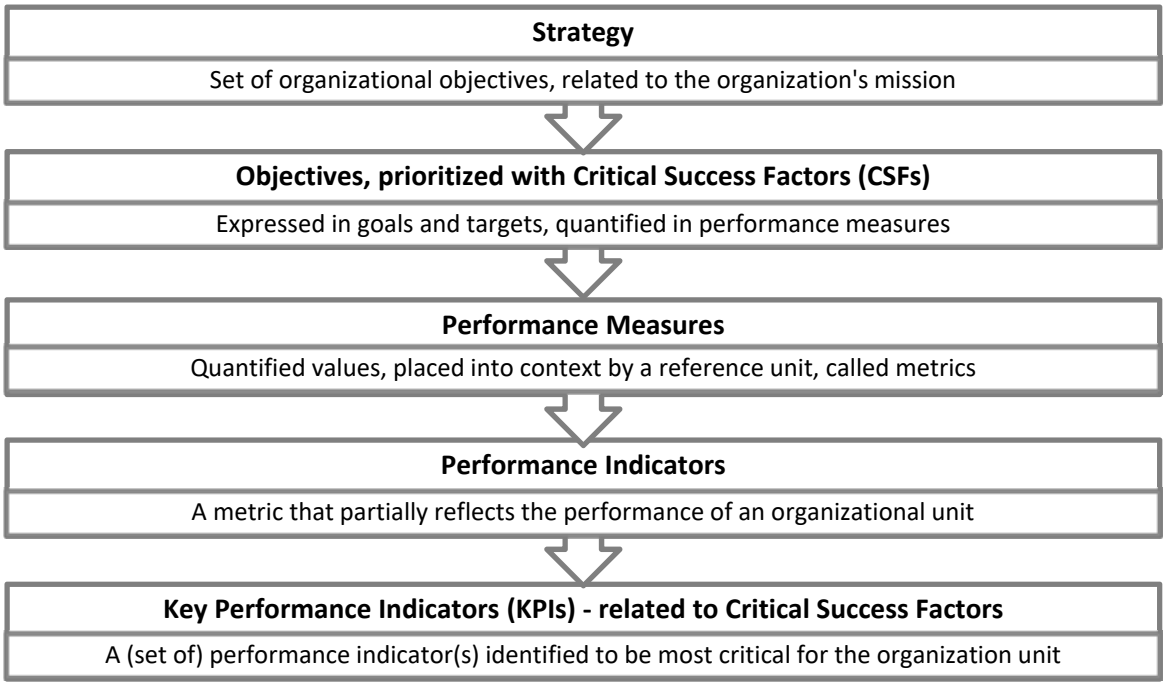


Figure 14: The Process of deriving Key Performance Indicators from Strategy, created by the author, based on Boynton and Zmud (1984), Lebas (1995) and Samsonowa (2011).

Critical Success Factors (CSFs) indicate priorities on a strategic level, while Key Performance Indicators (KPIs) translate these priorities into measures on an operational level and makes them more explicit.

Regardless of the level of management, Doran (1981) described a way to make objectives measurable and understand when an objective is achieved. Doran called it a S.M.A.R.T. way to write objectives. The letters are acronyms for:

- Specific – an explicitly specified target area to improve;
- Measurable – quantified or at least described by some indicator of progress;
- Assignable – assign a specific person or group of people who need to execute it;
- Realistic – expect results that can be achieved considering the available resources;
- Time-related – a point in time or a period when the result(s) can be achieved.

Doran (1981) described each level of management (e.g. strategic or operational) could have its own S.M.A.R.T. structure related to their (sub)objectives. Doran notes quantification at some level is very important to measure performance, however it is not always realistic for all components of S.M.A.R.T. to be quantified or used on all levels of the organization.

Doran (1981) describes the usefulness of the S.M.A.R.T. framework depends on the level, scope and purpose of the (sub)objectives. The framework should be applied in a flexible manner and mainly serve to initiate actions to improve performance. Neely, Gregory, and Platts (1995) complement this conclusion by describing performance is improved trough measurement and certain actions to improve performance by the dimensions: Quality, Time and Costs.

Samsonowa (2011) describes the context is important to understand effectiveness towards a goal and the efficiency, concerning the consumed resources towards to goal. A performance indicator is a metric that reflects performance and should be placed into context by a reference unit. The reference unit supplies additional information about the quantified units, e.g. sales, meters, points, and their scale. The scales can be standardized, for example 1 meter is a standardized unit or the scales can be pre-determined units by the organization, e.g. sales. The target can then be measured against specific quantities or a percentage of a pre-defined ratio of units.

Performance indicators can be combined and composed of multiple measures. Most performance measures reflect historical conditions. Historical based indicators are called *lagging* indicators. Additionally, Zarnowitz (1992) describes some indicators that appear to be useful for indicating a positive or negative trend and therefore have predictive value. Indicators that can be used for deriving trends or forecasting are called *leading* indicators.

Bititci, Turner and Begemann (2000) write a performance measurement system should be dynamic and adaptive to changes in the competitive environment. The authors conclude performance measurement should be used in a control loop to include monitoring and corrective actions. Active monitoring of performance measures is needed to maintain reliable internal control processes:

- An external monitoring system, for monitoring external developments and changes;
- An internal monitoring system, for the internal environment, when certain thresholds are researched a warning signal should be raised;
- A review system, using information from internal and external monitoring and the objectives set on a strategic level, to develop the internal measurement system;
- An internal deployment system for changing objectives and priorities.

Automated tooling could be used to make implementation and maintenance of the performance management and performance measurement systems less complex.

3.5.3 The inception of Business Performance Management

Business Performance Management (BPM) is defined differently from performance management. BPM developed from an Information Systems perspective as an umbrella term of processes and technologies intended to support performance management and performance measurement. This section describes developments leading to BPM and states the definition of BPM used in this research.

Historical Perspective

Business Performance Management evolved from Decision Support Systems (DSS) in the 1960s and developed throughout the following years into Executive Information Systems (EIS). The development of aggregated data storage, known as Data Warehousing (DW), lead to the inception of Business Intelligence (BI) in the late 1980s. Business Performance Management (BPM) builds on the foundations of BI, extending BI with planning, consolidation and process automation (Frolick & Ariyachandra, 2006).

Domain	Distinctive capabilities	Introduced
Decision Support System (DSS)	Databases and models to support analysis of unstructured and semi-structured problems.	1960s
Executive Information System (EIS)	File storage and editing, graphical charts for data visualization, data routines for quantitative analysis.	1980s
Data Warehousing (DW)	Central collection and aggregation of integrated data from one or multiple operational sources, often combined into a multi-dimensional database.	1980s
Business Intelligence (BI)	Online Analytical Processing (OLAP), data mining, process mining, complex event processing, benchmarking, text mining, predictive analytics and prescriptive analytics.	1980s-90s
Business Performance Management (BPM)	Planning & control and forecasting. Enhanced by process automation, such as process modelling and workflow.	2000s

Table 11: Developments of DSS to BPM, adapted from Frolick and Ariyachandra (2006).

Table 10 describes the developments that lead to the domain of Business Performance Management. Each domain described in table 10 builds upon technologies of the predecessor to advance further.

Business Performance Management defined

Business Intelligence included important developments from DSS, EIS and DW, however BI is mainly focused on reporting historical data. BPM extends the concepts of BI further with planning & control, forecasting and process automation (i.e. workflow, process modelling).

Business performance management is intended to enable organizations to define strategic goals and then measure and manage performance against those goals. Business Performance Management processes include financial planning, operational planning, business modeling, consolidation and reporting, analysis, and monitoring of key performance indicators linked to the organization's strategy.

Business Performance Management(BPM) is defined by Sharda, Delen and Turban (2014, p. 150) as "The business processes, methodologies, metrics and technologies used by enterprises to measure, monitor and manage business performance."

Synonyms for BPM are Corporate Performance Management (CPM) by Gartner research, Enterprise Performance Management (EPM) by Oracle and Strategic Enterprise Management (SEM) by SAP. In this research the term Business Performance Management (BPM) is used, because this term is not related to a specific organization or technology vendor.

3.5.4 Business Performance Management Technologies

Business performance management consists of performance management and performance measurement processes, as described in the previous sections. Performance Management focusses on the control and planning of business objectives. These processes are supported by technologies, mainly adapted from BI. BPM extents BI therefore relevant BI and BPM technologies will be described.

BPM is supported by a set of technologies for integrating and analyzing performance-relevant data, supporting decision making and facilitating the communication of decisions. Frolick and Ariyachandra (2006) describe BPM developed from DSS to EIS, then combined with Data Warehousing into Business Intelligence. Melchert, Winter and Klesse (2004) describe Business Performance Management is a combination of technologies from the domains: Business Intelligence, Business Process Modelling and Enterprise Application Integration. Combined with elements from Process Performance Management, Business Process Automation and Real-time Analytics. Figure 11 combines all BPM related technologies. All technologies are explained in detail on the following pages.

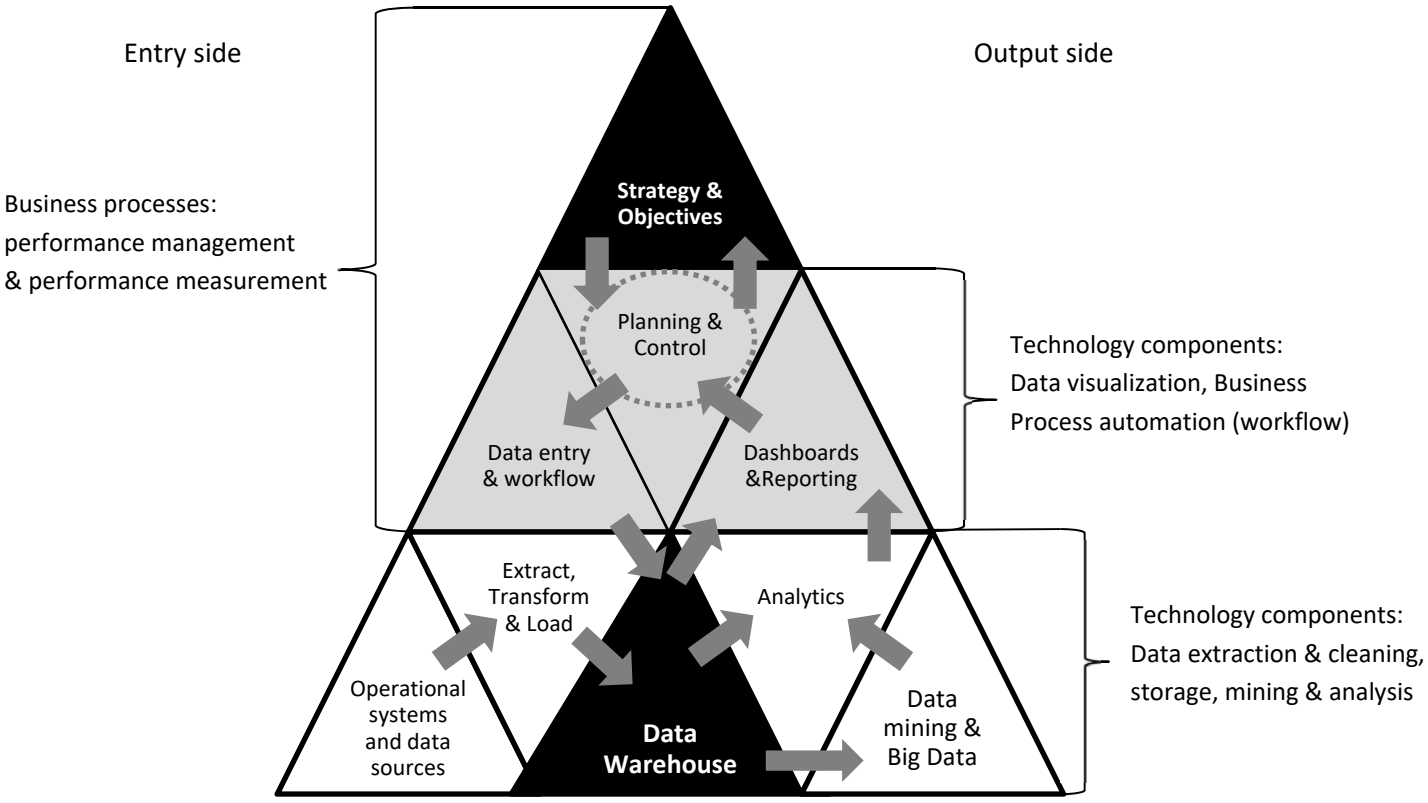


Figure 15: BPM pyramid; BPM related processes and supporting technologies, created by the author based on: Melchert, Winter and Klesse (2004), Frolick and Ariyachandra (2006), Samsonowa (2011).

The pyramid is composed of three different layers: Strategy and objective setting at the top, because that is the ultimate goal related to (strategic) management. The middle layer is an important interface layer between organizational planning & control and supporting technologies. Data entry and workflow enable planning on the entry side. Dashboards and reporting interface the results and enable controlling on the output side. The bottom layer is only technology related, facilitating input of clean source data on the entry side. Building on a Data Warehouse as central data storage, data mining and big data enhancing the data on the output side with analytics, as source for dashboards and reporting.

Operational data and source systems

The main goals of Business Performance Management are to support: planning, measuring, analyzing and monitoring of the performance on objectives. These activities are dependent on data found in operational systems and other data sources supporting the organization's operations, for example:

- Operational systems, often SQL based, such as:
    - Enterprise Resource Planning (ERP), including orders, production, products, etc.
    - Customer Relationship Management (CRM), incl. customers, sales, marketing, etc.
- Spreadsheets, text documents and other textual files, such as: pdf, txt, xml, html, log files, etc.
- External sources and services, such as: Amazon, Microsoft Azure, Google cloud, Salesforce, etc.
- An already existing data warehouse or (set of) data mart(s).

Extract, Transform & Load (ETL)

Data from operational systems often resides in many different files and systems and therefore the data is fragmented throughout organizations and systems. For efficient and effective analysis, data from different sources should be collected and stored in a (central) location suitable for analysis. Just placing all data together is often not enough, most data requires some form of transformation or data cleansing to ensure sufficient data quality before it can be used efficiently for analysis and reporting.

Operational systems are often designed with a transactional data structure to handle many separate transactions while being capable of storing data quickly and space efficient. Transactional systems benefit from normalized data structures, such as 3rd or Boyce-Codd Normal Form. Such structures allow for fast queries and at the same time reducing required storage space. Operational normalized data systems are often referred to as On Line Transactional Processing (OLTP) systems or data sources. OLTP data sources are often not suitable for detailed and fast analysis, because they require a large amount of Join operations that slow down calculations (Bog, Sachs, & Zeier, 2011).

Another problem arises from unstructured data and semi-structured data sources used in operational processes. Data sources, such as spreadsheets and textual files, are often not codified and contain unstructured texts that are hard to analyze using automated support. Additionally, semi-structured data sources often contain some data suitable for analysis, but are often incomplete. Therefore, Extract, Transform and Load processes are used to transform and move source data into high quality data suitable for analysis. Staging areas can be used to store data temporarily between transforms.

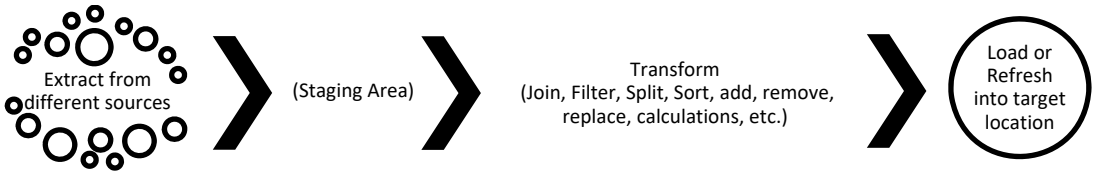


Figure 16: Overview of an ETL process, created by the author, based on Chaudhuri and Dayal (1997).

Chaudhuri and Dayal (1997) describe the process of ETL to get data consistent and integrated:

1. Design the ETL processes, create target repositories followed by mapping source and target;
2. Extraction, transfer all data from sources to staging area, while cleaning and profiling data;
3. Transformation, manipulate data to get the required structure by applying:
   filter, join, sort, add, remove, replace, calculations and aggregations;
4. Loading & Refresh, move data from staging into target location(s), usually a data warehouse.

Data Warehousing

A Data Warehouse (DW) facilitates centralized storage of integrated data from one or more sources. Data stored in a data warehouse is collected from operational systems and then transformed by ETL to an On Line Analytical Processing (OLAP) structure suitable for analysis. OLAP databases store aggregated, historical data in multi-dimensional schemas. The OLAP approach is used to analyze multidimensional data from multiple sources and perspectives.

The concept of the Data Warehouse was published in 1990 by Bill Inmon, who is nowadays known as "*The father of the Data Warehouse*". Inmon's idea is the construction of an enterprise wide centralized data warehouse, including all data of the entire organization. All departments need to conform to the schema in the centralized data warehouse, then different business areas can take a subset of the data from the data warehouse called a Data Mart. The Inmon approach is known as a top-down approach. The Enterprise DW approach requires many resources and long implementation time (Breslin, 2004).

In 1996 Ralph Kimball published a different approach to data warehousing. In Kimball's idea, every specific business area or department in an organization can setup its own data mart. When needed, data marts can be step-by-step integrated into a centralized data warehouse. This bottom-up approach requires less resources and delivers benefits within a reasonable short time (Breslin, 2004).

Data in a data warehouse is stored in a schema with central facts tied to different dimensions. The facts are measurable items e.g. units, number of sales, value, etc. Dimensions are contextual factors related to facts, e.g. product, customer, time, location, etc. The data can be stored in different ways:

- The simplest variant is a star-schema, consisting of one fact table surrounded by a 1 layer depth of dimensions. This schema contains redundant data; however, this schema allows for less complex queries, with less joins and therefore fast execution (Adamson, 2012).
- A snowflake schema is also centered around one fact table, but with multiple depths of dimensions. This type of schema requires less storage, because there is no data redundancy, however execution time and complexity can increase significantly because more queries with joins are required (Levene & Loizou, 2003).
- A Constellation (sometimes referred to as Galaxy) schema is tying dimensions to different fact tables, allowing for multiple facts having shared (conformed) dimensions while some facts have dimensions only related to specific facts. This type of schema is often applied when integrating data from multiple star and/or snowflake schemas (Moody & Kortink, 2000).

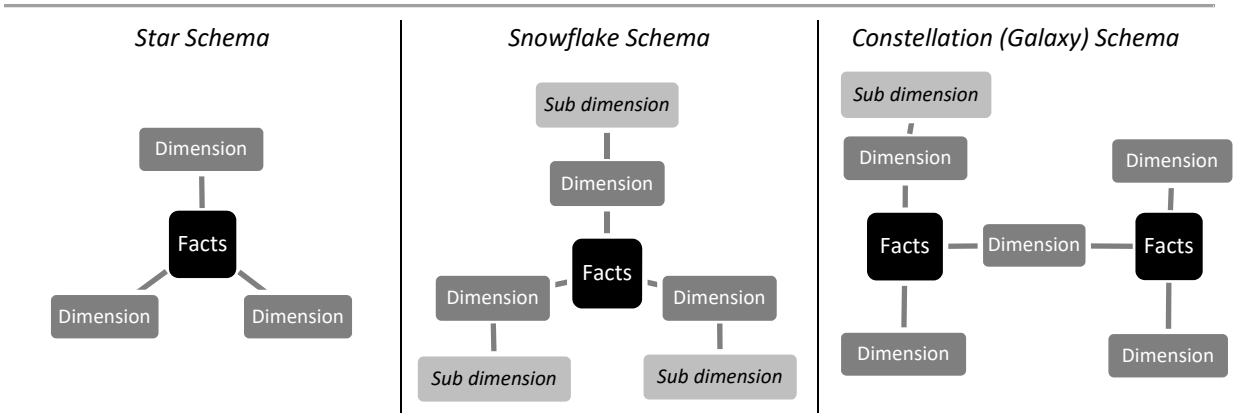


Figure 17: Overview of different data warehouse schemas, created by the author, based on: Moody and Kortink (2000); Levene and Loizou (2003).

Analysis

When a data warehouse is designed, and loaded, then analysis can be performed. Three types of analytics are described by Sharda, Delen and Turban (2014):

1. Descriptive analytics, containing visualizations, periodic or ad-hoc reporting and trend analysis;
2. Predictive analytics, including Statistical analysis and Data Mining;
3. Prescriptive analytics, Management science models and solutions.

Descriptive analysis is the most basic form of analysis about describing the data. This involves consolidations to find what is happening in the organization. When describing data, the summarized data can be further investigated by drill down into a specific set of data. The OLAP structure allows for slicing and dicing the data set into specific smaller sets suitable for detailed analysis. Roll up summarizes the data back to a higher level. An important part of describing is the visualization of data in graphics, dashboards and reports (Sharda, Delen, & Turban, 2014).

Predictive analytics uses patterns in the data warehouse environment and mathematical methods to predict future outcomes. Descriptive analysis focuses on describing historical data and is reactive in nature, while predictive analysis focuses on the future. The goal is to 'mine' in the data to find predictive models with reliable accuracy, e.g. capable of predicting the number of sales from a specific type of customers. Prescriptive analytics takes predictive models found by data mining to a more advanced level. A Rules engine is used that is able to advice a decision maker about a price (range) or combination of products for a specific group of target customers (Sharda, Delen, & Turban, 2014).

Data Mining

Data mining, also referred to as Knowledge Discovery in Databases (KDD), follows a semi-automated process of data selection, preprocessing, transformation, data mining and evaluation to derive new knowledge from patterns in the data (Fayyad, Piatetsky-Shapiro, & Smyth, 1996). Common techniques used for knowledge discovery are: association rule discovery, clustering, classification, regression, decision trees and other networks and algorithms.

Big Data

In recent decades, there has been an exponential increase in volume and velocity of data. The growth of internet connectivity and use lead to more volume of data, e.g. web shops, social media, internet of things. Additionally, the size of data increased, because of intensified use of photo, audio, video and video games. This phenomenon is often referred to as big data (Mayer-Schönberger & Cukier, 2013).

While big data enables more possibilities for KDD, traditional database architectures are not able to cope with the demand of volume and data velocity. Hadoop is a well-known platform for Big Data and contains: distributed computing & scheduling, distributed storage and MapReduce. Distributed computing is used for fast parallel data processing. Distributed storage allows high bandwidth data transactions. The scheduling system keeps track of all tasks. MapReduce is a technique to find and summarize clusters. The data footprint is then reduced by storing the summarized data (White, 2012).

Real-time Analytics

Hackathorn (2004) describes Real-time Analytics can increase value and action time. Lower data latency results in a lower analysis latency. That leads to a lower decision latency. Hackathorn describes a lower decision latency results in earlier action and thus reduces the time of action.

Dashboards & reporting: transforming data to information

Since the inception of Enterprise Information Systems (EIS) in the 1970s visualizing data is an important research theme within information systems development (Frolick & Ariyachandra, 2006). Graphics and rules can turn raw data into visual information for managers and executives. Examples are: time series charts, scatter diagrams, maps, motion graphics, sequence charts, and comparison-oriented graphs.

Eckerson (2010) writes a dashboard should provide a clean, integrated and consistent set of information. The information should be provided on time and adapted to the user's role to be able to respond to information. Eckerson describes three distinctive layers of information roles:

1. Graphical, dashboards with metric data, expressed in easy to understand and colorized graphics for monitoring, mainly strategic executives, usually a small number of users;
2. Dimensional data, summarized in reports for a medium number of tactical management users and (business) analysts, drill-down, slicing and dicing allow to dynamically navigate through a hierarchical set of OLAP data to find important data segments (e.g. best performing employees, or sales segment);
3. Transactional data, detailed for operational workers, supporting a large number of users.

A Graphical User Interface (GUI) is used to show the visualized information to a user. Graphical User Interface components used for Business Intelligence and Business Performance Management are: OLAP, Reports, Dashboards and Alerts (Golfarelli, Rizzi, & Cella, 2004).

Interface	**Report**	**OLAP**	**Dashboard**	**Alert**
Visualization	Numbers, Texts and Graphics	Numbers and Texts	Graphics	Text
Structure	Static	Dynamic	Static	Static
Interaction	Manual	Manual	Manual	Automated
Information type	Measures and Indicators	Measures	Indicators	Events

Table 12: Different interfaces and their characteristics, created by the author, based on: Bititci, Turner and Begemann (2000); Golfarelli, Rizzi, and Cella (2004).

Golfarelli, Rizzi, and Cella (2004) describe dashboards and reports can be created directly from data residing in the data warehouse or transformed in real time by a Right Time Integrator (RTI). The Right Time Integrator extracts data from a data warehouse, data streams, other applications or directly from operational systems. RTI then transforms data using a KPI manager a rule engine and/or data mining.

A KPI Manager computes pre-defined (Key) Performance Indicators on necessary levels, results are then visualized in dashboards and reports or can trigger an alert event based on predefined thresholds.

The Rules engine relies on models created by patterns found with data mining. The rules describe a routine and special statistical, financial, and other quantitative analysis procedure. This rules engine can also be used to trigger alert events. Bititci, Turner and Begemann (2000) write a rules engine should be capable of handling simple rules to facilitate performance management, including events leading to raising alarm signals, warning notices, etc. That should be linked to a system with limits and thresholds to provide an early warning of potential performance problems.

On Line Analytical Processing enables data exploration and allows the most flexibility for users formulating their own queries. This type of analysis is mostly used by analysts to gather new insights that are more detailed and not predetermined (Sarawagi, Agrawal, & Megiddo, 1998).

Data entry

Frolick and Ariyachandra (2006) describe the main distinctive features of Business Performance Management compared to Business Intelligence is the addition of a planning & control process composed of: strategic planning, monitoring, analysis and corrective action. This process requires goal setting on the strategic level and budgeting and planning on tactical level. Traditional data warehouse systems developed from Business Intelligence and are designed to support fast and advanced analysis by knowledge workers on the historical and current data (Adamson, 2012). The main difference of approach is the reactive character of BI compared to the forwards driven approach of BPM.

Business Performance Management technologies should support forward planning by providing a solution to set goals, manage available resources, related costs and controlling them. This results in a detailed plan of resource allocation and budgets towards the strategic goals. According to Marr (2009) Business Performance Management solutions should provide data entering capabilities in order to support planning & forecasting purposes. Budgeting is the most common example of data entry.

Schreurs, Roox, and Moreau (2004) write manual data input could be used to provide Performance Indicators. These indicators ensure that the processes of planning, budgeting, forecasting, and reporting are aligned with strategic goals. Entering data into databases is functionality for operational OLTP systems. OLAP technology was seen as read only data structure intended solely for analysis. Therefore, manual data entries directly into the data warehouse structure are seen as a Business Performance Management technology.

Collaboration & communication via workflow

The planning process of Performance Management results in in a detailed plan of resource allocation and defines available budgets towards strategic goals. This planning should be approved. Review and approval are important components of Business Performance Management (Cokins, 2004). Collaboration can be supported by a workflow, supporting execution, monitoring and communication.

The ideas of a workflow for use in Business Performance Management are influenced from Business Process Modelling and Business Process Automation. A Workflow system to support Business Performance Management should semi-automate the steps of execution by means of input forms and approval or reject stages (Melchert & Winter, 2004). A workflow system can be described as a system for creating a sequence of activities as a diagram or pre-defined stages that structure the required activities, support execution by providing an interface for entering data, provide functionality for approval & reject per stage and monitoring for the execution of this process.

Melchert and Winter (2004) describe forecasting and monitoring activities are closely related and therefore requires clear communication about tasks, targets and figures to realize a closed-loop performance management system. Ideally workflow systems should support communication around the execution of activities, distribution and presentation of information.

Bititci, Turner and Begemann (2000) write a review mechanism, should allow for notifications, tracking, and reminders. Additionally, performance information provided by activity monitoring could be combined to report on progress of objectives and allow decisions to be made about priorities on a strategic level.

3.6 Chapter conclusion

This chapter described essential background information and answers the first two research questions:

RQ1: " What is defined as the domain of Operational Risk Management? "

RQ2: " What is the definition of Business Performance Management technologies? "

Operational Risk Management was described from risk as a broad and general concept, that appears to be hard to define and even harder to quantify. Integrating risk management on an enterprise level is believed to provide several benefits for efficiency and alignment with business objectives.

When considering processes for managing risk from an organization wide view; COSO ERM and ISO 31000 provide a similar framework structure, which mainly differ in terminology. A generic structure starts with describing the context, followed by describing the objectives that form a basis for further risk management. Risk assessment is the process of risk identification, risk analysis and risk evaluation. Trough risk assessment each identified risk is scored and then evaluated for directions regarding mitigating measures (also known as controls). Mitigating measures should be tested and monitored over time, considering its presence and effectiveness. The state of risks and mitigating measured should be communicated regularly to different stakeholders. In order to enable continuous improvement the whole risk management process should be monitored and adjusted when needed.

Operational Risk is seen as a specific sub set of organization wide risk management (ERM) and is defined as "*risks resulting from inadequate or failed internal processes, people and systems or from external events.*" (Basel Committee, 2001, p. 2). This definition is formed from a financial perspective, but outside the financial services sector these types of risks are also present. Outside the financial services industry the only sector using the term operational risk is the energy industry, in other sectors operational risks are managed via Quality, Health, Safety and Environment management.

An important concept for operational risk is the three lines of defense model. This model is seen as essential for operational risks, since these types of risks involve anyone and everything involved with the organization's operations. The first line of defense includes domain experts in the day-to-day operations of the organization. The second line is the actual management and coordination of risks. The third line is audit, that can be internal and external, validating the first and second line.

Another important domain in this research are all technologies related to Business Performance Management (BPM). BPM evolved from Business Intelligence (BI) and extends BI with workflow and planning technologies in order to facilitate alignment with the organization's objectives. This alignment can be achieved with a planning and control cycle that is performed in a continuous cycle. In this cycle Business strategy is further detailed into specific goals and then planned using planning and workflow technologies. The data is often enriched using Business Intelligence. With BI technologies, the data is retrieved via Extract, Transform & Load (ETL) processes and loaded into a central data warehouse. The data in this central storage medium is used for several forms of analysis that enables the creation of dashboards and reports containing information about the actual performance in relation to strategy.

This chapter described the purpose and actual practices related to risk management and operational risks in relation to risk management. The structure of COSO ERM and ISO 31000 might be appropriate process structures for this research and is considered during maturity model development. Integration of risk management practices appears to benefit from several Business Performance Management technologies, such as workflow and data entry support collaboration between the three lines of defense. Analysis, dashboarding and reporting support communication and process monitoring.

4 Maturity model development

This chapter describes the process of maturity model development. As a starting point this chapter provides a summarized overview of existing maturity models. Additionally, maturity models for business intelligence and business performance management and their related technologies are briefly described to serve as context for the following sections.

The risk management process maturity measurement section describes how measures for process maturity of the operational risk management process were selected and adapted. The technology part is about software functionality that is identified through market analysis and is marketed by vendors as usable for operational risk. A panel of operational risk management experts was consulted to validate and rank the process maturity measurements and corresponding software functionality. Leading to the construction of the initial maturity assessment. This chapter is concluded by describing changes made to the initial model and assessment in order to improve quality of the maturity model.

4.1 An overview of different types of maturity models

This section provides a summarized overview of existing maturity models, starting from a historical perspective. Relevant maturity models are briefly described to service as context for development of a new maturity model for operational risk management based on BPM technologies.

4.1.1 Historical perspective on maturity models

Maturity models appear to be strongly influenced by developments in the domains of IT and Quality management. In 1973 Richard Nolan developed the stages of growth model for mature use of computer resources within businesses. This model included six different stages describing key elements and controls for successfully integrating IS/IT within a business organization (Nolan, 1973).

In 1979 Crosby developed a quality management maturity grid (QMMG) from a quality management perspective, intended to improve business processes. This grid was focused on improving quality management processes based on five levels of maturity uncertainty, awakening, enlightenment, wisdom and certainty (Fraser, Moultrie, & Gregory, 2002). Crosby's work was adapted by Watt Humphrey to create the first process maturity framework, aimed at improving software development practices (Humphrey, 1988).

Watts Humphrey's work laid the foundations for the Capability Maturity Model (CMM). The Capability Maturity Model (CMM) was developed by Paulk, Curtis, Chrissis and Weber (1993) from Carnegie Mellon University Software Engineering Institute (SEI).

The CMM provides five distinctive stages of maturity with corresponding capabilities that are built upon each other to reach a mature state of continuous improvement. Each stage is dependent on previous stages, therefore an organization can only progress to the next stage when all capabilities in the previous stages are satisfied.

The first stage is called: *Initial*, meaning success depends on individual efforts without structured processes and documentation, therefore ad-hoc. The second stage is called: *Repeatable*, meaning basic software project management techniques are implemented and documented, therefore the process becomes repeatable - also by other people. The third level is called: *Defined*, meaning an organization developed its own standard software development processes integrated and

documented. At the fourth level, called: *Managed* the processes are also monitored and controlled using metrics and measures collected from process data analysis. The fifth level is called: *Optimizing*, meaning the organization continuously improves processes using feedback from current processes and change processes to adapt to the organization's needs.

The first CMM model was solely based on Quality management of software products. Following the publication of the original CMM, many different CMM based models were developed with best practices in a specified discipline for e.g. Systems Engineering CMM, People CMM, Software Acquisition CMM. This resulted in implementation problems for service providing organizations and especially for organizations that tried to combine different flavors of CMMs. This resulted in expensive, confusing and conflicting process improvement programs (Ramanujan & Kesh, 2004).

Carnegie Mellon University Software Engineering Institute (SEI) recognized implementation issues for certain applications as well and therefore developed the Capability Maturity Model Integration (CMMI). CMMI was intended to integrate different CMM's into a set of integrated models. CMMI guides the evolution towards integration of different processes into more consistent integration. CMMI model has superseded the CMM, however CMM is not replaced and continues to be a general theoretical process capability model used for different domains (Chrissis, Konrad, & Shrum, 2003).

Introduced	Name	Goal	Levels	Stages
1991	CMM	Improve software product engineering	6	Level 0 (non-existent) Level 1 - Initial (Chaotic) Level 2 - Repeatable Level 3 - Defined Level 4 - Managed Level 5 - Optimizing
2009	CMMI	Universal/generic product & service improvement	5	Level 1: initial, unpredictable, poorly controlled and reactive Level 2: Managed, processes, reactive Level 3: Defined, processes tailored to the organization and proactive Level 4: Quantitatively managed, processes measured and controlled Level 5: Optimizing, process improvement

Table 13: Differences between CMM and CMMI.

CMMI is a framework with three different branches for different types of organizations:

- CMMI for product development;
- CMMI for Acquisition and outsourcing;
- CMMI for Service providers, standardized service;

Sixteen components are common and relevant for all branches, while each branch has some specific components, related to their intended use (Chrissis, Konrad, & Shrum, 2003).

Royce (2002) argues CMM is mainly focused on increasing performance of the processes, rather than supporting adaptations to actual needs of the organization. Meaning some less relevant processes can be overly focused on and thus not lead to improvement of actual product or service. CMMI supports iterative changes and adaptions to changing circumstances to actually improve the processes to better aid improved products and services rather than a strong focus towards the processes.

4.1.2 Maturity models for Risk management

Since the introduction of the CMM and CMMI many different maturity models have been developed. The concepts of maturity models expanded to different industries and specific applications. This is also the case for risk management maturity models. The following table provides an overview of some maturity models for risk management and their main characteristics.

Source	Name	Goal	Levels	Stages
(Hillson, 1997)	Risk Maturity Model	Enterprise Risk Capability	4	Naive, Novice, Normalized, Natural, measured in terms of four attributes: culture, process, experience and application
(RIMS, 2006)	Risk Management Society (RIMS) Risk Maturity Model	Enterprise Risk Management	9	10 point on each of the following scales: Capability, Proactivity, Coverage ERM adoption, Risk identification, ERM process management, Risk appetite, root cause discipline, Business Resiliency and Sustainability, performance management
(BDO, 2008)	Operational Risk Management Maturity Model	Adapt Capital Requirement for Operational Risk to the level of quality of the management system	5	1: traditional 2: Awareness 3: Monitoring 4: Quantification 5: Integration For each level measures based on: Culture, Processes, Application and Experience
(De Nederlandsche Bank - DNB, 2014)	Assessment Framework for Information Security	Quality of information security for operational management	6	0: Non-existent 1: Ad-hoc, initial 2: Repeatable but intuitive 3: Defined 4: Managed and measurable 5: Optimized
(U.S. Department of Energy, 2014)	Cybersecurity Capability Maturity Model (C2M2)	Improve electricity subsector cybersecurity capabilities	4	0: Not performed 1: Initiated 2: Performed 3: Managed + 10 model domains of cybersecurity practices for each maturity level
(Deloitte, 2015)	Deloitte Enterprise Risk Management Maturity	Enterprise Risk intelligence, value preservation & creation	3	1: fragmented 2: FRC expectation 3: Risk intelligent Oversight. Measures based on: Risk culture, strategy, risk appetite, governance Systems, incl. resources, infrastructure, external disclosure, risk monitoring & reporting Processes, incl. risk assessment, risk management.
(RSA Archer, 2015)	Maturity Model for operational risk management	Transforming operational risk to an advantage that enables to exploit opportunities	5	Siloed Transition Managed Transform Advantaged

Table 14: Overview of Risk Management Maturity models.

Seven different maturity models related to risk management are described in Table 14. Three of these models are focused on Enterprise Risk Management practices. While the other four models are aimed at operational risk management or a part of operational risk. Cybersecurity or information security is a limited part of operational risk.

None of the risk related maturity models appear to use terminology and structure of a standard risk management framework, such as ISO 31000 or COSO ERM. Additionally, there appears to be little focus on the use of software. Only RSA Archer's maturity model for operational risk considers software to be important for improving operational risk management. However, the model is focused on the functional processes of operational risk management, rather than specific software features.

4.1.3 Maturity models for Business Intelligence & Business Performance Management

From a technology perspective there are also maturity models on the domains of Business Intelligence and Business Performance Management.

Source	Name	Goal	Levels	Stages
(Wettstein & Kueng, 2002)	A maturity model for performance measurement systems	Performance improvement through new technology, processes, and instruments.	4	Level 1: Ad-hoc Level 2: Adolescent Level 3: Grown-up Level 4: Mature
(AMR Research, 2006)	Business Intelligence/Performance Management Maturity Model, Version 2	Framework for business to assess actions towards the deployment of business intelligence and performance management	4	Level 1: Reacting Level 2: Anticipating Level 3: Collaborating Level 4: Orchestrating
(Gartner, 2008)	Business Intelligence & Performance Management Maturity Model	Help companies improve their business intelligence and performance management initiatives.	5	Level 1: Unaware Level 2: Tactical Level 3: Focused Level 4: Strategic Level 5: Pervasive
(Aho, 2009)	Capability Maturity Model for Corporate Performance Management	Understanding CPM, towards a leading or advanced role of Corporate Performance Management.	6	0: Unaware 1: Ad-hoc 2: Repeatable 3: Defined 4: Managed 5: Optimized
(IBM, 2014)	Big Data & Analytics Maturity Model	Assess the value generated from big data investments towards supporting strategic business initiatives.	5	Ad-hoc Foundational Competitive Differentiating Break Away

Table 15: Overview of Business Intelligence and Business Performance Management maturity models.

Three models are related to Business Performance Management. These maturity models recognize Business Performance Management as a more mature application over 'standard' Business Intelligence. Business Intelligence is thus a requirement before moving to performance management. None of these maturity models is aimed specifically at improving risk management, however (Aho, 2009) writes risk management objectives can be used in Performance Management systems as well.

4.1.4 Why another maturity model?

Although no maturity model currently exists that describes specifically which BPM technologies are suitable for improving Operational Risk Management, the previous sections described some maturity models that do relate with ORM and software related technologies. This section is dedicated to describe and motivate why there should be a new maturity model on the domains of ORM and BPM.

Several studies describe software related technologies are a solution for more effective risk management, especially considering the increasing velocity and volume of (operational) risks:

- In general the following studies mention software should be used for risk management: Breden (2006), Tarantino (2008), Malik and Holt (2013), Nyenrode Business University (2014) Arnold, Benford, Canada and Sutton (2015);
- Beasley, Chen, Nunez & Wright (2006) indicate Balanced Scorecards including Key Performance Indicators could be used for improving risk management practices.
- Fraser, Simkins and Narvaez (2014) indicate that the same principles and technologies of Key Performance Indicators are applicable for Operational Risk Management, known as Key Risk Indicators and Key Control Indicators.
- Azvine, Cui, Majeed and Spott (2007) describe real-time Business Intelligence is suitable for supporting Operational Risk Management processes by providing an effective system for high velocity risks.

From the broad descriptions of these usable technologies it remained unclear which set of technologies can be used for improving ORM. Additionally it is still unclear what technologies are usable for which stage of maturity; most risk management maturity models do not focus on related technologies. Considering maturity models studied in the previous section, the following became clear:

- Most risk management related maturity models do not include a relationship with software technologies; when they do acknowledge this relation, these models are not detailed/incomplete about specific requirements suitable;
- Technology related maturity models often appeared to be focused on <u>one silo</u> of ORM, for example only the IS/IT or systems part of ORM. Additionally these models do not include a risk management cycle, these models do not support risk management processes sufficiently;
- Only RSA's ORM maturity model appears to focus on both software technologies and risk management, however is developed commercially and therefore vague about specific features. Additionally the RSA model appears to be very focused on their own product (RSA Archer) rather than support generic risk management practices with other solutions.

Next to the theoretical gap in knowledge this appears to be a problem with practical relevance as well. In practice there appear to be several issues with ORM software. Nyenrode Business University (2014) and Sadgrove (2016) describe unsatisfied users of current ORM software. Specific issues relate to reporting and insights and (difficult) integration with the Plan and Control cycle.

Business Performance Management includes tools for measurement, reporting and workflow. BPM is specifically developed towards the improvement of organizational performance to meet its strategic objectives. Concepts are Balanced Scorecards, KPIs and collaboration via (automated) workflow systems. BPM technologies appears to be a reasonably complete set of software technologies to be suitable specifically for improving operational risk management. No such maturity model exists, while there appears to be a need for a more specific description of suitable technologies related to ORM.

4.2 Measuring Operational Risk Management maturity

McCormack et al. (2009) write maturity models can be used to describe the current maturity stage and offer a specific guide on what is needed to improve a process. This section describes factors and measurements that could be used for assessing the risk management process maturity. This section is concluded with the actual factors and measurements as selected for maturity model development.

4.2.1 Risk related organization characteristics

Implementation of operational risk management practices and perspectives on enterprise risk management appears to be dependent on organization and sector related factors. This section describes factors and indicators from literature that are studied and found usable to measure the extent of enterprise risk management implementation. Table 16 shows a summary.

Factor	Influence on (Enterprise) Risk Management	Source
International organization	Higher ERM integration maturity	(Nyenrode Business University, 2014)
Organization size: Income / revenue	Income or revenue above 1 billion is more mature ERM	(Nyenrode Business University, 2014; Cope & Labbi, 2008)
Organization size: Full Time Equivalent (FTE)	Organization size in FTE relates to a higher operational risk	(Cohen & Kunreuther, 2007)
Stock market registration or presence	Higher ERM integration maturity	(Paape & Speklè, 2012; Kleffner, Lee, & McGannon, 2003)
Sector/industry	Different approaches for ERM in different industries	(COSO, 2004; Mitra, Karathanasopoulos, Sermpinis, Dunis, & Hood, 2015)
Financial services organization	Higher ERM integration maturity	(Nyenrode Business University, 2014)
Applicable laws and regulation(s) in the sector/industry	Laws and regulations influence behavior	(COSO, 2004, p. 18; Paape & Speklè, 2012)
Industry competition	Competitors selling similar products or services results in more need for ERM	(Gordon, Loeb, & Tseng, 2009)
Integrated risk management / risk management framework / Coordination of risk management	Silo based or Enterprise integration, centralized or decentralized	(Spikin, 2013)
Appointment of CRO (sometimes called Risk Officer or Risk Champion)	Independent dedicated CRO (or risk champion) - not as part of CFO role - results in more effective ERM	(Liebenberg & Hoyt, 2003; Kleffner, Lee, & McGannon, 2003; Paape & Speklè, 2012; Pagach & Warr, 2011)
Operational Risk Committee	Risk committees possibly result in more effective ERM	(Liebenberg & Hoyt, 2003)
Board independence & Involvement of CEO	Firms with independent board and separation of CEO and chairman show the highest level of ERM	(Kleffner, Lee, & McGannon, 2003; Desender, 2007)

Table 16: Factors that influence (Enterprise) Risk Management.

4.2.2 Frameworks and terminology to structure the model

An important part of operational risk management are the processes to manage risk. From literature it appears that operational risk management is often part of enterprise risk management (ERM) and its related risk management processes. Therefore the process structures for ERM are used for ORM.

Based on the existing maturity models for risk management (as described in chapter 4.1) and their different approaches with a proliferation of terminology, this maturity model uses standard terminology as found in the COSO ERM and ISO 31000 frameworks. This decision is made because COSO ERM and ISO 31000 describe best practice management processes for mature and thus integrated risk management practices. Additionally, both frameworks include an improvement cycle. Because this research intents to improve the operational risk management processes towards continuous improvement both frameworks are used to structure this maturity model and assessment.

Both ISO 31000 and COSO ERM frameworks provide a similar structure and are available in the assessment instrument. ISO 31000 serves as default, because ISO 31000 is intended for generic risk management practices. COSO ERM has a specific background on accounting and controlling based terminology. The automated assessment instrument allows switching between frameworks and corresponding terminology via a drop down menu in the assessment form.

<table>
<tr><th>COSO ERM (2004)</th><th>ISO 31000 (2009a)</th><th>MODEL structure</th></tr>
<tr><td>Internal Environment</td><td rowspan="2">Establish the context
- internal and external environment
- identifying and describing objectives</td><td>A - Environment</td></tr>
<tr><td>Objective setting</td><td>B - Objective setting</td></tr>
<tr><td rowspan="4">Risk Assessment:
1. Event Identification
2. Risk Assessment
3. Risk Response</td><td rowspan="4">Risk Assessment:
1. Risk Identification
2. Risk Analysis
3. Risk Evaluation</td><td>C – Risk Assessment - General</td></tr>
<tr><td>D – Risk Identification</td></tr>
<tr><td>E – Risk Analysis</td></tr>
<tr><td>F - Risk evaluation</td></tr>
<tr><td>Control activities</td><td>Risk Treatment</td><td>G – Control activities</td></tr>
<tr><td>Monitoring activities</td><td>Monitoring and review</td><td>H - Monitoring activities</td></tr>
<tr><td>Information and communication</td><td>Communication and consultation</td><td>I - Information & communication</td></tr>
</table>

Table 17: Frameworks used as structure for the initial maturity model.

4.2.3 Measuring Operational Risk Management process implementation (Quick Scan)

Characteristics as described in section 4.2.1 are indicators for enterprise wide risk management (ERM) implementation. Although the implementation of enterprise risk management is related to the implementation of operational risk management, this section describes factors and measures that can be used specifically for measuring actual operational risk management process implementation.

As a starting point for measuring specific characteristics of operational risk management existing models were studied. As described in chapter 4.1, various different maturity models for risk management exist. Only a select number of these maturity models are intended (partially) for operational risk, however their approach to distinctive maturity levels and corresponding characteristics to measure maturity might be used for the maturity model in this research.

On average maturity models for operational risk management appear to be composed of five maturity levels. A clearly visible distinction in maturity levels appears to be the inclusion or exclusion of a maturity level 0. Meaning not implemented or non-existing.

Name	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Operational Risk Management Maturity Model (BDO, 2008)	***Not in model***	Traditional, unaware of need to manage Operational Risks	Awareness, limited implementation of systematic controls and procedures	Monitoring, Controls in main processes, indicators and reporting	Quantification, Quantified indicators for performance measurement, standard routines	Integration, Yearly evaluation of processes, information for competitive advantage
Assessment Framework for Information Security (De Nederlandsche Bank - DNB, 2014)	Non-existent,	Ad-hoc, initial partially defined, inconsistent	Repeatable but intuitive, structured, consistent, but informal	Defined, structured, documented in a formal way, relatable to facts	Managed and measurable, effectiveness is periodically assessed and improved	Optimized, Enterprise wide integration, with control cycle, evaluation, proactive
Cybersecurity Capability Maturity Model (C2M2) (U.S. Department of Energy, 2014)	Not performed	Initiated, organization has a cybersecurity program strategy	Performed, objectives, priorities, governance, structured, senior mgt. support	Managed, updated with business changes or threat profile	***Not in model***	***Not in model***
Maturity Model for operational risk management (RSA Archer, 2015)	***Not in model***	Siloed, activities in place, but fragmented	Transition, focused on improving effectiveness and stabilize processes	Managed, Processes are effective, repeatable and sustainable	Transform, building bridges between risk management and business	Advantaged, processes are optimized and balanced by business context and business priorities.
Selected for use in this research:						
Maturity levels	0: Not implemented	1: Ad-hoc	2: Recurring execution	3: Formally defined	4: Managed & measured	5: Continuous improvement
Level criteria	Process not implemented	Not described, not frequent, unstructured execution, informal, chaotic risk management	Partially documented, not frequent, unstructured execution, partially formalized	Fully documented, frequent, structured execution of risk management processes	Quantified measures in place and part of structural management processes	Continuous improvement process, integrated with the organizational strategic processes

Table 18: Maturity levels and characteristics used to measure operational risk management.

Although all the maturity models as described in Table 18 are focused on (a part of) operational risk management, each maturity model appears to have a different approach in terms of maturity criteria. The Cybersecurity Capability Maturity Model (C2M2) appears to be the only maturity model that is not focused on integration of multiple silos of risks and risk related management practices. All other models in Table 18 have a top maturity level focused on organization wide integration of ORM.

In this research the goal is to improve operational risk management using technologies in order to reach full integration with Enterprise Risk Management. Operational risk management experts suggested to use the maturity levels for operational risk as described by the Dutch National Bank (DNB) maturity model. Therefore the original Capability Maturity Model and the DNB maturity model are used primarily as input to construct the maturity levels as described in Table 18.

The maturity levels as previously described, can be used for measuring the overall maturity of ORM. However in this research a more detailed, yet quick indication of operational risk management is planned. Therefore a few possible ways of measuring ORM implementation are imagined:

Factors for process maturity	**Answering options**
1 Is a process present or executed?	No (level 0) or Yes (at least level 1: ad hoc)
2 Process implementation or maturity level per process-step:	Level 1: not described, not frequent, unstructured execution, informal, chaotic risk management Level 2: partially documented, not frequent, unstructured execution, partially formalized Level 3: Fully documented, frequent, structured execution of risk management processes Level 4: measures in place and part of structural management processes Level 5: Continuous improvement process, integrated with the organizational strategic processes
3 Importance of (Operational) Risk Management process	Scale 1 to 10 (1 not important, 10 very important)
4 Frequency of execution (Operational) Risk Management process	Period/time span and (estimated) frequency
5 Frequency of execution validation (Operational) Risk Management process	Period/time span and (estimated) frequency
6 Frequency of effectiveness validation (Operational) Risk Management process	Period/time span and (estimated) frequency
7 Involved roles and amount of roles involved with (Operational) Risk Management process	CRO, Operational Risk Committee, et cetera and amount or frequency

Table 19: Factors proposed for Quick Scan Operational Risk Management Process implementation.

The first factor to consider is a basic question whether a (part) of the operational risk management process is actually present or not. This is actually a level 0 or level1, but in this case for the individual process steps. The second factor is similar to the overall maturity measurement, again now for individual process steps.

In order to gain a more detailed insight into the motivation the third factor is about the actual perceived importance of a certain process step. When a specific process step is regarded as more or less important than others this could explain a shift in focus.

Actual execution of the operational risk management processes are also presumed to be found when measuring frequencies of execution and validation cycles. Furthermore the involved roles in certain operational risk management processes could also indicate a certain degree of process maturity.

4.3 Software functionality for Operational Risk

Operational risk management appears to benefit from information systems by integration to centralize efforts. This assumption is dependent on its relation with operational risk management as a process. Therefore the importance of any form of software available and used for operational risk management should be measured. Additionally this section describes which functionality is actually provided in practice through already existing products for operational risk management and provides a starting point for further development of the maturity model.

4.3.1 Measure software importance for Operational Risk

Before diving into details regarding used software functionality is it presumed important to establish a premise regarding the actual importance of software for Operational Risk Management. The following table describes factors that can be used for measuring the importance of ORM software:

Factors for process maturity	Answering options
Presence of software for Operational Risk Management	Yes or No
Cost of ORM software, total yearly recurring software related fees, including maintenance, staff and licensing costs	Exact amount or estimate in euros
Perceived current importance of software	Scale from 1 to 10 (1 not important 10 very important) And open answer
Perceived importance of software in the future	Scale from 1 to 10 (1 not important 10 very important) And open answer
Satisfaction with software	Open answer

Table 20: Factors for measuring the importance of software for operational risk (own work).

The actual presence of a dedicated software for operational risk management is considered an important precondition, before being able to receive accurate answers to further details.

Software products usually include a yearly recurring fee for licenses, the yearly amount of money spend on this software is presumed to provide a measure of importance. Organizations spending a large sum of yearly licensing fees probably find the software more important than organizations that do not spend as much.

Another way to measure the importance of software for operational risk is to ask the participant for their perception. In this research two different approaches are presumed useful. A scale from 1 to 10 requires the participant to quantify their perception of importance, while the open answer provides context and motivation.

The 1 to 10 scale is used to allow participants to express their perception without having to choose one of the extremes. The 1 to 10 rating system is well known in the Netherlands for ratings and expressing grades. Deviations between the scores are not an issue since the main goal is to measure a relative position between two extremes and detect a difference between current and future scores that is measured on the exact same scale immediately after. There is a possible difference in current importance and expected future importance. Therefore both current and future perspectives are considered to be relevant. Additionally the actual satisfaction of the software might lead to new insights and possibly places the importance into another context.

4.3.2 Software market analysis

A starting point for maturity model development it is presumed important to know what software products already exist and what features are provided for use with operational risk management. Therefore 65 existing software products were selected on occurrence and relevance. The software products were selected based on their self-promoted or marketed terminology.

The terminology is used as described in chapter 3.4.2, meaning software named by the vendor as software for operational risk, but also for HSEQ and specific areas of ORM, as shown in Table 21.

Marketed as software for	Count No of products	percent
Enterprise Risk Management (ERM)	44	67%
GRC	43	66%
ORM	32	49%
Risk Area: IT Risk (cyber)	25	38%
Risk Area: BCM	14	22%
HSEQ	12	18%
Risk Area: Project Risk	10	15%
Third Party Risk	10	15%
Vendor Risk	7	11%

Table 21: Software products for operational risk management related practices.

All software products are marketed not only for one specific risk area, but multiple areas. Most software products marketed for operational risk management are also considering enterprise wide integration in the form of ERM or GRC. Some products only focused on a specific area of operational risk, e.g. IT risk or Third party risk.

Primary focus sector(s)

Marketed as software for	Count	percent
Financial Services	66	21%
Energy & utility	52	17%
Government	44	14%
Technology	43	14%
Healthcare	27	9%
Production & manufacturing	26	8%
Transport & Infrastructure	21	7%
Retail & consumer goods	15	5%
Education	13	4%
Legal	6	2%

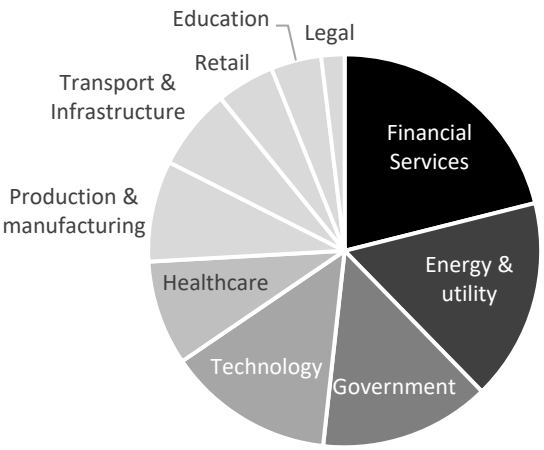


Figure 18: Operational Risk Management software marketed industries.

On average a software product for operational risk management is marketed at ~5 different sectors or industries. Most software for operational risk related practices is marketed for financial services, even though this research also included products for different terminology, such as HSEQ and specific areas of operational risk management, as used and known in other industries. Enterprise wide risk management practices as ERM and GRC appear to be well known. ORM is known as term by financial services and energy and appears also to be the most marketed sectors. Interestingly HSEQ is mentioned by just 18%, while the sectors using the term HSEQ are marketed by about 30%.

4.3.3 Software features for operational risk management

This chapter summarizes the found features that are applicable for operational risk management. Appendix B shows all found software features including their definitions and their relation to Business Performance Management Technologies.

All software features were included on the list on an incremental basis, meaning when not existing on the list, then they were added. Software features were identified using:

- product information and brochures from the product vendor websites;
- product demonstrations & screenshots;

ORM software functionalities are grouped based on their purpose, their corresponding process parts.

MODEL structure	Summary of functionalities
A - Environment	Organization structure, ownerships & responsibilities, business processes, sometimes using process flow modelling, process documentation & policy documents.
B - Objective setting	Risk appetite & tolerance levels, predefined compliance metrics, risk profiles & their configuration, objectives, risk performance indicators
C – Risk Assessment - General	Risk register, risk library or catalogue, risk categories, risk criteria (risk levels), operational risk assignment to different objects (business processes, individual process activities, assets, business units, other risks or organization objectives), risk scoring (qualitative scales, semi-qualitative scales or quantified), risk status dashboard, survey management.
D – Risk Identification	Event/Incident registration & reporting, internal & external loss data Expert survey, Brainstorming.
E – Risk Analysis	Risk matrix for risk profiles, risk source, risk causal modelling, CRSA Control and Risk Self-Assessment, risk voting, Bow Tie, waterfall analysis.
F - Risk evaluation	Risk profile calculation, risk profile comparison, Bow Tie, risk / scenario simulation.
G – Risk mitigation	Risk reducing measures, mitigating measure execution & planning, documents and evidence files, status/effectiveness mitigating measures issue register & action planning (action tracking).
H - Monitoring activities	Process indicators, audit planning & sampling, history of changes (audit trail), overview monitoring status & compliance.
I - Information & communication	Automated workflow, task overview, review, on screen or email notifications, dynamic dashboards & reporting.
Additional software functionality	Data import from operational systems, data export to various formats, rich text-editor

Table 22: Summary of identified software functionalities for Operational Risk Management.

Each of the identified software features was related to Business Performance Management technologies (see also appendix B). After analysis 63 of the 68 (94%) identified software features can be created using Business Performance Management Technologies. Examples are: hierarchical data storage for organization structure, analysis of risk profiles, workflow and dashboards & reporting.

Because 94% is considered a very high match for this specific application, all software features will be part of the assessment and reduced back afterwards. The availability of software features and actual use of software features is expected to give a detailed insight in the usefulness of BPM technologies.

4.4 Mapping software features to different maturity stages

A key characteristic for maturity models is that each maturity level provides a layer in the foundation for continuous process improvement. In this research the found software components as described in the previous section are mapped to process maturity stages. The order of appropriate process measurements and corresponding software features was determined by using expert opinions.

4.4.1 Expert Panel members

An expert panel of five operational risk management experts was consulted using the score voting method. The expert panel members have an average of 11 years' experience with operational risk. The votes were given anonymously using a voting system that worked with Kahoot, via the participants mobile/smart phone. On points were no dominant vote was given by the experts a discussion was held. All experts received all questions and possible answers 2 weeks before the actual panel session.

Type of organization	Org. Size FTE	Experience with operational risk
Business Consulting	18	13 years
Business Consulting	18	14 years
Business University	290	10 years
Financial Services	3600	3 years
Financial Services	390	15 years

Table 23: Members Expert Panel Operational Risk Management.

4.4.2 Selected to measure process maturity levels

The possible options to measure operational risk management regarding process implementation and process maturity (as discussed in 4.2.2) were rated by the five experts for suitability.

Suitable to measure process maturity (partial or fully)?	0 No vote	1 Not suitable	2 Somewhat suitable	3 Suitable	4 Very suitable
1 Is an operational risk management process present and executed?			2	3	
2 Process implementation or maturity level per process-step				1	4
3 Importance of (Operational) Risk Management process		1	1	3	
4 Frequency of execution (Operational) Risk Management process		1	3	1	
5 Frequency of execution validation (Operational) Risk Management process			3	1	
6 Frequency of effectiveness validation (Operational) Risk Management process		1	3	1	
7 Involved roles and amount of roles involved with ORM			2	3	

Table 24: Expert panel vote results, suitable process maturity indicators, Quick Scan.

Selected for actual measurement are the techniques voted by the experts as suitable and very suitable. The experts further proposed to use a combination of these techniques as a decent reference for process maturity. All other possible techniques were considered somewhat suitable and were not

presumed by the experts to sufficiently reflect maturity. The process will be measured for each of the process steps based on the model structure as described in Table 17 to provide the best level of detail.

4.4.3 Ranking of software features

All 68 software features as identified during the market analysis were showed to the expert panel. The software features were grouped according to their relating process steps and the experts was asked to determine a ranking of software features according to importance regarding operational risk. Table 25 provides an example of the ranking as provided by the expert panel. Appendix C: Expert Panel results provides all results for each of the software features.

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
A1 – Organization structure or hierarchy		4	1		
A2 – Ownership & Responsibilities		3	2		
A3 – Business processes entries		1	3	2	
A4 – Process documentation & policy documents		1	1	3	
A5 – Process flow modelling			2	3	

Table 25: Example of expert panel ranking results, Environment functionalities.

The software features as voted by the experts provide a ranking that was related to maturity levels. For each software feature the expert votes were counted and scored using the score voting technique. This means the highest number of votes wins. In some cases a clear winning vote was not immediately present, in those cases a discussion was held afterwards. The actual results of the ranking served as input for the development of the initial maturity model as described in the next section.

4.4.4 Additional features suggested by the expert panel

For validation of the practical completeness regarding features found during market analysis, each expert was asked to indicate missing software features. All five experts indicated the all of the identified software features were sufficient to support operational risk management processes.

Some experts described additional software features that could support operational risk management:

- Clear ownerships & responsibilities and functions. Who has what role, e.g. tester, reviewer;
- Automatically assigning a procuration matrix (power of attorney) to responsibility;
- In-control statement via software, automatically report to board, approval by manager.

A function matrix in the presence of a ownership and responsibility matrix was already present in the list of identified software features. Automatically assigning a procuration matrix to these ownerships & responsibilities could be possible, however was not found in existing software products. Therefore it was presumed very unlikely to encounter organizations using this specific software feature, thus this software feature was not included in the initial maturity model.

The in-control statement feature as described by one of the experts was not found in existing risk management products. The expert indicated this software feature was a wished software feature. The described functionalities to perform this specific task can be seen as part of reporting and workflow.

4.5 Initial/concept maturity model artefact

This section describes the initial maturity model that was constructed. The initial model is also available as automated assessment instrument from the appendices. The maturity model structure as used is described in chapter 4.2. The structure is combined with factors to measure operational risk management process maturity as described in chapter 4.2.

The identified software features as described in chapter 4.3 and ranked by the experts as described in chapter 4.4, are used to match corresponding parts to each of the process parts as basis for the initial model. Based on the first actual results from validation in practice some changes might be necessary. Changes to this initial model will be described in chapter 4.6.

Code	Process part	No of questions	Summary of related software features
A	**Environment** Presence: yes/no Importance: 1-10 Maturity of stage: 1-5	5	1. Organization structure or hierarchy 2. Ownership & responsibility 3. Business processes entries 4. Process documentation & policy documents 5. Process flow modelling
B	**Objective setting** Presence: yes/no Importance: 1-10 Maturity of stage: 1-5	4	1. Risk appetite 2. Predefined compliance metrics 3. Risk profiles & their configuration 4. Organizational objectives
C	**Risk assessment – in general** Presence: yes/no Importance: 1-10 Maturity of stage: 1-5	16	1. Qualitative scales (low, medium, high) 2. Risk Register 3. Filter & Sort Risk Register 4. Risk (type) categories 5. Risk assignment to individual (business) process activities 6. Current risk status dashboard 7. Risks are assigned to entire business process, not its individual activities 8. Risk Library or catalogue (RCSA) 9. Configurable risk assessment period 10. Semi-qualitative risk assessments 11. Risks related to asset 12. Risks related to Business Unit 13. Risks related to other risks (causal) 14. Risks related to organization objectives 15. Survey management 16. Quantitative risk assessments
D	**Risk identification** Presence: yes/no Importance: 1-10 Maturity of stage: 1-5	6	1. Incident reporting 2. Internal loss register (loss data) 3. CRSA Control and Risk Self-Assessment 4. Brainstorming 5. External loss data or incident data 6. Mobile incident reporting
E	**Risk analysis** Presence: yes/no Importance: 1-10	7	1. Risk matrix for comparing risk profiles 2. Risk source 3. Risk causal modelling

	Maturity of stage: 1-5		4. CRSA Control and Risk Self-Assessment 5. Risk voting 6. Bow Tie method 7. Waterfall Analysis
F	**Risk evaluation** Presence: yes/no Importance: 1-10 Maturity of stage: 1-5	5	1. Risk profile evaluation and calculation 2. Risk profile comparison using visualization 3. Risk profile comparison numeric 4. Bow Tie method 5. Risk / Scenario simulation
G	**Control activities** Presence: yes/no Importance: 1-10 Maturity of stage: 1-5	8	1. Risk reducing measures, with reduction factor 2. mitigating measure execution & planning 3. Documents and evidence files 4. Overview status/effectiveness mitigating measures 5. Issue register & action planning 6. mitigating measures testing - Control self-assessment (CSA) 7. Action tracking 8. Selecting relevant mitigating measures
H	**Monitoring activities** Presence: yes/no Importance: 1-10 Maturity of stage: 1-5	3	1. Audit planning & sample based checking 2. History of changes (audit trail) 3. Overview monitoring status & Compliance
I	**Information & communication** Presence: yes/no Importance: 1-10 Maturity of stage: 1-5	8	1. Tasks in software 2. Automated workflow 3. Task overview 4. Review 5. On screen notifications 6. Email notifications 7. Dynamic dashboards & reporting 8. Ad-hoc reporting
X	**Additional software functionality**	6	1. Data import from Excel 2. Data export to other systems 3. Data import from operational systems 4. Data export to Excel 5. One click export to MS Office 6. Rich text-editor
	TOTAL No. of questions	68	

Table 26: Summary of the initial maturity model structure.

The initial maturity model includes all 68 identified software features. These features should provide a complete overview of software availability and use. This full set of software features can be reduced back to Business Performance Management Technologies afterwards.

The diagram on the following page visualizes all dependencies and mapped software features. The inserted dependency diagram shows the technical relational structure of the initial maturity model that was created based on the features and results in the previous sections.

Maturity model Business Performance Management Technologies for Operational Risk (based on ISO 31000)

	Level 0: not present	Level 1: ad-hoc	Level 2: recurringly performed	Level 3: Formally defined	Level 4: Managed & measured	Level 5: Continuous improvement
A – Environment	Describe internal & external environment	At least ad-hoc → **Describe internal & external environment**	AND → A1 – organization structure; A2 – Ownership & responsibilities	AND → A3 – Business processes with name & description	AND → A4 – Process documentation & policy documents; A5 – Process flow modelling	AND → **Fully supported**
B – Describing Objectives	Describing objectives	At least ad-hoc → **Describing objectives**	AND	AND → B1 – Risk appetite settings	AND → B2 - Library / catalogue with rules from laws & regulations for compliance; B3 - Risk profile criteria; B4 - Organization objectives (scorecard or KPIs)	AND → **Fully supported**
C – Risk Assessment General	Risk Assessment	At least ad-hoc → **Risk Assessment**	AND → C1 – Qualitative scales (low, medium, high); C2 – Risk Register; C3 – Filter & Sort Risk Register; C4 – Risk (type) categories; C5 - Risk assignment to individual (business) process activities; C6 – Current risk status dashboard	AND → C7 - Risks are assigned to entire business process, not its individual activities; C8 - Risk Library or catalogue (RCSA); C9 - Configurable risk assessment period	AND → C10 - Semi-qualitative risk assessments; C11 - Risks related to asset; C12 - Risks related to Business Unit; C13 - Risks related to other risks (causal); C14 - Risks related to organization objectives; C15 - Survey management	AND → C16 - Quantitative risk assessments → **Fully supported**
D - Risk identification	Risk Identification	At least ad-hoc → **Risk Identification**	AND	AND → D1 – Incident reporting; D2 – Internal loss register (loss data); D3 – CRSA Control and Risk Self-Assessment	AND → D4 – Brainstorming; D5 – External loss data or incident data	AND → D6 – Mobile incident reporting → **Fully supported**
E – Risk Analysis	Risk Analysis	At least ad-hoc → **Risk analysis**	AND → E1 – Risk matrix for comparing risk profiles; E2 – Risk source	AND → E3 – Risk causal modelling; E4 – CRSA Control and Risk Self-Assessment	AND → E5 – Risk voting; E6 – Bow Tie method	AND → E7 – Waterfall Analysis → **Fully supported**
F – Risk Evaluation	Risk Evaluation	At least ad-hoc → **Risk Evaluation**	AND	AND	AND → F1 – Risk profile evaluation and calculation; F2 – Risk profile comparison using visualization; F3 – Risk profile comparison numeric; F4 – Bow Tie method	AND → F5 – Risk / Scenario simulation → **Fully supported**
G – Risk Response	Risk Response	At least ad-hoc → **Risk Response**	AND → G1 – Risk reducing measures, with reduction factor; G2 – mitigating measure execution & planning; G3 – Documents and evidence files; G4 – Overview status/ effectiveness mitigating measures; G5 – Issue register	AND → G6 – mitigating measures testing - Control self-assessment (CSA); G7 – Action tracking	AND → G8 – Selecting relevant mitigating measures	AND → **Fully supported**
H – Monitoring & Review	Monitoring & review	At least ad-hoc → **Monitoring & review**	AND → H1 – Audit planning & sample based checking	AND → H2 – History of changes (audit trail); H3 – Overview monitoring status & Compliance	AND	AND → **Fully supported**
I - Communication & Consultation	Communication & Consultation	At least ad-hoc → **Communication & Consultation**	AND → I1 – Tasks in software; I2 – Automated workflow; I3 – Task overview	AND → I4 – Review; I5 – On screen notifications; I6 – Email notifications; I7 – Dynamic dashboards & reporting	AND → I8 – Ad-hoc reporting	AND → **Fully supported**
X – Additional functionality			X1 – Data import from Excel; X2 – Data export to other systems	AND → X3 – Data import from operational systems; X4 – Data export to Excel; X5 – One click export to MS Office	AND → X6 – Rich text-editor	

4.6 Maturity model artefact improvements

With the design science method changes can be made to the artefact created. This section describes changes made to improve the maturity model and corresponding assessment. Some changes are made for efficiency or convenience, while some changes are for practices in specific industries.

4.6.1 Changes for efficiency

The first assessments were performed using the initial maturity model as described in the previous sections of this chapter. In practice the initial assessment appeared to consume too much time of the participants and contained repeated unnecessary questions.

Regarding the process maturity measurements selected the roles that are involved are now asked once, not per process activity. Asking each of the involved roles per process part was time consuming and often recurring with the same roles.

Another notable change is the individual steps of risk assessment: identification, analysis and evaluation are now receiving the same process priority, maturity and importance scores as risk assessment in general in order to save time.

Considering the actual maturity assessment on the technology domain many changes were considered necessary:

Code	Process part	No of questions	Change	Motivation
A	Environment	~~5~~ → 4	- Removed additional process information - Process documentation or files changed from level 4 to level 3	- Process entries are already a part of the organization structure - From the first assessments process documentation appears to be a common practice
B	Objective setting	4	- Configuration of risk profiles changed from level 4 to level 2 - Organization goals should also mention balanced scorecard - Library with pre-determined controls changed from level 3 to level 5	- Risk profiles appear to be seen by participants as essential to the risk matrix / heatmap. - Without mentioning the balanced scorecard not all participants understood KPIs related to objectives - A library with predetermined controls is considered by all interviewees as optional
C	Risk assessment – in general	~~16~~ → 15	- CRSA based technology rephrased to more general - Filter & sort removed	- CRSA was split into three distinctive parts of risk assessment, however was included three times

				- Filter & sort options are part of the risk register
D	Risk identification	~~6~~ → 4	- Moved CRSA - Removed mobile incident	- CRSA now part of risk assessment in general - Mobile or non-mobile incident registration is not a useful distinction, incident registration is important, not the tool
E	Risk analysis	~~7~~ → 6	- Moved CRSA	- CRSA now part of risk assessment in general
F	Risk evaluation	~~5~~ → 3	- Merged comparisons of different risk profiles, visual or numeric, it is about the possibility (removed 1) - Bow Tie option removed	- Risk comparison visual or numeric lead to confusion among participants, therefore was rephrased to comparison. - Bow Tie part of analysis
G	Control activities	~~8~~ → 6	- Moved action tracking to monitoring activities - Removed controls from library, because can be seen as part of adding controls	- Action tracking is part of monitoring activities - Controls from a catalogue or library are not often used and considered just adding controls or mitigations
H	Monitoring activities	~~3~~ → 4	+ Moved action tracking from control activities	+ Action tracking is part of monitoring activities
I	Information & communication	~~8~~ → 5	- Removed tasks - Removed reviews - Removed screen notification	- Removed tasks, because they are part of automated workflows - Removed reviews, because they are part of automated workflows - Removed screen notification, because they are part of automated workflows
X	Additional software functionality	~~6~~ → 4	- Removed one click export to excel, - Removed one click export to office	- now part of any export (e.g. format XML, PDF, XLS) - Export is now a free format field instead of a few fixed possible export options
	TOTAL	55		

Table 27: Changes to the initial maturity model to improve efficiency and clarity.

The 68 questions of the initial maturity model are reduced to 55 questions, resulting in a 20% reduction of questions. Further optimization was achieved by reducing length and clarity of questions where possible, without changing the integrity of the question.

4.6.2 Industry based changes

All organizations within the Aviation industry indicated they do not specifically rely on COSO ERM or ISO 31000 for integrated risk management practices. The aviation industry uses a Safety Management System (SMS) that is prescribed by the European Aviation Safety Agency (EASA). The SMS contains a strong focus on integration and a Plan-Do-Check-Act cycle for continuous process improvement.

International Civil Aviation Organization ICAO described a safety management system's purpose:

> "A systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures." (ICAO, 2013, p. xii)

EASA prescribes an Integrated Management System (IMS) that contains similar components as the already included ISO 31000 and COSO ERM. Main differences are in terminology and structure.

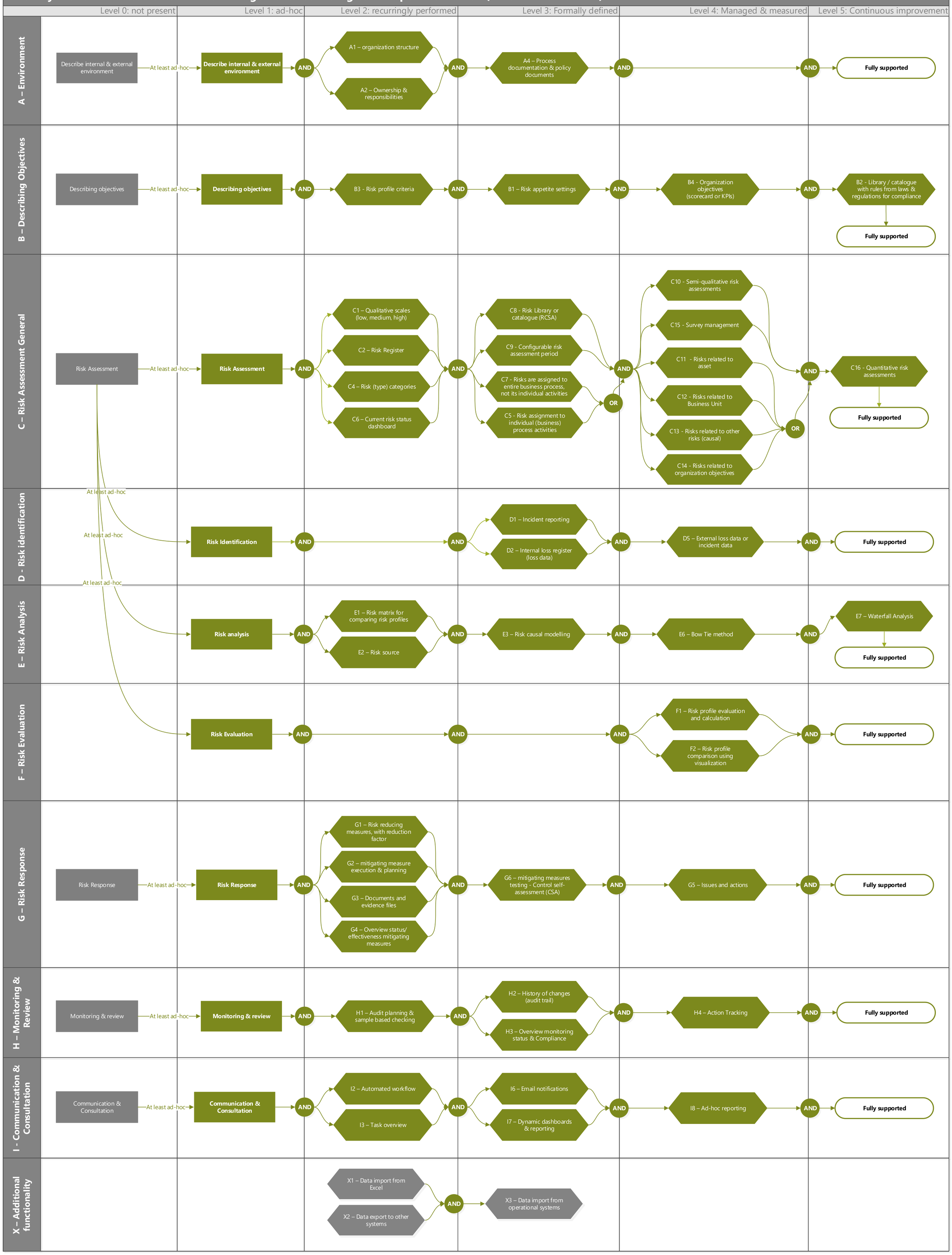
The environment, context, objective and risk assessment parts are very similar to ISO 31000 and COSO ERM. Main differences of Safety Management Systems appear to be safety assurance, as a combination of risk mitigation and monitoring. Regarding communication and safety promotion the Safety Management Systems have a strong focus on employee training.

COSO ERM (2004)	**ISO 31000** (2009a)	**(Integrated) SMS**
Internal Environment	Establish the context - internal and external environment - identifying and describing objectives	Safety Promotion, safety Policy; lines of responsibility documented processes
Objective setting		Safety objectives
Risk Assessment: 1. Event Identification 2. Risk Assessment 3. Risk Response	Risk Assessment: 1. Risk Identification 2. Risk Analysis 3. Risk Evaluation	Safety risk management, (includes: identification, analysis & evaluation)
Control activities	Risk Treatment	Safety Assurance
Information and communication	Communication and consultation	Safety Promotion, communication & training
Monitoring activities	Monitoring and review	Safety Assurance

Table 28: Structure of COSO ERM and ISO 31000 compared to Integrated SMS as used in the aviation industry.

Although the Integrated Safety Management System as prescribed by EASA is slightly different to COSO ERM and ISO 31000 there appear to be much similarities. An integrated Safety Management System was therefore added as experimental option for terminology in the improved maturity assessment.

Maturity model Business Performance Management Technologies for Operational Risk (based on ISO 31000)



5 The importance of Operational Risk Management

This chapter describes the importance of operational risk management as perceived by different participating organizations. The participating organizations are first introduced by describing some of their characteristics. Followed by a description of implementation of Operational Risk Management practices (from a process perspective) for each organization. Additionally software for operational risk and motivations for the current and future importance of this software are described.

5.1 Participating organizations & context

This section describes participating organizations by indicating the type of organization via its industry and some characteristics regarding their industry. Participating organizations are shown in Table 29.

k = thousands, m = millions, b = billions

Organization & industry	***Primary focus***	***International (outside NL)***	***Yearly income in € (euros)***	***FTE***	***Competitive pressure***
Energy 1	Energy provider	*Yes*	*1b – 5b*	*1k – 5k*	*Very high*
Energy 2	Energy provider	*Yes*	*1b – 5b*	*1k – 5k*	*High*
Financial services 1	Insurance services	*Yes*	*100m – 500m*	*250 – 500*	*Very high*
Financial services 2	Pension services	*No*	*100m – 500m*	*1k – 5k*	*Low*
Financial services 3	Banking services	*Yes*	*10b - 50b*	*50k – 100k*	*High*
Financial services 4	Banking services	*Yes*	*5b – 10b*	*10k – 50k*	*High*
Financial services 5	Banking services	*Yes*	*100m – 500m*	*1k – 5k*	*Very high*
Financial services 6	Insurance services	*Yes*	*500m – 1b*	*1k – 5k*	*Medium*
Healthcare 1	Patient treatment	*No*	*500m – 1b*	*1k – 5k*	*High*
Healthcare 2	Patient treatment	*No*	*100m – 500m*	*1k – 5k*	*Low*
Production & trade 1	Organic materials	*Yes*	*10b – 50b*	*1k – 5k*	*Very High*
Retail & consumer goods 1	Groceries	*No*	*5b – 10b*	*10k – 50k*	*Very high*
Retail & consumer goods 2	Health & beauty	*Yes*	*1b – 5b*	*10k – 50k*	*High*
Transport & Infrastructure 1	Airline services	*No*	*500m – 1b*	*1k – 5k*	*Very high*
Transport & Infrastructure 2	Airline services	*No*	*500m – 1b*	*1k – 5k*	*High*
Transport & Infrastructure 3	Infrastructure provider	*No*	*1b – 5b*	*1k – 5k*	*Very low*

Table 29: sixteen participating organizations and their characteristics.

Seventeen different organizations agreed to participate in this research. Sixteen organizations provided usable information to answer the research questions. One organization was omitted from the results because of insufficient information. Eleven organizations (69%) are privately owned. Five organizations (31%) are semi-public - run as a business, but owned by the Dutch government.

Nine organizations who participated are international organizations, meaning they have offices in the Netherlands and outside the Netherlands. The additional seven participating organizations are only located in the Netherlands.

The yearly income and Full Time Equivalent (FTE) indicate size of an organization. All participating organizations indicated a yearly income above 100 million euros and at least 250 FTEs in their organization. The largest organizations have a yearly income between 10 billion and 50 billion euros.

Only one organization in this study has a workforce above 50000 FTEs. Eleven participating organizations (69%) have a workforce between 1000 and 5000 FTE. Four organizations (25%) employ more than 10000 FTE. Only one organization (6%) employs less than 500 FTE.

5.1.1 Participants & role

Per participating organization at least one person was willing to participate in this research. Some organizations provided answers from multiple participants. In those cases the primary contact's information is described in Table 30: Participants by their role and experience.

Organization & industry	Function	in function	in organization
Energy 1	Advisor Operational Risk	6 years	10 years
Energy 2	Operational Risk Specialist	5 years	16 years
Financial services 1	Operational Risk Analyst	3 years	3 years
Financial services 2	Architect Quality & Change	7 years	7 years
Financial services 3	Head of Operational Risk	5 years	25 years
Financial services 4	Head of Operational Risk	4 years	20 years
Financial services 5	Head of Operational Risk	3 years	3 years
Financial services 6	Operational Risk Manager	9 months	11 years
Healthcare 1	Advisor Quality & Safety	7 years	17 years
Healthcare 2	Advisor Quality & Safety	14 years	21 years
Production & trade 1	Head of GRC Global	10 months	10 months
Retail & consumer goods 1	Risk & Security Specialist	8 years	8 years
Retail & consumer goods 2	Advisor quality & safety	8 years	8 years
Transport & Infrastructure 1	Head Quality & Safety	4 years	17 years
Transport & Infrastructure 2	Safety Consultant	7 months	16 years
Transport & Infrastructure 3	Preservation specialist	8 years	8 years
	Average	*5,2 years*	*11,9 years*

Table 30: Participants by their role and experience.

On average most participants appear to be employed twice as long in the organization as they are employed in their current risk related function. However, 7 of 16 (44%) of the participants are an equal time in their current function as they are in the organization.

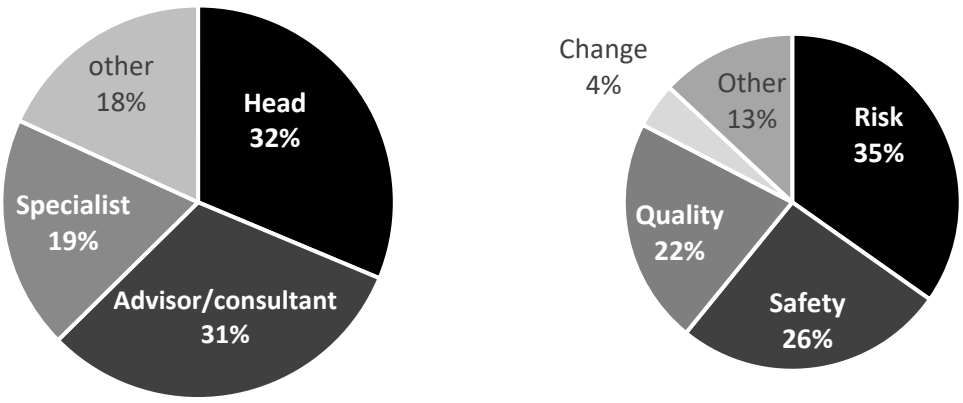


Figure 19: participants grouped by title and role.

Most of the participants appear to have a leading or consulting role. When considering the participant's title, operational risk appears to be well known in energy and financial services. In other industries operational risks are often managed by quality and safety management. This appears to be in correspondence with the terminology used in different industries as described in section 3.4.2.

5.1.2 Important laws and regulations per industry

All participants were asked to describe their top most important laws and regulations for their work and preferably related to operational risk or one of its sub topics.

Industry *(#distinctive reg.)*	***Reported as most important*** *(#mentioned reg. – descending)*
Energy (6)	Privacy law (2), Data Protection Act(1), Code Tabaksblat(1), Sustainability(1), Dutch Working Conditions Legislation - ARBO(1), rules for energy from Authority for Consumers & Markets - ACM(1)
Financial Services (12)	Basel II (3), Financial Regulation Law – WFT(3), Privacy law (3), Financial Economic Crime(2), Code Tabaksblat(2), IT Outsourcing - ISAE3402 (1), Sarbanes-Oxley – SOX(1), Solvency II(1), Markets in Financial Instruments Directive – MiFID (1), Foreign Account Tax Compliance Act – FACTA (1), International Financial Reporting Standards – IFRS (1), Dutch Pension Law (1)
Healthcare (4)	Law quality complaints and claims in healthcare - WKKGZ (2), Privacy law (2), Dutch law healthcare professionals - BIG(1), Medical Treatment Act - WGBO(1), Joint Commission Int. - JCI(1)
Production & Trade (10)	Markets in Financial Instruments Directive – MiFID (1), Privacy law(1), European Market Infrastructure Regulation – EMIR (1), Dutch Working Conditions Legislation - ARBO(1), Sarbanes-Oxley – SOX(1), Corporate Social Responsibility – CSR (1), Anti-money laundering – AML (1), Product approval (1), Anti-Bribery and Corruption (1), Anti-slavery - intensive labor(1)
Retail & Consumer goods (7)	Food safety law (2), Privacy law (2), Dutch Working Conditions Legislation - ARBO(1), Precursor reporting requirement – Counter Terrorist Act (1), Medication Act(1) Tax Law(1), Anti-Fraud Law(1)
Transport & Infrastructure (11)	European Aviation Safety Agency - EASA regulations(2), Dutch Working Conditions Legislation - ARBO(1), Dutch Law on Foreigners(1), Dutch law Safety Investigations – WVO(1), Dutch Aviation Law (1), ICAO – safety best practice(1), EU Regulation 376 civil aviation (1), Inspection Traffic and water management – IVW(1), IATA Operational Safety Audit – IOSA(1),Railways Act(1), European procurement/tendering Act(1)
Cross industry (5)	Privacy law (5), Dutch Working Conditions Legislation - ARBO(4), Sarbanes-Oxley – SOX(2), Code Tabaksblat(2), Markets in Financial Instruments Directive – MiFID (2)
Average (8,3)	

Table 31: Most important laws and regulations as described by the participants.

In total 50 distinctive laws and regulations were mentioned across the six different industries in this research. On average about 8 distinctive laws and regulations are mentioned in each sector. 5 laws and regulations are cross industry. When considering mentioned laws and regulations per industry on average around two (1,8) are mentioned. A large amount, 37 of 50 (75 percent) of all laws and regulations mentioned is once mentioned in a specific industry.

There appears to be a significant difference between industries providing services primarily within the Netherlands (Energy, Healthcare and Retail) and other industries (financial services, production & trade and transport & infrastructure). Organizations primarily focused on the Dutch market mentioned on average about 5,6 distinctive laws and regulations. The participants from financial services, production and transport industries mentioned on average 11 distinctive laws and regulations.

5.2 Implementation of operational risk management

This section details the extent to which the participating organizations implemented operational risk management processes and their perspective on maturity. The implementation of operational risk is presumed to be related to the integrated (or non-integrated) Enterprise Risk Management approach. Following the actual implementation of ORM is described. The implementation of ORM is believed to relate with perceived maturity and motivations for implementing operational risk management. This section is concluded by describing the cost of ORM in FTE's and software fees.

5.2.1 Enterprise Risk Management approach

The ERM approach as used by the participating organizations was measured based on integrated coordination, the presence of a Chief Risk Officer (CRO), the actual ERM framework the organization based their risk management practices on and the extent to which the Chief Executive Officer is involved with Operational Risk Management.

Organization & industry	Coordination	CRO role appointment	Enterprise Risk framework	CEO's ORM Involvement
Energy 1	*Centralized*	*No (CFO)*	*COSO ERM*	*Only reporting*
Energy 2	*Centralized*	*No (CFO)*	*COSO ERM*	*Only reporting & severe incidents*
Financial services 1	*Centralized*	*No (CFO)*	*COSO ERM*	*Audit findings, some reports*
Financial services 2	*Centralized*	*Yes*	*COSO ERM*	Only reporting
Financial services 3	*Centralized*	*Yes*	*COSO ERM*	Only reporting
Financial services 4	*Centralized*	*Yes*	*COSO ERM*	*Risk appetite, strategy*
Financial services 5	*Centralized*	*Yes*	*COSO ERM*	*Only reporting*
Financial services 6	*Centralized*	*No (CFO)*	*COSO ERM*	*Only reporting*
Healthcare 1	*de-centralized*	*No (COO)*	*No framework*	*Only reporting & severe incidents*
Healthcare 2	*Centralized*	*No (CEO)*	*No framework*	*Only reporting*
Production & trade 1	*de-centralized*	*Yes*	*COSO ERM*	*Not involved*
Retail & consumer goods 1	*Centralized*	*No (CFO)*	*No framework*	*Only Reporting*
Retail & consumer goods 2	*Centralized*	*Yes*	*No framework*	*Only reporting & severe incidents*
Transport & Infrastructure 1	*Centralized*	*No (CFO)*	*ISMS*	*Only reporting*
Transport & Infrastructure 2	*Centralized*	*Yes*	*ISMS*	*Chairman safety board*
Transport & Infrastructure 3	*Centralized*	*No (CFO)*	*ISO 31000*	*Only reporting*

Table 32: Enterprise risk management approaches as described by each participating organization.

14 of 16 (87,5%) of the participating organizations indicated to have a centralized coordination of organization wide risk management. This means a specific department or role is responsible. In most organizations there is a Chief Risk Officer at board level or ORM is part of the CFO's responsibility. In two organizations the responsibility for risk management is part of the CEO or COO.

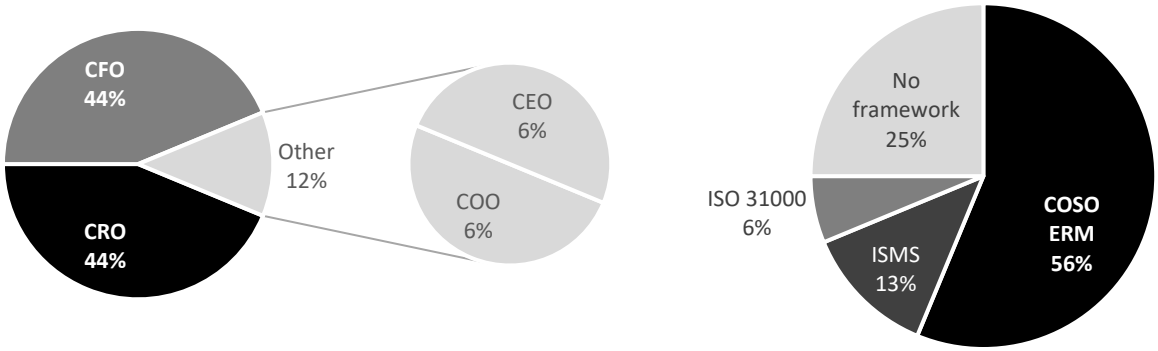


Figure 20: Frameworks for integrated and overall responsibility.

Most (9 of 16) organizations indicated to use COSO ERM as their framework for Enterprise Risk Management. In most cases the organization only used the COSO ERM framework as input for creating their own organization wide risk management framework or as reference for adapting best practices for risk management. A quarter (4 of 16) of the participating organizations indicated to have no specific framework for enterprise risk management.

In the aviation industry specific regulations describe risk management practices. Airline services are required to have an Integrated Safety Management System, which is similar to enterprise wide safety and risk management framework. Only one organization indicated to use the ISO 31000 framework.

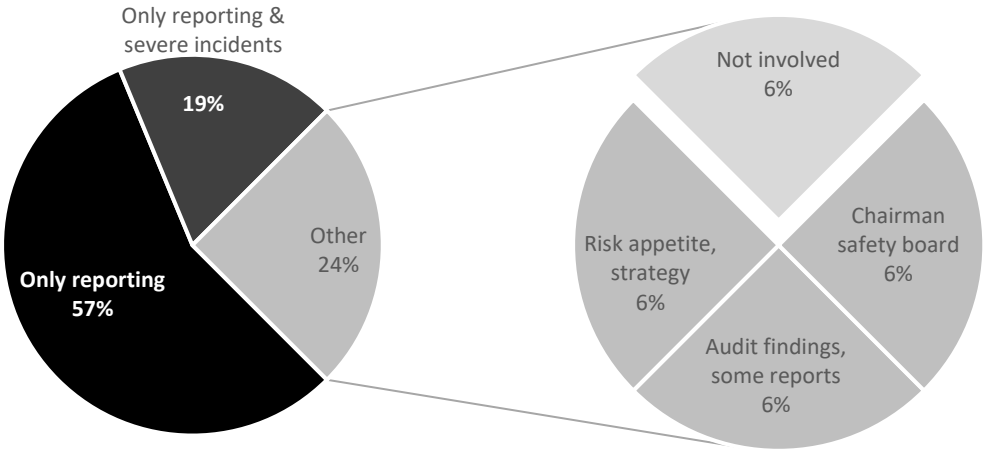


Figure 21: CEO involvement with Operational Risk Management practices.

Desender (2007) describes the involvement of a Chief Executive Officer (CEO) is an important indicator for ERM implementation. In this research the CEO involvement is in most organizations limited to frequent reporting of risks. In 3 of 16 organizations reporting is complemented by escalations with severe incidents shortly after occurring, in most cases overarching regular reporting intervals.

4 of 16 organizations indicated to have a different involvement with the CEO. One organization indicated the CEO is involved in setting risk appetite based on the organization's strategic goals. Another organization indicated the CEO was mainly briefed on audit findings and some reports. One organization described a high level of CEO involvement, where the CEO was chairman of the safety board and involved with important decisions regarding operational risks. Interestingly one organization described the CEO was not involved in any way, not even reporting.

5.2.2 Operational Risk Management implementation

The implementation of ORM is assumed to relate with certain preconditions, knowing the term operational risk and the importance of operational risks for the organization. 10 of 16 organizations were familiar with the term operational risk - as defined by Basel - without further explanation. The term Operational Risk was explained and then the importance of managing operational risks was rated from a board perspective on a scale from 1 (not important) to 10 (very important). On average participants considered operational risks to be important (7.6) from a board level perspective. This appears to be confirmed from interview analysis, where 11 of 16 (69%) participants indicated ORM to be very important and 4 of 16 (25%) indicated ORM to be just important.

Organization & industry	ORM as term	ORM committee	Importance ORM Processes (overall)	FTE dedicated for ORM	Frequently involved roles
Energy 1	*Yes*	*No*	*7*	*10*	*11*
Energy 2	*Yes*	*No*	*8*	*9*	*7*
Financial services 1	*Yes*	*Yes*	*3*	*2*	*13*
Financial services 2	*Yes*	*Yes*	*7*	*250*	*3*
Financial services 3	*Yes*	*Yes*	*9*	*2*	*3*
Financial services 4	*Yes*	*Yes*	*8*	*60*	*4*
Financial services 5	*Yes*	*Yes*	*8*	*4*	*4*
Financial services 6	*Yes*	*Yes*	*8*	*1*	*7*
Healthcare 1	*No*	*No*	*7*	*20*	*5*
Healthcare 2	*No*	*Yes*	*9*	*11*	*5*
Production & trade 1	*Yes*	*Yes*	*4*	*12*	*7*
Retail & consumer goods 1	*No*	*Yes*	*7*	*8*	*7*
Retail & consumer goods 2	*No*	*Yes*	*10*	*11*	*3*
Transport & Infrastructure 1	*No*	*Yes*	*8*	*10*	*2*
Transport & Infrastructure 2	*No*	*Yes*	*10*	*10*	*5*
Transport & Infrastructure 3	*Yes*	*Yes*	*9*	*25*	*5*
AVG	*62% Yes*	*81% Yes*	*7.6 (sd. 1.8)*	*27.8 (sd. 58.9)*	*5.7 (sd. 2.9)*

Table 33: Operational Risk Management implementation indicators.

Most organizations (81%) described to have a committee concerned with operational risks, meeting on regular intervals discussing operational risks and their current status. On average 27.8 Full Time Equivalents are dedicated to ORM related practices. However this average appears to be skewed, because of one peak regarding an estimate of 250 FTE. An average of 13 (sd. 14) FTE results when the peak of 250 FTE is left out of the calculation. However, the organization with this estimate of 250 FTE dedicated to ORM, describes to have all employees involved in operational risk management and therefore considered 250 FTE a valid estimate. The number of roles involved with operational risk management is based on the participant's view regarding the most important and frequently involved roles. On average almost six roles appear to be involved on a frequent basis.

Operational risk management processes

When considering the actual operational risk management processes, 15 of 16 (94%) organizations indicated to at least perform all steps in the ERM Risk management framework on an ad-hoc basis. In detail, one organization does not perform the processes objective setting, monitoring and communication & collaboration.

Model structure	At least ad-hoc implemented?	AVG Importance	AVG Perceived process maturity level
A - Environment	*100%*	*7.6 (sd. 1.8)*	*3.6 (sd. 1.5)*
B - Objective setting	*94%*	*8.3 (sd. 1.2)*	*3.4 (sd. 1.3)*
C - Risk assessment general	*100%*	*8.8 (sd. 0.8)*	*3.8 (sd. 1.0)*
D - Risk identification	*100%*	*8.8 (sd. 1.0)*	*3.6 (sd. 1.1)*
E - Risk analysis	*100%*	*8.4 (sd. 1.4)*	*3.6 (sd. 1.1)*
F - Risk evaluation	*100%*	*8.8 (sd. 0.8)*	*3.6 (sd. 1.1)*
G - Risk mitigation	*100%*	*8.7 (sd. 0.9)*	*3.8 (sd. 1.4)*
H - Monitoring	*94%*	*8.1 (sd. 1.2)*	*3.5 (sd. 1.6)*
I - Communication and collaboration	*94%*	*8.1 (sd. 1.0)*	*3.0 (sd. 1.5)*
AVERAGED	*98%*	*8.4 (sd. 0.4)*	*3.5 (sd. 0.2)*

Table 34: Actual implementation of ORM processes, over all organizations.

Overall the average importance and overall process maturity scores regarding all processes appear to be close to each other, with very small standard deviations. Describing the organization environment, regarding the organization structure, responsibilities and processes is considered the least important with an average score of 7.6. Risk assessment appears to be the most important, with an average importance of 8.8 with a standard deviation of 0.8 and one of the top ranking process maturity levels.

5.2.3 Motivations for ORM

Another aspect of importance is assumed to be related with motivation. In the structured interviews open questions allowed for interview analysis. Without specifically asking the participants for their motivation, interview transcript analysis allowed for the creation of the following table:

Motivation	No of times in different interviews	Percent
Image & Reputation	*8*	*50%*
Significant damage to assets & failure	*7*	*44%*
Money & capital	*7*	*44%*
Awareness & Participation	*5*	*31%*
Safety & care	*3*	*19%*
In Control	*3*	*19%*
Compliance with laws & regulations	*2*	*13%*
Learning & improvement	*2*	*13%*

Table 35: Motivations for implementing operational risk management related practices.

2 of 16 organizations did not describe a motivation for implementing operational risk management. at most 4 different reasons for implementing ORM were given by some of the participants. On average around two different motivations were given per interview for managing operational risks.

Preventing undesired effects, reputation damage, significant damage to assets & organization failure and monetary reasons appears to be the most important motivation for implementing Operational Risk Management processes.

Cultural components, such as awareness & participation, safety & care, being in control, compliance with laws & regulations and learning & improvement are mentioned in less than one third of the interviews, indicating to be of secondary importance for most organizations.

5.2.4 Perceived maturity level

This section describes the perception of average operational risk management process maturity as described by the participants and compares this to the results of the maturity model.

Organization & industry	Perceived maturity level	Maturity level calculation	Delta AVG vs perc.	Lowest process Maturity	Delta LOW vs perc.	Perspective on model accuracy
Energy 1	*4*	*3*	*-1*	*1*	*-3*	*Accurate*
Energy 2	*5*	*4*	*-1*	*3*	*-2*	*Accurate*
Financial services 1	*3*	*3*	*0*	*3*	*0*	*Accurate*
Financial services 2	*4*	*4*	*0*	*1*	*-3*	*Mostly Accurate*
Financial services 3	*5*	*5*	*0*	*5*	*0*	*Accurate*
Financial services 4	*5*	*5*	*0*	*1*	*-4*	*Accurate*
Financial services 5	*2*	*3*	*+1*	*1*	*-1*	*Accurate*
Financial Services 6	*2*	*2*	*0*	*1*	*-1*	*Accurate*
Healthcare 1	4	*4*	*0*	*3*	*-1*	*Accurate*
Healthcare 2	*2*	*3*	*+1*	*2*	*0*	*Accurate*
Production & trade 1	*3*	*1*	*-2*	*0*	*-3*	*Accurate*
Retail & consumer goods 1	*3*	*3*	*0*	*1*	*-2*	*Accurate*
Retail & consumer goods 2	*3*	*4*	*+1*	*1*	*-2*	*Mostly Accurate*
Transport & Infrastructure 1	*5*	*3*	*-2*	*1*	*-4*	*Mostly Accurate*
Transport & Infrastructure 2	*4*	*4*	*0*	*3*	*-1*	*Mostly Accurate*
Transport & Infrastructure 3	*5*	*4*	*-1*	*1*	*-4*	*Accurate*
AVG	*3.7 (sd. 1.1)*	*3.4 (sd. 0.99)*	*-0.25*	*1.75*	*-1.9*	*75% Accurate*

Table 36: perceived maturity levels versus maturity model calculations.

The participants rated their average maturity level before the assessment, based on the maturity level characteristics as described in section 4.2.3. This rating is about the process maturity, not including software or BPM technologies. On average most organizations indicated to have an overall process maturity between level 3 and level 4, with a tendency towards level 4.

The calculated average is based on the maturity levels as described by the participants on a more detailed level, namely each process in the model structure as described in section 4.2.2. On average most organizations still scored an overall process maturity between level 3 and level 4, however now with a tendency towards level 3. When considering the delta there is a small difference between perception of average ORM process maturity and the calculated average ORM process maturity.

The average process maturity is calculated over 9 distinctive process steps (as described in section 4.2.2), however on some parts organizations did not score full maturity. In many maturity models the lowest achieved process score is the overall maturity level. Then the maturity levels drastically change and on average each organization drops around two maturity levels.

According to most participants (75%), the results as generated by the automated assessment and the maturity model, accurately reflect the current state of ORM implementation in their organization. Some participants (25%) had their doubts about certain components and results in the model and therefore indicated the results mostly reflects current state. In the transport & infrastructure industry, the aviation sector indicated to use complementary process parts related to their (integrated) Safety Management System, which appears not to be one-on-one related to ORM.

5.3 Importance of software

The importance and maturity of operational risk management is assumed – in this research - to be related with the used tools. Software is for most organization seen as a tool to structure risk management practices. This section aims to show how important the software is for managing operational risk in the current situation and the near future (max. 5 years).

Organization & industry	Perceived score current	Perceived score future	Delta	Participant's view on Change
Energy 1	*7*	*8*	*+1*	*Organization changes*
Energy 2	*8*	*9*	*+1*	*More efficiency*
Financial services 1	*7*	*8*	*+1*	*More laws and regulations*
Financial services 2	*9*	*9*	*0*	*Cloud services, new types of risks, changing impact*
Financial services 3	*8*	*8*	*0*	*No change in importance software*
Financial services 4	*8*	*8*	*0*	*More laws & regulations, new types of risk*
Financial services 5	*8*	*8*	*0*	*More users*
Financial services 6	*8*	*8*	*0*	*No change in importance software*
Healthcare 1	*10*	*10*	*0*	*No change in importance software*
Healthcare 2	*10*	*10*	*0*	*Organization changes*
Production & trade 1	*3*	*6*	*+3*	*Available resources*
Retail & consumer goods 1	*7*	*9*	*+2*	*Changing impact of events*
Retail & consumer goods 2	*7*	*8*	*+1*	*Organization growth, efficiency, new types of risk*
Transport & Infrastructure 1	*10*	*10*	*0*	*Organization growth, increase in competition*
Transport & Infrastructure 2	*9*	*9*	*0*	*More users*
Transport & Infrastructure 3	*8*	*9*	*+1*	*More users*
AVG score	*7.9*	*8.5*	*+0.6*	

Table 37: Perception of importance software for ORM in the current situation and expected future.

All participants were asked to score the current and future importance of software for ORM on a scale from 1 (not important) to 10 (Very important). Based on the average importance score of 7.9 software for operational risk can be considered reasonably important. The average difference between the current and expected future importance indicate a minimal to no increase in importance.

From interview analysis there appears to be eleven distinctive reasons for the expected change in importance. 3 of 16 (18%) organizations expect no change in importance of the ORM software at all in the next 5 years. However, most organizations expect the impact of risks will change; new types of risks, such as cybercrime or other IT related risks (e.g. cloud services and outsourcing), organization changes or organization growth, more users that will be dependent on software for ORM, more or new laws and regulations increase dependency on software. Software is used as tool for efficiency, standardization and central storage instrument, that enables effective collaboration.

5.4 Cost of Operational risk management

Most organizations indicated managing operational risks is a responsibility shared by everyone in the organization. That does not mean everyone in the organization is working full-time, most organizations have one or more people dedicated to operational related risk management practices. Additionally the participants were asked to describe some of the most frequently involved roles with operational risk management. The amount of roles frequently involved is presumed to be an indicator of collaboration.

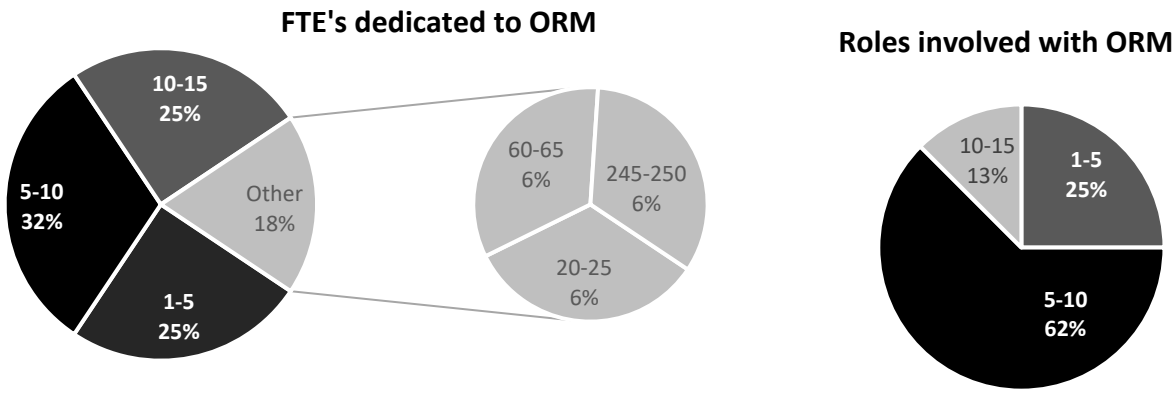


Figure 22:Full Time Equivalents and roles involved with operational risk management.

Most organizations indicated the FTE indication was excluding part time participation in the organization. For most organizations the amount of FTE's involved with ORM ranges from at least 1 to around 15. There are some exceptions, a large international banking organization employs more than 60 FTE to ORM. A much smaller financial services organization indicated to have around 250 FTE involved with ORM. This figure is in huge contrast with the other participating organizations, however this applicable organization describes management of operational risks to be such an important topic where they decided to include many employees on full time basis.

Another factor of costs for operational risks is assumed to be the costs of the used tooling. All participating organizations were asked to estimate their yearly costs for operational risk tooling.

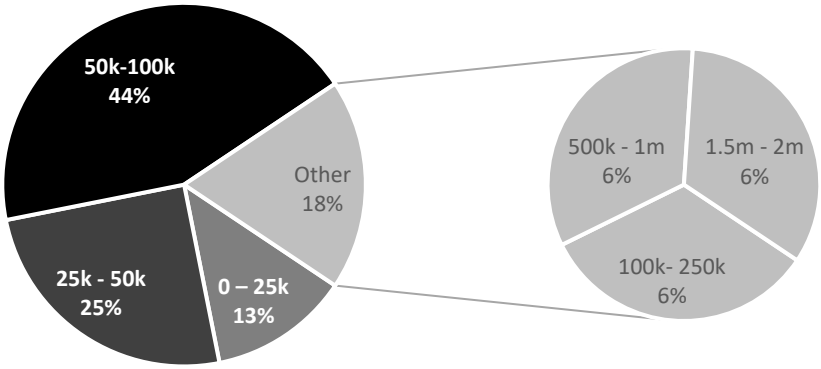


Figure 23: yearly software costs for ORM tooling as indicated by the participating organizations.

Most organizations indicate to spend between 50 and 100 thousand euros on a yearly basis. Mainly on yearly recurring license fees and maintenance. Two banking organizations indicated to spend more than half a million euros each year on software for operational risks. One retail organization indicated to spend around 200 thousand euros each year on fraud detection software.

5.5 Chapter conclusion

This chapter describes the importance of operational risk management as perceived by different participating organizations. The main research question this chapter answers is:

RQ5: " How important is Operational Risk Management in practice? "

Importance was measured with the actual implementation of ORM, perceived implementation or maturity level, importance of software, estimated investments regarding FTE's and software costs.

The implementation of an enterprise wide approach towards risk management was measured trough the coordination central or de-centralized. A central approach towards risk is recognized by most organizations. About 88% indicated to have a central department coordinating risk management.

The presence of a Chief Risk Officer (CRO) role on board level is another indicator of organization wide approach to risk management. Interestingly, 44% of the organizations delegate risk management to their Chief Financial Officer (CFO) compared to 44% appointing a dedicated CRO. In a few cases even the CEO or COO was responsible for all risks. The CEO in most organizations (76%) just received reports or received reports and was brought up to speed regarding severe operational risk related incidents.

An enterprise wide risk management framework is often also described to structure the organization and processes regarding risk management. COSO ERM appears to be the most popular by 56% of the participating organizations. While 25% of the participating organizations have no framework at all.

When considering Operational Risk Management about 62% of the participants knows the term ORM as defined by Basel. About 80% have a specific committee to discuss operational risk management related matters. Most organizations perform ORM processes to prevent a bad image or reputation, while learning from operational risks is not even described as a reason at all by almost all organizations.

ORM was given an overall importance of 7.6 (sd. 1.8) of 10. This indicates most organizations find ORM quite important, but not the most important. Most implemented (100%) and most important process of ORM is risk assessment (8.8 of 10), including risk identification, analysis and evaluation.

Most organizations have a relatively small ORM department. 82% of the participating organizations dedicate between 1 and 15 FTE to ORM, with some exceptions indicating higher numbers, mainly large international banks. On average an ORM department is made up with 13 FTE, however a standard deviation of 14 indicates high fluctuations from this average in both ways (positive and negative). Not only the ORM department is involved with operational risks. On average about 5.7 (sd. 2.9) different roles are mentioned to be involved with ORM on a regular basis.

Software is seen as an important aid for ORM with a 7.9 (of 10 very important) on average in the current situation. In the future software is expected on average to become not less important with a 8.5 (of 10 very important). ORM software does not appear to be a big money market 82% of all organizations spends less than 100k on yearly ORM software. Only a few large banks spend over 100k to a 2 million euros on yearly software fees, including maintenance costs.

The maturity of ORM processes overall was measured using perception of the participants and via calculation of the maturity scores. Most participants scored their current maturity level 3.7 of 5 (sd. 1.1) very similar to their calculated score of 3.4 (sd. 0.99). The initial results of the maturity model were considered to yield an accuracy of 75% accurately reflecting their current status. The next chapter further details the relations between ORM process maturity and the supporting BPM technologies.

6 Implementation level of ORM and use of BPM technologies

This chapter describes the actual implementation and use of business performance management technologies for operational risk management. For most organizations tooling for risk management is just known as software. Although BPM technologies is not equal to all software features, the actual use and availability of all software features is first described to provide context of tooling use. Then the software features are reduced towards the scope of this research and relate to BPM technologies.

6.1 Software for Operational Risk Management

This section describes the results regarding the implementation of ORM and used software. The actual use of software for ORM is first described. Then the actually used and available software features are described in more detail. This section is concluded by comparing satisfaction of current software and future improvements of ORM software.

6.1.1 ORM Software landscape

Most organizations, 14 of 16 (87,5%) indicated to use dedicated software for ORM, 2 of 16 (12,5%) organizations indicated to rely primarily on self-made excel solutions for risk assessment or reporting.

Vendor	Product name	Appeared industry	Appearance	Percent
ARIS (software AG)	Risk & Compliance Manager (RCM)	Energy, Financial Services	3	19%
Infoland	iRisk (or complete infoland suite)	Healthcare	2	13%
ideagen	Q-Pulse	Airline Services	2	13%
SAP	GRC	Transport & Infrastructure	1	6%
IBM	Open Pages	Financial Services	1	6%
RSA	Archer GRC	Financial Services	1	6%
Dynasec	Easy2Comply	Energy	1	6%
R-sam	GRC	Financial Services	1	6%
Secure	Anti-fraud	Retail & consumer goods	1	6%
Smile	Risk management software	Retail & consumer goods	1	6%
		TOTAL	14	88%

Table 38: Software landscape for operational risk management software.

ARIS RCM is most used and is an extension for the process modelling tool ARIS. Infoland software is used by all hospitals in this research. All airline companies in this research use Q-Pulse. The retail and consumer goods sector uses software products for ORM, not encountered in market research.

All participating organizations were asked why software is needed for operational risk management. From interview analysis it appears most organizations 11 of 16 (69%) primarily need the software for efficiency, without the software much more people are needed to perform the same tasks.

Half of the participating organizations 8 of 16 (50%) indicated the software for ORM leads to a better overview & insights regarding operational risks. Additionally, about one third 5 of 16 (31%) of the participating organizations indicated the integration of all operational risk related data in one integrated tool enables efficient and effective communication and collaboration.

6.1.2 ORM Software use & availability

This section describes the actually used and available software components for Operational Risk Management in practice. The use and availability is derived from interview transcript analysis and additionally measured during the maturity model assessment.

Dashboards & Reporting are the most used software features as indicated by 9 of 16 (56%) of the participating organizations. Half of the participating organizations 8 of 16 (50%), talk about risk assessment. Central storage or a central database, or data warehouse is described by 6 of 16 (38%). Process modelling is described to be used by one third 5 of 16 (31%). Incident registration 4 of 16 (25%). Workflow as a component of collaboration by 3 of 16 (18%). The use of a file manager for documents and reports is used by 3 of 16 (19%). Least used software features are Action Tracking by 2 of 16 (13%). Filter & sort features for reports and data sets by 2 of 16 (13%) organization. Only mentioned once features are a rules engine for fraud detection, control monitoring (measuring mitigation effectiveness) and operational risk workshop support.

MODEL structure	AVG group use	Most used software features	Percent use	Percent available	Delta
A - Environment	72%	A1 – Organization structure or hierarchy	81	88	+7
B - Objective setting	52%	B3 – Risk profile criteria	56	63	+7
		B4 – Organization objectives	56	75	+19
C – Risk Assessment - General	54%	C1 – Qualitative scales (low, medium, high)	88	88	0
		C4 – Risk (type) categories	81	88	+7
		C5 - Risk assignment to individual (business) process activities	75	63	-12
D – Risk Identification	56%	D2 – Incidents and internal loss register (loss data)	81	69	-12
E – Risk Analysis	37%	E1 – Risk matrix for comparing risk profiles	75	56	-19
F - Risk evaluation	42%	F1 – Risk profile evaluation and calculation	69	60	0
G – Control activities	66%	G3 – Documents and evidence files	81	81	0
		G4 – Status/effectiveness mitigating measures	75	88	+12
H - Monitoring activities	59%	H4 – Action tracking	75	88	+12
I - Information & communication	69%	I2 – Automated workflow	75	81	+6
		I3 – Task overview	75	75	0
X – additional software features	41%	X1 – Data import from Excel	56	56	0
		X2 – Data export to other systems	56	69	+12
TOTAL	55%	17 most used software features	72	74	+1.6

Table 39: Most used software features as measured from the assessments.

On average 37 (55%) distinctive software features are used for operational risk management, from the 68 identified software features in the market analysis. From the 17 most used software features it appears almost all available is also used, on average 1.6 percent point is not used. Embedding the organizational objectives is a feature that is available to 75% of the participating organizations, but in practice almost 20 percent points do not use this feature.

From Table 39 it appears software features for describing the organization environment, such as organogram and processes are most used by all organization. Qualitative scales for operational risk assessments are used by almost all organizations (88%) in this research. Risk assessment features (incl. the processes of identification, analysis and evaluation) appear to be used by most organizations, however around 12 percent point indicates these features are not actually available in the bought software and therefore these organizations rely on spreadsheet solutions.

For each process step the least used software features are described in the following table.

MODEL structure	Least used software features	Percent use	Percent available	Delta
A - Environment	A2 – Ownership & Responsibilities	63	88	+25
B - Objective setting	B1 – Risk appetite settings	44	38	-6
C – Risk Assessment - General	C16 – Quantitative risk assessments	6	0	-6
D – Risk Identification	D4 – Brainstorming	19	19	0
E – Risk Analysis	E7 – Waterfall Analysis	6	12	+6
	E5 – Risk voting	12	6	-6
F - Risk evaluation	F5 – Risk / Scenario simulation	12	12	0
G – Control activities	G6 – mitigating measures testing - Control self-assessment (CSA)	44	63	+19
H - Monitoring activities	H1 – Audit planning & sample based checking	44	38	-6
I - Information & communication	I7 – Dynamic dashboards & reporting	63	81	+18
	I8 – Ad-hoc reporting	63	75	+12
X – additional software features	X6 – Rich text-editor	6	12	+6
TOTAL	12 least used software features	32	37	+5.2

Table 40: Least used software features as measured from the assessments.

The least used software features as shown in Table 40 indicate the environment features are overall most used, confirming the trend in Table 39. When considering the availability it appears almost a quarter of the participating organizations have software features available but do not actually use for software features for describing ownership and responsibility for operational risks.

On average these least used software features are more often available than actually used. Risk appetite, audit planning & sampling and quantitative (statistical) calculations for operational risks are often used in other solutions outside of the bought software for ORM.

6.1.3 Satisfaction with ORM software

The implementation of software for operational risk is assumed to relate with the actual satisfaction of the software. From the assessments it appears that 62% of the participating organizations still end up using spreadsheet solutions for certain aspects of their operational risk management.

Organization & industry	Fallback to excel	Satisfaction	Satisfaction explained
Energy 1	*Yes*	Not satisfied	Missing integration, insufficient reporting, not user friendly.
Energy 2	*Yes*	Room for improvement	Software lacks a user friendly interface, insufficient insights.
Financial services 1	*Yes*	Not satisfied	Insufficient reporting functionalities.
Financial services 2	*Yes*	Fully satisfied	None
Financial services 3	*No*	Fully satisfied	None
Financial services 4	*No*	Fully satisfied	None
Financial services 5	*No*	Room for improvement	Room for central data integration, user friendly interface is important.
Financial services 6	*Yes*	Not satisfied	Reporting and insights not sufficient, Process standardization using workflow.
Healthcare 1	*No*	Room for improvement	Interface is not user friendly and confusing for some users.
Healthcare 2	*No*	Fully satisfied	None
Production & trade 1	*Yes*	Not satisfied	Available resources
Retail & consumer goods 1	*Yes*	Not satisfied	No process automation for continuity.
Retail & consumer goods 2	*Yes*	Room for improvement	Integration of different data sources.
Transport & Infrastructure 1	*No*	Room for improvement	Integration of data sources, better reporting solutions.
Transport & Infrastructure 2	*Yes*	Room for improvement	Integration into one safety data warehouse.
Transport & Infrastructure 3	*Yes*	Room for improvement	Integration into one central risk data warehouse.
	62% yes		

Table 41: satisfaction with ORM software as experienced in practice.

Only 25% of the organizations indicates to be fully satisfied with their software for ORM. While 44% indicate they have small points for improvements. About one third is not satisfied on important points.

When considering motivations for satisfaction, it appears most complaints (26%) relate to central integration into a central data repository for operational risks and resulting quality of reporting (18%). Usability in the sense of a user friendly interface is fairly big (18%) reason for being dissatisfied.

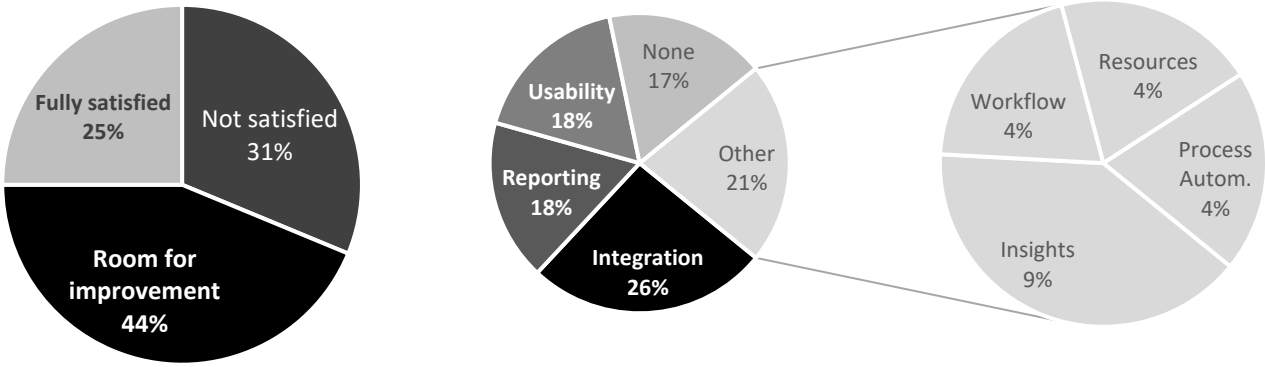


Figure 24: Satisfaction with ORM software summarized.

6.2 Use & availability of BPM technologies

The previous sections described the use of software as a whole. This sections describes the relation with Business Performance Management related technologies. From the 68 identified software features are 63 = 94% related to Business Performance Management Technologies. Not considered BPM technologies are process modelling functionalities, process documentation and policy documents (used by 69%) via a file system, risk voting (used by 12,5%), process or scenario simulation (used by 12,5%) and rich text editor functionality (used by 6%).

Organization & industry	BPMT Use (%)	BPMT Availability (%)	Software Use (%)	Software Availability (%)	Software use Not BPMT	Fallback to excel
Energy 1	*43*	*59*	*42*	*56*	*2%*	*Yes*
Energy 2	*54*	*44*	*52*	*43*	*2%*	*Yes*
Financial services 1	*33*	*61*	*33*	*58*	*2%*	*Yes*
Financial services 2	*69*	*86*	*65*	*84*	*2%*	*Yes*
Financial services 3	*75*	*78*	*69*	*75*	*0*	*No*
Financial services 4	*88*	*88*	*87*	*84*	*4%*	*No*
Financial services 5	*63*	*86*	*60*	*82*	*2%*	*No*
Financial services 6	*45*	*16*	*44*	*16*	*2%*	*Yes*
Healthcare 1	*69*	*86*	*67*	*84*	*3%*	*No*
Healthcare 2	*67*	*67*	*64*	*67*	*2%*	*No*
Production & trade 1	*27*	*33*	*25*	*33*	*0%*	*Yes*
Retail & consumer goods 1	*27*	*12*	*25*	*11*	*0%*	*Yes*
Retail & consumer goods 2	*61*	*51*	*56*	*47*	*0%*	*Yes*
Transport & Infrastructure 1	*61*	*75*	*56*	*71*	*0%*	*No*
Transport & Infrastructure 2	*71*	*55*	*69*	*53*	*3%*	*Yes*
Transport & Infrastructure 3	*63*	*65*	*62*	*64*	*3%*	*Yes*
AVERAGE	*57*	*60*	*55*	*58*	*2%*	*38% No 62% yes*

Table 42: Use and availability of BPM technologies vs all software technologies.

On average 2% of all used software features cannot be realized using business performance management technologies. Most notable features are process documentation & policy documents (used by 69%) via a file storage manager and process flow modelling (used by 75%). Currently the most used business performance management technologies from interviews are: dashboards & Reporting: 9 of 16 (56%), risk assessment 8 of 16 (50%), central storage or database 6 of 16 (37%), data entry for incident registration 4 of 16 (25%), workflow 5 of 16 (31%). Most of the participating organizations (62%) indicated to fall back using spreadsheet solutions for ORM, organizations utilizing more than 60% Business Performance Management Technologies available do not appear to have this fallback.

During interviews the participants was about their future (5 year) perspective regarding the software for Operational Risk Management. 10 of 16 (63%) expect data integration to become more important. 8 of 16 (50%) describe improvements of dashboards & reporting functionalities. Insights related to risks and mitigating measures by 5 of 6 (31%). 6 of 16 (38%) indicated context aware solutions, adapting to a specific role in organization (e.g. only information that is relevant for that specific person at a specific time) is an important improvement in the future. Additionally the usability, specifically user friendliness and easy to use interfaces are required by 4 of 16 (25%). Collaboration, process automation & process monitoring functionalities are described by 3 of 16 (19%) of the participants.

6.3 BPM technologies related to ORM maturity

In the previous sections the actual use of specific software functionalities and BPM technologies is described in detail. The goal of this section is to describe how the maturity levels relate with actually used technologies in order to describe its qualities and suitability for measurement.

The relationship between ORM process maturity and BPM technologies is measured on three distinctive levels:

- Abstract level → overall maturity scores of processes and used technologies;
- Maturity score level → process and technology scores with maturity levels as proxy;
- Technology level → the amount of individual technologies related to process maturity.

On the abstract level, the overall average of calculated ORM maturity scores are compared with overall average of BPM technologies regarding use and availability. On average calculated ORM process maturity has a strong (0.78) Pearson correlation with overall BPM technology use. A similarly strong correlation (0.75) was achieved when comparing the overall score with BPM technologies available.

BPM Technology maturity levels appear to have a weak correlation with process maturity levels (0.25). However after performing the technology level correlations the process steps of C (risk assessment in general) and I (communication) appear to distort this correlation. After correction BPM Technology maturity levels appear to have a moderate correlation with process maturity levels (0.32).

Considering individual sets of BPM technologies for each process, without technology maturity as a proxy, some steps appear to have a different relationship with the actual ORM process maturity.

	BPMT Use with maturity	BPMT Availability with maturity	Best correlation
A Environment	0.40	0.16	Moderate with Use
B Objective setting	0.25	0.53	Strong with Availability
C Risk Assessment General	0.08	-0.18	None
D Risk Identification	0.61	0.16	Strong with Use
E Risk Analysis	0.58	0.35	Strong with Use
F Risk Evaluation	0.38	0.26	Moderate with Use
G Mitigation & Controls	0.58	0.40	Strong with Use
H Monitoring	0.45	0.71	Strong with Availability
I Communication	-0.05	0.03	None

Table 43: Low level BPM technologies for each process, without technology maturity as a proxy.

Risk assessment in general and communication appear to have no reasonable correlation with the technologies used or available and the actual ORM process maturity. However, specific components of risk assessment (identification, analysis and evaluation) appear to have a good relationship with BPM technology use. Communication related BPM technologies, such as workflow and dashboards are often used, however the actual process maturity appears to be fluctuating among the participating organizations. Objective setting and monitoring related BPM technologies appear to be available more often with a higher level of ORM process maturity. However, their actual use of BPM technologies (or software technologies) does not appear to relate with actual ORM process maturity levels.

6.4 ORM characteristics related to maturity

The previous section described correlations related to the maturity model. This section extends this further by finding patterns of the characteristics as described in the previous chapter, now related to the maturity model. Weaker correlations than 0.20 alpha 0.05 are left out, because such correlations are so weak that considering the sample size they do not even indicate anything at all.

Characteristic (n =16 organizations)	AVG Process maturity	AVG Technology maturity	BPMT use %
No of FTE in organization	0.50	0.23	0.35
Yearly income (revenue)	0.26	No correlation or <.20	No correlation or <.20
No of laws and regulations	No correlation or <.20	0.27	No correlation or <.20
International organization	No correlation or <.20	No correlation or <.20	No correlation or <.20
Competitive pressure	No correlation or <.20	No correlation or <.20	-0.41
Presence of a framework for ORM	No correlation or <.20	No correlation or <.20	No correlation or <.20
Centralized coordination	0.28	No correlation or <.20	0.20
FTE dedicated to ORM	0.27	No correlation or <.20	No correlation or <.20
CRO is present	0.24	0.49	0.39
ORM committee	-0.21	No correlation or <.20	No correlation or <.20
Knowing the term ORM	No correlation or <.20	No correlation or <.20	-0.24
Cost of ORM tooling	0.42	No correlation or <.20	0.23
Satisfaction of ORM tooling	0.45	0.53	0.88
Presence of dedicated ORM tooling	0.50	0.57	0.47
Change in importance ORM tooling	-0.45	-0.57	-0.78
Fallback to excel	No correlation or <.20	-0.39	-0.60

Table 44: Organization characteristics compared to maturity levels and BPM technologies used.

Organization size, especially the amount of FTE appears to correlate moderately with ORM process maturity. Additionally, technology maturity and BPMT use show a weak relationship. A similar relationship is not found when considering the yearly income where only a weak relationship exists with maturity. Being an international organization or not does not appear to be a difference for ORM.

The number of laws and regulations for an organization do not appear to influence the actual maturity, however they have a weak relationship with the technology maturity. A higher perception of competitive pressure interestingly seems to relate moderate negative to the actual use of technology.

When considering the structure of ORM, the presence of a framework for ORM does not appear to be meaningful. The same appears to be true for the centralized or de-centralized approach, the correlations are so weak they do not really indicate anything. The number of FTE dedicated to ORM appears to have a weak relationship with ORM maturity. The same is true regarding a ORM committee.

The appointment of a Chief Risk Officer appears to have a moderate relationship with technology and BPMT use. Cost of the tooling does not need to increase with more technologies, but process maturity increases with higher software costs. There is a reasonably moderate to strong relationship with satisfaction and maturity. Very strong when using more BPM technologies.

Organizations scoring higher on maturity and BPM use appear to have the least expectations about future change in importance of ORM software. Additionally, these organizations use less spreadsheets.

6.5 Chapter conclusion

This chapter described the actual implementation and use of business performance management technologies for operational risk management. ORM software was just known as software by the participants, therefore software was described before scoping back to BPM technologies as planned:

> *RQ6: " What is the relation between the implementation level of Operational Risk Management and the supporting Business Performance Management technologies? "*

Most organizations have some form of dedicated software for ORM. Only two organizations indicated to use spreadsheet based solutions for ORM. The healthcare and airline industries appear to be well represented by the dominant vendors. Essentials for ORM software appear to be:

- Possibility for embedding the organization structure or hierarchy in the ORM software
- Qualitative risk assessment scales with high, medium and low risk scores
- Incident registration and internal loss data
- Possibility to add documents and evidence files in the ORM software.

ORM software does not need to include functionality for quantitative risk assessment using simulations and a rich-text editor. These results are both expected, because ORM is not about statistics and a rich-text editor is easy to work around with another text editor.

When considering satisfaction, only 25% of the organizations indicates to be fully satisfied with their software for ORM. Most complaints (26%) relate to central integration into a central data repository for operational risks and resulting quality of reporting (18%). Usability in the sense of a user friendly interface is fairly big (18%) reason for being dissatisfied.

Although BPM technologies are a feasible fit for resolving these issues, BPM technologies lack a file management system for process, policy and evidence documents, that are essential for ORM. Additionally process flow modelling (process diagrams) appear to be an important features missed by BPM technologies. On the other hand BPM includes ETL and should be able to integrate these sources.

On average calculated ORM process maturity has a strong (0.78) Pearson correlation with overall BPM technology use. When diving into more detail, the environment, risk identification, risk analysis, risk evaluation and mitigation steps are quite decently correlating with maturity and used technologies. Objective setting and monitoring functionalities appear to be available to organizations with higher maturity scores, but are far from as much used. Risk assessment in general might be too general, because it does not appear to have any relationship with maturity and technologies. No relationship was found for maturity and technologies to aid communication, but this might be explained by the fact that communication is a human process and does not necessarily rely on technology to be successful.

Comparing maturity scores to certain organization characteristics, most turned out to be weak. However the presence of a CRO appears to positively influence the use of technologies. When considering ORM maturity and software the presence of software relates with a higher maturity. While at the same time appears to have an effect on increasing costs and satisfaction of the ORM software. Spending more on technologies to support ORM does appear to pay off, this is also underlined by less need to fall back to self-made spreadsheet solutions.

Investing in more complete ORM software and the appointment of a CRO might relate to each other, however this is not studied here. It is very likely a dedicated CRO and more investments in ORM software indicate an organization is more serious about its operational risk management.

7 The use of BPM Technologies in different sectors

The previous chapters provided a general or summarized overview of all results. Therefore this chapter is intended to split these results into a different perspective for each industry. The main purpose of this chapter is to find how the maturity model as developed in this research matches certain industries.

7.1 Contextual differences between industries

This section describes some important differences between the participating organizations as grouped by industry. The differences between industries will be compared from the variation in importance of ORM, motivations for ORM and to conclude this section the importance of software.

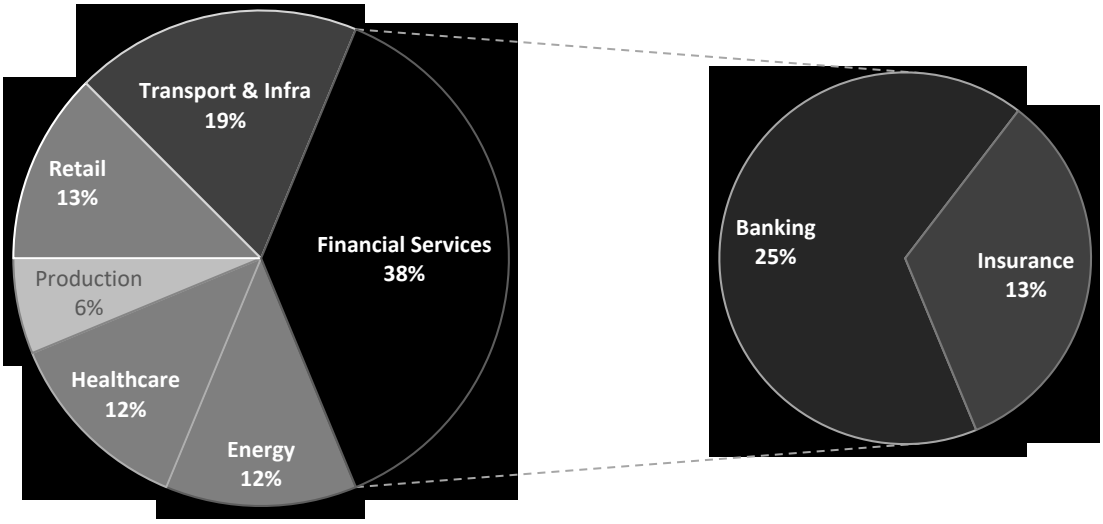


Figure 25: Participating industries and their distribution.

The financial services industry is the largest group of organizations, mainly composed of banks. Transportation and infrastructure is the second largest industry. Retail, Healthcare and Energy are al equally proportional in size. The production & trade industry is just one organization and will therefore be left out in some (but not all) comparisons.

Averages are used to describe the importance of operational risk management processes per industry. The comparison is created from interview analysis and average industry scores from the assessments.

Energy	Financial Services	Healthcare	Production	Retail	Transport
Very important	Important	Very important	Important	Very important	Very important
7.5	7.2	8	7	8.5	9

Table 45: Differences in average importance of ORM between industries.

Interestingly, the results for all industries appear to be consistent in their explicit rating from 1 to 10 and their implicit answers as given during the structured interviews. This is visible from Table 45, where higher scores (< 7.5) also correspond with a higher rated qualitative expression of importance. On average transport and infrastructure organizations rates management for operational risks as most important. Production and trade results in the lowest average scores for importance. However, production & trade is the only industry represented by just one organization.

When considering differences in motivations for operational risk management, there are organizations primarily concerned with prevention of adverse effects or using ORM as instrument for improvement.

Prevent adverse effects in this comparison include: significant damage & organization failure, risks calculated as money & capital, the image & reputation or compliance. Learning, improvement & awareness include: safety & care, learning & improvement and awareness & participation.

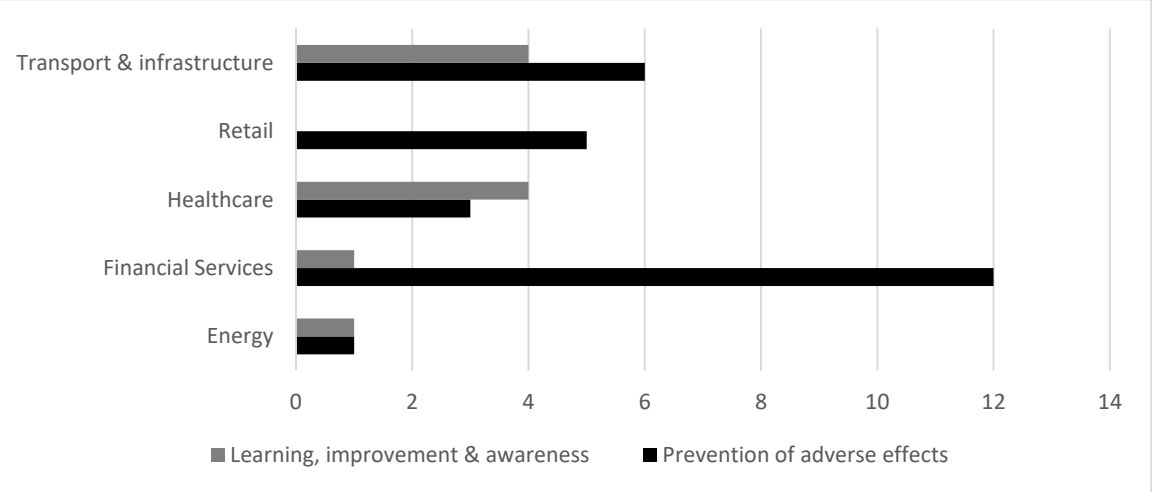


Figure 26: Different motivations for ORM per industry.

The financial services and retail industries indicate to manage their operational risks primarily for the prevention of adverse effects. The healthcare industry appears the only sector to focus primarily on learning, improvement and awareness with operational risk management. Transport and infrastructure and the energy industry appear to favor both perspectives.

For effectively managing operational risks software is used in most industries. Only the production & trade industry did not use a dedicated software solution for ORM and used spreadsheet solutions.

Industry	Importance from interviews	AVG current score	AVG future score	Delta = change
Energy	Very important	7.5	8.5	+1.0
Financial Services	Important for Efficiency	8	8.2	+0.2
Healthcare	Very important	10	10	0
Production	Other priorities	3	6	+3.0
Retail	N/A	7	8.5	+1.5
Transport	Very important	9	9.3	+0.3

Table 46: Differences in importance of software for Operational Risk Management.

The importance of software for operational risk management varies per industry. Overall most industries expect a slight increase in importance of software for ORM. Most industries find the use of dedicated software for ORM important or very important, in most cases the analysis from interviews corresponds with the given scores on a scale from 1 (not important) to 10 (very important).

On average the healthcare industry considers software a vital part of ORM and this is not expected to change in the near future (5 years). The production and trade industry is represented by just one organization and indicated they have other priorities at the moment, since they have just merged with another organization, they expect ORM software will become much more important in the near future.

7.2 Utilized Business Performance Management Technologies

Business Performance Management Technologies are a specific set of software features central in this research. This section describes the actual use and availability of BPM technologies and the differences between industries based on averages for each industry.

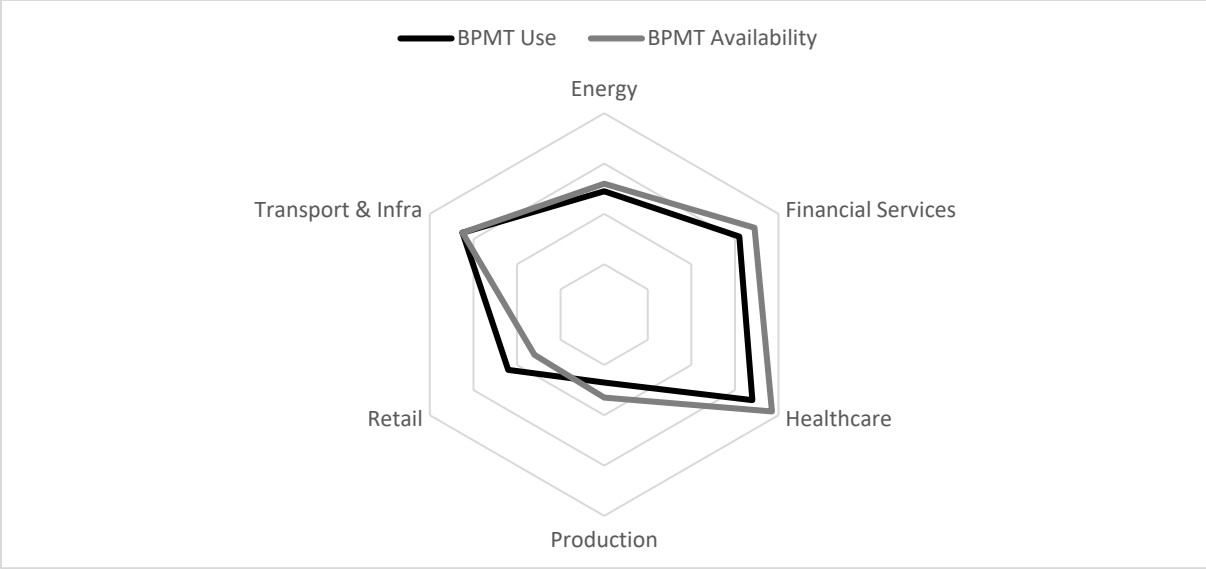


Figure 27: BPM technologies used and available, differences between industries.

Both Figure 27 and Table 47 represent the difference between the actual use and availability of Business Performance Management Technologies. The healthcare industry appears to be the industry with the highest BPM technology use and availability. About nine percent point of what is actually available is not used. However, their overall satisfaction of 75% and being the only industry without the need to rely on spreadsheet solutions outside the software, underline the importance of software.

Organization & industry	BPMT Use	BPMT Availability	Delta	Manual work in Excel	AVG yearly software fees	AVG satisfaction
Energy	*49%*	*52%*	*+3*	*100%*	*75k*	*25%*
Financial services	*62%*	*69%*	*+7*	*50%*	*500k*	*58%*
Healthcare	*68%*	*77%*	*+9*	*0%*	*60k*	*75%*
Production & trade	*27%*	*33%*	*+6*	*100%*	*75k*	*0%*
Retail & consumer goods	*44%*	*32%*	*-12*	*100%*	*80k*	*25%*
Transport & Infrastructure	*65%*	*65%*	*0*	*66%*	*50k*	*50%*

Table 47: Comparison of BPM technologies, fall back to excel, cost and satisfaction.

The retail and consumer industry appears to use more than actually available. This means these organization rely heavily on non-integrated spreadsheet based solutions for ORM. The average 80k yearly fees in this case are skewed because one retail organization uses expensive anti-fraud software.

The yearly software fees mainly include licensing and support costs. On average financial services organizations pay the highest yearly software fees. This is caused by a number of large banks with expensive and very complete ORM software. The BPM technologies used and available are much less by smaller financial services organizations.

The previous section provided a high level overview of differences between industries. This section aims to view the differences in actual BPM technology use on a more detailed level. In order to provide insights into important sets of BPM technologies for different industries. As described in chapter 4 (maturity model development) the use of BPM technologies is based on specific sets of technologies grouped with a certain goal for the risk management process. Table 48 displays the sets as determined by the maturity model and their actual use per industry.

Model structure	Energy	Financial Services	Healthcare	Production	Retail	Transport
A - Environment	75%	92%	100%	50%	0%	67%
B - Objective setting	38%	58%	38%	0%	88%	50%
C - General Risk assessment	48%	60%	63%	47%	43%	51%
D - Risk identification	25%	58%	63%	0%	75%	75%
E - Risk analysis	50%	43%	60%	0%	20%	47%
F - Risk evaluation	50%	75%	50%	0%	0%	83%
G - Risk mitigation	75%	72%	83%	67%	0%	78%
H - Risk and Control Monitoring	38%	63%	50%	25%	75%	75%
I - Communication and collaboration	40%	73%	100%	20%	60%	80%
AVG	49%	66%	67%	23%	40%	67%

Table 48: Heatmap of BPM technologies used per process set per industry.

The energy industry appears to focus on risk mitigation via tooling and has a strong focus on mapping the ORM environment. Little used are technologies for risk identification. The participating organizations within the energy industry indicated to favor workshops for risk identification.

The financial services industry is also focused on the ORM environment and risk mitigation, however also uses more risk assessment features. In some smaller financial organizations the actual risk analysis is still performed using spreadsheet solutions.

On average the Healthcare industry uses the most BPM technologies. Strong points are the environment and communication, where all possible technologies appear to be present.

The production and trade industry utilized the least BPM technologies of all participating industries. However, this result only reflects one particular organization, not using any software for ORM. Self-made excel solutions are used within this organization.

One of the least performing industries in this research while having purchased dedicated software for ORM is the Retail and consumer goods industry. The only industry not mapping the ORM environment and not using BPM technologies for risk mitigation activities. On the contrary appears most use of objective setting, risk identification and monitoring related BPM technologies.

Overall the transport and infrastructure industry utilized the most BPM technologies. Risk analysis was preferred via workshops and safety meetings.

7.3 Differences in maturity score and BPMT use

The final section of this chapter relates BPM technologies to ORM process maturity, similarly to the previous chapter. However, this section approaches the same data from a completely different perspective and compares cross industry results to find a matching industry for the maturity model.

All BPM technology maturity scores and ORM process maturity scores were averaged per industry.

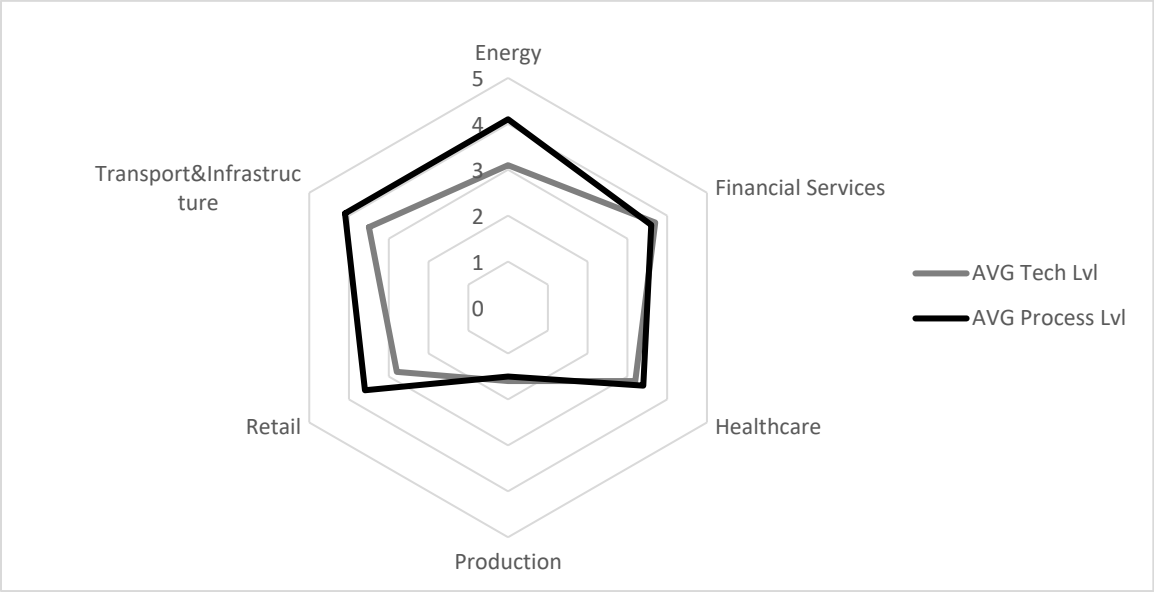


Figure 28: Average BPM technology maturity and ORM process maturity compared per industry.

The financial services and production industries scored slightly higher on BPM technology maturity than on the ORM process maturity scores. On average the financial services, production and healthcare industries have a BPM technology score close to their ORM maturity score.

Organization & industry	AVG Technology Score	AVG Maturity score	Delta	Perceived Overall importance
Energy	*3.1*	*4.1*	*+1*	*7.5*
Financial services	*3.7*	*3.6*	*-0.1*	*7.2*
Healthcare	*3.2*	*3.4*	*+0.2*	*8*
Production & trade	*1.6*	*1.5*	*-0.1*	*4*
Retail & consumer goods	*2.8*	*3.6*	*+0.8*	*8.5*
Transport & Infrastructure	*3.5*	*4.1*	*+0.6*	*9*

Table 49: Average BPM technology maturity, ORM process maturity and important compared per industry.

On average the energy and transport & infrastructure industries score the highest overall ORM process maturity with a 4.1 of 5. From a technology perspective, financial services scored the highest overall average technology maturity scores with a 3.7 out of 5. On this level of measurement there appears to be a very strong (0.88) correlation between a higher technology score and a higher ORM process technology score. This trend appears to correspond with the perception of ORM importance.

The production and trade industry has the lowest BPM technology score and ORM process maturity score. On average the importance of ORM is also rated significantly lower. This score should be noted with caution, because the score relates to only one participating organization in this industry.

The full set of actually used Business Performance Management Technologies (BPMT) and availability of these technologies were tested versus the average calculated ORM process maturity scores using a Pearson correlation. The samples sizes are too low for expressive power, but indicate a direction.

Organization & industry	BPMT use with maturity	BPMT available with maturity	Best match
Energy	0.25	0.14	Weak with use
Financial services	0.22	0.25	Weak with both
Healthcare	0.20	0.47	Strong with available
Production & trade	0.85	0.33	Strong with use
Retail & consumer goods	0.23	0.06	Weak with use
Transport & Infrastructure	0.24	-0.05	Weak with use

Table 50: Relationships of BPMT use and availability versus average ORM process maturity.

Most industries appear to have at least a weak relationship with BPM technologies used and ORM process maturity. The healthcare and production & trade industries appear to have a strong relationship with the average maturity scores. However, the healthcare industry appears to relate better with BPMT actually available than used.

The production & trade industry appears to relate strongly with BPMT use, however this is caused by having little BPM technologies in use and logically corresponding low maturity scores. Again this result is just based on one specific organization, representing the production & trade industry.

Considering the weak relationships as displayed in Table 50, decided was to try similar correlations on a more detailed level as shown in Table 51. With a more specific level of detail the cause of weak relationships could possibly be traced back to the origin. However, not enough data for each industry was available to go into more detail with a Pearson correlation. The analysis could only be performed for the financial services industry, since that is the largest industry in this research.

Financial Services *(n=6)*	BPMT Use with maturity	BPMT Availability with maturity	Best match
A Environment	0.32	0.05	Moderate with use
B Objective setting	0.15	0.51	Strong with availability
C Risk Assessment General	0.80	0.3	Strong with use
D Risk Identification	0.59	0	Strong with use
E Risk Analysis	0.72	0.67	Strong with use
F Risk Evaluation	0.65	0.43	Strong with use
G Mitigation & Controls	0.22	0.25	Weak with use
H Monitoring	0.49	0.83	Moderate with use
I Communication	-0.31	-0.22	None

Table 51: Correlations with BPMT use and availability related to ORM maturity for the financial services industry.

On a more detailed level the correlations between used BPM technologies and ORM process maturity appear to be stronger with process parts. In this case objective setting and communication technologies appear to influence the total result, where communication related technologies even negatively influences the overall correlation. Mitigation and controls appears to have a weak correlation with BPM technologies use and ORM maturity score.

7.4 Chapter conclusion

The main purpose of this chapter is to find how the maturity model as developed in this research matches certain industries. The goal of this chapter is to answer the following research question:

> *RQ7: " Which set of Business Performance Management technologies is utilized to support Operational Risk Management processes in different fields? "*

ORM was found most important with an average of 9 out of 10 in the transport industry, especially airline companies consider ORM to be of vital importance for safety of their passengers. Software for ORM is equally important for this sector and no change in importance is expected in the next few years. This sector is the only sector using exactly as much technologies as having available. However their ORM software is not complete, because 66% need solutions in Excel and the satisfaction with ORM software is only 50%. However, this sector achieved the highest ORM maturity scores.

The financial services sector is by far the largest field in this research. On average the importance of ORM is rated a 7.2 out of 10, which is lower than most other industries. The motivation culture for most financial organizations appears to be very strongly prevention of adverse effects, rather than learning from risks. Software is mainly important for efficiency and no change is expected in importance of the software in the next few years. Financial organizations have a reasonable complete ORM solution, much used and spend the most on ORM software. However they are not the most satisfied with their ORM software. It should be noted these figures are skewed because only some very large banks spend tons on ORM software and they indicated to be satisfied. While smaller organizations in this industry spend less and drop satisfaction.

The healthcare industry considers ORM to be very important as well with an 8 of 10 and is the only industry trying to learn more from operational risks rather than primarily preventing damages. Although this is of course related, but the culture appears to be very different – focused on patients wellbeing and safety. Interestingly the healthcare sector is the only industry where all organizations do not use excel and show the highest technology use, availability and satisfaction.

Retail organizations consider ORM very important with an 8.5 of 10. Their only motivation for ORM appear to be money and reputation based. ORM software is considered to increase in importance of the coming years. ORM software in this industry is scarce and most ORM related work is done using spreadsheet solutions. This lead to a low satisfaction of just 25%. Margins in this industry are very low and there is little budget for ORM software. There is an indication of high software cost, but this is caused by one organization spending tons of euros only on fraud detection, which is just a part of ORM.

The energy industry appears to be average on almost all aspects. The average importance of ORM was rated 7.5 out of 10. Not the lowest, but not the highest either. The motivational culture for ORM is equally distributed among prevention and learning. There is a slight change in importance expected in the next few years. Regarding the use and availability of technologies this industry scores average as well. The entire sector indicated to need spreadsheet solutions while none being fully satisfied with their software solution for ORM. Interestingly they achieved the highest ORM maturity level, but compared to their use of technology they lag the most of all industries.

The production and trade industry was just represented by one organization. Sadly this organization does not consider ORM to be important and does not have dedicated ORM software. This industry is therefore considered not representative and was only included for completeness.

8 Conclusions

Operational risks are seen as the root cause for many of the (large scale) financial failures in the past decades. Additionally, factors such as: globalization, an increasing volume of transactions, supply chain dependencies and growing organization complexity - made the impact of operational risks more significant than ever before.

Business Performance Management technologies are believed to provide a solution for effective Operational Risk Management (ORM). However, it is unclear whether the full spectrum of Business Performance Management technologies is suitable for improving operational risk management processes and whether the same set of Business Performance Management technologies are applicable for all types of organizations. This research aimed to provide some answers and therefore the main research question was formulated as follows:

" How can organizations incrementally improve their Operational Risk Management processes using Business Performance Management technologies? "

Seven sub questions were designed to provide a qualitative answer to the main research question. This research combines two domains, the first two research questions aimed to provide context.

RQ1: " What is defined as the domain of Operational Risk Management? "
Operational Risk is defined by the Basel Committee from the Bank of International Settlements as risks resulting from: Internal Processes, Humans, Systems and External events. In most organizations Operational Risk Management is part of Enterprise Risk Management (ERM). The term 'Operational Risk' is known by 62% of the participating organizations in this research. Other organizations relate to specific sets of operational risk, in most industries: 'quality' and 'safety management' often includes operational risk management related practices, such as risk identification, analysis and risk mitigation.

RQ2: " What is the definition of Business Performance Management technologies? "
Business Performance Management (BPM) complements Business Intelligence with an organizational process of planning and control. The planning and control cycle relates to performance measurement and developing Key Performance Indicators (KPIs) to measure organizational performance. BPM extents Business Intelligence with data entry and workflow for planning organizational performance using KPIs. The set of Business Intelligence technologies and additional technologies needed for Business Performance Management are seen as Business Performance Management Technologies.

Central in this research was the development and practical validation of a maturity model. The maturity model was constructed of a process part, related to operational risk management implementation and the technologies part, relating to BPM technologies used.

RQ3: " How to develop a quick scan for assessing the implementation level of the Operational Risk Management process within an organization? "
For development of the process part a so called 'Quick scan' of the ORM process was developed based on factors for implementation of ORM processes. ERM characteristics, such as industry, implementation of integrated risk management, process presence, perceived importance, frequencies and involved roles can be used as indicators for process maturity. Consulting five experts in Operational Risk Management, decided was a 'Quick scan' detailed to individual process parts of risk management appeared to be best suitable solution for reflecting the organization's ORM maturity.

RQ4: " Which set of functionality is required from Business Performance Management technology in order to accommodate the Operational Risk Management process? "

The technology part was developed from a broad software perspective. A market analysis of 65 distinctive software products for risk management lead to 68 distinctive software features. The full set of software features was related back to the described set of Business Performance Management Technologies and showed a very good (94%) match between risk management software and possible solutions with BPM technologies. The five ORM experts were consulted for ranking each of the 68 identified software features to the 'Quick scan' in order to create an initial maturity model.

The initial assessments performed in practice showed the initial maturity model could be improved for efficiency and clarity. The initial model contained 68 software features, while the improved version includes 55 software features. The maturity of ORM processes overall was measured using perception of the participants and via calculation of the maturity scores. Most participants scored their current maturity level 3.7 of 5 (sd. 1.1) very similar to their calculated score of 3.4 (sd. 0.99). The initial results of the maturity model were considered to yield an accuracy of 75% reflecting their current status.

RQ5: " How important is Operational Risk Management in practice? "

Importance was measured with the actual implementation of ORM, perceived maturity level, importance of software, estimated investments regarding FTE's and ORM software yearly costs.

The importance of ORM - as scored by the participants - resulted in an overall score of 7.6 on a scale from 1 (not important) to 10 (very important). Concluding, most organizations consider operational risks fairly important. ORM is most often (50%) used to prevent damage and other adverse effects, more than for learning, improvement or awareness (13%).

An enterprise wide risk management framework is often also described to structure the organization and processes regarding risk management. COSO ERM appears to be the most popular by 56% of the participating organizations. While 25% of the participating organizations have no framework at all.

Most organizations have a relatively small ORM department. 82% of the participating organizations dedicate between 1 and 15 FTE to ORM, with some exceptions indicating higher numbers, mainly large international banks.

Risk assessment is considered the most important risk management process with an average score of 8.8 (of 10). Risk assessment also appeared to be most mature process over all organizations with an average maturity around level 4 (of 5). On average the participant's perception of their organization's average ORM maturity was scored a 3.7 (out of 5), while the calculated overall average maturity is slightly lower 3.4 (of 5), meaning some participants overestimated the actual situation.

Software is seen as an important aid for ORM with a 7.9 (of 10 very important) on average in the current situation. In the future software is expected on average to become not less important with a 8.5 (of 10 very important). ORM software does not appear to be a big money market 82% of all organizations spends less than 100k on yearly ORM software. Only a few large banks spend over 100k to a 2 million euros on yearly software fees, including maintenance costs.

Operational Risk Management is important, but not essential for most organizations.

RQ6: " What is the relation between the implementation level of Operational Risk Management and the supporting Business Performance Management technologies? "

Business Performance Management Technologies can be seen as a subset of software related technologies. Therefore the measured software technologies were first analyzed and then scoped back to BPM technologies. Most organizations, 14 of 16 (87,5%) indicated to use dedicated software for ORM, 2 of 16 (12,5%) organizations indicated to rely primarily on self-made excel solutions for risk assessment or reporting. Essentials for ORM software appear to be:

- Possibility for embedding the organization structure or hierarchy in the ORM software
- Qualitative risk assessment scales with high, medium and low risk scores
- Incident registration and internal loss data
- Possibility to add documents and evidence files in the ORM software.

ORM software does not need to include functionality for quantitative risk assessment using simulations and a rich-text editor. These results are both expected, because ORM is not about statistics and a rich-text editor is easy to work around with another text editor.

On average calculated ORM process maturity has a strong (0.78) Pearson correlation with overall BPM technology use. When diving into more detail, the environment, risk identification, risk analysis, risk evaluation and mitigation steps are quite decently correlating with maturity and used technologies. Objective setting and monitoring functionalities appear to be available to organizations with higher maturity scores, but are far from as much used. Risk assessment in general might be too general, because it does not appear to have any relationship with maturity and technologies. No relationship was found for maturity and technologies to aid communication, but this might be explained by the fact that communication is a human process and does not necessarily rely on technology to be successful.

Comparing maturity scores to certain organization characteristics, most turned out to be weak. However the presence of a CRO appears to positively influence the use of technologies. When considering ORM maturity and software the presence of software relates with a higher maturity. While at the same time appears to have an effect on increasing costs and satisfaction of the ORM software. Spending more on technologies to support ORM does appear to pay off, this is also underlined by less need to fall back to self-made spreadsheet solutions.

Results of the assessments reveal there is a relationship between BPM technologies and ORM process maturity. Depending on the level measured this relationship is stronger or weaker. The maturity model and assessment created in this research are conceived by the participants as 75% accurate. Thus to conclude, maturity scores of BPM technologies are mostly related to the correct set of ORM processes.

RQ7: " Which set of Business Performance Management technologies is utilized to support Operational Risk Management processes in different fields? "

The importance of software for operational risk management varies per industry. Healthcare, Transport & infrastructure and the financial services industries utilize most BPM technologies. These Industries using more than 60% BPM technologies appear to be most satisfied with their software solutions for ORM. These same industries also have less need to fall back on using spreadsheet software.

ORM was found most important with an average of 9 out of 10 in the transport industry, especially airline companies consider ORM to be of vital importance for safety of their passengers. This sector is the only sector using exactly as much technologies as having available. this sector achieved the highest ORM maturity scores.

The financial services sector is by far the largest field in this research. On average the importance of ORM is rated a 7.2 out of 10, which is lower than most other industries. This sector is more mature on supporting technologies than any other, but scores average on ORM process maturity

The healthcare industry considers ORM to be very important as well with an 8 of 10. Interestingly the healthcare sector is the only industry where all organizations do not use excel and show the highest technology use, availability and satisfaction.

Retail organizations consider ORM very important with an 8.5 of 10. ORM software in this industry is scarce and most ORM related work is done using spreadsheet solutions. This lead to a low satisfaction of just 25%. Margins in this industry are very low and there is little budget for ORM software.

The energy industry appears to be average on almost all aspects. The average importance of ORM was rated 7.5 out of 10. Not the lowest, but not the highest either. Regarding the use and availability of technologies this industry scores average as well. The entire sector indicated to need spreadsheet solutions while none being fully satisfied with their software solution for ORM. Interestingly they achieved the highest ORM maturity level, but compared to their use of technology they lag the most of all industries.

The production and trade industry was just represented by one organization. Sadly this organization does not consider ORM to be important and does not have dedicated ORM software. This industry is therefore considered not representative and was only included for completeness.

To conclude this research the main research question is now answered, which was stated as:

" How can organizations incrementally improve their Operational Risk Management processes using Business Performance Management technologies? "

There appears to be no strong relationship with ORM process maturity and a specific supporting BPM technologies. This means sets of BPM technologies nor individual software features appear to influence the full extent of organizations - in any industry - to manage their operational risks. From interviews and the assessments, it appears ORM is for a large part still a manual job. Software is mainly used for reasons regarding automation and efficiency.

However, there are some relations with specific sets of BPM technologies found to influence the maturity of Operational Risk Management. Therefore, the maturity model as developed in this research could provide some useful guidelines on the applicability of certain technologies, especially for non-mature industries. The maturity model as developed in this research provides a suitable path with six stages for organization seeking to improve their ORM processes. The six stages provide an instrument to match appropriate technologies to the current stage of maturity and enables organizations to grow in maturity towards enterprise integration and continuous improvement.

9 Discussion

This chapter describes scientific and practical contributions of this research project from the perspective of the author. Additionally remarks and limitations regarding this research are discussed. The discussion is concluded by providing some reasonable directions for future research possibilities.

9.1 Contributions

The author considers this study has a number of scientific as well as practical contributions. From a scientific perspective this research adds to the theoretical domain with a detailed overview of the domain of operational risk management within an enterprise wide and integrated viewpoint. This is complemented with a cross industry perspective including differences in terminology. Additionally ORM specific activities were mapped to generic enterprise risk management frameworks.

An important theoretical contribution is delivered from a technology viewpoint. This research provides a detailed overview of Business Performance Management technologies. Business Performance Management is a domain mainly researched by (Racz, Weippl, & Seufert, 2010), however in this research the supporting technologies related to BPM are described into more detail. Pyramid of BPM is believed to provide an effective summary of BPM and underlying technologies.

The main contribution to the scientific body of knowledge is considered the developed maturity model artefact that is usable for different organizations and provides a basis for more empirical research. No existing maturity model was found, therefore a new maturity model was developed with a perspective not researched before, provides some answers into more detailed and specific technologies that can be used for Operational Risk Management. The maturity model artefact is complemented by an innovative approach to visualizing the maturity model.

This research provides a number of practical contributions as well. The practical results are important since the Design Science approach aims to provide practical contributions via a scientific path. The maturity model as developed in this research provides a first solution towards some of the practical problems with ORM software and via BPM technologies.

BPM technologies are believed to provide a decent solution for current ORM software issues, since alignment with the plan and control cycle and advanced reporting technologies are available. It was unclear whether the full spectrum of Business Performance Management technologies was suitable for improving operational risk management processes and whether the same set of Business Performance Management technologies are applicable for all types of organizations. This research provided more details about the suitability and actual use of BPM related technologies.

Additionally this research provides new - but limited - insights into the actual use and availability of BPM technologies in different industries. However these insights can be used for further empirical research projects and the results provide a kind of ranking about the feasibility or existence of a certain phenomenon as appeared in this research.

9.2 Important remarks concerning the used methods

This section discusses the research approach, used research methods and their remarks. The design science approach as described by Hevner et al. (2004) includes seven guidelines that will be discussed in relation with this research, followed by a discussion on specific research methods.

1. The first guideline of design science is: design as an artefact, meaning the research must produce a viable artefact. The author believes this guideline is successfully followed, since the artefact resulted in a maturity model with corresponding automated self-assessment instrument that is usable by interested people in practice.
2. As second guideline design science should include a technology based solution to a business problems. The author believes the maturity model as developed in this research complies with this guideline. The main business problem appointed by the maturity model artefact is describing suitable technologies to a certain stage of maturity of ORM processes.
3. Guideline 3 Design Evaluation: utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods: Multiple methods used with several moments for validation in this research. The methods are discussed below;
4. Guideline 4 Research contributions: Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies: The chapter of maturity model development rigorously describes how the maturity model is constructed and improved, additionally all results, versions of the models and assessments used as artefact, are available from the appendices.
5. Guideline 5 Research Rigor: Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact. Literature study and validation trough an expert panel as used in this research are believed to satisfy this guideline;
6. Guideline 6 Design as a Search Process: The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment. As much relevant literature as available was consulted, validated by an expert panel. All organizations were visited in person in order to obtain the best quality possible.
7. Guideline 7: Communication of Research: Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences. This research includes some very technical components, however the main results and maturity scores are considered readable and understandable by managers.

The Design Science approach was complemented in this research by a number of specific research methods. Each method has advantages and possible complications:

- Snowballing: method allows for incremental knowledge building as fits with design science;
- Market analysis: decent sample of 65 products. Counted single appearances of features that resulted in a reliable set of features. For more detailed market analysis more time is required;
- Expert panel: Good method for validation and embedding expert knowledge. A critical note is that only experts from a financial services background were present, a more diverse expert panel might have been better, however was not available within a reasonable timeframe;
- Interviews: Interviews provided very important detailed context information;
- Assessments: appeared to be long but effective instruments for communication with the participants. The real time results after completing the assessment provided the author with an additional moment for validation and feedback.

9.3 Limitations regarding Quality and reliability

This research is mostly qualitative in nature, therefore generalizations are limited. However, some new insights were explored via the Design Science approach by using different methods. Some decisions are made to maintain consistent quality, while some quality issues remained present.

Considering the general research design it is important to note; the selection criteria was not based on factual information, but merely own interpretation. Although this is not a requirement for this type of qualitative research, the results might be different when applying these criteria.

Only on Dutch organizations participated in this research. Results might not specifically true in other countries. The financial services industry is mostly harmonized in Europe by the EU regulations, but especially other sectors might result in severe differences in other countries and might be influenced by different aspects such as laws, regulations and culture.

During maturity model development the market research was limited to 65 products. However, there is not validation of the taken sample to be complete and representative for the whole ORM software market. The ORM software market size is unknown. Additionally only unique occurrences were included, while a more detailed analysis could have led to a weight in the amount of appearances. Although it should be noted, the results in this research are validated using an expert panel.

The expert panel served the purpose of validation and ranking of identified software features. The size of the expert panel was limited. Experts were only involved in one sector. Furthermore 5 experts were considered sufficient, however 8 or more experts would have been better. During the expert panel the range voting method was used. Although this method allowed for sufficient answers, this is not a Delphi method with full anonymity. There is no guarantee the expert panel was unbiased regarding their answers. However, a Delphi expert panel would have consumed too much time. Some bias was prevented using an anonymous voting system and holding a discussion afterwards.

A clear limitation of this research is the sample size. This situation puts limits on considering any generalizations. At this moment no real generalizations can be made, however there is still room for refining the reliability and validity of the scales of the maturity model. According to Hoyle (1999) a small sample as in this research for a Pearson r correlation does not have to be a problem for qualitative research (because you do not test a hypothesis) and when being aware of the fact that small samples are less reliable and do never reach a significance level lower than .05. Additionally the results in this research should not be seen as evidence, but as directions for future empirical research.

Not all answers as given by the participants appear to be reliable, for example one organization in the financial services industry indicated around 250 people are involved with ORM on a full time basis, this organization is much smaller than the largest bank in this research with 60 FTE dedicated to ORM.

One organization provided a participant appeared to be uncappable of providing sufficient answers during the interviews. This organization was left out due to missing results on several parts of the assessment and on request did not provide additional answers via email. The production and trade industry utilized the least BPM technologies of all participating industries. However, this result only reflects one particular organization, not using any software for ORM. Production & trade results should not be considered representative for this specific industry, because they are from one organization.

9.4 Future research

As this research provides some answers to unanswered questions, all research leads to new research possibilities. Therefore this section provides some future research directions. First some complementary research directions are discussed as possible direct result from this research. Followed by some new hypothetical research directions.

To start, more details are required regarding specific BPM technologies and specific industries. The goal of this research was to explore and detail a new maturity model. Larger samples are needed for further validation of the research model. Additionally, additional research should lead to further improvement of the maturity model. The current ranking appeared to relate with maturity, however this ranking appears not to be perfect on all parts, especially Improvement of the maturity model on risk assessment and communication features there is some confusion.

More research into different sectors, there appears to be a difference between industries but the samples for each industry are too shallow for real conclusions. For example the adaptation for different sectors. The integrated Safety Management System (ISMS) is required by regulators in the aviation industry. ISMS was added as experimental option in this maturity model, however the actual applicability should be researched in more detail.

BPM technologies are a very good fit with 94% match, but appear not to be the complete answer for supporting ORM. possibilities for process modelling and file/document management are not (often) included in BPM solutions. More detailed research could be performed into the consequences when missing out on these features and the possibilities of integration of this data using ETL.

One of the participants suggested maintainability of tooling for ORM is an issue. This suggestion could be related to dissatisfaction, complaints about user-friendliness and mismatch between tooling and ORM as described in this research.

During some of the interviews a clear cost benefit relationship of ORM was preferred but was described to be difficult. Although the motivation is often to prevent significant damage and failure, most organizations appear to have difficulties expressing operational risk in money.

Additionally this research lead to some possible new research directions, with reasonable indications towards the following relationships:

- Larger organizations (in terms of FTE) take ORM more seriously or is it about requirements for larger organizations?
- Competitive pressure more of an issue for organizations with less technology used?
- CRO has a positive effect on software use?
- The presence of an ORM committee negatively influences maturity?
- More expensive tooling results in higher maturity?
- There is a strong indication about satisfaction, can it be proven that satisfaction of ORM software really relates with higher ORM maturity and more ORM software use?
- Strong indication of a relationship between the presence of tooling and ORM maturity?
- Organizations using dedicated ORM software have less need to use excel based solutions?

References

Abbaspour, M., Toutounchian, S., Roayaei, E., & Nassiri, P. (2012). A strategic management model for evaluation of health, safety and environmental performance. *Environmental monitoring and assessment*, 2981-2991.

Adamson, C. (2012). *Mastering data warehouse aggregates: solutions for star schema performance.* Hoboken, New Jersey, USA: John Wiley & Sons.

Aho, M. (2009). *A Capability Maturity Model for Corporate Performance Management, an Empirical Study in Large Finnish Manufacturing Companies.* Logica.

Alexander, C. (2003). *Operational risk: regulation, analysis and management.* London, England, UK: Pearson Education.

AMR Research. (2006). *Business Intelligence/Performance Management Maturity Model, Version 2.* Boston, Massachusetts, USA: AMR Research.

Arnold, V., Benford, T., Canada, J., & Sutton, S. G. (2015). Leveraging integrated information systems to enhance strategic flexibility and performance: The enabling role of enterprise risk management. *International Journal of Accounting Information Systems*(19), 1-16.

Ashton, R. (1986). Combining the judgment of experts: How many and which ones? *Organizational Behavior and Human Decision Processes*, 405–414.

Azvine, B., Cui, Z., Majeed, B., & Spott, M. (2007). Operational risk management with real-time business intelligence. *BT technology Journal, 25*(1), 154-167.

BaFin. (2016). *Solvency I.* Retrieved from German Federal Financial Supervisory Authority: https://www.bafin.de/EN/Aufsicht/VersichererPensionsfonds/Aufsichtsregime/SolvencyI/solvency_I_node_en.html

Baird, I. S., & Thomas, H. (1985). Toward a contingency model of strategic risk taking. *Academy of management Review*(10), 230-243.

Basel Committee. (2001). *Definition of operational risk.* Basel, Switzerland: Bank of International Settlements.

Basel Committee. (2002). *Operational Risk Data Collection.* Retrieved from Bank of International Settlements: http://www.bis.org/bcbs/qis/oprdata.pdf

Basel Committee. (2003). *Sound Practices for the Management and Supervision of Operational Risk.* Retrieved from Bank of International Settlements: http://www.bis.org/publ/bcbs96.pdf

Basel Committee. (2011). *Principles for the Sound Management of Operational Risk.* Basel, Switzerland: Bank of International Settlements.

Basel Committee. (2013). *Basel III phase-in arrangements.* Retrieved from Bank of International Settlements: http://www.bis.org/bcbs/basel3/basel3_phase_in_arrangements.pdf

Basel Committee. (2014, October). *Operational risk – Revisions to the simpler approaches.* Retrieved from Bank of International Settlements: http://www.bis.org/publ/bcbs291.pdf

Basel Committee. (2015). *A brief history of the Basel Committee.* Retrieved from Bank of International Settlements: http://www.bis.org/bcbs/history.pdf

Basel Committee. (2016, March). *Standardised Measurement Approach for operational risk.* Retrieved from Bank of International Settlements: http://www.bis.org/bcbs/publ/d355.pdf

BDO. (2008). *Operational Risk Management Maturity Model.* Madrid, Spain: BDO Audiberia.

Beasley, M., Chen, A., Nunez, K., & Wright, L. (2006). Working hand in hand: Balanced scorecards and enterprise risk management. *Strategic Finance, 87*(9), 49-55.

Bititci, U. S., Turner, U., & Begemann, C. (2000). Dynamics of performance measurement systems. *International Journal of Operations & Production Management*, 692-704.

Blunden, T., & Thirlwell, J. (2012). *Mastering Operational Risk: A practical guide to understanding operational risk and how to manage it.* London, UK: Pearson.

Bog, A., Sachs, K., & Zeier, A. (2011). Benchmarking database design for mixed OLTP and OLAP workloads. *2nd ACM/SPEC International Conference on Performance engineering* (pp. 417-418). Karlsruhe, Germany: Association for Computing Machinery.

Boynton, A. C., & Zmud, R. W. (1984). An assessment of critical success factors. *Sloan management review*, 17-27.

Breden, D. (2006). Managing operational risk in a continuously changing environment. In P. Heikkinen, & K. Korhonen, *Technology-driven efficiencies in financial markets* (p. 137). Helsinki, Finland: Bank of Finland.

Breslin, M. (2004). Data warehousing battle of the giants. *Business Intelligence Journal, 7*, 6-20.

Carr, M. J., Konda, S. L., Monarch, I., Ulrich, F. C., & Walker, C. F. (1993). *Taxonomy-based risk identification.* Pittsburgh, PA, USA: Carnegie-Mellon University.

Chaudhuri, S., & Dayal, U. (1997). An overview of data warehousing and OLAP technology. *ACM Sigmod record*, 65-74.

Chernobai, A. S., Rachev, S. T., & Fabozzi, F. J. (2008). *Operational risk: a guide to Basel II capital requirements, models, and analysis* (Vol. 180 ed.). Hoboken, New Jersey, USA: John Wiley & Sons.

Chrissis, M. B., Konrad, M., & Shrum, S. (2003). *CMMI guidlines for process integration and product improvement.* London, UK: Longman Publishing .

Coca, D., de Blas, R., Gallejones, C., Moral, R., Calvo, J., Álvarez, J., & del Canto, Á. (2014). *Operational Risk Management in the energy industry.* Madrid, Spain: Management Solutions.

Cohen, M. A., & Kunreuther, H. (2007). Operations risk management: overview of Paul Kleindorfer's contributions. *Production and Operations Management*, 525-541.

Cokins, G. (2004). *Performance management: finding the missing pieces (to close the intelligence gap).* Hoboken, New Jersey, USA: John Wiley & Sons.

Cope, E., & Labbi, A. (2008). Operational loss scaling by exposure indicators: evidence from the ORX database. *Journal of Operational Risk*, 25-46.

Cornalba, C., & Giudici, P. (2004). Statistical models for operational risk management. *Physica A: Statistical Mechanics and its applications, 338*(1), 166-172.

COSO. (2004). *Enterprise Risk Management - Integrated Framework.* Committee of Sponsoring Organizations of the Treadway Comission.

Crenshaw, T. L., Robinson, C. L., Ding, H., Kumar, P. R., & Sha, L. (2006). A Pattern for Adaptive Behavior in Safety-Critical, Real-Time Middleware. *IEEE Real-Time Systems Symposium*, pp. 127-136.

Davies, J., Finlay, M., McLenaghen, T., & Wilson, D. (2006). Key risk indicators–their role in operational risk management and measurement. *AMA Approaches to operational risk* (pp. 1-32). Prague: RiskBusiness International.

De Bruin, T., & Rosemann, M. (2005). Towards a business process management maturity model. *ECIS 2005 Proceedings of the Thirteenth European Conference on Information Systems*, (pp. 26-28). Regensburg, Germany.

De Nederlandsche Bank - DNB. (2014). *Assessment Framework for Information Security.* Amsterdam, The Netherlands: De Nederlandsche Bank.

Deloitte. (2015). *Enterprise Risk Management A 'risk-intelligent'approach.* London, United Kingdom: Deloitte Risk Advisory.

Deloitte. (2015). *Five trends shaping the future.* København, Denmark: Deloitte.

Dentchev, N. A., Heene, A., & Gosselin, D. P. (2005). *Integrating corporate social responsibility in business models.* Ghent, Belgium: Hoveniersberg: Ghent University.

Desender, K. A. (2007). On the determinants of enterprise risk management implementation. *ENTERPRISE IT GOVERNANCE, BUSINESS VALUE AND PERFORMANCE MEASUREMENT*, 1-25.

Doerig, H. U. (2000). *Operational Risks in Financial Services.* London, UK: International d'Etudes Bancaires.

Doran, G. T. (1981). There's a S.M.A.R.T. way to write management's goals and objectives. *Management Review*, 35–36.

Doucette, J. N. (2006). View from the cockpit: what the airline industry can teach us about patient safety. *Nursing*, 50-53.

Eckerson, W. W. (2010). *Performance dashboards: measuring, monitoring, and managing your business.* Hoboken, New Jersey, USA: John Wiley & Sons.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI magazine*, 37-54.

Fernández-Muñiz, B., Montes-Peón, J. M., & Vázquez-Ordás, C. J. (2009). Relation between occupational safety management and firm performance. *Safety science*, 980-991.

Fontnouvelle, P., DeJesus-Rueff, V., Jordan, J., & Rosengren, E. (2003). *Using Loss Data to Quantify.* Boston, MA, USA: Federal Reserve Bank of Boston.

Fraser, J., & Simkins, B. J. (2008). A brief history of risk management. In Fraser, & Simkins, *Enterprise Risk Management* (pp. 19-29). Hoboken, NJ, USA: John Wiley & Sons, Inc.

Fraser, J., Simkins, B., & Narvaez, K. (2014). *Implementing enterprise risk management: Case studies and best practices.* Hoboken, New Jersey, USA: John Wiley & Sons.

Fraser, P., Moultrie, J., & Gregory, M. (2002). The use of maturity models/grids as a tool in assessing product development capability. *Engineering Management Conference, 2002* (pp. 244-249). Cambridge, UK: IEEE.

Frolick, M. N., & Ariyachandra, T. R. (2006). Business performance management: One truth. *IS Management*, 41-48.

Galesic, M., & Bosnjak, M. (2009). Effects of questionnaire length on participation and indicators of response quality in a web survey. *Public opinion quarterly*, 349-360.

Gartner. (2008). *Maturity Model for Business Intelligence and Performance Management.* Stamford, CT, USA: Gartner Inc.

Gatzert, N., & Martin, M. (2015). Determinants and value of enterprise risk management: empirical evidence from the literature. *Risk Management and Insurance Review*, 29-53.

Gillan, S., & Starks, L. T. (1998). A survey of shareholder activism: Motivation and empirical evidence. *Contemporary Finance Digest*, 10-34.

Girling, P. (2013). *Operational risk management: a complete guide to a successful operational risk framework.* Hoboken, New Jersey, USA: John Wiley & Sons.

Golfarelli, M., Rizzi, S., & Cella, I. (2004). Beyond data warehousing: what's next in business intelligence? *Proceedings of the 7th ACM international workshop on Data warehousing and OLAP* (pp. 1-6). ACM.

Gordon, L. A., Loeb, M. P., & Tseng, C. Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy, 28*(4), 301-327.

Grote, G. (2012). Safety management in different high-risk domains–All the same? *Safety Science*, 1983-1992.

Hackathorn, R. (2004). Real-time to real-value. *Information Management*, 24.

Haimes, Y. Y. (2015). *Risk modeling, assessment, and management.* Hoboken, New Jersey, USA: John Wiley & Sons.

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems*, 87-92.

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly, 28*(1), 75-105.

Hillson, D. A. (1997). Towards a risk maturity model. *The International Journal of Project & Business Risk Management*, 35-45.

Hoffman, D. G. (2002). *Managing operational risk: 20 firmwide best practice strategies.* Hoboken, New Jersey, USA: John Wiley & Sons.

Hoyle, R. H. (1999). *Statistical strategies for small sample research.* Sage.

Hsu, C. C., & Sandford, B. A. (2007). The Delphi technique: making sense of consensus. *Practical assessment, research & evaluation, 12*(10), 1-8.

Humphrey, W. S. (1988). Characterizing the software process: A maturity framework. *IEEE Software*, 73–79.

Hussain, A. (2000). *Managing operational risk in financial markets.* Oxford, UK: Butterworth-Heinemann.

IBM. (2014). *Big Data & Analytics Maturity Model.* Armonk, New York, USA: IBM.

ICAO. (2013). *Safety Management Doc 9859.* Montréal, Quebec, Canada: International Civil Aviation Organization.

IRM. (2010). *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000.* London, UK: Institute for Risk Management.

ISO. (2009a). *ISO 31000 Risk management - Principles and guidelines.*

ISO. (2009b). Risk Management Vocabulary. *Guide 73* (p. 1). Geneva, Switzerland: International Organization for Standardization.

ISO. (2009c). *ISO 31010 Riskmanagement and Risk assessment techniques.* Geneva, Switzerland: International Organization for Standardization.

Jones, S., Kirchsteiger, C., & Bjerke, W. (1999). The importance of near miss reporting to further improve safety performance. *Journal of Loss Prevention in the process industries*, 59-67.

Kaplan, R., & Norton, D. (1992). Balanced scorecard: measures that drive performance. *Harvard Business Review*, 71-79.

Kauppila, O., Härkönen, J., & Väyrynen, S. (2015). INTEGRATED HSEQ MANAGEMENT SYSTEMS: DEVELOPMENTS AND TRENDS. *International Journal for Quality Research*, 231–242.

Kavakr, F., & Spiegel, A. D. (2004). Risk management in health care institutions A strategic approach. *Journal for Healthcare Quality*, 2656-8.

Kenett, R. S., & Raanan, Y. (2011). *Operational Risk Management: a practical approach to intelligent data analysis.* Hoboken, NJ, USA: John Wiley & Sons.

Kleffner, A. E., Lee, R. B., & McGannon, B. (2003). The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. *Risk Management and Insurance Review*, 53-73.

Kloman, H. (1990). Risk management agonists. *Risk Analysis*(10), 201-205.

Koller, G. (2005). *Risk assessment and decision making in business and industry: A practical guide.* Boca Raton, Florida, USA: CRC Press.

Lam, J. (2014). *Enterprise risk management: from incentives to controls.* Hoboken, New Jersey, USA: John Wiley & Sons.

Lancaster, S. (2015). *Operational Risk Management.* Los Gatos, CA, USA: Smashwords Inc.

Lebas, M. (1995). Performance measurement and performance management. *International Journal of Production Economics*(41), 23-35.

Levene, M., & Loizou, G. (2003). Why is the snowflake schema a good data warehouse design? *Information Systems, 28*(3), 225-240.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk management and insurance review*, 37-52.

Linstone, H. A., & Turoff, M. (2002). *The Delphi Method. Techniques and applications.* Reading, Massachusetts, USA: Addison-Wesley.

Loader, D. (2011). *Operations risk: managing a key component of operational risk.* Butterworth-Heinemann.

Lopes, L. L. (1987). Between hope and fear: The psychology of risk. *Advances in experimental social psychology*(20), 255-295.

MacCrimmon, K. R., & Wehrung, D. A. (1990). Characteristics of risk taking executives. *Journal of Management Science, 36*(4), 422-435.

Malik, S. A., & Holt, B. (2013). Factors that affect the adoption of Enterprise Risk Management (ERM). *OR Insight, 26*(4), 253-269.

Marr, B. (2004). *Business performance management: current state of the art. A survey report.*

Marr, B. (2009). *Managing and delivering performance.* Routledge.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think.* Boston, Massachusetts, USA: Houghton Mifflin Harcourt.

McCormack, K., Willems, J., Van den Bergh, J., Deschoolmeester, D., Willaert, P., Štemberger, M., . . . Vlahovic, N. (2009). A global investigation of key turning points in business process maturity. *Business Process Management Journal, 15*(5), 792-815.

McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management: Concepts, techniques and tools.* Princeton, New Jersey, USA: Princeton University Press.

Melchert, F., & Winter, R. (2004). The enabling role of information technology for business performance management.

Melchert, F., Winter, R., & Klesse, M. (2004). Aligning process automation and business intelligence to support corporate performance management. *Proceedings of the Tenth Americas Conference on Information Systems*, (pp. 4053-4063). New York City, NY, USA.

Mensah, L. D., & Julien, D. (2011). Implementation of food safety management systems in the UK. *Food Control*, 1216-1225.

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business logistics, 22*(2), pp. 1-25.

Meulbroek, L. K. (2002). A senior manager's guide to integrated risk management. *Journal of Applied Corporate Finance, 14*(4), 56-70.

Miller, K. D. (1992). A framework for integrated risk management in international business. *Journal of international business studies, 23*(2), 311-331.

Mitra, S., Karathanasopoulos, A., Sermpinis, G., Dunis, C., & Hood, J. (2015). Operational risk: Emerging markets, sectors and measurement. *European Journal of Operational Research, 24*(1), 122-132.

Moody, D. L., & Kortink, M. A. (2000). From enterprise models to dimensional models: a methodology for data warehouse and data mart design. *Data Mining and Data Warehousing*, 5-11.

Moosa, I. A. (2007). Operational risk: a survey. *Financial markets, institutions & instruments, 16*(4), 167-200.

Morrison, S., & Winston, C. (2010). *The evolution of the airline industry.* Washington, DC, USA: Brookings Institution Press.

Moseley III, G. B. (2013). *Managing Legal Compliance in the Health Care Industry.* Burlington, Massachusetts, USA: Jones & Bartlett Publishers.

Mowbray, A., & Blanchard, R. (1961). *Insurance.* New York, USA: McGraw-Hill Book Company.

Neely, A., Gregory, M., & Platts, K. (1995). Performance measurement system design: a literature review and research agenda. *International journal of operations & production management, 15*(4), 80-116.

Nissen, V., & Marekfia, W. (2013). Towards a research agenda for strategic governance, risk and compliance (GRC) management. *Business Informatics (CBI)* (pp. 1-6). Vienna, Austria: IEEE.

Nolan, R. (1973). Managing the computer resource: A stage hypothesis. *Communications of the ACM*, 399–405.

Nyenrode Business University. (2014). *Tweede Nationaal Onderzoek Risicomanagement in Nederland.* Breukelen, The Netherlands: Nyenrode Business University.

OCEG. (2015). *The 2015 GRC Maturity Survey Report.* Scottsdale, AZ, USA: Open Compliance & Ethics Group.

OCEG. (2017). *GRC Defined.* Retrieved from Open Compliance & Ethics Group: http://www.oceg.org/about/what-is-grc/

Ofek, E., & Richardson, M. (2003). Dotcom mania: The rise and fall of internet stock prices. *The Journal of Finance*, 1113-1137.

Olson, D. L., & Wu, D. D. (2015). *Enterprise risk management* (Vol. 3 ed.). Singapore, Singapore: World Scientific Publishing Co Inc.

Olson, E. M., Slater, S. F., & Hult, G. T. (2005). The importance of structure and process to strategy implementation. *Business horizons*, 47-54.

Oxford English Dictionary. (2017). *Definition of risk in English.* Retrieved from Oxford English Dictionaries: https://en.oxforddictionaries.com/definition/risk

Paape, L., & Speklè, R. F. (2012). The adoption and design of enterprise risk management practices: An empirical study. *European Accounting Review*, 533-564.

Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. *Journal of risk and insurance*, 185-211.

Panjer, H. H. (2006). *Operational risk: modeling analytics.* Hoboken, NJ, USA: John Wiley & Sons.

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE software*, 18-27.

Peter, M. (2010). *Positioning GRC and ERM.* New York, USA: Risk Management Society.

Popov, G., Lyon, B. K., & Hollcroft, B. (2016). *Risk assessment: A practical guide to assessing operational risks.* Hoboken, New Jersey, USA: John Wiley & Sons.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty.* London, UK: Demos.

Power, M. (2005). The invention of operational risk. *Review of International Political Economy*, pp. 577-599.

Power, M. (2009). The risk management of nothing. *Accounting, organizations and society, 34*(6), 849-855.

Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. *Risk analysis, 30*(6), 881-886.

PwC. (2012). *Operational issues of Risk Management.* Paris, France: PwC.

Racz, N., Weippl, E., & Seufert, A. (2010). A frame of reference for research of integrated GRC. In B. De Decker, & I. Schaumüller-Bichl (Ed.), *Communications and Multimedia Security 2010 Proceedings. 11*, pp. 106–117. Berlin, Germany: Springer.

Racz, N., Weippl, E., & Seufert, A. (2011). Governance, risk & compliance (GRC) software-an exploratory study of software vendor and market research perspectives. *System Sciences (HICSS)* (pp. 1-10). 44th Hawaii International Conference: IEEE.

Rahimi, M. (1995). Merging strategic safety, health and environment into total quality management. *International Journal of Industrial Ergonomics*, 83-94.

Ramanujan, S., & Kesh, S. (2004). Comparison of knowledge management and CMM/CMMI implementation. *Journal of American Academy of Business*, 271-275.

Renn, O. (1992). *Concepts of risk: a classification.*

RIMS. (2006). *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management.* New York, NY, USA: Risk and Insurance Management Society (RIMS).

Risk Management Society. (2016). *What is ERM?* Retrieved from RIMS - The Risk Management Society: https://www.rims.org/ERM/Pages/WhatisERM.aspx

Rosenberg, J. V., & Schuermann, T. (2006). A general approach to integrated risk management with skewed, fat-tailed risks. *Journal of Financial economics*(79(3)), 569-614.

Royce, W. (2002). CMM vs. CMMI: From conventional to modern software management. *The Rational Edge*, 2-9.

RSA Archer. (2015). *Maturity Model for Operational Risk Management.* Bedford, MA, USA: RSA EMC Corporation.

Sadgrove, K. (2016). *The complete guide to business risk management.* Abingdon-on-Thames, UK: Routledge.

Samad-Khan, A. (2005). Why COSO is flawed. *Operational Risk, 6*(1), 24-28.

Samsonowa, T. (2011). *Industrial research performance management: Key performance indicators in the ICT industry.* Heidelberg, Germany: Springer Science & Business Media.

Sarawagi, S., Agrawal, R., & Megiddo, N. (1998). Discovery-driven exploration of OLAP data cubes. *Extending Database Technology* (pp. 168–182). Berlin, Germany: Springer Verlag.

Sarbanes, P., & Oxley, M. (2002). *Sarbanes–Oxley Act Corporate responsibility. Public Law 107-204.* Retrieved from U.S. Government Printing Office: https://www.gpo.gov/fdsys/pkg/PLAW-107publ204/html/PLAW-107publ204.htm

Scandizzo, S. (2005). Risk mapping and key risk indicators in operational risk management. *Economic Notes, 34*(2), 231-256.

Schreurs, J., Roox, D., & Moreau, R. (2004). A data warehouse system in business performance management in SME's. EUROSIS.

Schwert, G. (1990). Stock volatility and the crash of'87. *Review of financial Studies*, 77-102.

Sharda, R., Delen, D., & Turban, E. (2014). *Business Intelligence A Managerial Perspective on Analytics.* Pearson Education Limited.

Shtub, A., & Karni, R. (2010). Business process improvement. In A. Shtub, & R. Karni, *ERP* (pp. 217-254). USA: Springer.

Simkins, B., & Ramirez, S. A. (2007). Enterprise-wide risk management and corporate governance. *Loyola University Chicago Law Journal*(39), 571.

Simons, R. (2002). *Performance Measurement and Control Systems for Implementing Strategy.* Upper Saddle River, New Jersey, USA: Prentice Hall.

Society, R. M. (2017). *Risk Management Benchmarking and Progress.* Retrieved from The Risk Maturity Model: http://riskmaturitymodel.org/rims-risk-maturity-model-rmm-for-erm/

Spikin, I. C. (2013). Risk Management theory: the integrated perspective and its application in the public sector. *Estado, Gobierno y Gestión Pública*, 89.

Tabaksblat, M. (2003). *Code Tabaksblat.* Retrieved from Rijksoverheid: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/richtlijnen/2003/12/09/code-tabaksblat/code-tabaksblat.pdf

Tadayon, M., Jaafar, M., & Nasri, E. (2012). An assessment of risk identification in large construction projects in Iran. *Journal of Construction in Developing Countries*(17(1)), 57-69.

Tarantino, A. (2008). *Governance, risk, and compliance handbook: technology, finance, environmental, and international guidance and best practices.* Hoboken, New Jersey, USA: John Wiley & Sons.

Tattam, D. (2011). *A short guide to operational risk.* Farnham, UK: Gower Publishing, Ltd.

Tranchard, S. (2015). *The revision of ISO 31000 on risk management has started.* Geneva, Switzerland: International Organization for Standardization. Retrieved from http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1963

U.S. Department of Energy. (2014). *Cybersecurity Capability Maturity Model (C2M2).* Washington, D.C., USA: U.S. Department of Energy. Retrieved from https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

Van der Schaaf, T. W., Lucas, D. A., & Hale, A. R. (2013). *Near miss reporting as a safety tool.* Oxford, United Kingdom: Butterworth-Heinemann.

Väyrynen, S., Jounila, H., & Latva-Ranta, J. (2014). HSEQ assessment procedure for supplying industrial network: a tool for implementing sustainability and responsible work systems into SMES. *Advances in Safety Management and Human Factors*, 10.

Vogt, W. P. (1990). *Dictionary of Statistics and Methodology: A Nontechnical Guide for the Social Sciences.* London, United Kingdom: Sage.

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and software technology*, 1317-1339.

Wettstein, T., & Kueng, P. (2002). A maturity model for performance measurement systems. *WIT Transactions on Information and Communication Technologies*, 113-122.

White, T. (2012). *Hadoop: The definitive guide.* Sebastopol, California, USA: O'Reilly Media, Inc.

Yuan, H., Mahdavi, M., & Paul, D. (2011). Security: Digital Oil Field or Digital Nightmare? *Journal of Petroleum Technology*, 16-18.

Zarnowitz, V. (1992). Composite indexes of leading, coincident, and lagging indicators. *Business Cycles: Theory, History, Indicators, and Forecasting*, 316-356.

Appendices

PUBLIC available appendices:

Appendix A: Short Proposal

Appendix B: Market Analysis Features Defined

Appendix C: Expert Panel votes / scores

Appendix D: Initial maturity model & assessment

Appendix E: Interview Protocol

Appendix F: Coding tree, code definitions

Appendix G: Improved assessment Questions + Logic

Appendix H: Some additional data sets

For some specific people, CONFIDENTIAL files are available:

Appendix 1: List of expert panel participants

Appendix 2: List of interview participants

Appendix 3: Full set with structured interview results

Appendix 4: Interview transcripts

Appendix 5: Assessment results, filled actual data improved version

Appendix 6: MAX-QDA v12 files

Appendix 7: Correlation data sets

Appendix A: Short proposal

Appendix B: Market Analysis Features Defined

Appendix C: Expert panel results

Scores – ORM process Quick Scan (7)

Suitable to measure process maturity (partial or fully)?	0 No vote	1 Not suitable	2 Somewhat suitable	3 Suitable	4 Very suitable
1 Is an operational risk management process present and executed?			2	3	
2 Process implementation or maturity level per process-step				1	4
3 Importance of (Operational) Risk Management process		1	1	3	
4 Frequency of execution (Operational) Risk Management process		1	3	1	
5 Frequency of execution validation (Operational) Risk Management process			3	1	
6 Frequency of effectiveness validation (Operational) Risk Management process		1	3	1	
7 Involved roles and amount of roles involved with ORM			2	3	

Scores – A - Environment functionalities (5)

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
A1 – Organization structure or hierarchy		4	1		
A2 – Ownership & Responsibilities		3	2		
A3 – Business processes entries		1	3	2	
A4 – Process documentation & policy documents		1	1	3	
A5 – Process flow modelling			2	3	

B - Objective setting functionalities (4)

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
B1 – Risk appetite settings			3	2	
B2 – Library / catalogue with rules from laws & regulations for compliance			2	3	
B3 – Risk profile criteria		1	1	3	
B4 – Organization objectives (scorecard or KPIs)		2		3	

C - Risk assessment general (16)

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
C1 – Qualitative scales (low, medium, high)		3	1	1	
C2 – Risk Register		3	2		
C3 – Filter & Sort Risk Register		3	1	1	
C4 – Risk (type) categories		3	2		
C5 Risk assignment to individual (business) process activities		5			
C6 – Current risk status dashboard		3	1	1	
C7 – Risks are assigned to entire business process, not its individual activities		2	3		
C8 – Risk Library or catalogue (RCSA)		1	3	1	
C9 – Configurable risk assessment period		2	3		
C10 – Semi-qualitative risk assessments			2	3	
C11 – Risks related to asset		1		3	1
C12 – Risks related to Business Unit			2	3	
C13 – Risks related to other risks (causal)				4	1
C14 – Risks related to organization objectives			1	3	1
C15 – Survey management		1		4	
C16 – Quantitative risk assessments				1	4

D - Risk assessment specifically for Risk identification (6)

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
D1 – Incident reporting			4		1
D2 – Internal loss register (loss data)			3	2	
D3 – CRSA Control and Risk Self-Assessment			4	1	
D4 – Brainstorming			2	3	

D5 – External loss data or incident data			1	3	1
D6 – Mobile incident reporting				2	3

E - Risk assessment features specifically for Risk analysis (7)

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
E1 – Risk matrix for comparing risk profiles		4	1		
E2 – Risk source		3		2	
E3 – Risk causal modelling			3	2	
E4 – CRSA Control and Risk Self-Assessment		1	3	1	
E5 – Risk voting			1	4	
E6 – Bow Tie method			1	3	1
E7 – Waterfall Analysis				2	3

F - Risk assessment specifically for Risk evaluation (5)

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
F1 – Risk profile evaluation and calculation				5	
F2 – Risk profile comparison using visualization				3	2
F3 – Risk profile comparison numeric			1	3	1
F4 – Bow Tie method				4	1
F5 – Risk / Scenario simulation				1	4

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
G1 – Risk reducing measures, with reduction factor		4	1		
G2 – mitigating measure execution & planning		4	1		

G3 – Documents and evidence files		3	2		
G4 – Overview status/effectiveness mitigating measures		4	1		
G5 – Issue register & action planning		3	1	1	
G6 – mitigating measures testing - Control self-assessment (CSA)			3	2	
G7 – Action tracking		2	3		
G8 – Selecting relevant mitigating measures		1	1	3	

Software functionalities	**0 No vote**	**1 Basic for ORM**	**2 Important for ORM**	**3 Usable for ORM**	**4 Advanced or Optional**
H1 – Audit planning & sample based checking		3	1	1	
H2 – History of changes (audit trail)		2	3		
H3 – Overview monitoring status & Compliance			4	1	

Software functionalities	**0 No vote**	**1 Basic for ORM**	**2 Important for ORM**	**3 Usable for ORM**	**4 Advanced or Optional**
I1 – Tasks in software		3	1		1
I2 – Automated workflow		4	1		
I3 – Task overview		3	2		
I4 – Review		2	3		
I5 – On screen notifications		1	4		
I6 – Email notifications		1	3	1	
I7 – Dynamic dashboards & reporting		2	3		
I8 – Ad-hoc reporting			2	3	

Software functionalities	0 No vote	1 Basic for ORM	2 Important for ORM	3 Usable for ORM	4 Advanced or Optional
X1 – Data import from Excel		3	1	1	
X2 – Data export to other systems		3	2		
X3 – Data import from operational systems			4	1	
X4 – Data export to Excel		2	3		
X5 – One click export to MS Office			4		1
X6 – Rich text-editor				3	2

Appendix H:

Indicated income	amount	percent
100m - 500m	4	25%
500m - 1b	4	25%
1b - 5b	4	25%
5b - 10b	2	12,50%
10b - 50b	2	12,50%

FTE Range	amount	percent
500 - 1000	1	6%
50000 - 100000	1	6%
10000 - 50000	3	19%
1000 – 5000	11	69%

Role	*Appearance*	*Percent*
head	*5*	*31%*
advisor/consultant	*5*	*31%*
Specialist	*3*	*19%*
manager	*1*	*6%*
architect	*1*	*6%*
analyst	*1*	*6%*

Title	*Appearance*	*Percent*
risk	*8*	*50%*
operational risk	*7*	*44%*
safety	*6*	*38%*
quality	*5*	*31%*
Change	*1*	*6%*
Preservation	*1*	*6%*
GRC Global	*1*	*6%*
security	*1*	*6%*

Organization & industry	*Yearly ORM software license fees*	*FTE dedicated for ORM*	*No of involved roles*

Energy 1	*50k-100k*	*5-10*	*10-25*
Energy 2	*50k-100k*	*5-10*	*5-10*
Financial services 1	*50k-100k*	*1-5*	*10-25*
Financial services 2	*50k-100k*	*200-250*	*1-5*
Financial services 3	*500k - 1mil*	*1-5*	*1-5*
Financial services 4	*2 mil*	*50-75*	*1-5*
Financial services 5	*25k - 50k*	*1-5*	*1-5*
Financial services 6	*0 – 25k*	*1-5*	*5-10*
Healthcare 1	*50k-100k*	*10-25*	*1-5*
Healthcare 2	*25k - 50k*	*10-25*	*1-5*
Production & trade 1	*50k-100k*	*10-25*	*5-10*
Retail & consumer goods 1	*200k*	*5-10*	*5-10*
Retail & consumer goods 2	*0 – 25k*	*10-25*	*1-5*
Transport & Infrastructure 1	*25k - 50k*	*5-10*	*1-5*
Transport & Infrastructure 2	*25k - 50k*	*5-10*	*1-5*
Transport & Infrastructure 3	*50k-100k*	*10-25*	*1-5*

Energy 1	*43%*	*59%*	*4*	*3*	*7*	*7,1*
Energy 2	*54%*	*44%*	*5*	*4*	*8*	*7,8*
Financial services 1	*33%*	*61%*	*3*	*3*	*3*	*9*
Financial services 2	*69%*	*86%*	*4*	*4*	*7*	*8,2*
Financial services 3	*75%*	*78%*	*5*	*5*	*9*	*8*
Financial services 4	*88%*	*88%*	*5*	*5*	*8*	*7,7*
Financial services 5	*63%*	*86%*	*2*	*3*	*8*	*9,6*
Financial services 6	*45%*	*16%*	*2*	*2*	*8*	*9*
Healthcare 1	*69%*	*86%*	4	*4*	*7*	*8,3*
Healthcare 2	*67%*	*67%*	*2*	*3*	*9*	*8,3*
Production & trade 1	*27%*	*33%*	*3*	*1*	*4*	*8,7*
Retail & consumer goods 1	*27%*	*12%*	*3*	*3*	*7*	*8,6*
Retail & consumer goods 2	*61%*	*51%*	*3*	*4*	*10*	*7*
Transport & Infrastructure 1	*61%*	*75%*	*5*	*3*	*8*	*9,9*
Transport & Infrastructure 2	*71%*	*55%*	*4*	*4*	*10*	*9*
Transport & Infrastructure 3	*63%*	*65%*	*5*	*4*	*9*	*8,3*
	57%	*60%*	*3,7*	*3,4*	*7,6*	*8,4*
			(sd, 1,1)	*(sd, 0,99)*	*(sd, 1,8)*	*(sd, 0,8)*

Organization & industry	*BPM Use*	*BPM Availability*	*Delta*	*AVG perceived maturity*	*AVG calculated maturity*	*Delta*

Energy	*49%*	*52%*	*+3*	*4.5*	*3.5*	+1
Financial services	*62%*	*69%*	*+7*	*3.5*	*3.6*	-0.1
Healthcare	*68%*	*77%*	*+9*	*3*	*3.5*	-0.5
Production & trade	*27%*	*33%*	*+6*	*3*	*1*	+2
Retail & consumer goods	*44%*	*32%*	*-12*	*3*	*3.5*	-0.5
Transport & Infrastructure	*65%*	*65%*	*0*	*4.7*	*3.6*	+1.1

	Prevent adverse effects	Learning, improvement & awareness
Energy	1	1
Financial Services	12	1
Healthcare	3	4
Retail & Consumer Goods	5	0
Transport & Infrastructure	6	4