Nijmegen School of Management
MSc in Strategic Management

Risk management in Innovation Projects:

The Contribution of Strategic and Operational Risk Management in Innovation Projects

Personal information:
Name: Max Lodewijks
Student number: s1064626

Supervisors:
Supervisor: Gerrit Willem Ziggers
Second examiner: Peter Vaessen

Abstract

Risks are normal in organizational projects, but nowhere are the risks as high as in innovation projects. The failure rate is therefore high in innovation projects. Despite these high risks, it is important to be innovative for organizations to survive. Therefore it is important to control these risks as much as possible. The aim of this study is to find out what the influence of strategic and operational risk management is on the success rate of innovation projects. The following research question is formulated for this purpose: 'How do strategic and operational risk management influence the success rate of innovation projects and how does strategic risk management influence operational risk management?' To answer the research question, eight different people were interviewed at four different organizations. Four of these respondents are involved in setting up risk management and the other four respondents are involved in executing risk management. The answers of the interviews show that strategic risk management has a positive contribution to the success rate of innovation projects as well as to operational risk management. In addition, the results show that operational risk management has no unequivocal effect on the success rate of innovation projects.

Contents

Chapter 1

Introdution

Every organization faces risks, but not every activity of the organization brings as many risks as others. Risk is normal in all projects of an organization, but there is even more risk in innovation projects (27, Stevens & Burley, 1997). Innovation projects are more risky than any other project, since innovation projects make use of new information and knowledge to create a new product or service (1, Afuah, 2003). This ensures there is no complete guarantee that an innovation project will be successful (19, Nechaev et al., 2017). Therefore it is seen as a high-risk business activity. An example of risk in an innovation project is the uncertainty whether the innovation fits the target market. By improving an already existing product, it is already known it fits the target market. When innovating and coming up with a new product, this is not known yet. Research confirms innovation implies a lot of risk and that a high failure rate is normal (26, Simon, 2009). In some industrialised countries the failure rate of new products is 85 percent and among some developing countries it is 98 percent (20, Ozer, 2006).

Despite these risks, being innovative as an organization is very important to survive (34; 32, Zhao, 2005; Wang et al., 2010). Organizations should not avoid innovation projects because the risk of failure is high, given the value of innovation within organizations. Avoiding risks does not improve the organization and help the organization survive. Organizations should not aim to avoid all risks, but instead they should prepare themselves and manage risks as well as possible (34; 32, Zhao, 2005; Wang et al., 2010). Preparing and managing risks as well as possible helps the organization to adapt the

balance between success and failure of innovation projects (18; 13, Mu et al., 2009; Johnson, 2010). To manage these risks, explicit risk management could help. Risk management is the process by which a company copes with risks and threats to minimize the volatility of returns and to make sure the organization survives. Therefore, risk management is fundamental to effectively filter the good and bad prospects of innovation projects (4, Bogodistov & Wohlgemuth, 2017). Risk management involves identification and assessment of risks which affect the organization, and the execution of a strategy to manage those risks (6, Bromiley et al., 2015). Research indicates risk management helps in achieving success in innovation projects (5, Bowers & Khorakian, 2014).

Reconfiguring proper risk management within an organization is a risk management capability. Risk management can be divided into operational risk management and strategic risk management. The operational level deals with risks right now and the strategic level deals with establishing risk management within the organization in the long term (4, Bogodistov & Wohlgemuth, 2017). The aim of this study is to understand how risk management (both at the strategic and operational level) influences the success rate of innovation projects. This shows the importance of risk management and provides insights for other organizations to achieve better risk management and risk management capabilities, which can help to deal with risks in future innovation projects.

1.1 Research Objective

The objective of this research is to find out how operational and strategic risk management influence the success rate of innovation projects. Risk is seen in all projects of a company, but there is even more risk in innovation projects. Innovation is seen as a high-risk business activity and the failure rate of innovation projects is very high (34; 32, Zhao, 2005; Wang et al., 2010). To filter the good and bad prospects of innovation projects, risk management could help (4, Bogodistov & Wohlgemuth, 2017). Other studies show that focusing on risk management activities and strategies, an organization can enhance the success rate of innovation projects in a normal environment (5; 11, Bowers & Khorakian, 2014; Genus & Coles, 2006). While those studies focused particularly on risk management activities and strate-

gies, this study focuses on different levels of risk management. This study is an addition to these studies by making a distinction between strategic risk management and operational risk management. This distinction makes the concept of risk management capabilities more comprehensive. Strategic risk management focuses on how risk management is established within the organization in the long term and operational risk management focuses on carrying out risk management in a short-term horizon. These two risk management levels have different characteristics (6, Bromiley et al., 2015). This is the reason this distinction is made in this study: to gain more knowledge about these two levels of risk management separately and how they interact. For an organization, undertaking risk management can be seen as a capability which can lead to a competitive advantage over other companies (4, Bogodistov & Wohlgemuth, 2017). Therefore, the knowledge that follows from this study can be useful for other organizations in the future to create better risk management to foster innovation projects. In Section 1.3 it is further explained why it is important to investigate this.

1.2 Research Question

This research contributes to the literature of risk management and innovation by answering the following research question:

How do strategic and operational risk management influence the success rate of innovation projects and how does strategic risk management influence operational risk management?

In answering the research question, this study links risk management with innovation. Risk management is divided into strategic risk management and operational risk management. It is examined if these two levels of risk management influence the success rate of innovation projects. To answer the main research question, this study is additionally concerned with the following sub-questions:

- How is risk management organized?
- How does risk management influence the success rate of innovation projects?

- What are the differences in organizing between strategic and operational risk management?
- What are the differences in organizing between strategic and operational risk management?
- How does strategic risk management influence operational risk management?

1.3 Theoretical Relevance

The contribution of this study is that it links strategic and operational risk management with the success rate of innovation projects. A lot of research on risk management and innovation has been carried out, but not specifically on strategic and operational risk management and innovation. Other studies focus mainly on risk management activities and strategies. These studies show that an organization focusing on risk management activities and strategies can enhance the success rate of innovation projects. Risk management can ensure to reduce and manage risks that are unforeseen. This makes risk management very important in strategic management (5; 11, Bowers & Khorakian, 2014; Genus & Coles, 2006). By focusing on strategic and operational risk management, a distinction is made between how risk management is established within the organization in the long term and how risk management is carried out in the short term (4, Bogodistov & Wohlgemuth, 2017). These two levels of risk management have different characteristics and consequently different routines and processes as well (6, Bromiley et al., 2015). It is important to investigate these two levels of risk management separately, because in this way it becomes clear whether the establishment and the execution of risk management have a big impact on innovation projects. It is known that risk management has a positive influence on innovation projects (5, Bowers & Khorakian, 2014). However, by looking at different levels of risk management, it becomes visible whether both levels of risk management have a positive influence on innovation projects. Besides, it becomes clear whether strategic risk management influences operational risk management. The contribution of this study leads to a more comprehensive understanding of risk management. Not just the influence of risk management on the success rate of innovation projects is investigated, but the influence of different levels of risk management is investigated. This can show which level of risk manage-

ment needs more focus to stimulate innovation projects. In this way more in-depth information about risk management is gained. This makes it interesting to look at these two levels separately. The inclusion of these two levels of risk management provides a better understanding of the concept of risk management.

1.4 Practical Relevance

The aim of this study is to understand how strategic and operational risk management influence the success rate of innovation projects. It provides insights for other organizations on how they can improve their risk management, both at the strategic and operational level (4, Bogodistov & Wohlgemuth, 2017). This study provides examples of how risk management can be set up and executed and possibly how it is better not to be set up and executed. An organization can have a routine, for example, in which certain steps are to be followed to respond to a high-risk event. Other organizations can learn from this and possibly implement ideas within their own organization. This can also be used by other organizations which are innovating or want to improve their risk management. It also provides insights for other organizations which level of risk management has more influence on innovation projects. It may become clear whether more attention is needed from management to establish risk management properly or from the employees who carry out risk management. This is relevant for almost every organization. Every organization, even if it is a very innovative organization or a less innovative organization, will have to deal with innovation activities at some point in time. Since innovation is a high-risk business and implies a lot of risk, it is good to have risk management to reduce these risks as much as possible (5, Bowers & Khorakian, 2014). This shows the usefulness for almost every organization to gain more knowledge about the influence of strategic and operational risk management on innovation projects. The information from this study can help other organizations improve their risk management in a more targeted and effective way to foster innovation projects.

1.5 Outline of the thesis

This thesis proposes a descriptive study that is qualitative in nature to evaluate the influence of strategic and operational risk management on the success rate of innovation projects. To answer the research question, this paper is structured as follows. Chapter 1 is the introduction, followed by a theoretical framework in Chapter 2 to provide some theoretical background from other studies. Chapter 3 outlines the method of research applied in this study. Chapter 4 presents the results of the qualitative analysis. The final two chapters include the conclusion and discussion, respectively, which provide an answer to the research question, followed by the limitations, providing boundaries to the scope of the research, and suggestions for further research.

Chapter 2

Theoretical background

In this chapter, relevant theories and concepts are evaluated and discussed. This study examines all theories and concepts which help to answer the research question. First, a capability view on risk management is provided, followed by risk management. After that, the concept of success of innovation projects is discussed, followed by the relationship between risk management and the success of innovation projects. Finally, the conceptual model is given.

2.1 A Capability View on Risk Management

The dynamic capabilities theory appeared as a response and an enlargement of the already existing resource-based view (RBV). The resource-based view has the inability to interpret the development and redevelopment of capabilities and resources in an environment that is rapidly changing (30, Teece, Pisano & Shuen, 1997). The dynamic capability theory compensates the shortcomings of the resource-based view. Dynamic capabilities are "the organizational and strategic routines by which firms achieve new resource configurations as markets emerge, collide, split, evolve and die" (8, Eisenhardt & Martin, 2000, p. 1107). Dynamic capabilities can be seen as a competitive advantage and give organizations the possibility to build, integrate and reconfigure their capabilities and resources. In this way organizations can adapt better to environments that are rapidly changing (2, Bleady, Ali & Ibrahim, 2018).

A risk management capability can be seen as a dynamic capability. Risk management capabilities are the organizational and strategic routines, capabilities and competencies that help to perform good risk management (9, Elahi, 2013). These are the conditions which are necessary for an organization to be able to properly carry out risk management. Risk management capabilities contain two overarching abilities. The ability to prevent occurrences or events and the ability to respond to unanticipated occurrences that have happened in the past. These are the organizational and strategic capabilities which can improve dealing with risks and threats; and looking for alternatives and opportunities to handle the risks (4, Bogodistov & Wohlgemuth, 2017). Risk management capabilities go further than just forecasting possible risks by responding to unanticipated events. This is called organizational resilience (29, Teece, 2007). Resilience is the ability to change, adapt and reinvent business models and strategies in an environment that is changing (12, Hamel & Valikangas, 2003). It is the capability to respond to unanticipated events (4, Bogodistov & Wohlgemuth, 2017). When an unlikely occurrence happens, risk management capabilities can ensure an organization is able to adapt successfully. For example, the capability to assess the likelihood and impact of a risk helps an organization to adapt better. If the likelihood and impact of the risk can be assessed, the organization is better able to prepare for this risk and the consequences that follow. In this way the organization might prevent unfavorable events or respond better to events which have already happened. Another risk management capability is reconfiguring risk management within an organization. These capabilities have the biggest impact when they are embedded (in an integrated and systematic way) in the culture, structure and operational processes of the company (4, Bogodistov & Wohlgemuth, 2017).

2.2 Risk Management

There is not a lot of conformity about the definition of risk, since it is defined differently in different fields. In this paper risk is defined as the likelihood with regard to the appearance of a potential loss (15, Kaplan & Garrick, 1981). The exposure to loss is any event or occurrence in which a loss is possible, irrespectively if the loss actually occurs. The likelihood is a result of incomplete information about the future. It is a situation in which managers and organizations do not have enough information right now to forecast fu-

ture events and outcomes (7; 16, Carbonara & Caiazza, 2010; Krickx, 2000). According to Luhmann (17, 2005) risk indicates a certain area for decision making about the future. Hence, risk management develops an expectation of decidability and control of potential loss and opportunity (23, Power, 2007).

Similarly to the definition of risk, risk management is defined differently in different fields as well. As mentioned before, in this study risk management is defined as the process of coping with risks and threats to minimize the volatility of returns and to make sure the organization survives (4, Bogodistov & Wohlgemuth, 2017). This can be a competitive advantage for an organization if it is managed well. In this study a distinction is made between two levels of risk management: strategic risk management and operational risk management. Strategic and operational risk management have different characteristics and consequently different routines and processes as well (6, Bromiley et al., 2015). Figure 2.1 (4, Bogodistov & Wohlgemuth, 2017, p. 242) shows the relations between the definitions.

2.2.1 Strategic Risk Management

The strategic level of risk management deals with how risk management is established within the organization. The focus lies on understanding how risk management has to be structured within the organization. It focuses on the long term to keep the operational income stream sustainable in the future (4, Bogodistov & Wohlgemuth, 2017). The ultimate goal is to protect and create shareholder value (10, Frigo & Anderson, 2011). To get to know whether risk management is established well within an organization, different tools and frameworks can be used. This study adopts the COSO ERM model. This model has become one of the leading models in risk management (21, Paape & Swagerman, 2006). The components of the model do not only concern strategic risk management, but in this study it is used to measure how well risk management is established within an organization. The five components of the model are therefore also interpreted with a view to establishing risk management. Figure 2.2 shows the five elements and associated principles (31, COSO, 2011, p.7).

The first element deals with governance and culture, that is, whether risk management has been considered in top management and whether this is reflected in the culture. For example, this can be visible when a risk management team has been appointed by top management and when they are

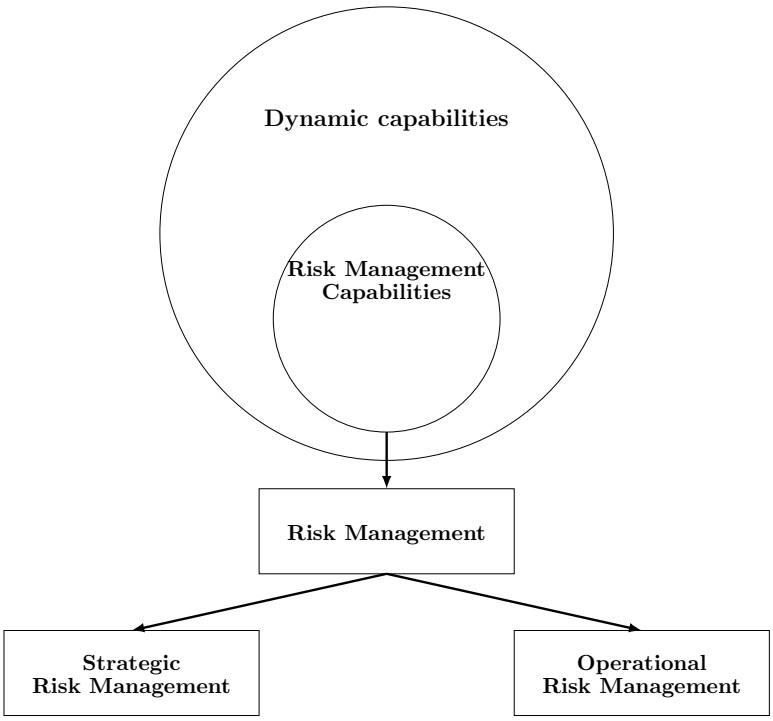


Figure 2.1: Risk Framework. Reprinted from "Enterprise risk management: a capability-based perspective", by Bogodistov, Y. & Wohlgemuth, V., 2017, The Journal of Risk Finance, p. 242.

resourced by top management. The second element deals with strategy and objectives. It can be assumed this has been considered when, for example, a risk management framework is used to determine a strategy with regard to risks. Another indicator could be whether the risk appetite is known to all employees involved in risk management. The third element of the model is performance. This is concerned with whether top management has thought about how risks are mapped out. The fourth element treats how the risk management process is monitored. An indicator could be whether an organization has a plan how to act in case of identified shortcomings. The last element deals with how information regarding risk management is communicated and reported (31, COSO, 2017). An indicator could be whether an organization has a plan about how to communicate important information to external and internal stakeholders.

Figure 2.2: COSO ERM Model. Reprinted from "Enterprise Risk Management—Integrating with Strategy and Performance", by (31, COSO, 2017, COSO, p. 7).

2.2.2 Operational Risk Management

When risk is dealt with immediately, it is called operational risk management. It is the execution of risk management. An example is mapping risks and their impact. Risks with the highest priorities are addressed first. After the main risk is addressed, the personnel can address the remaining, less important risks (4, Bogodistov & Wohlgemuth, 2017). There are several risk management tools and techniques to measure whether risk management is executed well. This study applies the risk maturity model (24, Proença et al., 2017). This model rates the maturity of a company's risk management. It shows how well risk management is executed within an organization. Organizations' operational risk management can be divided into five different levels at which the degree of maturity increases at each level. These five levels are: initial, managed, defined, quantitatively managed and optimizing. The descriptions of the different levels are as follows (24, Proença et al., 2017).

- Level 1: Initial
  The organization is not aware of the need for risk management. The organization is not engaged in learning from risk experiences or preparing for risks and uncertainties in the future. Some risk management activities may be applied, but mostly ad-hoc and chaotic.
- Level 2: Managed
  The organization experiments with applying risk management, but does not do this in a structured and formalized manner. Risk management is supported by one or more officers.

- Level 3: Defined
  The organization's risk management is structured. General risk processes have been set up and are implemented in various places within the organization, however not consistently everywhere.
- Level 4: Quantitatively managed
  The organization applies risk management to almost all processes and projects. Risks are actively used to further improve the organization.
- Level 5: Optimizing
  The organization proactively approaches risk management throughout the organization. Risk management is fully integrated into the culture of the organization and is a permanent part of decision-making processes.

To evaluate which risk maturity level applies to an organization, more specific criteria can be used. The framework which is used here is ISO 31000. This is a framework which provides criteria on how to measure, evaluate and continuously improve an organization's risk management (24, Proença et al., 2017). The article of Proença et al. (24, 2017) links the criteria of ISO 31000 with the risk maturity model. Figure 2.3 shows these criteria. An organization's risk management improves when it moves from a lower to a higher maturity level.

To execute operational risk management well, it is important risk management is established well at the strategic level. If the top management team does not consider risk management, for example, employees who have to execute risk management will not have tools to use. It would also be hard for employees to execute risk management when the top management team has not thought about a plan on how to identify risks or how to assess. Employees will not have a plan or framework then they can use to identify and assess risks. This means without establishing risk management at the top of an organization, the execution of risk management is harder within the organization. This shows strategic risk management sets the priorities for operational risk management (4, Bogodistiv & Wohlgemuth, 2017). The first proposition is formulated accordingly.

Proposition 1. ***The better strategic risk management is established, the better operational risk management is executed.***

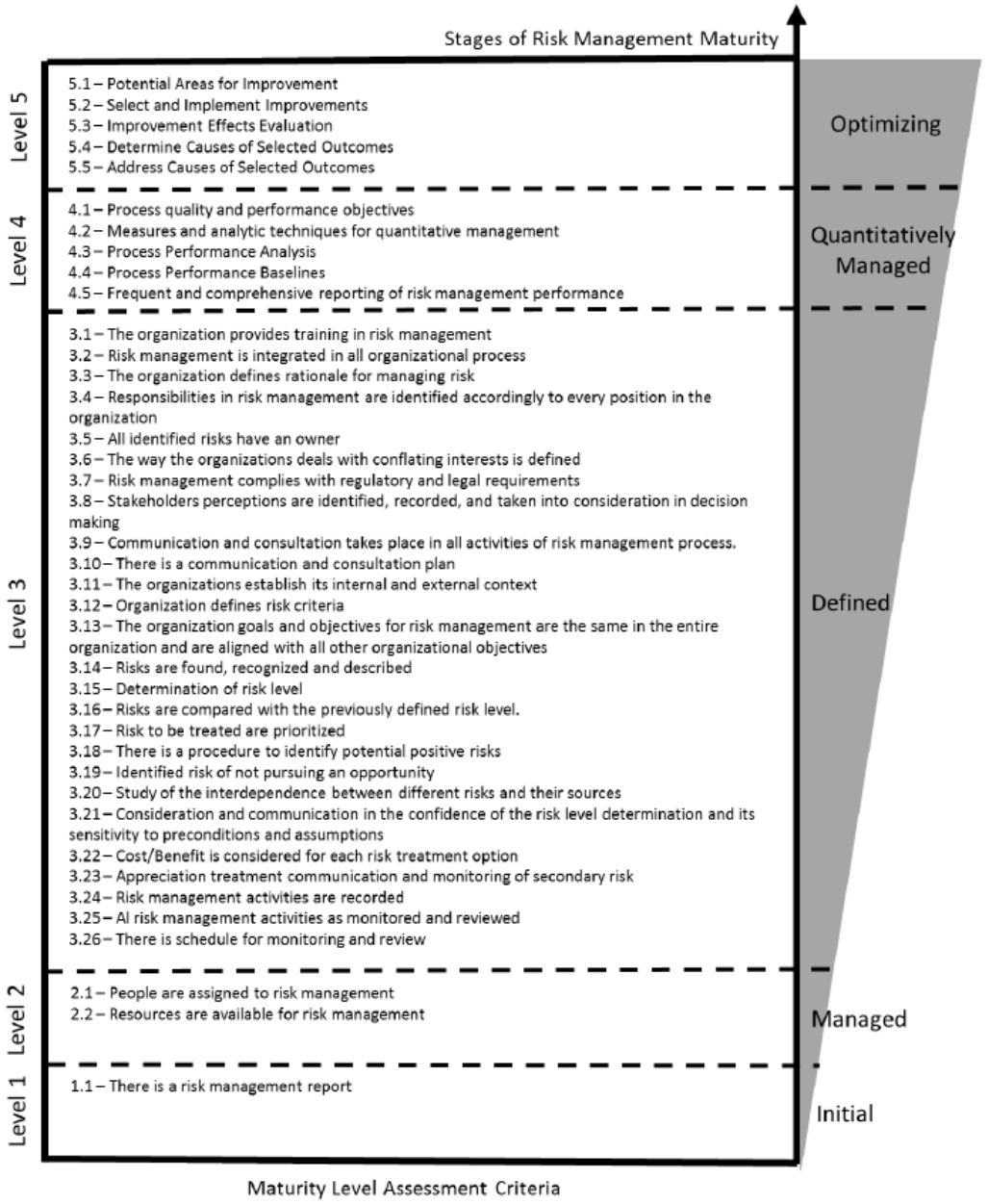


Figure 2.3: Maturity Level Assessment Criteria. Reprinted from "Risk Management a Maturity Model based on ISO 31000", by (24, Proença et al., 2017, IEEE, p. 106.)

2.3 Success of Innovation Projects

The environment organizations are operating in is constantly changing. This means organizations have to innovate to survive and stay competitive (28, Taplin and Schmyck, 2005). According to (1, Afuah (2003)) innovation is the use of newly obtained knowledge in creating, developing and implementing a new product or service. Novelty has a central role in innovation and this brings risks. Innovation is seen as a high-risk business activity (34; 32, Zhao, 2005; Wang et al., 2010). Every project an organization works on brings risk, but it is especially found in innovation projects. This causes a high failure rate of innovation projects and means a lot of innovative projects do not work out as they would like. It shows innovation projects are not very successful in general (26, Simon, 2009). However, to stay sustainable competitive as an organization, it is necessary to innovate. It is risky and it contains a high failure rate, but it is important for the survival of an organization. Despite innovation often failing, organizations have to accept that failure is part of innovation. They should not aim to reduce risk by discouraging and stifling innovation (28, Taplin & Schymyck, 2005). Accepting there is a possibility that an innovation project fails is part of innovation. Being scared of failure can be harmful for a company. To define the success of innovation projects, different indicators can be used. The number of active innovation projects or the number of innovative ideas submitted can be taken as an indicator for innovation success, for example. In this study a successful innovation project is defined as an innovation project which creates differentiated value for the people involved (22, Palmberg, 2002). This is measured by asking the respondents about their perception about this.

2.4 Relationship Between Risk Management & Success of Innovation Projects

According to Bogodistov and Wohlgemuth (4, 2017) strategic risk management is about how risk management is established within the organization in the long term. It focuses on establishing risk management within an organization. Further it is noted that operational risk management is about executing risk management and focuses on the short term. Both levels are part of risk management. Bowers and Khorakian (5, 2014) indicate that risk management helps in achieving success in innovation projects. By apply-

ing proper risk management, bad innovation projects can be abandoned on time. It offers an effective lens to better distinguish good and bad prospects and helps to direct the continuing research which is essential in innovation projects (5, Bowers & Khorakian, 2014). Therefore, risk management is fundamental to effectively filter the good and bad prospects of innovation projects (4, Bogodistov & Wohlgemuth, 2017). Based on these findings, this study expects that the better strategic risk management is established, the more successful innovation projects are. Further, this study expects that the better operational risk management is executed, the more successful innovation projects are. Accordingly, the following propositions are formulated.

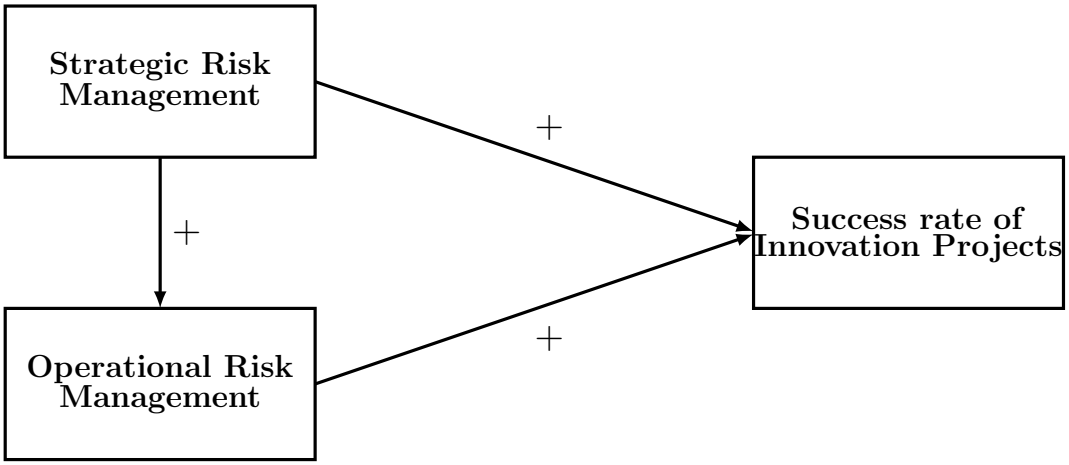
Proposition 2. ***The better strategic risk management is established, the more successful innovation projects are.***

Proposition 3. ***The better operational risk management is executed, the more successful innovation projects are.***

2.5 Conceptual Model

To summarize the propositions mentioned before:

- The better strategic risk management is established, the better operational risk management is executed. (Proposition 1)
- The better strategic risk management is established, the more successful innovation projects are. (Proposition 2)
- The better operational risk management is executed, the more successful innovation projects are. (Proposition 3)



Chapter 3

Methodology

This chapter discusses the implementation and the quality of the methodology that is used in this research. First, the methodological approach is discussed, followed by the research methods. After that the operationalization is reflected, showing the dimensions and indicators of this study. Then the case selection is reviewed, followed by the data analysis. Thereafter, the limitations are discussed to end with the ethics of the research.

3.1 Methodological Approach

The study that was executed is descriptive qualitative. The goal of a descriptive study is to describe. Descriptive studies are mostly used to gather data to describe a certain event, situation or person. This can be either qualitative or quantitative in nature. Quantitative data can be scaled and counted; and qualitative data is more descriptive and can be ordered based on features. In this study the aim was to gather qualitative data. Descriptive studies can help researchers in multiple ways. It can help to understand characteristics of an event, present ideas for further research or help to make decisions (25, Sekaran & Bougie, 2016). Qualitative research describes a phenomenon that takes place in a specific context. The findings of the research lead to a better understanding of the phenomenon (14, Justesen & Mik-Meyer, 2012). This is in line with this research, since the aim of this study is to get a better understanding of the phenomena "risk management" and "innovation". This way it can be described how risk management influences the success rate of

innovation projects.

3.2 Research Methods

The data collection method is interviewing respondents. Interviews can be structured, unstructured and semi-structured. In this study semi-structured interviews are used. This means there is an interview scheme made in advance with general questions, but it is allowed to deviate from this scheme. Not the entire interview and the sequence of the interview is planned beforehand. An advantage of a semi-structured interview is that the interviewer can determine during the interview which topics or issues need more in-depth investigation (25, Sekaran & Bougie, 2016). This is especially useful in this research, because employees with different tasks are interviewed. The way risk management influences innovation projects depends heavily on how the risk management is established and executed. By making use of semi-structured interviews, in-depth information can be gathered about the establishment and execution of risk management and the influence on innovation projects. Further, all the interviews are held online via Microsoft Teams because of the COVID-19 policy by the Dutch government. This is done to secure the safety of the representatives from the investigated organizations. Not being able to interview the respondents face-to-face had some disadvantages and advantages. It was harder to build a relationship and trust, because the interviewer and interviewee did not see each other in real life. On the other hand, conducting interviews online is easier due to geographical reasons. The interviewer and interviewee could conduct the interview from home, what made it easier and more flexible to plan the interview (25, Sekaran & Bougie, 2016).

The information gathered with the use of interviews needs to be as free as possible of bias. If the measure is without bias it is ensured the measurement is consistent over time and across various items in the instrument. In that case, the research is called reliable then. Bias is defined as inaccuracies or errors in the data gathered (25, Sekaran & Bougie, 2016). This can be caused by either the interviewer, the interviewee or the circumstances. The data is possibly biased when there is no trust and no good relationship between the interviewer and the interviewee, when the answers of the interviewee are misunderstood or when the interviewer unintentionally pushes the answers of the interviewee in a certain direction through gestures and

facial expressions (25, Sekaran & Bougie, 2016). To make sure there was trust and a good relationship between the interviewer and interviewee in this research, the interviews started with a neat introduction of the interviewer. Besides, the interviewee is anonymous in this research which should provide the respondent the freedom to answer all the questions without restraint. To minimize misunderstandings, the interviewee listened attentively, was honestly interested, practised tact in asking questions and iterated and clarified questions if they were not totally clear to the interviewee. Another thing the interviewer did to make sure he understood issues right, was restating or rephrasing information said by the interviewee. This clarified the issue to make sure it was understood what was actually meant (25, Sekaran & Bougie, 2016). Furthermore, the interviewee was asked at the beginning of the interview if he was fine with recording the interview. This enabled the interviewer to hear the interview again, which helped to minimize misinterpretations. To make sure the interviewer did not push the answers of the interviewee in a certain direction, only unbiased questions were asked. Unbiased questions are questions that do not contain terms which show the interviewer's own perceptions about the subject.

This research also aimed for face validity. Face validity is defined as using the right measures for the variables that are investigated (33, Yin, 2015). To ensure face validity, the transcripts of the interviews were given back to the respondent so they could evaluate it. If there were any misunderstandings or deficiencies in information, the respondents could correct the transcript. In this way it is more likely that the concepts that are investigated in this research are measured correctly. Further, external validity ensures the research is generalizable (25, Sekaran & Bougie, 2016). It is hard to obtain external validity in qualitative research since the results are rarely generalizable (3, Bleijenbergh, 2015). Since this study is qualitative in nature and aimed to gain insights, the results are limited to this case. Finally, validity is also performed in this study through selection of interviewees. By briefly explaining to the contacts within each organization what kind of knowledge was needed, they were able to contact the most appropriate people in terms of knowledge and experience about risk management.

3.3 Operationalization

As described earlier in this paper, the phenomena "risk management" and "innovation projects" are investigated. The independent variable in this study is risk management. A distinction is made between strategic risk management and operational risk management. These two concepts are the first two topics as well. The subtopics of the topic of strategic risk management are based on the risk maturity model (31, COSO, 2017). The subtopics of the topic of operational risk management are based on the risk maturity criteria (24, Proença et al., 2017). The dependent variable in this study is the success of innovation projects. Based on this, the third topic 'success of innovation projects' is established. To find out the relationship between the concepts, the fourth topic 'contribution to innovation projects' is established. In response to these four topics, fourteen different subtopics are constructed to answer the research question. The topics and subtopics of this study can be found in Table 3.1.

Topic 1: Establishment of risk management
Governance & culture
Strategy & objective-Setting
Performance
Review & revision
Information, communication & reporting
Topic 2: Execution of risk management
Resources & responsibility
Objectives
Quality of risk control
Review & revision
Communication & reporting
Topic 3: Success of innovation projects
Amount of innovation projects which deliver differentiated value for the people involved
Topic 4: Contribution to innovation projects
Contribution of establishment of risk management on success rate of innovation projects
Contribution of execution of risk management on success rate of innovation projects
Contribution of establishment of risk management on execution of risk management

Table 3.1: Topics and subtopics

3.4 Case Selection

In this research the interviewees come from four different organizations: Radboudumc, Philips, Coolrec and Essent. Radboudumc is active in the healthcare branch as a hospital. At the Information Management department of Radboudumc, the service desk incident coordinator and the quality and compliance officer were interviewed. They deal with ICT risks that occur within the hospital. Besides, Philips works on medical systems for healthcare. An integral project manager and the project excellence lead of the Development department were interviewed. They are concerned with risks that occur in development projects. Furthermore, Coolrec is a recycling company, which has different branches. All these branches carry out different activities in the recycling process. A SHEQ (safety, health, environment and quality) manager of one of these branches and the SHEQ officer who supervises the SHEQ managers were interviewed. They are concerned with safety, health, environment and quality risks in recycling activities. Lastly, Essent works in the energy branch. They also provide digital security services for their clients at the Sales department. At the Sales department, the sales support specialist and the compliance specialist (former risk officer) were interviewed. They focus on digital security risks.

Since the interviewees are from four different organizations with different functions, it is a heterogeneous group. To be able to draw representative conclusions from this research, eight persons are interviewed (25, Sekaran & Bougie, 2016). The representatives of the organizations who are interviewed are persons who are related to and have knowledge of risk management. Four persons who are interviewed have more of a managing role and have knowledge about the establishment of risk management within the organization. The other four persons who are interviewed are closely related to the execution of risk management, which means they have knowledge of the execution of risk management. To ensure that the organizations in this research have risk management skills and experiences, organizations older than ten years are selected. In this way the organizations have had time to actually build risk management capabilities. Furthermore, all of the case study organizations selected have a significant degree of innovation experience. This was secured by asking the respondents in advance whether the organization they work for has a significant degree of innovation experience.

3.5 Data Analysis

The transcription of the interviews took place shortly after conducting each interview. The verbatim transcribing method was used. All words were written down, but hesitation and stop words were ignored. The full transcripts can be found in appendix A. After that, the semi-structured interviews were analysed and coded based on a deductive approach. A deductive approach means investigating the present or past and testing this with existing theories (3, Bleijenbergh, 2015). This was useful here since other studies had investigated the phenomena "risk management" and "innovation" before. This was done with the help of the application Atlas. The coded versions can be found in Appendix B.

The transcription of the interviews took place shortly after conducting each interview. The verbatim transcribing method was used. All words were written down, but hesitation and stop words were ignored. The full transcripts can be found in Appendix 6.5. After that, the semi-structured interviews were analysed and coded based on a deductive approach. A deductive approach means investigating the present or past and testing this with existing theories (3, Bleijenbergh, 2015). This was useful here since other studies had investigated the phenomena "risk management" and "innovation" before. This was done with the help of the application Atlas. The coded versions can be found in Appendix 6.5. The results of risk management were interpreted based on the theory described in Chapter 2. The level of operational risk management was determined based on the descriptions of the different levels according to Proença et al. (24, 2017), by looking at which description best suited the results of each organization. The results of strategic risk management were interpreted based on the components of the COSO ERM Model (31, 2017). If three to five components have been fully thought of, it is quite well to very well established. If less than three components have been fully thought of, it is not well established.

3.6 Limitations

There are a couple of considerations which have not been taken into account in this research. Firstly, while looking at organizations to investigate, only organizations which exist at least ten years are considered. This means start ups and young ventures are not considered to ensure the investigated orga-

nizations have at least some risk management capabilities. Start ups and young ventures can have risk management capabilities as well, but it takes time to build these capabilities. That is why the boundary of ten years is chosen. Further, this research focuses solely on risk management and does not focus on other capabilities. A lot of organizations might have more capabilities, but we choose to focus on the distinction between strategic and operational risk management, and hence why other capabilities are left out.

3.7 Research Ethics

As interviews are conducted, ethical considerations have to be taken into account. To ensure this, we started each interview by informing the interviewee about the goal of the study and what kind of questions they could expect. Besides, permission was asked to record the whole interview so the interviewer had the possibility to hear the answers again. Moreover, it was stated that the answers the interviewee provides are only used for scientific purposes and that the respondent stays anonymous. Finally, the researcher of this study had to sign an integrity form to confirm academic integrity. This shows the researcher warranted transparency in gathering the data and presenting the results.

Chapter 4

Results

This chapter discusses the results following from the interviews. The interviews have been transcribed and coded before the results could be analyzed. This chapter starts with the characteristics of strategic risk management, followed by the characteristics of operational risk management. After that the influence of strategic risk management on operational risk management is discussed. Then, innovation projects and the contribution of risk management are analyzed. Finally, the differences between the organizations are listed and some areas for improvement are given.

4.1 Characteristics of Strategic Management

The COSO ERM model is introduced in Chapter 2. This model is used in this study to find out whether an organization's risk management is established well. This model contains the following five components: 'Governance & Culture', 'Strategy & Objective-setting', 'Performance', 'Review & Revision' and 'Information, Communication & Reporting'. It is indicated below whether the organizations comply with these components.

4.1.1 Governance & Culture

Risk management is becoming more important at the Information Management department within Radboudumc. The management team started to see that too, which resulted in a new function of quality and compliance officer

one year ago. Risk management at IM is coordinated by top management. Besides, there is a general Risk & Audit department, which is concerned with setting up the strategic risk management of the entire Radboudumc. The Information Management department adopts knowledge and tools from this department. There is no risk manager or risk department at IM. The risk management activities are embedded in the Quality and Compliance department.

At the Development department of Philips, risk management is seen as one of the most important things. When risks are managed, it can be ensured a project is successful. Risk management is coordinated from the board, because they can see risks at the horizon which can influence projects or departments. At the corporate level there is a risk department which coordinates the risk managers at different departments.

A look at Coolrec shows that risk management is considered important as well, because it has an impact on their continuity if they do not control their risks. If they do not have a continuous process, they cannot satisfy their customers. At Renewi level (parent company) there is a risk management department. From this department, risk management is also coordinated within Coolrec. At Coolrec level there is coordination from the director, SHEQ manager and operations manager on risk management.

Finally, at the Sales department of Essent risk management is seen as very important, even more so than at the core business of Essent. This is because of the supervisory perspective and compliance risks at Sales. However, there is no coordination from top management at the Sales department. There is no CFRO at Essent, the responsibility lies with the staff units within the department. There are two risk departments within Sales. One is called commercial risk management and the other one is called quality and internal control. These are first and second line risk management departments.

4.1.2 Strategy & Objective-setting

The management team sets goals for Information Management within Radboudumc, depending on what they think is most important. They have goals for IT provision, cyber security, continuity, etc. It is clear within the department how risk tolerant they are. If it is a low risk they accept the risk. If it is a medium or high risk, immediate action has to be taken. Whether it is a

low risk or not is considered in the risk analysis.

At Philips they do not really pay attention to goals regarding risk management. This is because the risks can be quite unique and different. On the other hand it is clear how risk tolerant they are, though it depends on the risk itself. Just like at Radboudumc, they accept a low risk and try to mitigate a medium or high risk.

At Coolrec they have goals as well, such as no accidents with absenteeism. Much attention is paid to achieve these goals. Every month the risk management goals are considered in a business review. This is a meeting between the management team and the site managers. The risk tolerance is clear as well. If the initial risk is low it is accepted. If the initial risk is too high, control measures are taken. The residual risk then remains. When the residual risk is brought back to an acceptable level, it is accepted.

At Essent they do not consider internal control objectives regarding risk management. It is not a subject within Essent. Meanwhile they know exactly how risk tolerant they are at certain risks. The risk tolerance regarding financial risks at fraud is 0 Euros, for example, and the risk tolerance regarding invoicing is a certain percentage of the total annual order.

4.1.3 Performance

Thought has been given to how risks are identified, assessed and addressed at Radboudumc. The way risks are identified at Radboudumc is diverse. It may become clear when they have an incident. This is the most common form of identification. It can also arise from an audit in which findings are made. When a risk is identified it is assessed using a heatmap. With this heatmap the probability is multiplied by the severity. Then based on the score of the assessment, further action is taken. This depends on the size of the risk. If it is a low risk it gets accepted, an improvement is necessary for a medium risk and immediate action is necessary for a high risk.

At Philips they want to identify risks at the beginning of a project when it is still in the initiation phase. They have monthly project risk meetings where all members come together. New risks are brought up in this meeting and the mitigation state for the existing risks is discussed. Then, they assess the risks using their risk registration tool. They assess the risk based on the impact and probability. They take action depending on the nature of the

risk. Depending on the impact and probability of the risks, due times are assigned to the risks. This is discussed in the project risk meetings as well.

At Coolrec risks get identified when there is a new machine or when new risks are faced at an already existing machine. Risks get assessed with the help of a matrix. The impact and likelihood are multiplied in this matrix, giving a score. This score indicates the magnitude of the risk. In this way the risks get prioritized as well. If the risks are too high, a plan of action follows. This is done in a systematic way. The frequency of actions depends on the amount of deficiencies.

Finally, Essent uses the COSO model to identify risks. All processes are written down first and then the operational risk management team clusters all the risks. Then the risks get assessed based on the impact and probability. All high risks will become key risks. When the risk turns out to be a key risk, a control mechanism is built around it. This means you frequently have to upload proof that you are in control and then you are assessed every six months. Besides, when a risk turns out to be a key risk, the process has to be adjusted if possible or otherwise the process has to be rebuilt. If both are not possible, the risk is accepted and the process is set up detectively.

4.1.4 Review & Revision

The idea is to review the risk management process at Radboudumc once a year. However, this is done by the quality and compliance officer, who drafts and decorates the framework of standards regarding risks himself. Therefore, the management team is instructed to request the internal audit service to do an internal audit. Besides, Radboudumc wants to be certified with the ISO-27001. This is the international standard for information security. Hence, an external audit is carried out every year, whereby the process is reviewed as well.

At Philips they think differently about how to review the risk management process. They do not want to do it at regular intervals, but when there is a change in the project. The process gets reviewed when there is a change based on the best experiences, lessons learned or continuous improvement of actions.

At Coolrec the goal is to review the process once a year. They want an RI&E to be carried out once a year. It is then checked whether everything is still

current and up-to-date.

Finally, at Essent an internal audit was carried out in April 2020, whereby the risk management process got reviewed. It was reviewed whether the risks are correct, complete and whether the right mechanisms are being followed. If the internal audit happens to get hold of the risk management subject, it gets reviewed. Otherwise, it does not get reviewed. The process does not get reviewed at regular intervals.

4.1.5 Information, Communication & Reporting

At Radboudumc they use a risk register in which the various risks are registered, including the associated probability and impact. This risk register is stored in their management system. However, progress can be made on communicating these risks periodically. Thought has not really been given to communication.

At Philips they use their own tool to register risks. A lot of information is stored in this tool, like the impact, the cause, the financial impact and so on. This information is communicated during monthly project risk meetings. The information is then communicated at different levels.

At Coolrec there is a standard risk register and a standard risk matrix is attached to the risk register. This is defined at Renewi (mother company) level. The same approach is used whether it is a risk analysis in the field of safety, environment, fire or business risks. All results that emerge from the risk management process are recorded in the risk register. The communication of these risks is adapted to the stakeholders. However, for every stakeholder it always happens in a fixed way. The internal communication is done during toolbox meetings which take place once a month.

At Essent they have guidelines on how to record risks. It is registered in the risk register system called Zenya. It records things like description, cause and effect. The communication about risks is really an area for improvement at Essent. They recognize it is hard to get the management team involved, because there is a lack of communication. Some time ago the risk specialist joined an MT meeting to give a voice-over of what was going on, but this is not done anymore.

4.1.6 Summary

Based on the theory of the COSO ERM model from Chapter 2, it can be concluded that risk management at Radboudumc is well established. Much attention has been paid to the first four components. Only the last component 'Information, Communication & Reporting' could be given more attention, because communication about risk management has not actually been considered.

At Philips risk management is quite well established as well. They could pay some more attention to the components 'Strategy & Objective-setting' and 'Review & Revision'. No thought has been given to any goals regarding risk management and no thought has been given to review the risk management process at regular intervals. They only want to review the process when there are changes, but then it might happen that there is no review at all for a long period. In the meantime, the risk management process may still be improved through new insights and experiences, for example.

It can be concluded that risk management is very well established at Coolrec. Much thought has been given to all five components of the COSO ERM model.

Finally, risk management is not very well established at Essent. All components except 'Performance' could be paid more attention to. There is no coordination from top management, which shows risk management is not seen as very important. Besides, no thought has been given to objectives regarding risk management. Further, no thought has been given to review the process at a regular interval. It only gets reviewed when the internal audit happens to get hold of the risk management subject. Finally, it is not considered how to communicate regarding risks. They recognized it is hard to get the management teams and other teams involved.

4.2 Characteristics of Operational Management

The characteristics of a good execution of risk management are given in Chapter 2, Figure 2.3. The presence of these characteristics at the companies is tested below. Based on the presence of these characteristics, the risk

maturity is determined.

4.2.1 Radboudumc

The new quality and compliance officer position shows that there is urgency in risk management. This also results in a lot of resources available for execution in the form of procedures, tools and people. The people who execute risk management are responsible to sound the alarm when they face risks. They are responsible to inform the team workplace as soon as possible. The team workplace is then responsible for the actions they have to perform. The ultimate responsibility lies with the managers of the IT department. When risk management is executed, laws and regulations are always taken into account. Radboudumc is a company that is partly funded by the government as a university hospital. That is why it is very important to always abide the rules. Despite the fact that, according to the quality and compliance officer, there are goals regarding risk management, the employee who executes risk management does not know about any concrete objectives. They have some smaller objectives, but these can be seen more as KPIs, like achieving a certain service level agreement or a certain time to solve risks, for example. Risks get identified when an incident happens within the hospital. This is communicated to the IT service desk. The risks then get assessed based on how many users are affected and to what extent they can still carry out their work. If it is a smaller incident it may not be addressed immediately, because other activities are then given higher priority. If it is a larger malfunction it has to be called through immediately to the second-line teams so they can start looking for a solution straightaway. This process goes on constantly. Most risks almost have no influence, because it concerns one user who experiences a bit of trouble. However, it is a continuous process in case a major risk arises in the hospital so an adequate response can be given immediately. In case of a major risk, the process of that risk gets reviewed as well. After a solution is found and the risk is in control, two tickets are created automatically in which malfunction reports must be written. This is where it is noted what went well and what could be improved. These malfunction reports are listed in the risk register system that is used. The whole process also gets reviewed once a year. In their risk register system all risks are recorded, including the priority and impact. Risks can then be sent to second-line teams via this system. In this way it is communicated as well. When it is a high risk, it can also be communicated in another way

like sending an email, sending a Radboud alert or posting a message on the Radboudumc website, for example. There are five different types of possible internal communication about risks in total. The way of communication depends on the size of the risk and how long it lasts. However, it is not clearly established which type of communication has to be used exactly at every moment. With regard to risk maturity, Radboudumc falls under level four, 'Quantitatively managed'. Risk management is carried out well, although some processes could be improved, such as setting goals and communication about risk management.

4.2.2 Philips

At Philips different employees are added to development projects to manage risks. They are responsible for the risks which are faced. The ultimate responsibility lies with the project management team. This is the foundation of the department. The people who are responsible for risks also have knowledge of laws and regulations that apply to certain matters. They have to demonstrate they have this knowledge by means of tests or checklists. Philips is a regulated business so complying to laws and regulations is very important. The objective of risk management at Philips is to keep projects manageable. This means preventing loss of investment. For this to be achieved, all risks that could affect the project must be known. However, they do not have specific goals regarding risk management. Every month they have meetings with the project teams to find and discuss risks. All the people at the meeting have to write down new risks they have faced. As soon as a risk is identified it gets assessed as well. Templates and guidance are used for that to see what the severity and impact are. Part of the identification and assessment of risks is the performing analysis. This is of vital importance, especially with product risks, because you need to know the cause to solve it. When the risks are discussed, a date is linked to it. Within that time it has to be solved. It depends on the severity and impact of the risk whether the risk is addressed immediately or not. The risk management process runs once a month. Besides, they work with milestones. When a milestone is reached the risk management process is performed as well. It is not really looked at whether the process performs and works well for everybody. When a problem is encountered they look at it, but there is no frequent review. The risks that are faced are all recorded in a risk register system called Clarity. Other information like the cause and impact are recorded here as well. Risks

are communicated very often. There are weekly meetings and every month the project team has to send a report to the managers about the state of the project. One of the boxes that has to be filled in is 'the top 3 risks that are faced'. With regard to risk maturity, Philips falls under level four 'Quantitatively managed'. Risk management is executed quite well, however there is still room for improvement. There are no specific goals and the risk management process is not reviewed either.

4.2.3 Coolrec

The management team and SHEQ manager of Coolrec provide tools and procedures which help with executing risk management. The responsibility of risks goes bottom-up. Firstly, when risks are faced the people in the workplace are responsible to report it. Then, the SHEQ officer is responsible for taking action to mitigate the risk. The ultimate responsibility lies with the site manager when a risk leads to an incident, for example. Coolrec has to check every year whether they are compliant with laws and regulations. The laws and regulations get updated every year, which means it has to be checked every year as well. Further, the top management team suggests objectives regarding risk management. An example of an objective is zero accidents. A risk analysis is performed when a new machine is installed or when there is a new regulation. When the line changes, the risk analysis is updated. They take a close look from the beginning till the end of the machine. Every risk that is seen is recorded. When people start working they report near misses or incidents and update the risk analysis. After identifying risks they get assessed with the help of the Kinney method. This is a risk classification method. The cause of the risk always becomes clear when the risk is identified and mapped. After the risk analysis, immediate action is taken. If it is easy to solve, it will be done the same day. If it is hard to solve, somebody will be asked to do it. The risk analysis is reviewed once a year if there are no changes. An external auditor of ISO told them it is not necessary to review it when there are no changes. They get audited by ISO once a year, but also by WEEELABEX and ECOLOGIC once a year. The auditors always want to see the risk reports. Therefore, all the risks are recorded in the risk analysis. Risks are always communicated during toolbox meetings once a month. Besides, at every machine and line there is a 'Lock Out Tag Out' station. Everybody who works at the workplace has knowledge about the risks, but here it can be seen what the risks are as well.

With regard to risk maturity, Coolrec falls under level 5 'Optimizing'. Risk management is fully integrated into the culture of the organization and is a permanent part of the decision-making processes. All processes are executed well.

4.2.4 Essent

At Essent risk management is seen as important. Therefore, people are assigned to those processes and money is set aside for this. The people who perform risk checks and carry out the operational matters are responsible for executing this. The ultimate responsibility lies with the risk and compliance manager. Further, Essent is very strict about complying to laws and regulations. Legislation really is a pillar. They focus on privacy and information security. On the other hand, they do not really have objectives regarding risk management. They only have some KPIs regarding quality and fraud, for example. To achieve these KPIs, they carry out monthly self-control assessments. Identifying risks is part of this control. The risk assessment is done in advance at Essent. If a risk has a major impact, weekly or daily checks are performed. It does not only involve the impact, but also the probability. The cause mostly becomes clear when a problem arises. The processes are set up based on the cause and assessment. If a major risk is identified it is addressed immediately. When it concerns a smaller risk it can be addressed later or be accepted. How often this risk management process is performed depends on the risks and problems. Most often it is done every month, but if it concerns a smaller risk it can be done annually as well. Besides, this process is reviewed every month as well. They are very strict about what you hand in and whether you hand it in on time. It all gets checked. The risks that are identified are recorded in their risk register system called Zenya. This is just a new system that they are using and all information regarding risks is stored here. There is some communication with the help of Zenya, but not a lot. There are a lot of people who are probably not aware that some risk analyses are performed. This shows there is a lack of communication. With regard to risk maturity, Essent falls under level four 'Quantitatively managed'. Risk management is carried out well, although some processes could be improved, such as setting goals and communication regarding risk management.

4.3 Influence of Strategic Risk Management on Operational Risk Management

At Radboudumc they indicate that the establishment of risk management makes a positive contribution to the execution of risk management. There are plenty of tools and documentation to help with this. However, they notice that many people have no experience with these tools and documentation, so that the contribution is smaller than it could be. As a result, too little support is provided at the moment. A method that works well with the tools and documentation has to be found for everybody. At Philips they indicate as well that the establishment of risk management makes a positive contribution to the execution of risk management. It just does not work without proper tools. Everybody works on the same platforms, which makes it very easy for project and program managers to get an overview of what is happening across the projects. They say this contributes to mitigating and tackling risks. At Coolrec they think the establishment of risk management supports the execution of risk management as well. Since two years they are working more systematically and everybody is getting more familiar with the platforms and tools. It gets increasingly clear to everyone where to find what and how to use it. The knowledge level of the entire organization is growing in that area. For example, they have procedures on all machines. So, if there is someone who does not know how to do something safely with the machine, they can see it there. This helps a lot. Lastly, at Essent they think as well that the establishment of risk management has a positive influence on the execution of risk management. Risk management is very structured at Essent with a first, second and third line. The procedures they have got are also fairly mature and the tooling they use is very extensive. They indicate this helps a lot to find and handle risks. All in all, all interviewed companies believe that the establishment of risk management makes a positive contribution to the execution of risk management. Tools, platforms and procedures that are used make things very clear and easier to tackle risks.

4.4 Contribution To Innovation Projects

At Radboudumc there is a lot of innovation. They are constantly working on continuous improvement to do everything better for healthcare, but also for their own processes. However, these innovations are not always rolled out

successfully. Sometimes there is a lack of communication about the innovations and sometimes problems come up when it is implemented. This means that it sometimes has to be rolled back. At Philips they are always trying to innovate as well, but the projects they work on are very long processes. It is hard to assess how successful their innovations are, because the innovations take so long. The projects always pass through different phases in which they are tested again and again. At Coolrec they innovate quite successfully. In the last two years they have been doing these processes much more systematically. In addition, they have built in more milestones to verify whether they are still on the right track. Because of this it hardly happens that they implement an innovation and then stop again, because otherwise they would have stopped doing it at an earlier stage already. Lastly, Essent does try to innovate but not that much. When they want to innovate it takes a very long time before the innovation is fully implemented, because it has to work and be completely safe. It has to be checked very carefully. Because of this the innovations are mostly implemented successfully. When they want to innovate, it usually involves large innovation projects.

4.4.1 Contribution Of Strategic Risk Management

At Radboudumc they think that the establishment of risk management can both have a positive and negative influence on the success of innovation projects. This depends on how well the risk management is established. They are convinced that there is only room to innovate when the basics are in order, which is aided by structuring risk management. When the basics are in order there is more stability which contributes to innovating more and better. However, when the basics are not in order they experience there is no room for innovation. It is more of a brake on innovation in that case. At Philips they consider that strategic risk management contributes to the success of innovation projects. The systems and tools which are used for risk management show the innovators what they have to take into account. However, there is room for improvement in this area at Philips. It has to be better ensured that it is known to the innovators what has to be taken into account. For this, communication must be better organised, there must be a process around it and structured meetings must be set up for this. At Coolrec they think it contributes to the success of innovation projects as well. All risks and procedures are recorded in their management system. There is more overview now than there was previously. Analyses and risks can

be found easily. Based on the information following from this, innovations might come up. Lastly, at Essent they think it can have both a positive and negative influence. It can have a positive influence, because it provides structure for innovation. The risk department has set up business support meetings where one gets approval from all staff units to continue with a project. This provides structure, content and speed. However, they also notice that staff units try to remove a piece of innovation from the project and try to stop the innovation. In some cases this is not necessary, because the risks have a very low probability. In this way the set up of these business support meetings can have a negative influence. All in all, not all companies think alike when it comes to the influence of strategic risk management on the success of innovation projects. Philips and Coolrec believe that it has a positive contribution. Radboudumc and Essent believe that it can both have a positive and a negative contribution.

4.4.2 Contribution Of Operational Risk Management

At Radboudumc they indicate that the execution of risk management has a positive contribution to the success of innovation projects. There are certain risks and malfunctions that come to light in the risk management process that is carried out at Radboudumc. These risks and malfunctions can lead to changes. This means that what they carry out in terms of risk management can actually lead to changes within their process. However, at Philips they think that the execution of risk management does not have an influence on the success of innovation projects. Innovators should just come up with ideas and not be immediately held back by risks that are identified. They should always develop the benefits from the idea as well as possible. Then all the risks and problems have to be solved one by one. At Coolrec they think it contributes to the success of innovation projects. With every change the possible impact is figured out. That is in fact the mapping of new risks or changes in risks. With every change they start with risk management to find out what the possible risks of that change are. This helps them with implementing the change. Just like at Philips, at Essent they think the execution of risk management has no influence on the success of innovation projects. The execution of risk management is very important for Essent. It has to be done well and everyone is aware of that, but it is not something that is very much included in innovations. It is mostly not taken into account when they are looking for innovations. The risk analyses they do are for their customers.

For example, they look at customer fraud. This has not much to do with innovations within their own department or organization. It would only have to do with it if they want to innovate fraud detection for customers. All in all, the perceptions about the contribution of operational risk management on the success of innovation projects are divided. Radboudumc and Coolrec think it has a positive contribution, while Philips and Essent think it does not contribute in any way.

4.5 Differences and Areas For Improvement

Earlier in this chapter, based on the theory from Chapter 2, we looked at how risk management is established and executed at four different organizations. In addition, the influence of this on innovation projects within these companies was examined. The similarities and differences between the organizations in these areas are summarized below in Tables 4.1 and 4.2. Based on this table, points for improvement are then given.

4.5.1 Similarities and differences

Subject	**Radboudumc**	**Philips**
Establishment of Risk Management		
Governance & Culture	Coordination from top management. Risk & Audit department at corporate level.	Coordination from the board. Risk department at corporate level.
Strategy & Objective-Setting	The management team has set up risk management goals. Risk tolerance is clear within the IT department.	No attention has been paid to set up risk management goals. Risk tolerance is clear.
Performance	A risk framework has been set up to identify, assess and handle risks.	A risk framework has been set up to identify, assess and handle risks.
Review & Revision	The risk management process has to be reviewed once a year.	The risk management process does not get reviewed at regular intervals, but when there are changes.

Table 4.1 – continued from previous page

Subject	**Radboudumc**	**Philips**
Information, Communication & Reporting	Risks have to be registered in the risk register. No thought has been given to communication regarding risks.	Risks have to be registered in their own risk register. Risks have to be communicated during monthly risk meetings.
Execution of Risk Management		
Resources & Responsibility	Resources are provided for risk management. People are assigned to risks and laws and regulations are taken into account.	Resources are provided for risk management. People are assigned to risks and laws and regulations are taken into account.
Objectives	Risk management goals are not known.	They have to keep projects manageable, but there are no specific goals.
Quality of Risk Control	Risks are identified, assessed and handled. This is a continuous process.	Risks are identified, assessed and handled. This is done once a month.
Review & Revision	Risk management process is reviewed once a year.	Risk management process only gets reviewed when there are problems.
Communication & Reporting	Risks are registered in their risk register system. They have five different ways of communication, not clear which way to use in what situation.	Risks are registered in Clarity. Risks are communicated during weekly meetings.
Success of innovation projects and the contribution to innovation projects		
Contribution of establishment of risk management on execution of risk management	Positive contribution	Positive contribution
Degree of successful innovation projects	Innovations are not always rolled out successfully.	Hard to assess how successful their innovations are, because their innovations take so long.

Table 4.1 – continued from previous page

Subject	Radboudumc	Philips
Contribution of establishment of risk management on success rate of innovation projects	Can have a positive and negative contribution.	Positive contribution
Contribution of execution of risk management on success rate of innovation projects	Positive contribution	No contribution

Table 4.1: Similarities and differences; Radboudumc and Philips

Subject	Coolrec	Essent
Establishment of Risk Management		
Governance & Culture	Coordination from director, SHEQ manager and operations manager. Risk management department at mother company.	No coordination from top management. Risk departments within the Sales department.
Strategy & Objective-Setting	Risk management goals have been set up. These are considered as very important. Risk tolerance is clear.	No attention has been paid to set up risk management goals. Risk tolerance is clear.
Performance	A risk framework has been set up to identify, assess and handle risks.	A risk framework has been set up to identify, assess and handle risks.
Review & Revision	The risk management process has to be reviewed once a year.	No real thought has been given to reviewing the risk management process, only happens if the internal audit gets hold of it.

Table 4.2 – continued from previous page

Subject	**Coolrec**	**Essent**
Information, Communication & Reporting	Risks have to be registered in a standard risk register. Risks have to be communicated during monthly toolbox meetings.	Risks have to be registered in the risk register system called Zenya. No thought has been given to communication regarding risks.
Execution of Risk Management		
Resources & Responsibility	Resources are provided for risk management. People are assigned to risks and laws and regulations are taken into account.	Resources are provided for risk management. People are assigned to risks and laws and regulations are taken into account.
Objectives	Goals are suggested by top management.	Risk management goals are not known.
Quality of Risk Control	Risks are identified, assessed and handled. This is done when there is a new machine or when an existing machine has changed.	Risks are identified, assessed and handled. This is done once a month.
Review & Revision	Risk management process is reviewed once a year.	Risk management process is reviewed once a month.
Communication & Reporting	Risks are registered in the risk analysis document. Risks are communicated during monthly toolbox meetings.	Risks are registered in Zenya. Hardly no communication regarding risks.
Success of innovation projects and the contribution to innovation projects		
Contribution of establishment of risk management on execution of risk management	Positive contribution	Positive contribution
Degree of successful innovation projects	Their innovations are most often implemented successfully.	Their innovations are most often implemented successfully.

Table 4.2 – continued from previous page

Subject	Coolrec	Essent
Contribution of establishment of risk management on success rate of innovation projects	Positive contribution	Can have a positive and negative contribution.
Contribution of execution of risk management on success rate of innovation projects	Positive contribution	No contribution

Table 4.2: Similarities and differences; Coolrec and Essent

4.5.2 Points For Improvement

In this subsection, the points for improvement are formulated per organization on the basis of Tables 4.1 and 4.2.

With regard to Radboudumc, the following points for improvement can be identified from the analysis above:

- Top management/risk managers have to explain the risk management objectives to the employees within IM. This is important, so that it is clear to everyone what exactly is focused on.
- Choose one or a few ways instead of five ways of communicating with regard to risk management. In this way, those involved know which ways will be used in what situation.
- Make it clear when exactly which form of communication has to be used.
- Hold monthly or weekly risk meetings with managers from different departments within IM. In this way everyone knows what is going on and where the focus lies.

- Instruct the MT to request the internal audit service to do an audit regarding risk management (they are already planning to do this).
- Give presentations or training to employees so that they know better how to work with documentation and tools.

With regard to Philips, the following points for improvement can be identified from the analysis above:

- Set up risk management goals. This is necessary to keep the focus on what is important.
- Communicate these goals to everybody who works with risks. In this way everybody knows where the focus lies.
- Review the risk management process on a regular basis. When you are only going to review it when there is a problem, you are already too late.
- Set up meetings on a regular basis with innovators and employees from risk management. They also indicated that they want to do this, because in their eyes it can be beneficial for the innovators. In this way, they can know what to take into account.

With regard to Coolrec, no points for improvement can be identified from the analysis above. They both establish and execute risk management very well.

With regard to Essent, the following points for improvement can be identified from the analysis above:

- Involve top management in the subject of risk management, so that it is not only supported by the Sales department.
- Set up risk management goals. This is necessary to keep the focus on what is important.
- Communicate these goals to everybody who works with risks. In this way everybody knows where the focus lies.
- Set up a plan regarding reviewing the risk management process. This is not clear right now. Nothing has been established, however it is still executed once a month.

- Hold monthly or weekly risk meetings with managers from different departments within Sales. This way everyone knows what is going on and where the focus lies.

Chapter 5

Conclusion

This study seeks to answer the question: 'How do strategic and operational risk management influence the success rate of innovation projects and how does strategic risk management influence operational risk management?' To this end, a qualitative study was conducted at four different organizations.

The first proposition is: 'The better strategic risk management is established, the better operational risk management is executed.' The results show this is consistent with this study. All interviewees of the organizations indicate this. By having a good structure in the field of risk management, everyone knows where to find what information. The presence of documentation, tools and platforms that are used by everyone make it easier to carry out a risk analysis in the end. However, it must be said that one organization has not established risk management properly, making it difficult for them to know exactly what the influence is of strategic risk management on operational risk management.

Further, the second proposition is: 'The better strategic risk management is established, the more successful innovation projects are.' This is in line with the results of this study as well. Two organizations indicate that strategic risk management has a positive influence on the success of innovation projects, because the systems and tools show the innovators what to take into account and innovations may arise from this. The third organization indicates it has a positive influence when strategic risk management is well established, because it provides more stability, which aids in innovation. However, if it

is not well established, it can hamper innovation. The fourth organization indicates that strategic risk management provides structure, content and speed in innovation projects. On the other hand, innovation projects must be approved by multiple staff units when risk management is well established. They notice that these staff units could try to remove a piece of innovation from the project because of risks. This is sometimes unnecessary, because the risks involved are small. As a result, it can have a negative influence on the success of innovation projects. However, the fourth organization has not established its risk management properly, so that they cannot really determine what effect it has on the success of innovation projects. Therefore, their perception of success cannot be included in the concluding answer.

Finally, the third proposition is: 'The better operational risk management is executed, the more successful innovation projects are.' This is not in line with the results of this study, since it has emerged that there is no unambiguous effect of operational risk management on the success of innovation projects. Two organizations indicate that it makes a positive contribution, because risks and malfunctions become visible by carrying out risk management. This helps with the development of innovations or it can make it clear that innovation is required. The other two organizations indicate that it has no effect on the success of innovation projects. This is because risk management is not taken into account in innovation projects. Innovators should simply focus on ideas and innovations and not be immediately held back by risks. Based on risk maturity, all organizations execute risk management well. This also allows these organizations to determine whether this affects the success of innovation projects within their organization.

This qualitative research has shown that the better strategic risk management is established, the more successful innovation projects are. Besides, it has shown that strategic risk management has a positive influence on operational risk management as well. Furthermore, it is seen that operational risk management does not have a clear effect on the success of innovation projects. When it is taken into account, it can have a positive influence. However, in practice it is not always taken into account, because the degree of innovation can stagnate as a result. Based on these results, we conclude that organizations should focus on properly establishing risk management. This can contribute to organizations that focus on innovation projects as well as organizations that focus on executing risk management.

Chapter 6

Discussion

This chapter discusses the conclusions and recommendations drawn based on the results of the interviews. The results are interpreted first, followed by the contribution to the knowledge. After that the practical implications and limitations of the study are discussed. Finally, some directions for further research are given.

6.1 Interpretation of the Results

Not all results of this study match the expectations. However, the first proposition 'the better strategic risk management is established, the better operational risk management is executed' is consistent with the results. All organizations indicate that they experience that the presence of tools, documentation and platforms contribute to a good execution of risk management. This is in line with the theory in which Bogodistov and Wohlgemuth (4, 2017) indicate that strategic risk management sets the priorities for operational risk management.

Besides, we observe that the results of this study match the second proposition 'the better strategic risk management is established, the more successful innovation projects are' as well. Three organizations indicate it has a positive influence, due to various reasons. It is said that tools and systems which are set up show innovators what to take into account. Besides, it is also said that it provides more stability which helps in innovation projects. This is

in line with the theory of Bowers and Khorakian (5, 2014) who state that risk management in general helps in achieving success in innovation projects. They indicate that risk management is fundamental to effectively filter the good and bad prospects of innovation projects. In other words, it means that it makes clear what should and should not be taken into account. Only the fourth organization indicates it can have both a positive and negative contribution. However, they have not well established their risk management, so that their perception has not been included in the final answer.

Finally, the last proposition 'the better operational risk management is executed, the more successful innovation projects are' does not match the results of this study. Two organizations indicate that it has a positive influence, because risks and malfunctions become visible by carrying out risk management, which helps with the development of innovations. If high risks or malfunctions become clear by executing risk management in the initial phase of an innovation, the innovation project can be abandoned or moved in a different direction. This is in accordance with the theory of Bowers and Khorakian (5, 2014) as well, because they state that by applying proper risk management in general, bad innovation projects can be abandoned in time. On the other hand, the other two organizations indicate that operational risk management has no influence on the success of innovation projects. According to them, this is because the execution of risk management is not taken into consideration in innovation projects. They say innovation projects should not be held back immediately by possible risks. A solution for immediate risks at a later stage. This does not correspond with the theory of Bowers and Khoarkian (5, 2014), because in the theory they assume that risk management is taken into consideration in innovation projects. Based on the results from this study, it can therefore be stated that if risk management is taken into consideration, it can have a positive contribution to the success of innovation projects. However, in practice it is not always taken into consideration in innovation projects, because it can stand in the way of innovation as well.

The results show that it is important to set up risk management properly. It not only contributes to the execution of risk management, but also to the success of innovation projects. It appears that setting up tools, documentation, platforms, systems and so on provides structure and stability, which is useful in innovation projects. However, the execution of risk management does not have an unequivocal positive contribution to innovation projects.

It can show which risks must be taken into account, but it can also unnecessarily stagnate the degree of innovation. As a result, it is often not taken into account in innovation projects.

6.2 Contribution to the Knowledge

The contribution of this study to the existing knowledge is that it is especially important to properly establish risk management with regard to innovation projects. This is more important than properly executing risk management. Strategic risk management provides structure and stability, which not only benefits the execution of risk management, but also the process of innovation. In addition, the fact that operational risk management does not always contribute to innovation projects is also a new insight. It can have a positive contribution, because it shows which risks must be taken into account. On the other hand, it is not always taken into account, because it can unnecessarily and undesirably stagnate the degree of innovation. Furthermore, it is also found that strategic risk management has a positive influence on operational risk management. All interviewees indicated this. However, Bogodistov and Wohlgemuth (4, 2017) stated this as well already. They said that strategic risk management sets the priorities for operational risk management. This is therefore not a new insight, but a confirmation of the existing theory.

6.3 Practical implications

The results of this study serve as an example for other organizations. The results can give other organizations ideas on how to better set up and execute their risk management. In combination with the models given in Chapter 2, other organizations can take a look at how well their risk management is structured and where there is room for improvement. In this study organizations from different markets were interviewed. These organizations have set up their risk management in very different ways. As a result, there are varied examples that show how you can structure your risk management. This can bring up ideas that organizations themselves had not yet thought of. It is useful for organizations who focus on innovation, but also for organizations who are less innovative and just want to improve their risk management.

Furthermore, the information from this study is also useful for the organiza-

tions that participated in this study of course, because they can see in which aspects they can improve. In addition, they can also learn from the set up and execution of risk management at other organizations.

6.4 Limitations

This study has a number of limitations. Firstly, the research was carried out at four different organizations, which means that the results of this study can only be applied to these four organizations and cannot simply be extrapolated to other organizations. In addition, only two employees were interviewed at every organization. This does not provide a comprehensive view of risk management across the whole organization. At Radboudumc two employees were interviewed from the department Information Management, for example. This provides a good view of risk management at Information Management within Radboudumc. However, it does not provide a view of risk management at other departments. Risk management at other departments can be quite different, because totally different risks are faced. This shows there is no comprehensive view of risk management across the whole organization.

Moreover, this study shows that Essent has made relatively limited efforts to establish risk management. As a result, a number of variables from the COSO ERM model could not or could hardly be measured. In a follow-up study it would be useful to only have organizations who have set up risk management well. Furthermore, the communication with one respondent was a bit hard sometimes. He works and lives in Belgium, making French his native language. He does not speak English very well, so he sometimes did not understand the questions properly. This made communication difficult at times. Finally, one respondent had only been working for the relevant organization for three months at the time of the interview. This made it difficult for this person to tell how successful innovation projects are. The respondent did have an idea about this and answered the question, but he still found it difficult to estimate how successful innovation projects are. In a follow-up study, it could therefore be useful to only interview employees who have been working at an organization for one year, for example.

6.5 Directions for Further Research

This study mainly looks at the establishment and execution of risk management. A number of variables in the establishment of risk management could hardly be measured, because one organization had hardly set up their risk management. It would therefore be a good idea to conduct the study again at organizations which have all fully set up their risk management. Besides, it would also be a good idea to look at more than four organizations. Then the results may be more generalizable as well.

Further, it would be good to do more extensive research within the organizations. This study is based on interviews from two employees from every organization. In this way it is hard to get to know whether risk management is established and executed well within the whole organization. At Radboudumc, for example, this study interviews two employees of the Information Management department. This gives a good view of risk management within the Information Management department, but it does not provide insights on how other departments have organized and implemented their risk management within Radboudumc. To get a general picture of Radboudumc's risk management, people from several departments should be interviewed. In this way it can be checked whether risk management has also been set up in a proper way throughout the whole organization.

To assess how well a company has established risk management, the COSO ERM model is used in this study. The COSO ERM model contains five different components: 'Culture & Governance', 'Strategy & Objective-Setting', 'Performance', 'Review & Revision' and 'Information, Communication & Reporting'. The organizations in this study were assessed on each component based on specific questions. However, the impact of these components has not been examined. It might be possible that one component is seen as more important to foster innovation projects than other components. It could be interesting for further research to get more in-depth information about the components of the COSO ERM model. This can then reveal which components are the most important according to organizations and which therefore have the most influence on innovation projects. With that knowledge, you could also pay more attention to certain parts of risk management as an organization.

Chapter 7

Bibliography

[1] Afuah, A. (2003). Innovation Management: Strategies, Implementation, and Profits, 2nd ed., Oxford University Press, New York, NY.

[2] Bleady, A., Ali, A. H., & Ibrahim, S. B. (2018). Dynamic Capabilities Theory: Pinning Down A Shifting Concept. Academy of Accounting and Financial Studies Journal, 22(2), 1.

[3] Bleijenbergh, I. (2015). Kwalitatief onderzoek in organisaties (2e druk). Den Haag: Boom Lemma Uitgevers.

[4] Bogodistov, Y., & Wohlgemuth, V. (2017). Article information: The Journal of Risk Finance, 18(3), 234–251

[5] Bowers, J., & Khorakian, A. (2014). Integrating risk management in the innovation project. *European Journal of Innovation Management*, 17(1), 25–40. https://doi.org/10.1108/ejim-01-2013-0010

[6] Bromiley, P., McShane, M., Nair, A. and Rustambekov, E. (2015). "Enterprise risk management: review, critique, and research directions", Long Range Planning, Vol. 48 No. 4, pp. 265-276.

[7] Carbonara, G., and Caiazza, R. (2010). "How to Turn Crisis into Opportunity: Perception and Reaction to High Level of Uncertainty in Banking Industry", Foresight, Vol. 12, No. 4, pp. 37-46.

[8] Eisenhardt, K.M. & Martin, J.A. (2000). Dynamic capabilities: what are they? Strategic Management Journal, 21(10-11), 1105-1121.

[9] Elahi, E. (2013). How Risk Management Can Turn into Competitive Advantage: Examples and Rationale. UMASS Boston.

[10] Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. Journal of Corporate Accounting & Finance, 22(3), 81–88. https://doi.org/10.1002/jcaf.20677

[11] Genus, A., & Coles, A. (2006). Firm Strategies For Risk Management In Innovation. International Journal of Innovation Management, 10(02), 113–126. https://doi.org/10.1142/s1363919606001429

[12] Hamel, G. & Valikangas, L. (2003). "The quest for Resilience", *Harvard Business Review*, Vol. 81, No. 9, pp. 52-63.

[13] Johnson, M.W. (2010). "Risk management and innovation", Business-Week.com, 11 September,p. 2.

[14] Justesen, L. N., & Mik-Meyer, N. (2012). Qualitative research methods in organisation studies: Gyldendal.

[15] Kaplan, S. and Garrick, B. J. (1981). "On the Quantitative Definition of Risk", Risk Analysis, Vol. 1, No. 1, pp. 11-27.

[16] Krickx, G. A. (2000). "The Relationship Between Uncertainty and Vertical Integration", The International Journal of Organizational Analysis, Vol. 8, No. 3, pp. 309-329.

[17] Luhmann, N. (2005). Risk a Sociological Theory, Aldine Transaction.

[18] Mu, J., Peng, G. and MacLachlan, D.L. (2009). "Effect of risk management strategy on NPD performance", Technovation, Vol. 29 No. 3, pp. 170-180.

[19] Nechaev, A. S., Ognev, D. V., & Antipina, O. V. (2017). Analysis of Risk Management in Innovation Activity Process. Irkutsk National Research Technical University, 548–551.

[20] Ozer, M. (2006). "New product development in Asia: an introduction to the special issue", Industrial Marketing Management, Vol. 35 No. 3, pp. 252-261.

[21] Paape, L., D.M. Swagerman, (2006). — Risicomanagement - De Praktijk In Nederland, rapport Rijksuniversiteit Groningen.

[22] Palmberg, C. (2002). Successful innovation The determinants of commercialisation and break-even times of innovations. VTT Technical Research Centre of Finland, 1–74.

[23] Power, M. (2007). Organized Uncertainty – Designing a World of Risk Management, Oxford University Press.

[24] Proença, D., Estevens, J., Vieira, R., & Borbinha, J. (2017). Risk Management A Maturity Model based on ISO 31000. IEEE, 99–108.

[25] Sekaran, U., & Bougie, R. (2016). Research Methods For Business. Wiley.

[26] Simon, R. (2009). "New product development and forecasting challenges", Journal of Business Forecasting, Vol. 28 No. 4, pp. 19-21.

[27] Stevens, G. A., Burley, J. (1997). 3,000 raw ideas = 1 commercial success!. Research-Technology Management, 40(3), 16-27.

[28] Taplin, R. and Schymyck, N. (2005), "An interdisciplinary and cross-cultural approach", in Taplin, R. (Ed.), Risk Management and Innovation in Japan, Britain and the United States, Routledge, London, pp. 1-20.

[29] Teece, D. J. (2007). Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319–1350. https://doi.org/10.1002/smj.640

[30] Teece, D.J., Pisano, G. & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7): 509-533.

[31] The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management - Integrating with Strategy and Performance. COSO.

[32] Wang, J.T., Lin, W. and Huang, Y.H. (2010). A performance-oriented risk management framework for innovative R&D projects, Technovation, Vol. 30 Nos 11-12, pp. 601-611.

[33] Yin, R. K. (2015). Qualitative research from start to finish: Guilford publications.

[34] Zhao, J.G. (2005). "Marrying risk register with project trending", AACE International Transactions, Vol. 10 No. 6, pp. 1-6.

Appendix

Appendix A: Interview Reports

Coolrec - SHEQ Manager

1. Risk management is very important on a very broad level. It starts with risk management of business risks. Mapping out the risks of your market, your customers, safety, the environment and calamities. So very broad. We have a risk matrix at business line level. Then also at the various sites, so at site level. As well as risk matrices, the TRAs (Task Risk Analysis) at activity level. The TRA we have on the refrigerator line, FDA line or whatever. So risk management is completely in our DNA, I might say. If you do not control your risks, you will simply have an impact on your continuity. Then it may be that, for example, part of your installation burns down, then you cannot meet the customer's wishes. So what our main drive is, is to satisfy the customer and to do that you just have to have a continuous process. Continuing on business operations, but also ensuring that no incidents occur. If someone loses their arm tomorrow, we have a problem. So that continuity is just very important and you do that by looking ahead. So manage your risks.

2. At Renewi level (parent company) we have a risk management department and there are a number of standards there. From there, Coolrec is already coordinated. At Coolrec level there is coordination from both the director, myself and our finance man who are continuously working on various implementations related to risk management. We also have systems for that. Our operations director is also continuously working on minimizing the risks of his operations, otherwise he cannot meet the requirement to just run every day.

3. There is a risk management department from Renewi (parent company). Within Coolrec I have an active role as a risk manager to coordinate it from my SHEQ side. From the Q: quality and S: safety. These parts include risk management as well.

4. Yes, for example to keep it close to home: no incidents with absenteeism. So prevent people from losing limbs, for example. But there are also objectives with regard to improvement processes, to make processes run even better with even fewer disruptions. That is also risk management: the fewer failures, the fewer risks you have. Much attention is paid to achieve these goals. Every month in the business review, so when the MT has discussions with the sites, we look at the objectives. Some goals are not achieved or are achieved later, but that is part of life, let's say. I think most goals are realistically achieved.

5. Yes, we have certainly thought about that. Safety first. We use the system: you have an initial risk, then you quantify that risk. You do that with a matrix. Then you quantify whether it is a high, medium or low risk and you can then add a number to that. You will then take control measures to reduce the risk. Ultimately, you are left with a residual risk and if that residual risk is very low, you accept that. For example, I am in a car and the risk of an accident is not 0, because we know that there are accidents. But I accept it, so we are trying to bring it down to an acceptable level and we're actually trying to do that in all areas. In all areas we use the system of initial risk, control measures, residual risk and bringing it to an acceptable level. You can quantify that.

6. Yes, I just explained that. We have a fixed system for that. We have an initial risk and we quantify it. We do this with a matrix. Then we quantify whether it is a high, medium or low risk and we can then add a number to that.

7. Yes, we do indeed look at the impact of the risk and the likelihood that the risk will occur. These two factors times each other give a score, which indicates how high or low the risk is rated. In this way they can also be prioritized.

8. Yes, if there are risks that are still too high, we must take additional measures. These come in a plan of action and we follow this regularly. This is done in a systematic way. How often this is done, of course, depends on

how often there are deficiencies.

9. Yes, this has definitely been thought through. An RI&E is carried out once a year to see if there is anything new. For example, it may happen that the risk is still quite high, but that there are no known measures yet to reduce it. This is then reflected in such an RI&E. So there is an inner circle in that: I have a measure and I have to take action on it. There is also an outer circle in terms of assurance in which you check whether everything you have come up with is still current. We do this once a year. We assess the business risks (inner circle) every quarter and the general risks (outer circle) we assess once a year.

10. Yes, there is a standard risk register and a standard risk matrix is attached to it, which is defined at Renewi level. Results that emerge from the risk management process are recorded here. This is therefore the same for everyone, for all branches that carry out different activities. Whether it is a risk assessment in the field of safety, the environment, fire or business risks. We all do this with the same approach.

11. It is certainly communicated, but it is not always the same. Because you can imagine that communication to a customer is done in a different way than to an employee. You adapt your communication to the stakeholder. For example, looking again at my field: induction program for new employees. You provide insight into the risks of the work and thus limit the risks. This always happens the same way. Customers always receive our house rules, which also contain all kinds of rules to reduce the risks. This always happens in a fixed way.

12. Yes, I certainly think so. I have been working there for about two years now. When I came here, we started to take it more systematically. I do notice that it is becoming increasingly clear to everyone where to find what and how to read it. So by doing it systematically and uniformly, you also increase the knowledge level of the entire organization in that area. Of course it can always be better. We are linked to systems and also to systems from Renewi. Systems always have their limitations. You continue to keep your wishes, but I think compared to two years ago that we have already made many steps forward.

13. I think that in the last two years with the arrival of our new director, we have been doing this kind of process much more systematically. In addition,

we have built in more milestones to verify whether we are still on the right track. So it hardly happens that we start something and then stop again, because otherwise we would have stopped doing it at an early stage. It would have been stopped before we started it, because it does not produce what we want. Whether that will always be the case in the long run, sometimes you just have to try something and then you have to quit with it later, that is possible. In general this is going quite well.

14. Yes, I think it contributes to innovations. Having our risks in control is very important for us. We have all our risks recorded in our management system and all our procedures are in here as well. As I said before, people get to know better where and what they can find here. There is more overview in the structure. This contributes to innovations as well. Analyses and risks can be found easily, which may help with implementing innovations. Based on this, innovations might come up.

Coolrec - SHEQ Officer

1. Yes, sure. We have tools and procedures put in place by the management team. By the SHEQ manager. There are two kinds of risks. You have risks which you see and encounter everyday and you have risks which you find when you do a risk analysis. It means that when you have a new machine installed, you have to update the risk analysis. You take one, two or three people of the line and one of the management team. Then you start from the beginning where the machine is working until the end. You go to the people who work on the workstation. They have to tell you what they see and what they encounter as a risk. You write down all the risks and you ask them to take measures to avoid the risks. There are no specific people assigned to take measures. We do it on site. When we do a risk analysis we take people who work in that specific place and we take people from the management team. So also someone who is responsible for the production or the techniques. Then you do your risk analysis by asking people what they see as a risk and what measures we can take to avoid these risks.

2. The risk manager is responsible. First we define the risk. We take a look if we have seen or discussed this risk before. Legally the risk officer is not responsible for an accident for example. The site manager is responsible for his site and of all the risks. If there was a risk and this risk was written in the risk analysis, but no measures were taken. For sure the people at the production are responsible first and then the SHEQ manager. Then it depends on the accident whether it is fatal or not. The responsibility then goes from the bottom to the top. If a risk is new. This happens everywhere. You see the risks, but day by day you have new risks. For this reason people have to report all the risks in the workplace. It means it is a risk they have not seen before. You have to do a risk analysis everyday. Everyday things change and everyday you have to update things. This means people in the workplace are responsible to always report the risks. If this is done, measures can be taken. If accidents still occur, the managers are responsible.

3. Yes sure, absolutely. Every year you have new laws and regulations, so every year we have to update the laws and regulations we have to manage as well. Every year we have to check if we are still compliant or not. You always have to be compliant regarding the law and the authorities. So you need to be very aware of the new laws and how to deal with them.

4. If we talk about accidents for example, the goal is defined by the board. They tell us zero accidents, but this is not possible. They push you to reduce the number of accidents. How we can reduce the number of accidents is by reporting the near misses (dangerous situations which could lead to accidents in the future) and by working on the near misses. When a near miss is not reported, it becomes an accident. We always have to do the same job and we always have new things to update our risk analysis. We have to report to ensure a near miss does not become an accident. So we have goals which are suggested by the top management. They say for this year we want zero accidents for example. Everybody knows it is not possible, but we have a target and everybody is fixed on zero accidents.

5. The risks are identified when you install a line or when you make some changes on your line. First you have to identify your first risks. This means that you have to put protective measures concerning the conveyor belt, the stairs etc. Everything you see at the first time, you have to report them. You deal with it in your risk analysis. Then when people start working, they report the near misses or the incidents and you update the risk analysis regularly. This depends on the nature of the incident that is reported. The procedures are known by everybody. For example when you have a conveyor belt, everybody knows you have to cover it. When you have a motor, you have to cover it. When you have stairs and it is slippery, you have to put something on the stairs to prevent it from being slippery. Everybody knows it by the procedures. The first time you see a machine everybody knows the risks by knowing all the procedures. Then day by day you discover new risks and you update the risk analysis.

6. When you do the risk analysis, we use a method called Kinney in Belgium. It means that when a risk is in the range from 1 to 3, it is acceptable. If it is in the range from 3 to 4 you have to take measures. If it is from 5 to 7, it becomes red. Then you have to give a material response. For example you have a conveyor belt. This is a very high risk, so that means you have to take physical action. It means you have to cover the conveyor belt. When stairs are slippery, you can cover the stairs which avoids falling. If not, you can ask them to clean the stairs everyday. So for example you can put in procedure the first shift has to clean the stairs at 6 o'clock and the second shift has to clean the shift at 2 o'clock. So you put in procedures. Then you can manage the risk and everybody knows the risk. To ensure everybody knows about the risk, you have to do toolbox meetings.

7. Let's take the example of the conveyor belt again. When you do a risk analysis you first look at the place or spot where the risk occurs. The second part is to say what is the risk. So then you do your calculation and look at the measures you have to take. So you are going to cover the conveyor belt or I am going to ask people to clean the stairs periodically etc. You know the spot, then you identify the risk and then take a measure you need to take. When the risk is identified and mapped, normally it always gets clear what the cause of the risk is. The conveyor belt is a risk because it is moving and you can fall if people would stand on it for example. People could do that if something gets stuck for example. The stairs are a risk because it gets dirty and wet often, which makes it slippery.

8. Yes, risks are addressed immediately. For example when there are cables which cross the footpath, this could lead to people falling. If the measure is easy to fix, it can be done today and the risk analysis does not necessarily have to be updated. If it is harder to fix, because the cables can not easily be eliminated from the footpath for example, the risk analysis has to be updated. Then you ask someone to fix the problem.

9. When we have a new machine or when we have a new regulation, the risk management process is performed. Besides, when a new risk is seen at an already existing machine for example, the risk analysis is updated. So not the whole process is done again then, but it is updated.

10. Sure you have to review it, because every day, week, month or every time people report an incident, you have to reconsider your risk analysis. You have to make some adjustments in your risk analysis. For example, if you have cables at the entrance of a line which crosses the footpath. The first time you did not see it or you did not consider it as a risk. When people start saying you have to be careful, because they fell there, you have to consider this risk. There are two options: you ask to make changes in the cables or something and you report it. You can report it in the risk analysis and you ask people to fix the situation. Even if you would not write it down in your risk analysis, the work has to be done on the site. If it is not done, you will always have this problem. The other option is not to report it, but then you have to fix the problem today. We always work to avoid having problems on your line by reporting near misses and fixing them. The risk analysis is reviewed once a year if there is no change. I remember one day I was audited by ISO and the guy told me he had seen the risk analysis. It was updated

this year, but if there is no change on the line you do not have to update it.

11. It is all recorded in the risk analysis. The first thing an auditor will do is ask you about the risk analysis. He will see if it is updated or not. If it is not updated, you can say it is not updated because the line did not change. The line is in the risk analysis. We get audited often. ISO once a year, WEEELABEX once a year, ECOLOGIC once a year. You can be audited three, four, five times a year depending on the client and what type of audit. So all the risks are reported in the risk analysis, which we need for the audits as well. The impact and measures are noted there as well.

12. Risks are not communicated to clients or stakeholders, because they are not involved in the risks on the lines. The risk analysis is done internally and for people in the factory. You do not have to communicate it to the external part, because the external part is not going to work on the line. People who face the risk, have to know the risks of the line. Yes, all the risks are communicated well internally. Let's take the conveyor belt again as an example. When you cover it, you follow a procedure: Lock Out Tag Out. People have to be aware of the risk of the conveyor belt when it is not covered. Even if people do not know exactly all the risks of the line, we put in place procedures and toolbox meetings once a month. During the toolbox meeting we talk about risks and about procedures. This means they are aware about the risks of the line.

13. I think it is very useful. For example in Recydel, at each line we have a Lock Out Tag Out station. All the procedures of each machine about how you can work in safe conditions are in there. Even if people are new and do not know exactly the risks of the line. We have a toolbox meeting every year for the Lock Out Tag Out and how we deal with it. If we take an example from the technical department. If someone did attend the toolbox meeting, because he is new for example and does not know exactly the risks, we ask the management to teach him the Lock Out Tag Out. Then he has to do some maintenance on the line. He knows he has to take the locks and he knows by the procedures which are hanging at the Lock Out station what he has to do to work in a safe condition. It means for example he has to lock this electrical part and mechanical part before he can start working. So to answer your question, I think it helps a lot.

14. There is a lot of innovation and we are searching everyday for methods on how to work in a safe condition and without incidents. The innovations are

implemented successfully most of the time. Before we implement something, we have several meetings to know how it will work, what the risks will be and how we can deal with the risks. So you first do a study about this innovation and then you give it to the management team at the board of Coolrec and they approve it if they think it will go well.

15. Yes, I think it has a positive effect. That is what we mean by continuous improvement. There are ongoing projects at our location to improve our process. If you do that, we also have a procedure for that. One of the steps you start with is mapping out the possible consequences and possible impact of that change. So there you actually already do a risk assessment right at the start of your continuous improvement process. I am going to improve something, what are the possible effects? You can imagine if I use a different shredder somewhere or remove an air filter, that could have an effect on the fire risk or on the health of the employees. So that is actually always mapped. With every change the possible impact is figured out. That is in fact the mapping of new risks or changes in risks. Precisely because of how we have set it up and the systematic approach of the change. With that I think we can say that these things contribute positively.

Philips - Development - Project Excellence Lead

1. At Philips and in general what is called project management is risk management. I have not only heard this at Philips, but also in other places. Project management is about controlling all the processes from A to Z or the project from A to Z. Normally you have to be able to see which risks are on the horizon, catch them as soon as possible, identify and mitigate them to tackle them before they come too close to you. So in this aspect, I find it one of the most important things. When it is good, it can be ensured the project will be successful.

2. Risk management is coordinated from the board. There are meetings happening at different levels. So you can consider that the risks come from disciplines and it goes to the project manager, because the project manager has all the discipline leads. So all the risks come from the bottom to the project manager. The project manager is reporting to the department/program manager. If the projects cannot manage the risks at their level, they report it to a higher level. Then the program managers are reporting to the board. In that way it goes bottom up, but it also goes top down, because the organization has their own risks. When they look at the horizon they see risks at the organization level and they can influence the projects or departments in this way.

3. At the corporate level of Philips there could be a risk department, but I am not totally sure of that. I have only been working at Philips for 3,5 months, so that is why I am not sure at this moment. I know quite a lot, but I have not heard about risk compliance and risk at the corporate level, but there must be. If you have a minute, I am gonna ask my colleague. My colleague says there is a risk department at the corporate level. Lower in the organization we have project managers, who lead projects. They are risk managers as well, as I said earlier as well.

4. Goals are considered, but there is no standard guideline, because the risks can be quite unique and different. It is more like that you look at the risk, the definition of it and what it implies. Then you decide: sometimes you accept the risk, sometimes you mitigate the risk or sometimes you just take the risk of waiting, because you then need to measure how much it costs to mitigate versus the impact of the risk to decide to do nothing or mitigate.

5. It is like I explained at the previous question, it depends on the risk, the

definition of the risk and the initial evaluation and analysis of the risk. One thing that we do not do at my department is quantifying the risk in euros. That part we are not doing. We are qualifying the risks for their impact level and for their probability and depending on that we are taking action, but we are not quantifying.

6. Yes, the goal is to identify risks at the beginning of the project of course when the project is at the establishment/initiation phase. Then there are monthly project meetings, project risk meetings, where all members come together. They state any new risks coming into the picture and they discuss the mitigation state for the existing risks.

7. Yes, actually a tool is guiding us to assess risks. Our risk registration tooling. In the risk registration tooling we are entering and defining the risks, then we are qualifying the risk with the impact (high impact, low impact and legal impact) and the probability the risk is going to happen (percentages). Then we define the risk actions, so there are a lot of attributes for one risk which we are identifying. So it is not only a text for the risk definition, but all kinds of other attributes that come along with it. These are listed in the meetings and then followed up.

8. Yes, we set due dates for the risk to be lost, because some risks are only long term like one and a half years. You do not need to mitigate them right away. You need to make a priority among them. So for that reason, in those meetings it is discussed and due times are assigned. The idea is to close the risks before the due dates. What kind of action you take depends on the nature of the risk of course.

9. Let me think about it. If I say no, I am too quick, because it is done. The next one is done by myself for example. The process itself is written of course at Philips globally and at the departmental level. As we proceed with the continuous improvement, it is revised as well. This is not at regular intervals, so not every month or year for example. The process is reviewed only when there are changes. The changes are triggering the reviews. Because we do not have regular reviews every 6 months or year, we do it the other way around. When there is a change, we come back to the process and revise it. When there is a change based on the best experiences, lessons learned or continuous improvement actions.

10. Yes, those are the attributes I have mentioned earlier. One of the at-

tributes is the impact of the risk, the cause of the risk, the financial impact and so much. This is all recorded in the tool we use.

11. During regular risk meetings, monthly project risk meetings for example, that is when the risks are communicated at different levels. There are monthly risk meetings about the projects.

12. Yes, it makes it nicely ordered. Everybody is working on the same platform. It is very easy for the project managers, but also the program managers to have an overview of what is happening across the projects. This contributes to mitigating and tackling risks, so I definitely believe it is helping.

13. For that one I think I need to know a bit more about the organization at all, since I have only been working here for three and a half months. So my answer cannot be complete here. But I would say, as far as I have seen, they are successful. I mean sometimes they are later, but that is the nature of innovation.

14. Yes, I think it helps the engineers/innovators, because it shows them what they have to take into account, but there is room for improvement. Especially for the bottom up risk identification. Like disciplines and engineering. The engineers are the ones who are actually right on top of the innovation, they are the ones who are executing the innovation. We should be able to get all the risk in their mind which we have on paper. There we have room for improvement and that is identified by the higher management. That is actually one of the reasons why I am employed. In such large organizations the communication cannot take place just naturally. It needs to be organized, a process around it is needed, structured meetings and each meeting needs to have a certain agenda and such. So these things need to be located. This means it is more lacking in the process than lacking communication.

Philips - Development - Integral Project Manager

1. Yes, that is part of the project, managing risks. Different people are added to the projects from the different functions and they also have to reserve time for managing risks. Certainly in projects that are being started, you have sessions to determine the initial risks. This means the starting point. Once you have that and you pass milestones, you usually go through the risks on a weekly basis. What is the status? We had made some arrangements there to figure out things to integrate or whatever. You then implement this until you are finished with the project. If all goes well, the number of risks is getting smaller and smaller.

2. It all comes within the project team and all functions are represented within the project team. If you have very specific risks in the factory, then the owner becomes the factory. So the factory representative gets that risk and he has to try to do something with it. You can do a number of things with that. First, we accept the risk. If it happens we will survive or we consider the chance very small that it will happen. You can also say: it is not acceptable, we have to find out, because it has major consequences with regard to the feasibility of the project or product. Then a feasibility study can be carried out to see if something is possible. You want to see certain behavior of the system, certain speed or certain qualities. The person who then owns such a risk will then make a constellation with his team to view the risk. These are usually product risks. You can also say: we need to have a plan B in case it does happen. For example, the risk is that it will run out. If that is absolutely unacceptable, we need to have a plan B. Then we will escalate and provide extra people, extra money or whatever. It is also often important that you have a plan B when it occurs. A plan B is devised by a risk owner and it is then reviewed by the project team. Eventually you will go through a number of milestones with the project team and at each milestone you need permission to pass that milestone. Then you go to the PMT (project management team). That is the umbrella organization that approves milestones. That is the foundation of the department. Part of that report is always the risks you have and what you have done with them. Depending on the severity and impact of such a risk, you can say: we do not accept this. The risk is there, but we do want to sort it out before going any further because the impact is too big or something like that. So they also look at those risks when passing milestones.

3. Yes sure, anyway. We have to be very strict about that. We are a regulated business. The amount of paperwork is huge. One of those things is that you capture risks in the right way. Even if there is an audit in which the question arises: how did you deal with this and what was the evidence to close that thing? We must certainly comply with the law and regulations. For example, we see a problem with safety or privacy where this cannot always be guaranteed. Our system also has a network. You can also just plug in a plug and get to it. That is of course not acceptable and is therefore a risk. People who do that substantive work and who are concerned with guaranteeing privacy must know exactly what those specific privacy rules mean. They must know them. These people must therefore demonstrate that they meet these requirements by means of tests or checklists. If there is a risk that we will not be able to meet certain circumstances, then a solution must be found. So the employees at those functions also have knowledge of the laws and regulations that apply to certain matters.

4. We want to keep projects manageable. Risks are surprises. In the worst case, that can mean that you lose your investment and all the work has been for nothing. You want to prevent that and you have risk management for that. You look at all the risks you have and to what extent they can influence the project. The managers and we do not like surprises. It is really about mastering the project. Ultimately, a product that you eventually bring to the market must always comply with all safety, privacy and legal regulations. If you come up with something and it does not meet it, you can stop. That makes no sense.

5. We have meetings for that. Then we ask all people to write down what they have. This is often for the initial risks. These are then defined according to a certain format. We will then discuss this in the group. Is this a real risk? Of course, you can also include everything that is not really relevant or is so small that when it occurs, you are not going to use everything to capture it, but we do not. Such a meeting is always held once a month within the project teams. Once a week is too much. Unless you have a hot item that requires you to pick it up for a certain milestone. Then of course you sit down with the teams to ensure that it is accelerated. You go through all the risks on a monthly basis.

6. This is done immediately as soon as they are identified. We have templates and guidance for that. To see what is the severity and the impact. We have

matrices of that. If you multiply those together and you are in the red area, it has a huge impact. If you just end up in the green area, it is less intense and you can probably just accept it. Usually if the severity of impact is large and that combination of those, then you have to do something with it. That way they are prioritized.

7. For this we perform analyses, which are part of the identification and assessment of risks. That is also being looked at. This is of vital importance, especially with product risks, because if you do not know the cause, you cannot solve it. If you look at more project-related risks that influence the planning, it could be that you do not have certain expertise on board or that people get sick or something like that. You always look at the cause of risks, but it is much more important with product-related risks.

8. The risks are discussed first and then the date is updated. Usually, of course, there is homework for the owner, to find out within his teams by doing tests or something like that. Then they come back to that later.

9. It runs once a month and always when milestones are reached. Then you pay extra attention to that, because then you also have to go to the boss. You must then have cleaned up that entire list, so that they have a clear overview of the risks of the next phase. At the start of the project, you usually have 3 milestones within six months. A project initiation, value proposition and then the project design committed. Those 3 are in the initial phase. After these milestones, it can take anywhere from a few months to a few years until the next milestone. Depending on the size of the project.

10. Not so much. Of course we all want to do it efficiently and if there is a lot of nonsense, we will of course give that feedback, but that has already crystallized quite a bit. Let's just say it is right for the job. It works well for me. The owners of the processes receive feedback from different teams and projects. If they see that there is a problem that everyone encounters, then they will do something about it. It is never solved in a project. This then happens in the line where the staff sees: a lot of things go wrong here, we have to adjust that in the process or in the template or something like that. The risk management process is not systematically reviewed every so often.

11. We have tools for that. Clarity in this case, we have been using it for a few weeks now. Before this we had a homemade thing from Philips: Cliff View. That was outdated so to speak. Now we are in Clarity, which

keeps track of more things about a project: budget schedules and things like that. Risks have now been added. This also records the impact, cause, etc. Everything that belongs to a risk, until it is no longer a risk and then we close it. Clarity is completed once a month. Usually we open the list and go through it one by one and if there are updates, we adjust them right away.

12. Usually within the Development organization. Of course you have weekly and monthly report outs. If a risk is really out of control and has a major impact, so that we have to do something about it, it is also reported. The actions that are then taken are also reported. We have all kinds of meetings every week and formally we have a report out every month to our bosses about the state of the project. One of the boxes that must be filled in there are the top 3 risks associated with it and the trend associated with such a risk. Is it getting worse or is it going in the right direction?

13. This is all recorded in processes. You look at it once when you come to work at Philips and then you believe it. Then you move on to the tools. Those tools are really necessary and it also supports it well to record things. In addition, it also shows the overviews with regard to the risks. It just does not work without such a tool. You also just want to be transparent, so everyone should be able to access it. Secondly, you also have a daily management board for each project, as it should be. We do not do it daily, but it is updated weekly. One of those fields is the risks that are open at that moment. Some people go through that once in a while and then ask questions about it. You absolutely have to have that somewhere online, especially in corona time to be able to share otherwise it just will not work.

14. That is difficult to assess, because the innovations are very long processes to do. We are of course in a mature market and you are always looking for innovations. Then when they come, you have to start with clinical studies. Our innovation team has an idea and then a clinical study has to be done at 1 hospital. Once that is done, you go to 10 or 20 hospitals to get feedback there. Then you will market it very broadly. Those processes just take years. You will be working on real major innovations for at least 5 years before they are on the market. We want to get there faster, but that is not working very well yet. Of course, technology is also changing. What we have seen a lot in recent years are smart catheters. They all just come and you want to integrate them. Secondly, what you also see is that in 1 operating room you want to have different analysis tools, to offer them to the doctor. Combining

ultrasound images with X-ray images, for example. You want to see that on 1 monitor at a table where the patient is lying. Then they have more information and can better determine what to do. You see more and more integration coming. What remains very important is to bring out the best pictures. If we can innovate in this area, we will certainly do so.

15. Not really, I think the people of innovation should just come up with ideas and not be immediately held back by the risks that are there. You have to develop the idea further and there are always risks involved. You have to work it out piece by piece. You should always make sure that from the idea you have, you work out the benefits as well as possible. This must then outweigh the risks or side effects it has. That is again a consideration. That is continuous interaction within a team. Ultimately, they have to come up with a solution that is safe and meets all requirements. One by one they will have to grab them and smash them flat. In the beginning, at the idea phase, you really just have to see how good the idea is and what we can do with the idea. Ultimately, from that idea phase you start building something and you increasingly move towards the actual product that will be worked on for the customer. Then you have to solve all problems and risks step by step. Sometimes it just works that you have to do. Then you just schedule it and just do it.

Radboudumc - Information Management - Quality & Compliance Officer

1. I think it is becoming more important and that it is seen as more and more important. I think that people paid less attention to this at first, but certainly with the arrival of my colleague and I, we started to draw more attention to it. I think people see that it can help to prioritize and keep insight into what you need to do. That is what it should do as far as I am concerned and I think the management team is slowly starting to see that too. Therefore, the importance is also increasing. Before me and my colleague worked here, there was not much risk management being done. There was a risk analysis done once, quite operational. That was a project, purely on information security, which concerned itself with the outcome to improve the identified shortcomings and measures. This was not really part of the organization and we try to embed it much more in the operation by making the PDCA cycle that surrounds it really work. We have both been here since November, so almost a year now.

2. The risk management we have set up is really Information Management specific. Before this I was the IT auditor of the Radboudumc. I was just part of the internal audit. The audit service is called audit and risk. In itself a somewhat special combination, but it is concerned with setting up the strategic risk management of the entire Radboudumc. This is a difficult process, but it is slowly getting off the ground. Of course we try to match that. One of the concrete examples we have done is that during an audit we have drawn up a risk classification matrix and we apply it there. We simply adopted it as a risk classification matrix for Information Management. That we at least use the same scales to determine opportunities and impact. With this you have a lot of integration and furthermore there is integration mainly in the area of risk at a strategic level, namely IT failure: cyber risk. A very broad concept. What that means must be mastered. How do we do that? We do this with an ISMS, in which we translate the risks into tactical and operational risks that Information Management runs. Do we control it? If you do all of that right, you have mitigated that strategic cyber risk.

3. We have the Strategy & Policy department and I can show you something about that. Within that unit is the Architecture & Security unit, which houses three tactical security officers. The Quality & Compliance unit is also part of this unit. That is me, with the process managers underneath. These

are the people who are tactically involved in risk management. Ultimately, of course, it is the responsibility of the line. We do not really have a separate risk department or someone with the risk manager position within Information Management.

4. Yes, they are mainly on the ISMS part, so the information security. We have a number of objectives, which we have also described and have published on the Q portal. I will see if I can show it that way. We did not really set a time frame for those goals. The system works in such a way that we have a management review every year. The management can then say, in this case the MT, which goals they find important and therefore pay more attention to. In addition, which is quite recent, is strategic risk management. We also have strategic cyber risks and the question is how this will translate. We actually linked that to the digital vision of Information Management, which are actually the objectives for Information Management. We have translated that digital vision into concrete goals with regard to risk management. IT provision, cyber security, continuity, etc. are part of this. It also concerns: how do we ensure that IT becomes a primary part of the process? Also how we ensure that we create value from data at IM. Then we translate that into KPIs.

5. Yes, it is best to show that with the system. Here we look in the Q portal, where the ISMS can also be found. The schedule looks like this. We identify a risk. This can be from an incident that has occurred, an external audit or you name it. That has to be assessed. That is what the risk owner does. In many cases this is a team leader or a MT member. He is supported by the Security team or by me, depending on the subject. For risks relating to the stock, for example, we had no insight into that before, I am the one who supports it. The stock is maintained by service desk logistics, which is part of the service desk and workplace logistics. The risk owner then has a conversation with the leaders of one of these teams, depending on the domain in which the problem is located. Then another conversation with the person who manages the leaders of these teams. Here you will discuss what the exact risk is. Then an estimate is made. We can then choose to accept the risk. Then we will record it in the ISMS: the quality management system. In addition, we can also choose not to accept it. If it is low risk, you can go pretty standard to acceptance. If it is medium or high risk, by definition we will not accept it. The most you can do then is say that we do not have time to solve it now and delay it. That is possible with a risk waiver. So

you look at how we want to improve it, then we go to an improvement plan and we monitor that. The moment we say we do not have time for it, it still remains a risk. We then set up a risk waiver. We will then take follow-up steps, which we are not taking yet, and a possible compensating measure to solve the problem somewhat. The risk waiver has a limited validity period, so it must be reassessed. Based on the level of risk, this must be approved by the associated echelon. At low risk this is a MT member, at medium risk this is the entire MT and at high risk this is the executive board. In this way we ensure that risks are consciously delayed or resolved.

6. Yes, but it can be very diverse how that comes about. We may notice in an incident that we are running risks. We have had a data breach, of course. This showed that we still ran more risks than we had imagined. We already had some of those risks in the ISMS. It can also, for example, arise from an audit in which findings are made, which are then included in this.

7. Yes, this is done using a heatmap that we use. Here, the probability is multiplied by the severity. In other words, probability times impact. An opportunity is actually a time axis and the impact can be on the following aspects: environment, operational, financial, compliance or personnel.

8. Yes, that is in the part I just explained. In principle, you can simply accept the low risks. With the medium risks you have to make an improvement. This is linked to how long it may take: for example 3 or 6 months. It also states who should do it. You can only postpone it if you do not have time right now, for example. If the risk is high, the risk cannot be accepted and action must be taken immediately.

9. Yes, in principle this is done once a year. We do that ourselves. We have noted that no independent review has taken place. We have therefore instructed the MT in the management review to request the internal audit service to have an audit carried out on this. We also want to be certified in November. In preparation, we had an internal audit carried out for this, but I did it. I did this on the basis of a framework of standards, I carried it out and published a report. However, I am involved in drafting and decorating these pieces, so it is kind of crazy that I did that. For ISO-27001 we will have an external audit every year. The ISO-27001 is the international standard for information security. The NEN-7510 is the same standard, but then the translation for Dutch healthcare.

10. Yes, we have a risk register within information management. You can see that here in Topdesk. This contains the various risks and the associated probability and impact. An improvement plan is then drawn up for each risk based on our risk register. In this way we can then react to shortcomings.

11. No, thought has not really been given to that. The management team has access to the risks and can just see it. We still have to make some progress on bringing forward periodically. There is also a tactical security report, which in any case contains information security risks. These are reported to the management team once a month, I believe. Furthermore, it is mainly the case that an improvement plan is drawn up for the risks that we identify. This is always done together with the owner and the person who has to improve it.

12. Yes, I think so. However, I am not completely satisfied yet. From a risk management point of view, I think the Q Portal works quite well, but not yet from a compliance point of view. We are also working on this with the supplier. The risk story is good. The procedures are clear. They also lead to a lot of awareness. We also notice that it is found and that it is also actively acted on on risks, mitigating risks and also on the conscious use of risk waiver to keep focus on things we are doing so that you can avoid other things to make. So at MT level towards the board of directors things are going well. At the level of team leaders and the concrete implementation of improvement measures, I think it needs to be even better. In this, for example, I think that the Q portal still provides too little support. It is not so much a question of Q Portal, but more that we still have to find a good working method. Sometimes it goes very well, but sometimes the progress also stalls. That is also a bit of a novelty. Not all team leaders are used to having a role in this, for example. In addition, the people who support this are not always well able to do so. This is often due to a lack of competences. When I look at my own team, part of it has a different background. With a different thought, they once entered this team and the team is now developing more and more into a real second-line quality function. People find that role difficult. Then you notice, for example, that they find that progress very difficult. We then try to keep them on their toes, to make better agreements about the realization of improvements. That is one more thing.

13. There is a lot of innovation at the Radboudumc. People are eager to do innovative projects. Enter digital signs and you name it. However, we do not always have the time for this. Last couple of months we have been

rolling out a new security project called MFA (Multi-Factor Authentication). All employees who want to login into Radboudumc platforms from another location than the Radboudumc do not only need a username and a password, but also a confirmation approval with their phone. This protects the accounts better. However, this project has not been rolled out successfully straightaway, since instructions and communication was not very clear. This happens more often with innovative projects, just like when we wanted to roll out Windows 10 to replace Windows 7. A lot of problems came up, which forced us to roll it back.

14. Innovations did not take place on the basis of risk management within Information Management before. Risk management was really on the management side. How we deliver a stable, robust environment. Information Management found that difficult enough. Innovation then gets in the way. I think it was more of a brake on innovation at that moment, but on the other hand, it is just how you look at it. The last few years we have structured our risk management much better. I am absolutely convinced that you only get room to innovate if you have the basics in order. Risk management does help to get the basics in order. By getting the basics in order the last few years, providing more stability and working proactively rather than reactively, I am convinced that it contributes to innovating more and better. Well in that order and not as we have often tried in the past to do both a bit, that just does not work. So before it was a drag, because it became more and more obvious the more we did risk management well, that we did not have time to focus on innovation. We had to get things in order first. The priority should also be there and not with innovation. In the past it was therefore actually a brake for us, but now when it is properly set up, it can have a positive effect with regard to innovations. I am convinced that when you lay down a good foundation, you can also innovate. In the past we did not find it interesting enough to structurally deal with that foundation and that meant we had no room for innovation.

Radboudumc - Information Management - Servicedesk Incident Coordinator

1. Yes, we certainly have a lot of procedures to help with this, documentation. Procedures lay down how many risks/malfunctions can be remedied or how to act if it cannot be solved immediately. Furthermore, there are many colleagues who are available who we can ask for help. During the day there is always an incident coordinator who does not call and is therefore always available to ask questions to. In addition, we also have colleagues from the second line, who have knowledge of specific topics. We can also contact them or forward problems/malfunctions to them so that they can take it further.

2. In the first instance it is us, the employees of the service desk on the phone. For example, if we take phishing, we are the first to see it come in. We then have to sound the alarm and see whether this is urgent or non-urgent phishing. Making that dichotomy by doing a classification. Then we are responsible, if it is urgent phishing, to inform the team workplace as soon as possible by telephone and e-mail. They are then responsible for the actions they have to perform. The ultimate responsibility will always lie with the managers of Information Management. They just don't have much to do with the process.

3. Of course I was not involved in drawing up those procedures, but I can say for almost 100% that we do. We are of course a company that is also partly funded by the government as a university hospital. That is why it is very important that we stick to the rules. So there will certainly have been people behind it, such as the people from security and privacy, who know very well what we can and cannot ask. So in short, yes for sure.

4. No concrete objectives as far as I know in any case. In any case, the aim is to keep the risks as small as possible. To do this, we have to seal the procedures as well as possible. If we again take phishing as an example, make sure that once in a while someone checks the inbox to see if any phishing mail has arrived. However, I do not know exactly what the agreements are with regard to precise objectives with regard to managing risks within Information Management. What we do have, of course, is if we push through urgent phishing mail, there is a service level agreement. This is about the time in which the problem must be solved. That is a certain time and this is an appointment that we make to deal with this phishing email within

that time. This can therefore also be seen as objectives. It is difficult to set goals for as few disruptions as possible or as little phishing as possible, for example, because you cannot completely control this yourself. Phishing emails come from outside, for example, we cannot do much about it ourselves except to solve it as well and quickly as possible. We do set objectives for this, depending on the urgency of the phishing or malfunction.

5. Risks are generally identified by hospital staff. For example, we cannot see if there is a sudden printer failure or if a phishing mail is forwarded, without employees from the hospital notifying us. Employees call or email us and then it is actually classified using the pyramid of priorities. We look at whether one user, several users or the entire business process is affected. We then see whether they can continue, whether they are bothered by it or whether they are unable to continue with their work at all. We actually do everything on that basis.

6. Risks are always assessed, as I just indicated, on the basis of the pyramid of priorities. We look at whether one user, several users or the entire business process is affected. We then see whether they can continue, whether they are bothered by it or whether they are unable to continue with their work at all. Everything is done on this basis and any malfunctions are passed on to other specialized teams to solve the problem as quickly as possible.

7. When there are smaller problems which have occurred more often, we have established procedures for this that state what the solution is. The problem is then already outdated and this is generally done by second-line teams that have specific knowledge about certain matters. If it concerns a larger malfunction, the problem is always forwarded to a second line who then carries out analyzes to find out where the problem lies. We have to communicate this immediately so the problem can be handled immediately. I do not know exactly how this is done either. It is especially important if you want to solve malfunctions, to see where things go wrong. For example, if they released a change like last week and we see that some of the printers in the hospital are being thrown out, it is important that we quickly know that that change was the cause. Then we can quickly reverse this. However, it is not always important that we know the cause, because if, for example, we have a general Vodafone outage throughout the country, then it does not matter to us what the cause of that outage is. As long as Vodafone solves it. So it depends a bit on where the problem is. It is then especially important

to us how we deal with it and how we approach it.

8. Usually based on the priority. In any case, everything that comes in to us is processed the same day. So whether an attempt is made to tackle it directly or it is passed on to another team if we cannot immediately solve it ourselves. All problems and malfunctions that are reported to us are in principle risks, because they can slow down or stop business operations. If there are major risks, it will be dealt with immediately and called through in consultation with the day coordinator. If the risks are less significant, it may not be addressed immediately, because other activities are then given high priority.

9. I actually think constantly with what comes in. Then we see what influence it has on the business process. Almost most of it, of course, has almost no influence, because it often concerns one user who experiences a bit of trouble. This is what we do constantly and also with the second line.

10. Yes we do that. We review everything once a year. This is done by ourselves. Another thing we do is when we have completed a priority two risk and we close that ticket in Topdesk, then two new tickets are automatically created in which malfunction reports must be written. For example, I did that last week as a result of last week's outage. Based on that, you will see how it went and what could be improved. They do the same for the second line. So it is being looked at, but I do not know if there is more behind it, what else is done with it. I know my failure report went to the duty manager. I do not know what she will do next. Furthermore, new procedures are regularly added and old procedures are regularly updated, because they are no longer up-to-date. It is therefore regularly checked whether the procedures for solving certain problems are still up to date and working properly. Furthermore, the procedure for incident coordination has recently changed. We have a document of this and it has been amended fairly recently. Now, for example, there is a different form of communication, if necessary. From now on we can also contact communication if a message has to be placed on the Intranet (information site for all employees). We did not have that line ourselves at first, it went through the manager. We can now do that ourselves if necessary. I do not know if improvements are also being looked at in a systematic way.

11. Everything is recorded in Topdesk. This is a program in which we can report problems, requests and malfunctions. You can then indicate the pri-

ority and impact and you can possibly pass it on to the second line. Possible causes are not necessarily listed. For example, if we have someone on the phone who says something is not working, we can start thinking about what it could be. Of course, we do not always know this either, so we have to leave that to the second line.

12. Some things are communicated, for example with the data breach we recently had. We kept that quiet for a while. Internally, this was brought out fairly quickly, so that we at least knew that something was up. This way we knew how to answer questions if we got questions about this on the phone. In the end they also communicated that to the rest of the employees and beyond, but those are very extreme things. To take a smaller example: if the second line is going to make an adjustment, they actually also do a kind of impact analysis. They always communicate this with us. So it will certainly be looked at before the major changes. As incident coordinator, we can determine in consultation with the duty manager whether we send an email, put it on the self-service portal or send an itel alert. Those are actually the three things that happen most often. Then you also have the reporting on the intranet itself, as with the data breach, but that goes a long way. Then there is a really big problem. This may also include a Radboud alert, which is a pop-up that anyone can force to appear on their computer screen. So we actually have five different types of internal communication about failures. Which one we use depends on the size of the risk and how long it lasts. What we also do is actively follow the most critical departments to ask what the impact is for them of a particular malfunction. That way we can estimate it better, which is also a kind of communication.

13. For me it certainly helps, because it is very clear to me. This is because I have already done it a lot (being an incident coordinator in the event of a major malfunction). What I notice with colleagues is that a lot of people have never done this before and then get a little stressed when they have to do it. There is documentation, but it is very much. Then you may have read it before, but if you really need it, you will not have it ready right away, because you are not going to learn it by heart. What I personally think is that we should practice with this much more often. Practicing is not difficult at all. When this was introduced to us, because this task has not always been ours, we received a course about this from the general incident coordinator. In any case, this has helped us or me a lot. This became very clear by working on it. Today this course no longer happens. So if you ask

me, it could be better.

14. As an ICT department, we are of course constantly working on continuous improvement to do everything better for healthcare and also for our own processes. The only thing you hear a lot here internally is that changes are very slow. This applies to Radboud as a whole. We are working at Radboud a lot, but I also find it difficult to say anything about it properly, because I am not involved in that myself. I do notice, however, that innovations are not always implemented successfully, which was also visible during the data breach. Then they all change things at the last minute and then they forget to communicate that. That can really be better. An update was also recently made in Epic (patient register). This was also not implemented properly, so that it no longer worked for many employees. As a result, the update had to be rolled back. If you consciously continue to implement something and it is not in our IPN calendar (In Production Name of changes), that should of course not be possible. It is important that these innovations happen, but it is important that you also inform us about them to ensure that it runs smoothly.

15. I think it contributes to the successful implementation of change because there are certain things that come to light in the process we carry out. For example, certain problems/malfunctions may come to light here, which must be remedied and should also not occur or occur as little as possible in the future. The things that come to light with us or with the second line, who have more specific knowledge about certain matters, can lead to changes. So what we carry out in terms of risk management can actually lead to changes within our process. In addition, procedures that we have in place to solve certain problems are also regularly adjusted. By continuously identifying the problems/malfunctions, it sometimes emerges that certain procedures no longer work for certain problems, for example. They then have to be adapted, which is actually an innovation of our process that we carry out.

Essent - Sales - Compliance Specialist (former risk officer)

1. Within Essent, if you had to scale it on a scale of 1 to 10, you would be on a 7. It is important, but it is more a product that has to be delivered than a process that has to run smoothly. Within the Sales business unit itself, it is an 8 or a 9 because of the supervisory perspective and compliance risks that are important in this regard.

2. Risk management is not coordinated from top management/board. We do not have that at Essent. We have staff units, second-line risk management teams who are looking for sponsors within the MT. This is not a coordinating position with a board member, but a person with ultimate responsibility. We do not have a CFRO and therefore we have second-line risk management.

3. We have two risk departments within Essent. We have commercial risk management, which you can call operational risk management. We also have quality and internal control, which is a first line of risk management. Then we actually also have a third line of risk management and that is an internal audit. Very classically, you actually have lines one to four. Line one is closest to the business and is often referred to as the business. That is where the support of quality and control comes in. So they really do the risk management on processes, set up controls, etc. at a lower level. The second-line risk management is the operational risk department. This department is responsible for governance, policy and management. So what needs to be done in a year, drawing up annual plans. The third-line risk management is the internal audit. Objectively checking as a role. The fourth line is your external audit, which is KPMG with us.

4. No, we now only have a project on compliance risks. However, that is more about taking control of the Sales network. Real internal control objectives are not set in that way at our place. It is not a subject within Essent. It is more about a product that has to be delivered, than a final process. However, I do think we need it. At Essent we have staff units and within the business we have managers who have to take on the leading roles. They are so insufficiently facilitated or have so little knowledge of the subject that it is difficult to draw up the right objective for this. We want to ensure that the CSAs, i.e. the controlling actions, run smoothly and that is it. Furthermore, there are no additional objectives from the business in detail. At least with

us, within Sales.

5. Yes, sure. So you have financial risks and everything that has to do with fraud. The risk tolerance here is 0 euros. Everything that has to do with invoicing, you are often on a percentage of the total annual order in which people are prepared to recognize fluctuations. For compliance risks, this is also close to 0, because people are not prepared to have compliance risks or exposure.

6. Yes, sure. We follow the COSO model. That is a top model that we follow. We do work from the second line, but we are already working on that in a project, on process identification and we are building that into a chain. So all processes are written down first. There will be a risk workshop and a control workshop. The second line, i.e. operational risk management, then involves clustering so that you get domains within your internal control framework. So we do go bottom-up instead of top-down.

7. Yes, we do this on the basis of impact and probability. We will take those two. Then you have low, medium and high. All high risks will become key risks anyway. Once it is a key risk, a control mechanism must be built around it. This is often referred to as a control self assessment or management testing. This means that you are demonstrably in control. You have to upload proof in your tooling and then you will be assessed once every six months. A control statement will then be issued. That is the whole framework.

8. Yes, we have thought about that. It depends. If you look at how we do it, you identify a risk and you scale it. If you are on a high impact, you will be given a number of assessment criteria: whether it should be preventive or detective. With everything that can be adjusted preventively, we will check whether a process adjustment needs to be made. If that is not possible, we will have to rebuild the process. If that is also not possible, we will accept the risk as it is and we will set it up detectively. If you can mitigate it preventively, you will adjust the process with a process consultant, for example.

9. An internal audit was performed on this in April 2020. This is done ad hoc. So if the internal audit happens to get hold of that subject. It is actually a product of your second-line operational risk management. They must continue to assess whether the risks you have in the ICR are correct and complete and whether the right mechanisms are being followed. So

it is actually a key mechanism of the second line. 10. Yes, sure. We have guidelines in that. This is about how to write down a risk: description, cause and effect. This is also included in the COSO model. We then pick up that notation and then you have a number of labels that we have in our tooling. We use Zenya, which is a risk management tool. We can then actually fill in everything with the labels and then you have it complete in the end. That is actually the notation we use.

11. That is really an area for improvement. It is mainly a party from first and second line risk management. You notice that it is difficult to get the management team involved in this. There have been a few projects. You have your risk cascading to make it manageable of what your risks look like. More of a business partner role should be taken on. So indicate which risks do not run well in a CSA. People are still looking for the best way to do this. Making difficult matters easy. You notice that it is a far from your bed show for many MT members. You have activation and operation. With activation, which is what we are in, it is just hard to get attention to the topic from a risk management perspective. You can do that fairly quickly on compliance issues, because that is an urgent subject. Getting the financial control right is often difficult, you notice. What I did myself for a while, when I was still a risk specialist, is join the MT once every two months to simply give a voice-over of what was going on. That did help. Very sporadically just put braindumps on the mail, so that you can see the status of the internal control and what is happening there. So actually very small, in two or three lines, presenting information and then appearing more often. That also helped. That does not actually happen anymore, they do not have the men for that either. That department is just understaffed.

12. That is very mature within Essent. We have a first, second and third line. So it is very structured. The procedures within it are also fairly mature. The tooling that is applied within it is very extensive, so we have a very large framework of 2000 risks and controls. Only the description within the roles of first and second line could be better. So you notice that they have been looking for two years now for who should do what. To come back to your question, it is very complete what it says. This certainly helps in the proper execution of risk management.

13. Essent does try to innovate, but you notice that we are an ex-government body. We now have a large project running at Sales. Then you notice that

it is difficult to get urgency for the subject there. One project has now been running for almost one to one and a half years. Which is a necessary thing to improve your Sales manpower. However, you notice that it is simply difficult to innovate within large organizations. The innovative projects which do exist, which I just mentioned, are often successfully implemented. However, there is then so much poldering that it is not a 100% version that is implemented, but a 70% version, for example. Then we have to go slow again to pull it to 100%.

14. I think it can have both a positive and a negative effect. If we take the initiative level. So if we have a major new initiative within Essent, risk has set up a business support meeting. You actually get approval from all staff units to continue. So there they really provide structure, content and speed. At the project level, you notice that they then try to close it and remove a piece of innovation from the project by mitigating risks that, for example, have such a low probability that you will win the lottery as a company even sooner than that risk materializes. That is the balance that one still has to find. Take on the business partner role in projects more. They can provide the structure for innovation. The implementation of innovation can sometimes get in the way.

Essent - Sales - Sales Support Specialist

1. Yes, we have set up processes. So people are also assigned to those processes. I now largely do the fraud check myself, so of course that takes hours. That is seen as something important. It is grabbed and once they have grabbed it, they will not let go. Money does not really play a role in this at Essent. They prefer to be in control. It is not that Essent will say that setting up the process or assigning people is too expensive.

2. In principle, the compliance specialist is ultimately responsible. We have more of the operational among us. We check and when that goes wrong, you have the compliance specialist and the risk department. Those two actually combined. We carry out CSA checks every month and we submit to the risk department what went well and what went wrong. We actually have a double check on that. I do say that the compliance specialist is ultimately responsible, but that is actually the risk department. They do not really do anything with it. They set up the processes. They are responsible for risk management, but the operational matters rest entirely with us. We are responsible for ensuring that the checks are carried out and that everything in the business runs smoothly.

3. Yes, continue. We are very strict about that. Legislation is really a pillar for us that we take into account. For example, if an email is sent between our partners with customer data, it must already be encrypted and secured. For this we use filezilla with SFTP servers. These are actually secure environments in which we can share information with partners. So does our customer service. That is checked very carefully. For example, if you are talking about a data breach, which we had two years ago, that is just very much under a magnifying glass.

4. We do not really have goals. We actually have KPIs on a lot of things. Then you have to think of complaints, cancellations, and customer satisfaction. I could name ten more. We have many KPIs on quality and numbers. We do not have any goals like we want to detect so much fraud per year, for example. There are no targets, they are controls. We may have a target when we talk about a partner of ours, for example: BBC. We carry out fraud checks there on a daily basis, which we submit every month. If I do not hand in my fraud analysis, I will immediately receive an email that the term has expired and that I still have to hand it in. We do have targets for

completeness and the delivery of documents.

5. Identifying risks is part of the CSA controls. If we take the example of fraud at the BBC again. On almost all burdens of proof, with customers you have written requirements when you conclude a contract and an interview, there are processes and also CSAs on it. Everyone has their own wallet and returns it every month, some even every week. In that case, CSA checks are always carried out. There really is a system to it.

6. The impact of risks is determined in advance. If a risk has a major impact, weekly or daily checks are performed. For example, the BBC came out. It is not that bad now, but in the past there have been very large fraud cases. Such an impact determination is actually made in advance, when we start setting up such a process. This involves looking at the impact, but also at the probability of the risk. Based on this, it is also determined how often those checks are.

7. The processes are set up based on the cause. You simply see certain problems arise and on that basis we look at how we can mitigate and prevent them. Occasionally, problems arise in practice that cause risks. Some things are more reactive and some things are more proactive. The check on fraud at the BBC, for example, is very proactively structured on a number of pillars that we have come across in practice. The action you take also depends on the risk you identify.

8. That depends on the risk. If it concerns a major risk, we react immediately. If we take the example of the BBC. There we found out that there were major fraud cases, which is of course a very high risk. A process is then immediately drawn up, in which the risks must be mitigated as quickly as possible. If it concerns a smaller risk, it may also be that the risk is simply accepted because the chance is so small that it will actually cause damage.

9. Some things are also only checked annually. If there is very little risk and you see few problems, we may only do that once a year. At Essent, we simply want to have things in control and in order. Most are monthly. Those processes are then simply set up and there is a check on them every so often, depending on the risk. The checks that check whether new risks also arise are quite reactive. The fraud control at the BBC, for example, is reactive. We noticed that there were problems and then we set it up. Some things are also designed preventively, but we mainly do that for our core business.

Usually you run into something in the business and then we think we need to be more in control. We will then set up processes based on that.

10. That is checked every month. A week before my deadline I get an email that I have to hand it in. If I am a day late, they immediately come after me. These emails are all automated. In addition, they really look at what I hand in and whether it is all good. I think in general we have about 200 processes, each person has 2 or 3, where all of this is checked. There are all very strict processes involved.

11. Risks are recorded in Zenya. This system is just new. This is where everything is stored. This is completely automated. So I keep an excel file every day. I have added that file and I have to indicate whether there has been fraud and whether I have followed everything etc.

12. The communication purely on the processes is going well. There is a fixed rhythm. Like I said, if I am a day late I already get an email. So it is very well automated. There are people like me who have a certain portfolio on which they have to do a risk analysis. I think there are a lot of people, including within our team, who do not even know it is happening. I must add that that is not our core business either. It is really just about making sales and we facilitate our agents and partners in doing so. Risk analysis is something that is taken very seriously. Only the communication could be better, because everyone does it a bit on their own actually.

13. Yes, I do think that contributes. How my statue is actually on the market is as follows. The small parties will soon collapse. The rules are getting stricter. We have the capabilities and the staff to set up this kind of business. You can see that if there is an urgency at a given moment, a FTE is simply released. A function is just created to do that. I think the major parties such as Eneco and Vattenfall are also doing this. We also feel that urgency. You also have small parties that barely have customer service. They do not have the capabilities for that. I think we are making a very important step in that regard. That is really preventive, so that we have everything in order. I think that will certainly help us to carry out our risk management better.

14. We are a classic company. It is often very bureaucratic, we are very large. It is all reasonably preserved. It is just very vicious, if you want to innovate something it just takes a very long time before you can get something

through it. We recently implemented Zenya, for example. This is a new risk management software. Entering Zenya actually went really well, but it is also very similar to the previous system we were using. There are also things that were a bit more difficult to implement. In customer service, for example, we are also switching to a new system, but this has already been going on for 2.5 years. So we have been building and improving for 2.5 years. Even if you really want to implement some bigger things, it just takes a lot of time. This takes so long, because it really has to be completely watertight because there is so much confidential information involved.

15. I think risk management is more of an obligation for us. It is something that is just very important in the market and you just want to limit the risks as much as possible. It is just something we have to do well and everyone is aware of that. But it is not something I think we are going to put extra effort into or that it helps with innovation. I also do not think it is very much included in innovations. Take the example of the BBC, for example. We do risk analyses for them to detect possible fraud. This has not much to do with innovations within our own department or Essent. It would only have to do with it if we want to innovate the way of fraud detection for the BBC.

Appendix B: Questionnaire

Questionnaire for respondents with knowledge of the establishment of risk management:

Strategic risk management

1. How important do you think setting up risk management is within your organization and why?
2. How is risk management coordinated from top management/board?
3. How is risk management organized within your organization?
4. Have risk management goals been considered? If so, why?
5. Has thought been given to how risk-tolerant you are with regard to certain risks within the organization? If so, do you have an example?
6. Has thought been given to how risks are identified? If so, how?
7. Has thought been given to how risks are assessed? If so, how?
8. Has thought been given to how to respond to shortcomings in terms of risks? If so, how?
9. Has thought been given to how the risk management process should be reviewed and assessed? If so, how?
10. Has thought been given to how results from risk management are recorded? If so, how?
11. Has thought been given to how risks are communicated? If so, how?

Success of innovation projects

12. Do you think that how risk management is established has an effect on how risk management is ultimately executed in the workplace? If so, why?

Contribution to innovation projects

13. How successful are innovation projects within your company/department?

14. Do you think that how risk management is established has an effect on how successful innovations are implemented within the organization? If so, why?

Questionnaire for respondents with knowledge of the execution of risk management:

Operational risk management

1. Are there any resources available for managing risks? If so, what kind of resources?
2. Who is responsible for potential risks?
3. Do you ensure that all activities within risk management comply with laws and regulations? If so, how?
4. What kind of goals do you have with regard to risk management?
5. How are risks identified?
6. How are risks assessed in terms of impact?
7. How is the cause of risks identified?
8. Are risks addressed immediately? If so, how?
9. How often is the risk management process (identifying, assessing risks etc.) performed?
10. Is the risk management process reviewed? If so, how?
11. How are risks (and associated impact, cause, etc.) recorded?
12. How are risks communicated?

Success of innovation projects

13. Do you think that how risk management is established has an effect on how risk management is ultimately executed in the workplace? If so, why?

Contribution to innovation projects

14. How successful are innovation projects within your company/department?
15. Do you think that how risk management is executed has an effect on how successful innovations are implemented within the organization? If so, why?

Appendix C: Coding Scheme

Topic 1: Establishment of risk management

- Subtopic 1: Governance & culture
  - Importance of risk management
  - Coordination from top management
  - Risk department layout
- Subtopic 2: Strategy & objective-setting
  - Considering risk management goals
  - Considering risk tolerance
- Subtopic 3: Performance
  - Considering risk identification
  - Considering risk assessment
  - Considering how to respond to risks
- Subtopic 4: Review & revision
  - Considering to review the risk management process
- Subtopic 5: Information, communication & reporting
  - Considering how to record risks
  - Considering how to communicate risks

Topic 2: Execution of risk management

- Subtopic 1: Resources & responsibility
  - Resources
  - Responsibility of risks
  - Compliance laws and regulations
- Subtopic 2: Objectives
  - Risk management goals

- Subtopic 3: Quality of risk control
  - Identification of risks
  - Assessment of risks
  - Cause of risks
  - Addressing risks
  - Repetition of risk management process
- Subtopic 4: Review & revision
  - Review of risk management process
- Subtopic 5: Communication & reporting
  - Recording risks
  - Communication of risks

Topic 3: Success of innovation projects

- Amount of innovation projects which deliver differentiated value for the people involved

Contribution to innovation projects

- Effect of execution of risk management on success rate of innovations
- Effect of establishment of risk management on success rate of innovations
- Effect of establishment of risk management on execution of risk management