

Implementation of a risk management system into an SME

Master thesis
of
Markus Übeleis

Graz University of Technology

Faculty of Mechanical Engineering and Economic Sciences

Institute of Business Economics and Industrial Sociology

O.Univ.-Prof. Dipl.-Ing. Dr.techn. Ulrich Bauer

Graz, September 2015

In cooperation with:

Turbinen- und Kraftwerksanlagenbau
EFG - Energieforschungs- und
Entwicklungsgesellschaft m.b.H. & Co. KG.



EIDESSTÄTTLICHE ERKLÄRUNG

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt und die den benutzten Quellen wörtlich und inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

Graz, am

.....

(Unterschrift)

STATUTORY DECLARATION

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

.....

date

.....

(signature)

Abstract

Turbinen- und Kraftwerksanlagenbau EFG - Energieforschungs- und Entwicklungsgesellschaft m.b.H. & Co. KG is a leading Austrian company in manufacturing Francis and Pelton turbines. A further core competence, which is becoming more and more important, is the general refurbishment of pre-existing hydropower plants. EFG requires a risk management system in order to react to internal or external changes. This measure should create transparency of identified and until now unknown risks.

The purpose of this master thesis is the conception and implementation of a risk management system tailored to EFG's needs. The developed risk management system is implemented into existing structures and processes in order to ensure a simple and quick realisation within EFG. This structure forms the base for risk awareness and establishment of a risk culture within EFG. With the developed risk management system an extension at a later date is possible, if necessary. As part of this master thesis, the development of a risk management tool tailored to EFG's needs is illustrated.

The first chapter is a short introduction and describes the initial situation, objectives as well as the scope of tasks and the practical approach of this master thesis. The second chapter is based on an extensive literature research and outlines the risk management process according to ONR 4900x:2015 series. At the end of each theoretical process step description the implementation within EFG is presented. In addition, methods, which are used for the practical realisation of the risk management system, are presented and their assumptions are justified. In order to establish a consistent understanding concerning risk management important terms are explained. Furthermore, relevant legal obligations for top management and important standards are described. Basics of emergency, crisis and continuity management based on *ONR 49001-3:2014* are explained, which allow companies to properly react in case of emergency situations. Additionally, various organisational implementation possibilities are shown and finally the implemented risk management structure within EFG is described.

The third chapter illustrates the risk management tool developed in Microsoft Excel more detailed. Based on acquired knowledge during literature research functionality and usability of this tool by means of the developed user interface is shown. The fourth chapter describes the created operation of process for the updated ISO 9001:2015. With the help of a realistic example single risk management process steps are passed through. This offers guidance and assistance for future identified risks.

In this master thesis described methods as well as the developed risk management tool enables EFG to react on existing or new arising risks in order to either avoid or minimise them. This foundation allows the establishment of a company-wide risk culture by involving all employees as well as all departments.

Kurzfassung

Die Firma Turbinen- und Kraftwerksanlagenbau EFG - Energieforschungs- und Entwicklungsgesellschaft m.b.H. & Co. KG ist ein führendes österreichisches Unternehmen in der Herstellung von Francis und Pelton Turbinen. Eine weitere Kernkompetenz, die in den letzten Jahren immer mehr an Bedeutung gewonnen hat, ist die Generalsanierung und Modernisierung von bereits bestehenden Wasserkraftanlagen. Um auf die sich verändernden internen und externen Rahmenbedingungen eingehen zu können, bedarf es innerhalb der EFG eines Risikomanagementsystems. Dies soll Transparenz über bestehende und nicht bewusste Risiken schaffen.

Ziel dieser Masterarbeit ist die maßgeschneiderte Konzeption und Einführung eines Risikomanagementsystems für die EFG. Dabei wird das Risikomanagementsystem in bereits bestehende Strukturen und Prozesse eingebunden, um eine einfache und rasche Umsetzung zu gewährleisten. Diese Struktur legt den Grundstein für ein risikobewusstes Handeln und die Bildung einer Risikokultur innerhalb der EFG. Das erstellte Risikomanagementsystem ist so ausgelegt, dass es eine Erweiterung zu einem späteren Zeitpunkt ermöglicht. Im Zuge dessen wird ein an die Bedürfnisse der EFG angepasstes Risikomanagement-Tool in Microsoft Excel erstellt.

Das erste Kapitel dient als Einleitung der Masterarbeit und beschreibt die Ausgangssituation, die gesetzten Ziele sowie die Aufgabenstellung und die praktische Herangehensweise. Im zweiten Kapitel wird basierend auf einer ausführlichen Literaturrecherche der detaillierte Risikomanagement-Prozessablauf gemäß der ONR 4900x:2014 Serie aufgezeigt. Am Ende jedes theoretischen Prozessschrittes wird auf die jeweilige Ausführung innerhalb der EFG eingegangen. Zur Schaffung eines einheitlichen Verständnisses bezüglich Risikomanagement werden wichtige Begriffe erklärt. Um auf auftretende Notfälle angemessen reagieren zu können, sind die Grundzüge des Notfall-, Krisen- und Kontinuitätsmanagement basierend auf ONR 49002-3:2014 erklärt. Des Weiteren werden unterschiedliche organisatorische Gestaltungsmöglichkeiten beschrieben und schlussendlich die innerhalb der EFG implementierte Risikomanagementstruktur erläutert.

Das dritte Kapitel geht ausführlich auf das in Microsoft Excel entwickelte Risikomanagement-Tool ein. Basierend auf dem durch die Literaturrecherche angeeigneten Wissen wird dessen Funktionalität und Bedienung mit Hilfe der erstellten Benutzeroberfläche detailliert beschrieben. Das vierte Kapitel erläutert den für die aktualisierte ISO 9001:2015 Norm erstellten Prozessablauf. Anhand eines realitätsnahen Beispiels werden die einzelnen Risikomanagement-Prozessschritte durchlaufen, die so eine Hilfestellung für zukünftig identifizierte Risiken bieten sollen.

Mit Hilfe der in dieser Masterarbeit aufgezeigten Methoden und dem entwickelten Risikomanagement-Tool ist es der EFG in Zukunft möglich, auf vorhandene sowie neue Risiken zu reagieren und diese erfolgreich zu vermeiden beziehungsweise zu vermindern. Dieses Fundament ermöglicht der EFG die Etablierung einer unternehmensweiten Risikokultur, in die sämtliche Mitarbeiter sowie Abteilungen mit einbezogen sind.

Table of Contents

1	Introduction	1
1.1	Initial situation	1
1.2	Area of investigation.....	3
1.3	Objectives of thesis	3
1.4	Scope of tasks and practical approach.....	4
1.4.1	Establishing the context	5
1.4.2	Risk identification.....	6
1.4.3	Risk analysis.....	6
1.4.4	Risk evaluation	7
1.4.5	Risk treatment.....	7
1.4.6	Communication and consultation	8
1.4.7	Monitoring and review	8
2	Introduction to risk management	9
2.1	Basic definitions and general framework	9
2.1.1	Terms and definitions.....	9
2.1.2	Definition of small and medium-sized enterprises (SMEs).....	11
2.2	Legal foundations.....	12
2.2.1	Austrian Business Code (<i>aUGB</i>).....	13
2.2.2	Austrian Business Reorganisation Law (<i>aURG</i>).....	15
2.2.3	Austrian Law on Public Limited Company (<i>aAktG</i>) and Law on Limited Liability Company (<i>aGmbHG</i>)	15
2.2.4	Corporate Sector Supervision and Transparency Act (<i>KonTraG</i>).....	16
2.2.5	Austrian Code of Corporate Governance (<i>ACCG</i>).....	17
2.2.6	ISO 31000 – Risk management	19
2.2.7	<i>ONR 4900x:2014</i> – Risk Management for Organizations and Systems.....	19
2.2.8	ISO 9001 – Quality management	22
2.2.9	Additional standards	22
2.3	The risk management process according to <i>ONR 4900x:2014</i>	23
2.3.1	Establishing the context	24
2.3.1.1	Establishing the external context	25
2.3.1.2	Establishing the internal context	26
2.3.1.3	Defining risk criteria	27
2.3.1.4	Risk criteria at EFG.....	29

2.3.2	Risk assessment.....	30
2.3.2.1	Risk identification.....	30
2.3.2.2	Risk identification at EFG.....	33
2.3.2.3	Risk analysis.....	34
2.3.2.4	Risk analysis at EFG	36
2.3.2.5	Risk evaluation	43
2.3.2.6	Risk evaluation at EFG	46
2.3.3	Risk treatment.....	49
2.3.4	Communication and consultation	53
2.3.5	Monitoring and review	54
2.4	Risk reporting at EFG.....	55
2.5	Crisis management	57
2.6	Organisational structures of risk management systems.....	60
2.6.1	People involved in risk management.....	60
2.6.2	Implementation possibilities of the risk management	63
2.6.3	Risk management implementation at EFG.....	65
3	Structure of the risk management tool	67
4	Practical example of ISO 9001 process description.....	73
5	Summary and outlook.....	76
	References.....	77
	List of Figures.....	82
	List of Tables	84
	List of Abbreviations.....	85
	List of Translations	87
	List of Symbols.....	88
	List of Appendices	88

1 Introduction

This chapter describes the history and core competences of Turbinen- und Kraftwerksanlagenbau EFG - Energieforschungs- und Entwicklungsgesellschaft m.b.H. & Co. KG. as well as objectives of this master thesis. Furthermore, a brief introduction concerning the used risk management process is given.

1.1 Initial situation

The company Turbinen- und Kraftwerksanlagenbau EFG - Energieforschungs- und Entwicklungsgesellschaft m.b.H. & Co. KG. (EFG) is a medium-sized, Austrian enterprise based in Feldkirchen, Carinthia. EFG is specialised in construction and manufacturing of Francis and Pelton turbines. Additional core competences are general refurbishment of pre-existing hydropower plants and job order production. As part of the general refurbishment outdated technology of pre-existing hydropower plants are brought up-to-date. These actions ensure a maximum performance and long durability. In job order production EFG has acquired special knowledge in machining difficult materials by using up-to-date technologies.

Due to the lack of suitable solutions in hydropower industry EFG's founders established the company in 1984. Ever since, the company has continuously grown and employs approximately 47 people at present. Since the foundation EFG has set special value on their products' quality, high customer satisfaction as well as up-to-date, innovative and technical solutions.

Over the intervening years EFG has been able to gain a comprehensive knowledge in the area of construction and manufacturing of hydropower plants. This knowledge was gathered in close cooperation with academic institutions and research by their own. Numerous registered patents prove their stage of development.

Customers of EFG are spread all over the world. However, the majority of their projects are done in Austria. Its customer base consists of private power plant operators, cooperatives, communities, industrial enterprises and public-sector energy companies in Austria and abroad. EFG is responsible for several of the around 1,700 hydropower plants in Austria, which are responsible for 60% of total electricity production.^{1,2}

At present profound changes in the environment of many companies take place. These changes force companies to reconsider their perspective and establish a new strategic focus. To ensure the continued existence of a company it is important to identify existing and future risks in a very early stadium, to evaluate them and set countermeasures.

¹ Both direct and indirect quotations were done by the author in this master thesis.

² Cf. BARRIGA F. (2014), p. 8.

The Austrian Code of Corporate Governance (ACCG), which is compulsory for Austrian exchange-listed companies, provides a framework for management and control of enterprises based on the Austrian Corporation Law. The elaborated framework enables companies to create a sustainable and long-term value by using an internal control system. This ensures a high level of transparency for all stakeholders. Furthermore, the Code recommends companies to voluntarily follow it even if they are not be obligated to do so.³ For quite some time effort has existed in creating a consistent Code of Corporate Governance for small and medium-sized enterprises (SMEs). Because of the large diversification of SMEs, it does not make sense to elaborate such consistent Code. It is more important that each company tailors its own Code of Corporate Governance according to their needs.⁴ § 22 of the Law on Public Limited Companies (*aGmbHG*) requests an internal control system, which has to fit to company needs. It is stated that top management is responsible for the supply of internal control systems.^{5,6}

The continuously growing EFG is faced with new challenges on every day basis. On the one hand these challenges are a great opportunity but on the other hand they also present a life-threatening risk. For example, one of these risks can be subcontracting of certain services to a partner company. This action causes a knowledge transfer from EFG to the partner company, which can easily acquire the hard-won achieved knowledge by EFG. Furthermore, they can become a serious competitor through this action. Another risk can be the absence of employees in key positions. A replacement cannot be found very easily because many employees have been working there for several years and have grown into their positions. But also the dependency on few subcontractors can evolve to a severe problem. These opportunities and risks have to be identified by those who are involved and considered by their daily actions. At the moment EFG does not have such tools to identify, evaluate and display arising risks. These tools are developed as part of this master thesis.

³ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 9 ff.

⁴ Cf. REINEMANN, H.; BÖSCHEN, V. (2008), p. 14.

⁵ Cf. *ONR* 49000:2014, p. 3.

⁶ Cf. *ÖNORM S* 2410:2010, p. 13.

1.2 Area of investigation

In terms of a holistic approach EFG's areas are diversified during the risk identification phase in order to identify as many risks as possible. Therefore, a combination of top-down and bottom-up approach is used. This combination takes different hierarchical levels and employees into consideration in order to ensure the involvement of various perspectives. Figure 1 illustrates the different areas of EFG, which are taken into account during the risk identification phase.

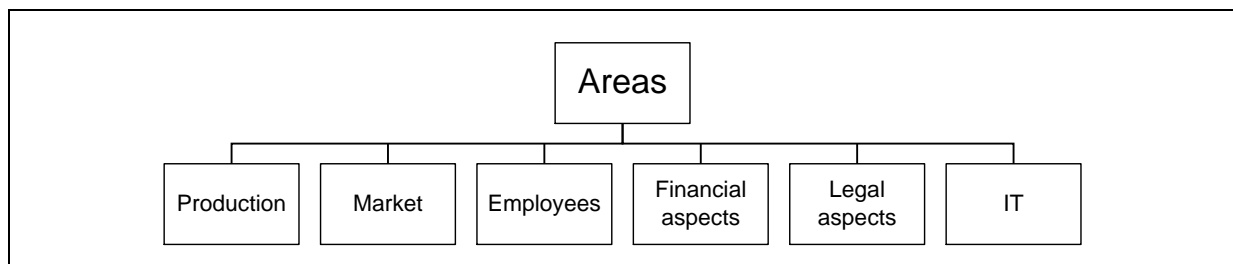


Figure 1: Area of investigation

1.3 Objectives of thesis

The purpose of this master thesis is the establishment and implementation of a risk management system tailored to EFG's needs. Therefore, two main goals have been defined in accordance with EFG's management. To accomplish the two main goals each individual subgoal has to be fulfilled. The first main goal is the identification and illustration of existing and undiscovered risks in Microsoft Excel. The second main goal is the development of a risk management tool in Microsoft Excel. All in advance defined main goals and subgoals are listed below.

1. Main goal – Identification and illustration of risks in Microsoft Excel
 - Subgoal 1 – Identification and illustration of existing risks in Microsoft Excel
 - Subgoal 2 – Identification and illustration of future risks in Microsoft Excel
2. Main goal – Development of a risk management tool according to *ONR 49000:2014* and *ÖVE/ÖNORM EN 31010:2010* in Microsoft Excel
 - Subgoal 1 – Developing a consistent risk assessment template
 - Subgoal 2 – Developing a risk catalogue for continuous monitoring of identified risks
 - Subgoal 3 – Displaying of identified risks in a risk matrix and estimation of the risk level
 - Subgoal 4 – Risk management process description as preparation for ISO 9001:2015

1.4 Scope of tasks and practical approach

The following chapter summarises the fundamental structure of the risk management (RMGT) process. Furthermore, each process step is briefly described and suitable methods are listed. The risk management process according to *ONR 49000:2014* (see Figure 2) also includes the Deming wheel (Plan-Do-Check-Act) (see Figure 8), which also takes elements from the management into consideration.⁷ This process follows a sequential and predefined order. Due to the fact that subsequent stages are based on previous ones, the specified sequence from Figure 2 has to be followed.⁸

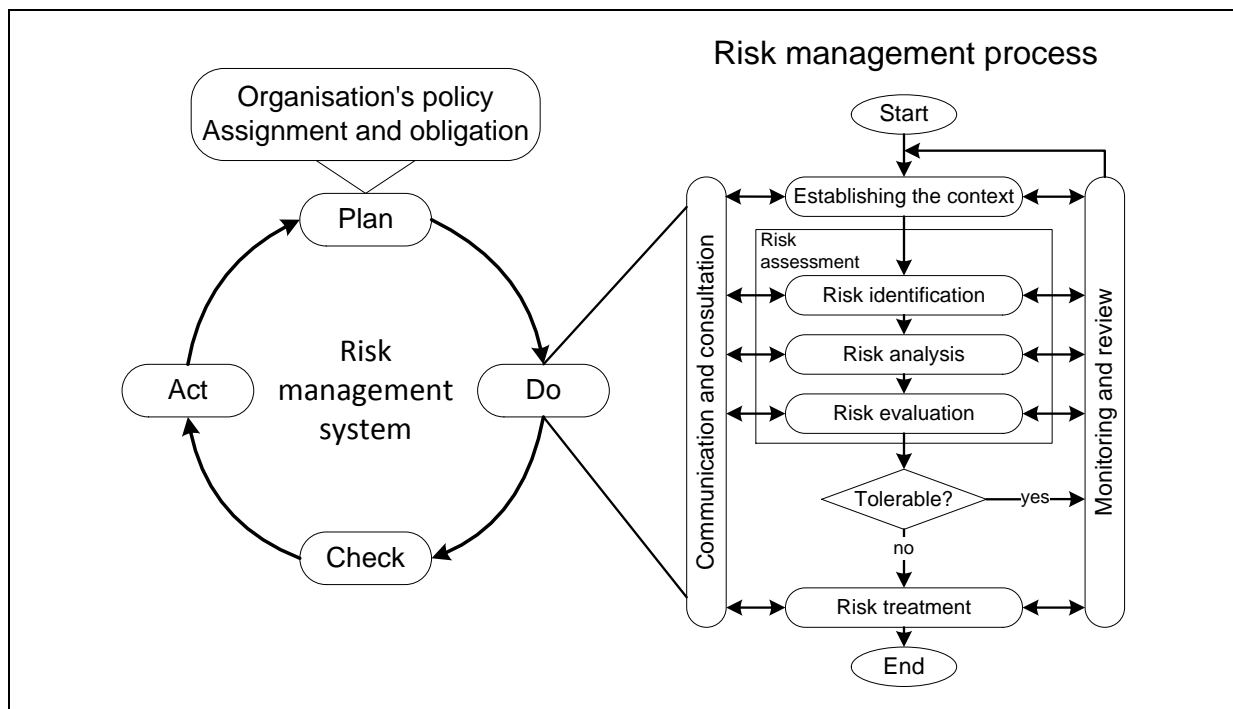


Figure 2: Risk management system according to *ONR 49000:2014* and *ÖVE/ÖNORM EN 31010:2010*^{9,10}

A more simplified but in fundamentals very similar chance and risk management system describes *ÖNORM S 2410:2010*. This standard considers enterprises as a consistent system and is especially designed for SMEs. *ÖNORM S 2410:2010* is based on the corner pillar responsibilities and elements, which provides guidance among others in increasing risk and chance awareness within the enterprise, reaching business goals and sustainable efficiency increase. The purpose is primarily the continued existence of the enterprise, establishment of a risk culture, increasing success potentials and compliance with all legislation. The structure of chance and risk management system is displayed in Figure 3, which is based on the standards of *ONR 49000:2014* and *ISO 31000:2009*.¹¹

⁷ Cf. BRÜHWILER, B. (2011), p. 52.

⁸ Cf. *ONR 49000:2014*, p. 19.

⁹ Adapted from *ONR 49000:2014*, p. 19.

¹⁰ Adapted from *ÖVE/ÖNORM EN 31010:2010*, p. 10.

¹¹ Cf. *ÖNORM S 2410:2010*, p. 3 ff.

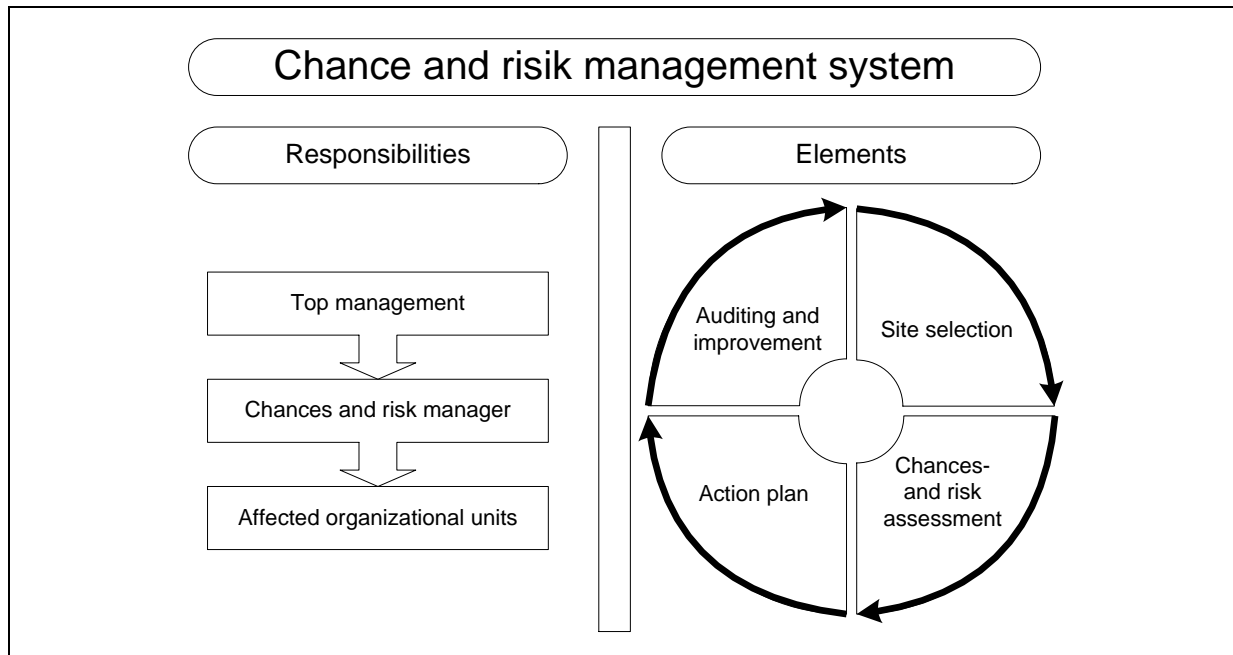


Figure 3: Chance and risk management system according to ÖNORM S 2410:2010¹²

Due to the higher level of detail the standards of *ONR 49000:2014* and *ÖVE/ÖNORM EN 31010* are used to conduct this master thesis instead of *ÖNORM S 2410:2010*. The following is intended to provide an overview of the sequential steps of this master thesis, according to *ONR 49000:2014* and *ÖVE/ÖNORM EN 31010*.

1.4.1 Establishing the context

The first step of the risk management process is to establish the context. This includes among other things the following: definition of objectives and used approach, risk management's purpose as well as system boundaries, which is done with the assistance of the risk manager and the management.¹³ In case of EFG at the moment no employee is in charge as a risk manager. Therefore, the management agreed upon system boundaries.

For instance objectives concerning leadership, risk assessment and results of the risk managements process can be defined.¹⁴ The precise objectives have to be defined individually for each case of application.

The used approach is a combination of a top-down and a bottom-up approach (see Figure 9) to ensure risk identification in a holistic way. The top-down approach guarantees the collection of financial, strategic and operational risks, whereas the bottom-up approach aims at the identification of risks, which arise in production.¹⁵ System boundaries can be set for each individual area or process but also for the whole company.¹⁶

¹² Cf. *ÖNORM S 2410:2010*, p. 12.

¹³ Cf. *ONR 49001:2014*, p. 18.

¹⁴ Cf. BRÜHWILER, B.; ROMEIKE, F. (2010), p. 92 f.

¹⁵ Cf. *ONR 49000:2014*, p. 17 f.

¹⁶ Cf. *ONR 49001:2014*, p. 18.

1.4.2 Risk identification

The goal of this process step is the identification of all existing risks, future developments and trends by using a combination of a top-down used and bottom-up approach, which will be described later on in detail.¹⁷ To identify risks in a holistic way different methods are used depending on each situation.¹⁸ Suitable methods for the risk identification phase are:^{19,20,21,22}

- Check-lists
- Brainstorming
- Delphi method (expert interview)
- Oral interviews
- Ishikawa diagram (cause-and-effect analysis)
- FMEA (failure mode and effects analysis)
- SWOT analysis (strengths, weaknesses, opportunities, threats analysis)
- Risk assessment sheets

In this master thesis the following methods are used to achieve the first main goal from chapter 1.3. At the beginning of this process step oral interviews and brainstorming meetings are conducted to get a first impression of occurring risks. On consultation with the management identified risks are checked for completeness. For the identification of risks concerning the market and competitors a SWOT analysis is performed. A FMEA analysis is suitable to evaluate process flows with respect to occurring risks.

At the end of this process step determined risks are grouped into predefined risk categories and entered in a risk catalogue. This catalogue displays all identified risks in a detailed list and serves as base for the next process step of the risk management process.²³

1.4.3 Risk analysis

The risk analysis forms the base for the risk evaluation and is used as a first rough estimation for identified risks, which are listed in the risk catalogue. The purpose of this process step is a very detailed and plausible description of risks in order to help people understanding causes and sources of risks. Furthermore, it is necessary to determine the likelihood and consequences of each risk and the effectiveness of applied countermeasures in order to prioritise them. In many cases it is not possible to evaluate the **likelihood** with quantitative values. Therefore, the company has to define qualitative risk criteria like “unlikely”, “rarely” and “frequently”. The same applies to consequences. Qualitative criteria for **consequences** are for instance “insignificant”, “noticeable” and “catastrophic”. Qualitative criteria, which are applied in the risk management tool for EFG are defined and explained in

¹⁷ Cf. BRÜHWILER, B. (2011), p. 120.

¹⁸ Cf. EBERT, C. (2013), p. 22 ff.

¹⁹ Cf. ONR 49002-2:2014, p. 5.

²⁰ Cf. ROMEIKE, F. [a] (2003), p. 174.

²¹ Cf. ÖVE/ÖNORM EN 31010:2010, p. 20.

²² Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 98.

²³ Cf. ROMEIKE, F. [a] (2003), p. 179.

chapter 2.3.1.3. For a successful conclusion of this process step a common sense of all participants is necessary. This helps to properly assess risks and get a feeling for identified risks.^{24,25}

1.4.4 Risk evaluation

In this process step the determined risk level from risk analysis is compared with the risk criteria, which were set while establishing the context. The knowledge gained during the risk analysis is taken into account. There is a need to clarify whether a risk is tolerable or not. With the recently obtained information from previous process steps more detailed decisions about further procedures can be made.²⁶ Potential methods for the process steps, risk analysis and risk evaluation are:^{27,28}

- Environmental risk assessment
- Structure “What if?” (SWIFT)
- Root cause analysis
- Consequence/probability matrix
- Scenario analysis
- Confidence interval
- Monte Carlo simulation

It is necessary to ensure that the selected method is appropriate for each individual situation. The objective of the selected method is to enhance the understanding of risks and also its traceability and verifiability afterwards. The choice of the selected method should be given with respect to applicability and suitability of the method.²⁹

1.4.5 Risk treatment

Risk treatment introduces available measures, which can be taken by EFG to cope with identified risks. It is possible to distinguish between different approaches.^{30,31}

- Preventive risk management
The objective of preventive risk management is to find ways of reducing or preventing risks from occurring. Selected measures shall prevent risks from happening or reducing their likelihood and consequences in advance. Human factors, technical and organizational factors play an important role in this approach.

²⁴ Cf. ÖVE/ÖNORM EN 31010:2010, p. 11.

²⁵ Cf. BRÜHWILER, B. (2011), p. 124 ff.

²⁶ Cf. ÖVE/ÖNORM EN 31010:2010, p. 14.

²⁷ Cf. ÖVE/ÖNORM EN 31010:2010, p. 20.

²⁸ Cf. ONR 49002-2:2014, p. 5.

²⁹ Cf. ÖVE/ÖNORM EN 31010:2010, p. 17.

³⁰ Cf. BRÜHWILER, B. (2011), p. 139 ff.

³¹ Cf. ONR 49001:2014, p. 24 ff.

- **Claims management**
Despite all taken preventive measures to reduce or prevent risks from happening, it is still possible that remaining risks occur. Therefore, claims management, also known as emergency and crisis management, exists. For this type of risks, the company needs to develop emergency plans in order to react immediately to new circumstances. Emergency plans can for instance be developed for accidents, natural disasters, fires, technical disruptions or disruptions to operations.
- **Risk financing**
Risk financing is one important tool of risk treatment and has a significant value for the insurance industry. It is only possible to insure risks which result from a damaging event. Risks based on negative constellations or wrong decisions cannot be insured.

Unfortunately, despite all preventative measures taken by the company, it is not possible to identify all risks. The company has to deal with remaining risks. Remaining risks are risks that are not identified. Likelihood and consequences might endanger the survival of the company or cannot be reduced for technical, economical or practical reasons.³²

1.4.6 Communication and consultation

People who are involved in the risk management process often have different opinions about likelihood and consequences of risks. Therefore, communication plays an important role in risk management. Communication ensures that all people involved understand the reasons for implemented measures and their necessity.^{33,34}

1.4.7 Monitoring and review

During the whole risk management process single process stages are monitored and reviewed. The objective of monitoring is to peruse trends of remaining risks and identify new arising risks. In case of high likelihood and high consequences countermeasures are set. Main tasks of the review process are evaluation of countermeasures, effectiveness and checking the execution of single process steps.³⁵

Besides literature research, gathered information is used to conduct the risk management process steps. Based on the outcome of this literature research a risk management tool according to EFG's needs is developed in Microsoft Excel. Furthermore, a risk management process description as preparation for the ISO 9001:2015 is realized.

³² Cf. BRÜHWILER, B. (2011), p. 148.

³³ Cf. ONR 49001:2014, p. 17 f.

³⁴ Cf. BRÜHWILER, B. (2011), p. 149.

³⁵ Cf. BRÜHWILER, B. (2011), p. 154.

2 Introduction to risk management

Based on literature research the following chapter goes into detail regarding basic definitions, existing standards and the risk management process. Important legal standards concerning this master thesis are explained and others are mentioned to indicate their presence. The sequential order from *ONR 49000:2014* is used to describe the risk management process.

2.1 Basic definitions and general framework

The following subchapter defines important terms and basic vocabulary concerning risk management in order to develop a common understanding of risk management. As EFG can be classified as SME, on further consequence the SME category is described as well as relevant international and national binding and non-binding legal standards.³⁶

2.1.1 Terms and definitions

Both standards – ISO 31000:2009 and *ONR 49000:2014* – refer, regarding their terms and definitions, to ISO Guide 73:2009 - Risk management - Vocabulary. Below, some essential terms regarding risk management are discussed.

Risk

According to ISO Guide 73:2009 a risk is defined as an “effect of uncertainty on objectives.”³⁷ Furthermore, the word effect is defined as a deviation from the expected either in a positive or negative way. A risk is often described as combination of likelihood and consequences.³⁸ *ONR 49000:2014* goes one step further and distinguishes between two different sources and causes of risks, displayed in Figure 4. On the one hand threat or opportunity is described as a potential source of a risk, which can lead to a negative or positive change of circumstances. These changes of circumstances take place in a gradual way. On the other hand hazard is defined as a potential source of a risk that can result in a suddenly occurring loss event. An event is defined as a sudden occurrence of a certain combination of circumstances. The results of these risk sources or causes are either a so-called scenario or a hazard. A Scenario describes a concrete and pictorial representation of a risk with the assumption of possible correlations. A scenario will be particularly authentic if people involved have already experienced this situation. The risk contents are described with a top-down approach. Whereas, hazards influence people as well as the environment and objectives in a negative way and describe the risk contents with a bottom-up-approach.³⁹

³⁶ Cf. ISO GUIDE 73:2009, introduction.

³⁷ ISO GUIDE 73:2009, chap. 1.1.

³⁸ Cf. ISO GUIDE 73:2009, chap. 1.1.

³⁹ Cf. *ONR 49000:2014*, chap. 2.1.2, 2.1.3, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 2.1.16.

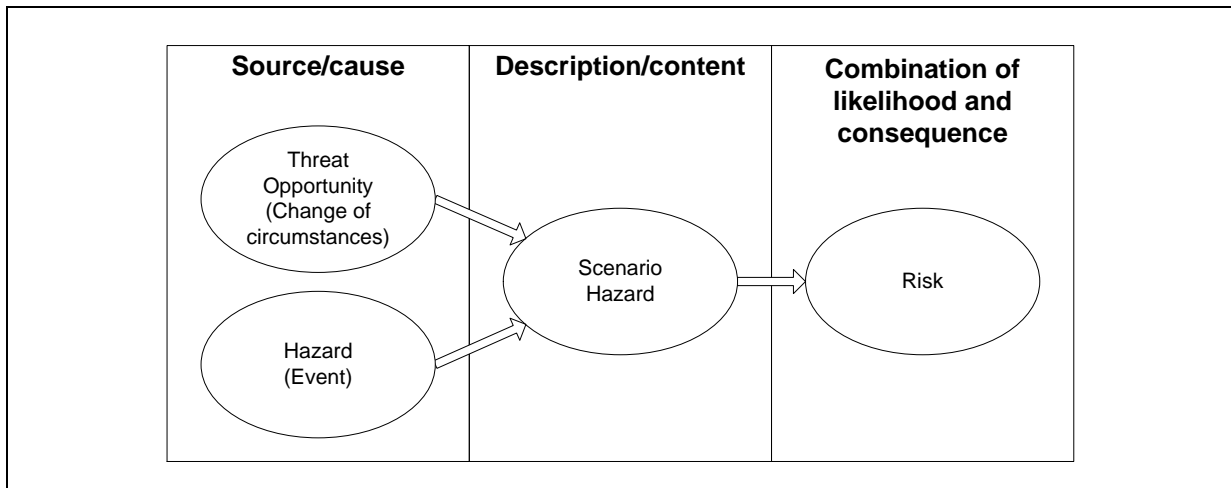


Figure 4: Sources of risks⁴⁰

As mentioned above, a risk is the combination of likelihood and consequences. In literature a risk is often described as the product of likelihood and consequences ($R = L \times C$). It is essential to understand that this product can only be seen as an expected value, which refers to an expected mean value of the risk. The credible worst case of the risk is not considered.⁴¹

Consequence

ISO Guide 73:2009 defines consequence as “outcome of an event affecting objectives.”⁴² In this context the word event is determined as the “occurrence or change of a particular set of circumstances”.⁴³ The resulting consequences caused by the event can either have positive or negative effects on the company’s objectives, which can be described in a qualitative or quantitative way. In everyday speech the words “incident” or “accident” are used as a substitute for event.⁴⁴

Likelihood

ISO Guide 73:2009 defines the term likelihood as a “chance of something happening.”⁴⁵ This chance of something happening can be “defined, measured or determined objectively or subjectively, qualitatively or quantitatively in general or mathematical terms.”⁴⁶ In some languages the term likelihood does not have a direct equivalent and the term probability is used. The intent of ISO Guide 73:2009 is that the term likelihood is equivalent to probability regarding risk management.⁴⁷

⁴⁰ ONR 49000:2014, p. 7.

⁴¹ Cf. BRÜHWILER, B. (2012), p. 30.

⁴² ISO GUIDE 73:2009, chap. 3.6.1.3.

⁴³ ISO GUIDE 73:2009, chap. 3.5.1.3.

⁴⁴ Cf. ISO GUIDE 73:2009, chap. 3.5.1.3, 3.6.1.3.

⁴⁵ ISO GUIDE 73:2009, chap. 3.6.1.1.

⁴⁶ ISO GUIDE 73:2009, chap. 3.6.1.1.

⁴⁷ Cf. ISO GUIDE 73:2009, chap. 3.6.1.1.

2.1.2 Definition of small and medium-sized enterprises (SMEs)

The Austrian Law does not provide any mandatory definition for SMEs, but references to the recommendation of the European Commission (EC) concerning the definition of SMEs.⁴⁸ The recommendation emerged from the idea to avoid inconsistencies by different definitions at community level and national level. In 1996 EC recommended common rules for a single market without internal frontiers. By establishing these rules, it is guaranteed that actions set by the community and member states are consistent. In 2003 EC presented an updated version of this recommendation, which was entered into force in 2005 and had considered the economic development since 1996. Today 90% of all businesses in the EU are SMEs. The number of registered SMEs increased in Austria in the period between 2012 and 2014 from 314,855 to 426,364, which is equal to an increase of 35.42%. Whereas the number of employed people decreased from 2,508,793 to 2,242,847.^{49,50} This is due to the fact that the number of small and medium-sized enterprises is declining while the number of micro enterprises is growing. EC defined four criteria in total to distinguish the different enterprises.^{51,52,53} Table 1 shows specified criteria and current maximum thresholds.⁵⁴

- Headcount: Annual Work Unit (AWU)
- Annual turnover or
- Annual balance sheet total
- Autonomy

Enterprise category	Headcount: AWU	Annual turnover	or	Annual balance sheet total	Autonomy
Medium-sized	< 250	≤ € 50 m		≤ € 43 m	< 25% holding
Small	< 50	≤ € 10 m		≤ € 10 m	
Micro	< 10	≤ € 2 m		≤ € 2 m	

Table 1: Definition of SMEs [m...million]^{55,56}

Headcount: Annual Work Unit (AWU)

The staff headcount is the most important criterion for determining the right category of an SME. This criterion takes full-time, part-time and seasonal staff into account. A person who has worked full-time within the company during the entire reference year is counted as one unit. People who have not worked the full year at the enterprise are counted as fraction of

⁴⁸ Cf. *WIRTSCHAFTSKAMMER ÖSTERREICH* (2013).

⁴⁹ Cf. *WIRTSCHAFTSKAMMER ÖSTERREICH* (2012).

⁵⁰ Cf. *WIRTSCHAFTSKAMMER ÖSTERREICH* (2014).

⁵¹ Cf. EUROPEAN COMMISSION [a] (2003).

⁵² Cf. EUROPEAN COMMISSION [b] (2005), p. 6 f.

⁵³ Cf. EUROPEAN COMMISSION [c] (-).

⁵⁴ Cf. EUROPEAN COMMISSION [a] (2003).

⁵⁵ Cf. *WIRTSCHAFTSKAMMER ÖSTERREICH* (2013).

⁵⁶ Cf. EUROPEAN COMMISSION [b] (2005), p. 14.

AWU. Not included as staff are persons like apprentices or students employed in vocational training with apprenticeship or vocational training contracts, maternity or parental leave.⁵⁷

Annual turnover and annual balance sheet total

For the comparison with competitors it is necessary to introduce also a financial criterion. Therefore, enterprises can choose depending on their branch between annual turnover or annual balance sheet total, because enterprises in the trade and distribution sector might have a higher annual turnover than enterprises in the manufacturing sector. By choosing one of these criteria it is possible to exceed the other one.⁵⁸

Autonomy

This criterion is introduced to sort out SMEs, which are not autonomous enterprises. To be autonomous means that the enterprise has no partner or is not linked to another enterprise, which provides any kind of support. EC sets the threshold for the capital or voting rights controlled by outsiders at less than 25%.⁵⁹

The staff headcount, the annual turnover and the annual balance sheet total are calculated on an annual basis, based on the latest approved accounting period. Exceeding one of these criteria for one year, will not affect the status of the enterprise unless those criteria are exceeded over two consecutive accounting periods. For newly founded enterprises without any approved accounts a bona fide estimate is done during the course of the financial year.⁶⁰

By taking into account the staff headcount of EFG from chapter 1.1 and their annual balance sheet total (financial year 2013), which is for data protecting reasons not allowed to publish, EFG is a small-sized enterprise according to EC recommendation. The definition ensures that measures in a single market without any internal barriers are in favour of SMEs.⁶¹

2.2 Legal foundations

The following chapter provides a short inside into different guidelines and legal standards, which demand the implementation of risk management into the daily business of an enterprise. Figure 5 shows a relevant selection of guidelines and legal standards for this master thesis, divided into the following frameworks.⁶²

- Austrian binding legal standards
- International standards
- Non-binding legal standards
- Guidelines of credit assessment and rating procedures

⁵⁷ Cf. EUROPEAN COMMISSION [a] (2003).

⁵⁸ Cf. EUROPEAN COMMISSION [a] (2003).

⁵⁹ Cf. EUROPEAN COMMISSION [a] (2003).

⁶⁰ Cf. EUROPEAN COMMISSION [a] (2003).

⁶¹ Cf. EUROPEAN COMMISSION [b] (2005) p. 6.

⁶² Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 42.

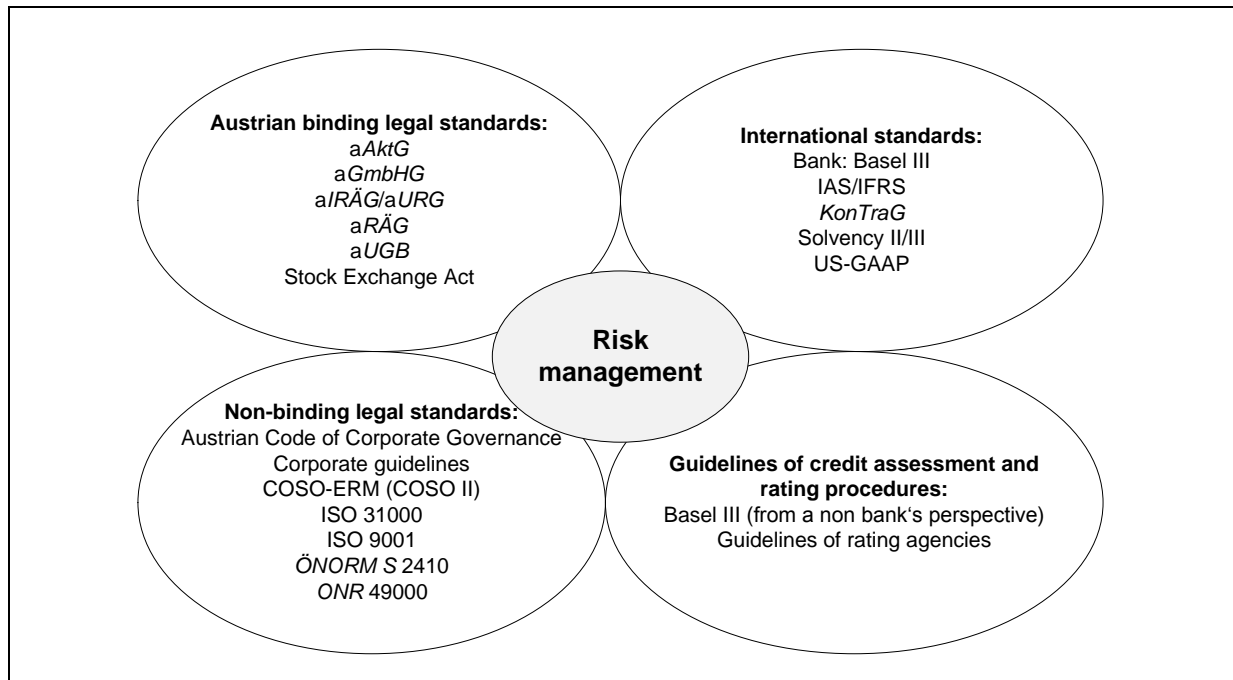


Figure 5: Overview of institutional frameworks^{63,64}

Some important legal standards in Figure 5 are described below. Due to the fact that the target audience of this master thesis is German speaking, paragraphs are only briefly described in English and the exact wording of the law is kept in German. The year of introduction of different legal standards is illustrated in Figure 6.

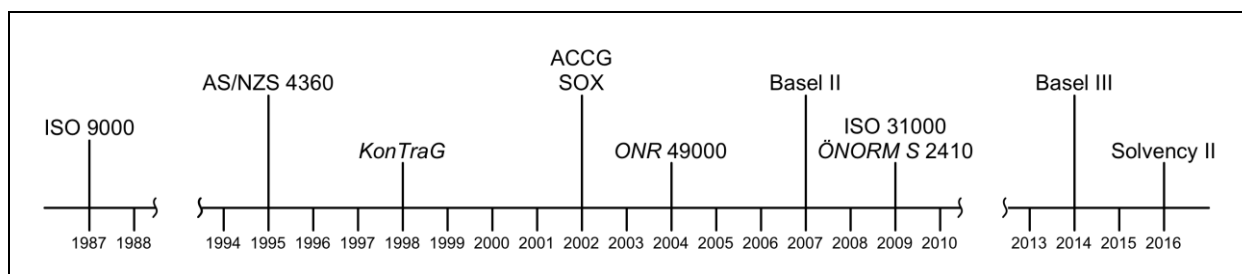


Figure 6: Legislative initiatives with effect on risk management⁶⁵

2.2.1 Austrian Business Code (aUGB)

On 01 January 2007 the reformed and renamed Austrian Business Code (aUGB), formerly Commercial Code (aHGB), came into force. The new version of this law also contains regulations for corporations concerning the application of risk management. According to § 221 aUGB EFG is classified as a small Company Limited by Shares by taking into account their staff headcount from chapter 1.1 and their annual balance sheet total (financial year 2013), which is for data protecting reasons not allowed to publish. If a company exceeds the limits of specified criteria for two consecutive fiscal years, the status concerning small,

⁶³ Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 42.

⁶⁴ Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2006), p. 11.

⁶⁵ Adapted from KROLAK, T.; MORZFELD, K.; REMMEN, J. (2009), p. 1417.

medium sized or large Company Limited by Shares changes in the following fiscal year. Furthermore § 243(4) aUGB exempts small Companies Limited by Shares from exhibiting an annual report. § 267(1) aUGB is very similar to § 243(1) aUGB concerning reporting with the only difference that it refers to the group annual report. The exact wording of these paragraphs is presented in Table 2.

<p>§ 221 aUGB</p>	<p>„(1) Kleine Kapitalgesellschaften sind solche, die mindestens zwei der drei nachstehenden Merkmale nicht überschreiten:</p> <ol style="list-style-type: none"> 1. „5 Millionen“ Euro Bilanzsumme; 2. „10 Millionen“ Euro Umsatzerlöse in den zwölf Monaten vor dem Abschlussstichtag; 3. im Jahresdurchschnitt 50 Arbeitnehmer. <p>(4) Die Rechtsfolgen der Größenmerkmale (Abs. 1 bis Abs. 3 erster Satz) treten ab dem folgenden Geschäftsjahr ein, wenn diese Merkmale</p> <ol style="list-style-type: none"> 1. an den Abschlußstichtagen von zwei aufeinanderfolgenden Geschäftsjahren überschritten beziehungsweise nicht mehr überschritten werden. ... <p>(6) Der Durchschnitt der Arbeitnehmeranzahl bestimmt sich nach der Arbeitnehmeranzahl an den jeweiligen Monatsletzten innerhalb des Geschäftsjahrs.“⁶⁶</p>
<p>§ 243 aUGB</p>	<p>„(1) Im Lagebericht sind der Geschäftsverlauf, einschließlich des Geschäftsergebnisses, und die Lage des Unternehmens so darzustellen, dass ein möglichst getreues Bild der Vermögens-, Finanz- und Ertragslage vermittelt wird, und die wesentlichen Risiken und Ungewissheiten, denen das Unternehmen ausgesetzt ist, zu beschreiben.</p> <p>(3) Der Lagebericht hat auch einzugehen auf</p> <ol style="list-style-type: none"> 5. die Verwendung von Finanzinstrumenten, sofern dies für die Beurteilung der Vermögens-, Finanz- und Ertragslage von Bedeutung ist; diesfalls sind anzugeben <ol style="list-style-type: none"> a) die Risikomanagementziele und -methoden, einschließlich der Methoden zur Absicherung aller wichtigen Arten geplanter Transaktionen, die im Rahmen der Bilanzierung von Sicherungsgeschäften angewandt werden, und <p>(4) Kleine Gesellschaften mit beschränkter Haftung (§ 221 Abs. 1) brauchen den Lagebericht nicht aufzustellen.“⁶⁷</p>
<p>§ 267 aUGB</p>	<p>„(1) Im Konzernlagebericht sind der Geschäftsverlauf, einschließlich des Geschäftsergebnisses, und die Lage des Konzerns so darzustellen, dass ein möglichst getreues Bild der Vermögens-, Finanz- und Ertragslage vermittelt wird, und die wesentlichen Risiken und Ungewissheiten, denen der Konzern ausgesetzt ist, zu beschreiben.“⁶⁸</p>

Table 2: Important paragraphs of aUGB

⁶⁶ aUGB dRGBI 1897/219 as amended BGBl I 2015/22.

⁶⁷ aUGB dRGBI 1897/219 as amended BGBl I 2015/22.

⁶⁸ aUGB dRGBI 1897/219 as amended BGBl I 2015/22.

The application for subsidies on EU level requires companies to fulfil the EC recommendations from above. These new recommendations are adapted for the increasing number of micro enterprises. However, according to a *UGB* in Austria registered Companies Limited by Shares are obligated to follow national laws.

2.2.2 Austrian Business Reorganisation Law (a*URG*)

According to § 1 a*URG* an entrepreneur may request a reorganisation process for a company. This reorganisation is a measure to improve her/his financial and profit situation for a sustainable continuation of a company.⁶⁹ § 22 a*URG* describes the liability of authorized representatives if they do not register a reorganisation process despite the fact that equity ratio drops below 8% and fictive debt repayment period rises above 15 years.⁷⁰ § 23 and § 24 of a*URG* specify the details of the calculation of equity ratio and fictive debt repayment period.^{71,72}

2.2.3 Austrian Law on Public Limited Company (a*AktG*) and Law on Limited Liability Company (a*GmbHG*)

The Austrian Law on Public Limited Company (a*AktG*) as well as the Law on Limited Liability Company (a*GmbHG*) regulates by law the existence of an internal control system and legal obligations. According to § 82 a*AktG* and § 22 a*GmbHG* the management board and management have to provide an accounting and internal control system that is tailored to the needs of a company. § 81 a*AktG* and § 28a a*GmbHG* obligate the management board and management to inform the supervisory board about the expected development of the company by providing an annual, quarterly and special report. These laws do not explain how companies should execute the demanded actions concerning risk management. Below, Table 3 shows the exact wording of important paragraphs.

<p>§ 81 a<i>AktG</i></p>	<p>„(1) Der Vorstand hat dem Aufsichtsrat mindestens einmal jährlich über grundsätzliche Fragen der künftigen Geschäftspolitik des Unternehmens zu berichten sowie die künftige Entwicklung der Vermögens-, Finanz- und Ertragslage anhand einer Vorschaurechnung darzustellen (Jahresbericht). Der Vorstand hat weiters dem Aufsichtsrat regelmäßig, mindestens vierteljährlich, über den Gang der Geschäfte und die Lage des Unternehmens im Vergleich zur Vorschaurechnung unter Berücksichtigung der künftigen Entwicklung zu berichten (Quartalsbericht). Bei wichtigem Anlaß ist dem Vorsitzenden des Aufsichtsrats unverzüglich zu berichten; ferner ist über Umstände, die für die Rentabilität oder Liquidität der Gesellschaft von erheblicher Bedeutung sind, dem Aufsichtsrat unverzüglich zu berichten (Sonderbericht).“⁷³</p>
---------------------------------	--

⁶⁹ a*URG* BGBl I 1997/114.

⁷⁰ a*URG* BGBl I 1997/114 as amended BGBl I 2010/58.

⁷¹ a*URG* BGBl I 1997/114 as amended BGBl I 2005/120.

⁷² a*URG* BGBl I 1997/114 as amended BGBl I 2005/120.

⁷³ a*AktG* BGBl 1965/98 as amended BGBl I 1997/114.

§ 81 aAktG	„(2) Der Jahresbericht und die Quartalsberichte sind schriftlich zu erstatten und auf Verlangen des Aufsichtsrats mündlich zu erläutern; sie sind jedem Aufsichtsratsmitglied auszuhändigen. Die Sonderberichte sind schriftlich oder mündlich zu erstatten.“ ⁷⁴
§ 82 aAktG	„Der Vorstand hat dafür zu sorgen, daß ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen.“ ⁷⁵
§ 22 aGmbHG	„(1) Die Geschäftsführer haben dafür zu sorgen, daß ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen.“ ⁷⁶
§ 28a aGmbHG	<p>„(1) Die Geschäftsführer haben dem Aufsichtsrat mindestens einmal jährlich über grundsätzliche Fragen der künftigen Geschäftspolitik des Unternehmens zu berichten sowie die künftige Entwicklung der Vermögens-, Finanz- und Ertragslage anhand einer Vorscheurechnung darzustellen (Jahresbericht). Die Geschäftsführer haben weiters dem Aufsichtsrat regelmäßig, mindestens vierteljährlich, über den Gang der Geschäfte und die Lage des Unternehmens im Vergleich zur Vorscheurechnung unter Berücksichtigung der künftigen Entwicklung zu berichten (Quartalsbericht). Bei wichtigem Anlaß ist dem Vorsitzenden des Aufsichtsrats unverzüglich zu berichten; ferner ist über Umstände, die für die Rentabilität oder Liquidität der Gesellschaft von erheblicher Bedeutung sind, dem Aufsichtsrat unverzüglich zu berichten (Sonderbericht).</p> <p>(2) Der Jahresbericht und die Quartalsberichte sind schriftlich zu erstatten und auf Verlangen des Aufsichtsrats mündlich zu erläutern; sie sind jedem Aufsichtsratsmitglied auszuhändigen. Die Sonderberichte sind schriftlich oder mündlich zu erstatten.“⁷⁷</p>

Table 3: Important paragraphs of aAktG and aGmbHG

2.2.4 Corporate Sector Supervision and Transparency Act (KonTraG)

In 1998 a legal standard called Corporate Sector Supervision and Transparency Act (*KonTraG*) was established in Germany. This standard is addressed to Public Limited Companies (gAG) and their board members but can also be applied to other legal forms. Since *KonTraG* is not a separate law, it introduces some major changes to the Law on Public Limited Company (gAktG), Law on Limited Liability Company (gGmbHG) and other laws. § 91(2) gAktG implies that the management board is obligated to install suitable monitoring systems, which ensures the continued existence of the enterprise and the early identification of emerging risks. Therefore the management has to deal with each single step of the risk management process (see Figure 2) to be successful. § 93(2) gAktG and § 43(1) gGmbHG implies that the management board and the management have to prove their due diligence towards the company. This requires the continuous documentation of the risk management

⁷⁴ aAktG BGBI 1965/98 as amended BGBI I 1997/114.

⁷⁵ aAktG BGBI 1965/98 as amended BGBI I 1997/114.

⁷⁶ aGmbHG RGBI 1906/58 as amended BGBI I 1997/114.

⁷⁷ aGmbHG RGBI 1906/58 as amended BGBI I 1997/114.

process. The exact wording of § 91(2) gAktG, § 93 gAktG and § 43 gGmbHG can be seen in Table 4.^{78,79}

§ 91 gAktG	„(2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“ ⁸⁰
§ 93 gAktG	„(2) Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast.“ ⁸¹
§ 43 gGmbHG	„(1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.“ ⁸²

Table 4: Important paragraphs of KonTraG

2.2.5 Austrian Code of Corporate Governance (ACCG)

The Austrian Code of Corporate Governance (ACCG) was introduced on 1 October 2002 by the Austrian Working Group for Corporate Governance and has been reworked many times since then. Chapter 1.1 mentions the main goals of this code. The ACCG explicitly points out that the German text is the exclusively binding version. Concerning risk management the code contains some important rules, which are displayed in Table 5. Essential facts related to risk management are, for example: the management board has to give the supervisory board comprehensive information, an audit committee monitors the effectiveness of the internal control system and the description of the mainly used risk management instruments with respect to non-financial risks. Furthermore, categories of rules are defined by the code as follows:⁸³

- Legal requirement (LR): This rule refers to mandatory legal requirements.
- Comply or explain (CE): This rule is to be followed; any deviation must be explained and the reasons stated in order to be in compliance with the Code.
- Recommendation (REC): The nature of this rule is a recommendation; non-compliance with this rule requires neither disclosure nor explanation.

⁷⁸ Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 43.

⁷⁹ Cf. ELLER, R.; HEINRICH, M.; PERROT, R. (2010), p. 149.

⁸⁰ gAktG BGBl I 1965/1089 as amended BGBl I 2015/642.

⁸¹ gAktG BGBl I 1965/1089 as amended BGBl I 2015/642.

⁸² gGmbHG BGBl III 1892/- as amended BGBl I 2015/642.

⁸³ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 5 ff.

Chapter III-9 (LR)	<i>„Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle relevanten Fragen der Geschäftsentwicklung, einschließlich der Risikolage und des Risikomanagements der Gesellschaft und wesentlicher Konzernunternehmen. ...“⁸⁴</i>
Chapter IV-18 (CE)	<i>„In Abhängigkeit von der Größe des Unternehmens ist eine interne Revision als eigene Stabstelle des Vorstands einzurichten oder an eine geeignete Institution auszulagern. Über Revisionsplan und wesentliche Ergebnisse ist dem Prüfungsausschuss zumindest einmal jährlich zu berichten.“⁸⁵</i>
Chapter V-37 (CE)	<i>„Der Aufsichtsratsvorsitzende bereitet die Aufsichtsratssitzungen vor. Er hält insbesondere mit dem Vorstandsvorsitzenden regelmäßig Kontakt und diskutiert mit ihm die Strategie, die Geschäftsentwicklung und das Risikomanagement des Unternehmens.“⁸⁶</i>
Chapter V-40 (LR)	<i>„Unabhängig von der Größe des Aufsichtsrats ist bei börsennotierten Gesellschaften ein Prüfungsausschuss einzurichten. Der Prüfungsausschuss ist für die Überwachung des Rechnungslegungsprozesses, die Überwachung der Arbeit des Abschlussprüfers, die Prüfung und Vorbereitung der Feststellung des Jahresabschlusses, des Vorschlags für die Gewinnverteilung und des Lageberichts zuständig. ... Darüber hinaus hat der Prüfungsausschuss die Wirksamkeit des unternehmensweiten internen Kontrollsystems, gegebenenfalls des internen Revisionssystems und des Risikomanagementsystems der Gesellschaft zu überwachen. ...“⁸⁷</i>
Chapter VI-69 (LR)	<i>„Die Gesellschaft legt im Konzernlagebericht eine angemessene Analyse des Geschäftsverlaufes vor und beschreibt darin wesentliche finanzielle und nicht-finanzielle Risiken und Ungewissheiten, denen das Unternehmen ausgesetzt ist sowie die wichtigsten Merkmale des internen Kontrollsystems und des Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess.“⁸⁸</i>
Chapter VI-70 (CE)	<i>„Die Gesellschaft beschreibt im Konzernlagebericht die wesentlichen eingesetzten Risikomanagement-Instrumente in Bezug auf nicht-finanzielle Risiken.“⁸⁹</i>
Chapter VI-83 (CE)	<i>„Darüber hinaus hat der Abschlussprüfer auf Grundlage der vorgelegten Dokumente und der zur Verfügung gestellten Unterlagen die Funktionsfähigkeit des Risikomanagements zu beurteilen und dem Vorstand zu berichten. Dieser Bericht ist ebenfalls dem Vorsitzenden des Aufsichtsrats zur Kenntnis zu bringen. ...“⁹⁰</i>

Table 5: Important paragraphs of ACCG

⁸⁴ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 18.⁸⁵ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 20.⁸⁶ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 28.⁸⁷ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 29 f.⁸⁸ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 42.⁸⁹ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 42.⁹⁰ Cf. AUSTRIAN CODE OF CORPORATE GOVERNANCE (2015), p. 47.

2.2.6 ISO 31000 – Risk management

In 2009 ISO 31000:2009 was proposed with its main goal to combine two different categories of standards. These two categories are on the one hand sector-specific risk management standards and on the other hand management-specific standards like ISO 9001.⁹¹ This new risk management standard has evolved from *ONR 4900x* series, which was introduced in 2004 and is again based on the Australian/New Zealand (AS/NZS)-Standard 4360. AS/NZS 4360 was established in 1995 with the aim to provide an easy and simple risk management approach for public, private or community enterprises, groups and individuals. This standard helps to accomplish a better identification of opportunities and threats, trust and better corporate governance pro-active rather than re-active management and improved stakeholder confidence. ISO 31000:2009 offers like AS/NZS 4360 principles and generic guidelines for any public, private or community enterprise, association, group or individual. The main difference between these two standards is the suitability for the purpose of certification. ISO 31000:2009 explicitly informs the reader that the standard is not suitable for the purpose of certification.^{92,93,94}

2.2.7 ONR 4900x:2014 – Risk Management for Organizations and Systems

As already mentioned, the Austrian Standards Institute established *ONR 4900x* series in cooperation with the network of risk management from Austria and Switzerland in 2004. The *ONR 4900x* series is designed to help by the practical implementation of the generic guidelines of ISO 31000. In revision 2014 this series is structured into several elements as listed below and shown in Figure 7:⁹⁵

Risk Management for Organizations and Systems –

- Terms and basics (*ONR 49000*)
- Risk Management (*ONR 49001*)
- Part 1: Guidelines for embedding the risk management in the management system (*ONR 49002-1*)
- Part 2: Guideline for methodologies in risk assessment (*ONR 49002-2*)
- Part 3: Guidelines for emergency, crisis and business continuity management (*ONR 49002-3*)
- Requirements for the qualification of the Risk Manager (*ONR 49003*)

⁹¹ Cf. BRÜHWILER, B.; ROMEIKE, F. (2010), p. 82.

⁹² Cf. BRÜHWILER, B. (2011), p. 50 f.

⁹³ Cf. AS/NZS 4360:2004, p. 1 f.

⁹⁴ Cf. ISO 31000:2009, p. 1.

⁹⁵ Cf. *ONR 49000:2014*, p. 3 f.

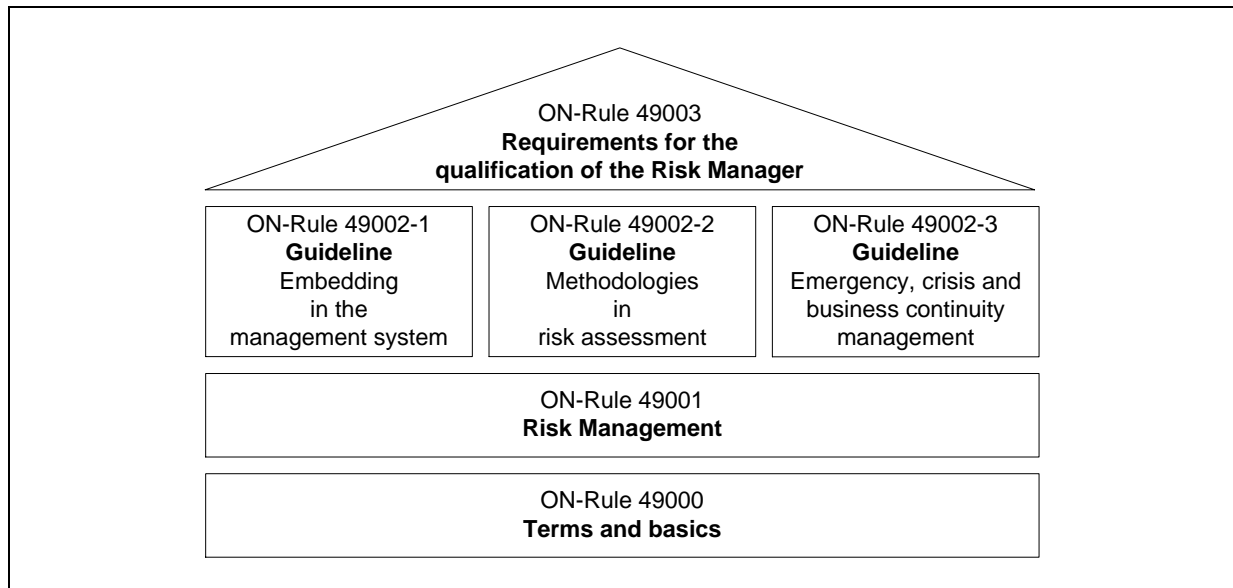


Figure 7: Structure of *ONR 4900x:2014 series*⁹⁶

In Figure 7, *ONR 49000* forms the lower base of this “risk management house” and defines fundamental terms and basics concerning risk management. Some of these terms are adapted from ISO Guide 73 and others are extended to fit the needs of this standard. Furthermore, it describes objectives and principles of the *ONR 4900x:2014 series*.⁹⁷ The upper base is formed by *ONR 49001*, which explains the general procedure of a risk management system and in detail the sequence of the risk management process (see Figure 2).⁹⁸ Chapter 2.3 explains the single stages of the risk management process more detailed. *ONR 49002-1*, the first pillar of this house, shows possibilities concerning embedding the risk management system into a pre-existing or an independent management system. A proposal regarding the integration into the quality management system (ISO 9000) is also part of *ONR 49002-1*. The second pillar, *ONR 49002-2*, lists for each risk management process stage suitable methods and a brief description. The entire list of risk assessment methods is displayed in Table 13. The list describes the applicability of each method as being either strongly applicable, applicable or not applicable for the different stages of the risk management process. The third pillar, *ONR 49002-3*, deals with the emergency and crisis management of companies. Due to the fact that it is not possible to prevent all risks from happening, companies have to deal with remaining risks. *ONR 49002-3* provides a framework to companies for a quick and proper reaction in case of an emergency. Emergency and crisis management are not included in ISO 31000.^{99,100,101} *ONR 49003* forms the rooftop of this “risk management house” and describes the requirements for the education and qualification of risk managers.¹⁰²

⁹⁶ Cf. *ONR 49000:2014*, p. 4.

⁹⁷ Cf. *ONR 49000:2014*, p. 3.

⁹⁸ Cf. *ONR 49001:2014*, p. 4.

⁹⁹ Cf. *ONR 49002-1:2014*, p. 4 f.

¹⁰⁰ Cf. *ONR 49002-2:2014*, p. 4.

¹⁰¹ Cf. *ONR 49002-3:2014*, p. 4.

¹⁰² Cf. *ONR 49003:2014*, p. 4.

As already mentioned in chapter 1.4 *ONR 4900x* series extend *AS/NZS 4360* standard by including the Deming wheel (see Figure 8). Elements of the management are taken into consideration and companies get an indication of a proper implementation of risk management systems into their organisation. Many other standards like *ISO 31000* and *ISO 9001* are based on the Deming wheel because it provides a systematic approach for the solution of problems on different levels. The Plan-Do-Check-Act (PDCA) cycle was established in 1950 by William Edwards Deming and consists of four phases. The first phase of this cycle is “plan”, it evaluates the current state. Based on the outcome of this analysis an improvement plan and realistic objectives are defined. In the second phase “do” involved employees get informed, and planned improvements are implemented. The third phase “check” gathers information from different areas and checks if the objectives from the first phase are achieved. “Act” is the last phase of this cycle and does a target/actual check. Depending on the outcome of this target/actual check, actions from phase two are either standardised or phases one and two are repeated as often as necessary to achieve the defined objectives. In order to eliminate old grievances it is important to standardise successful implementations. To continue improvements after a successful run through PDCA cycle it is important to define new objectives.^{103,104}

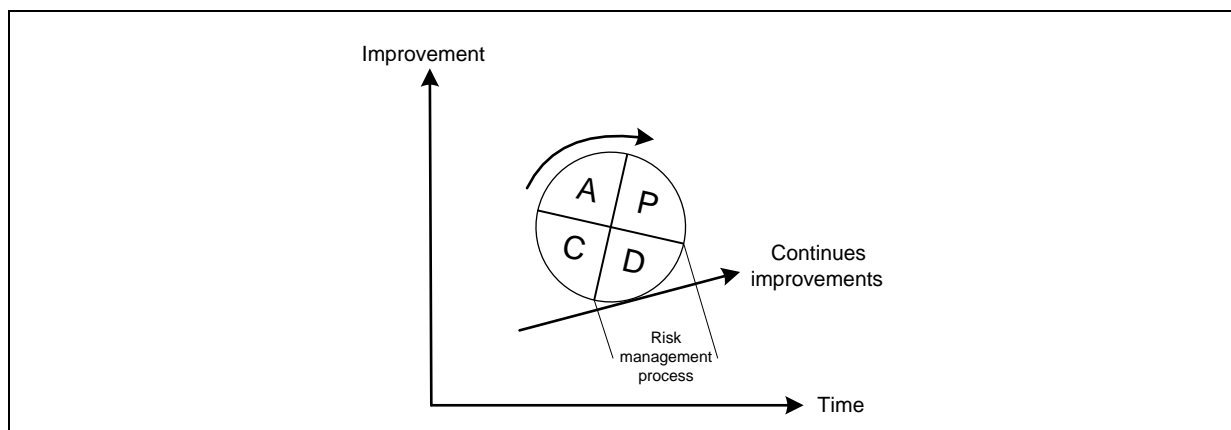


Figure 8: The PDCA cycle¹⁰⁵

Implementing and maintaining risk management into a company can achieve the following objectives:¹⁰⁶

- Increase the likelihood of achieving objectives;
- Be aware of the need to identify and treat risks throughout the organization;
- Improve the identification of opportunities and threats;
- Improve operational effectiveness and efficiency;
- Enhance health and safety performance, as well as environmental protection;
- Minimize losses; and
- Improve organizational learning.

¹⁰³ Cf. BRÜHWILER, B. (2011), p. 52.

¹⁰⁴ Cf. KOCH, S. (2015), p. 118 ff.

¹⁰⁵ Adapted from GASTL, R. (2005), p. 26.

¹⁰⁶ ISO 31000:2009, p. v f.

2.2.8 ISO 9001 – Quality management

In 1987 the first version of the ISO 9000 was published.¹⁰⁷ Since then several revisions have been released of the world's most popular quality improvement standard. In 2008 the last revision was proposed with some minor changes. A new revision will be published by the end of 2015, which contains some radical changes to their structure. This new "high-level structure" will be used in all future management system standards and ensures that all management system standards contain the same section headings and core texts. In addition, the topic of risk management has been taken up. The ISO/DIS 9001:2015 draft requests identification and treatment of occurring risks but does not require a standardised risk management. EFG is one of over one million certified organisations world wide, which is affected by these changes. A three-year transition period is granted to all organisations to adjust their quality management system to the revised standard.^{108,109} As the ISO 9001:2015 had not yet been published when this master thesis was finished, the author cannot go into detail regarding the additions of risk management.

2.2.9 Additional standards

This chapter briefly describes international standards for banks, insurances and international companies that have registered equity or debt securities within the United States (U.S.). While Basel III and Solvency II regulations are revised on a regular basis (see Figure 6) the U.S. government does not have any intentions revising the Sarbanes-Oxley Act.

Basel III

In 2004 the Basel Committee on Banking Supervision (BCBS) introduced a new capital accord (Basel II) for banks to strengthen the safety and reliability of the financial system, enhance the level playing field and identify occurring risks more reliable. Therefore Basel II consists of three complementary pillars:¹¹⁰

- Regulatory capital
- Supervisory review
- Market disclosure

In 2010 BCBS proposed new recommendations concerning capital accord (Basel III). These recommendations are based on Basel II and the insights after the global financial and economic crisis. The goal of Basel III is to stabilise the international financial world by increasing the minimum equity requirements and introducing capital buffers. Basel III is not legally binding in Austria but the new recommendations get incorporated into the European Banking Supervision Law. The mandatory date of the initial application was the 1 January 2014.^{111,112}

¹⁰⁷ Cf. HOYLE, D. (2009), p. 16.

¹⁰⁸ Cf. TÜF SÜD AMERICA (2014), p. 1 ff.

¹⁰⁹ Cf. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION.

¹¹⁰ Cf. BUNDESMINISTERIUM DER FINANZEN [a] (2015).

¹¹¹ Cf. BUNDESMINISTERIUM DER FINANZEN [b] (2015).

¹¹² Cf. AUSTRIAN FINANCIAL MARKET AUTHORITY (2015).

Solvency II

Solvency II, a EU-wide project proposed in 2009, is addressed to insurance companies in the European Union (EU) with the aim of supervision. The outcome of this proposal is a new Insurance Supervision Act, which will come into force on 1 January 2016. Like Basel II it is based on three pillars:

- Quantitative requirements
- Qualitative requirements and supervisory rules
- Reporting and disclosure

The revised version focuses strongly on qualitative requirements and business management tools especially risk management. This approach points out risks of insurances and helps them to identify, manage and control these risks. To make this possible the supervision provisions of Solvency II go far beyond the provisions of the Bank Supervision Law.^{113,114}

Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) came into force in 2002 with its intention “to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities’ laws, and for other purposes.”¹¹⁵ SOX was proposed due to loss of confidence of investors in management caused by financial reporting scandals. It is obligatory to all U.S. and international companies that have registered equity or debt securities with the Securities and Exchange Commission (SEC). The most important sections of SOX concerning risk management are:^{116,117}

- SEC. 302. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS.
- SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.
- SEC. 906. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS.

2.3 The risk management process according to *ONR 4900x:2014*

Reasons for the use of risk management are often external trends, development, legal requirements as shown in chapter 2.2 or “best practise”. Special attention is paid to topics like obligations of top management, work safety, environmental safety and product safety. A proper implemented risk management increases the risk awareness of employees’ and teaches them how to deal with arising risks instead of avoiding them. In order to be successful, companies have to take risks. These risks can become opportunities that bring the desired level of success. Nowadays many companies have risk management processes for single sub-applications within a company in place, but the integration into a holistic management system is often missing. Therefore, the establishment of an integrated risk management that combines the top-down and bottom-up approach is necessary (see

¹¹³ Cf. AUSTRIAN FEDERAL MINISTRY OF FINANCE (2015).

¹¹⁴ Cf. BRÜHWILER, B. (2011), p. 100.

¹¹⁵ SARBANES-OXLEY ACT (2002).

¹¹⁶ Cf. SOX-ONLINE (2012).

¹¹⁷ Cf. BRÜHWILER, B. (2012), p. 20.

Figure 9). The top-down approach is a holistic view of a company or system and considers essential risks of a company. Managers with good overview and detailed knowledge about the company conduct the risk identification concerning possible chances and risks. The exclusive use of this approach minimises the chances to identify all risks. This is due to the fact that top management does not have the level of detail required for identifying risks in all areas. Furthermore, the time of the management is limited and the risk management process requires a continuous supervision throughout the process. However, the bottom-up approach goes deeper into detail and takes technical concepts, service processes and the daily business into account. By involving a broader range of hierarchical levels chances to identify more risks increase and risk awareness of employees gets deeply rooted in the companies' culture. The objective of the management has to be to establish a risk management system, which combines the advantages of the top-down and bottom-up approach.^{118,119,120,121,122}

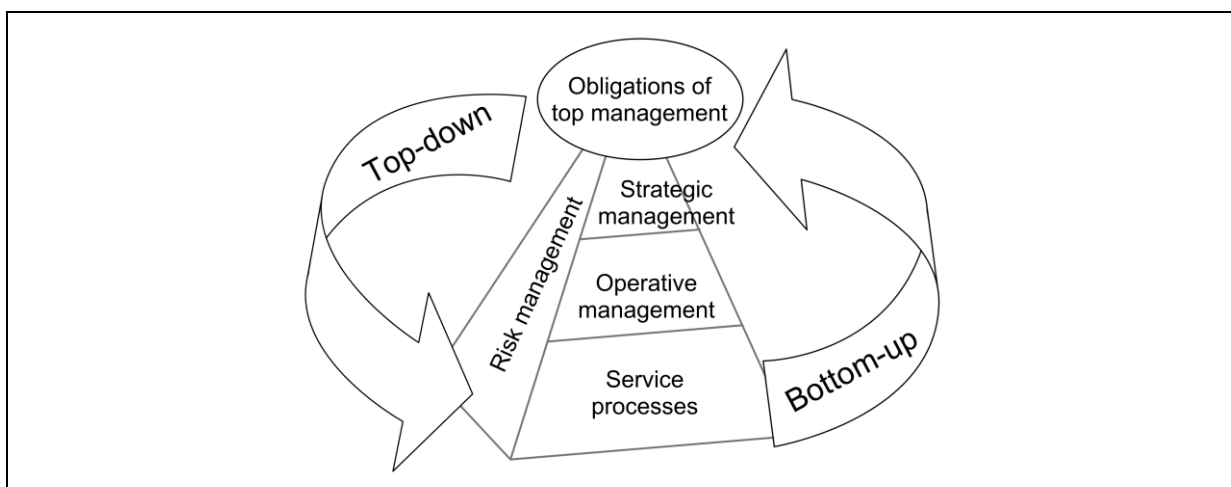


Figure 9: Top-down and bottom-up approach¹²³

Below, each single process step of *ONR 49001:2014* is illustrated in more detail. Furthermore, defined objectives, approaches and methods used concerning EFG are described.

2.3.1 Establishing the context

As already briefly described in chapter 1.4 the task of this first process step (see Figure 2) is the specification of objectives, approaches used, expectations, strategies, functions and processes of the company. Furthermore, the internal and external factors and the risk criteria for the risk assessment have to be defined.^{124,125}

¹¹⁸ Cf. DENK, R.; EXNER-MERKELT, K. (2008), p. 85 ff.

¹¹⁹ Cf. *ONR 49000:2014*, p. 17 f.

¹²⁰ Cf. BRÜHWILER, B. (2011), p. 104.

¹²¹ Cf. DAHMEN, J. (2003), p. 34.

¹²² Cf. BRÜHWILER, B. (2011), p. 134.

¹²³ Cf. *ONR 49000:2014*, p. 18.

¹²⁴ Cf. BRÜHWILER, B. (2011), p. 104.

¹²⁵ Cf. *ONR 49001:2014*, p. 18.

2.3.1.1 Establishing the external context

The external context is the external environment in which a company tries to accomplish its objectives and includes among others social and cultural, political, legal, regulatory, financial, technological natural and competitive conditions, whether international, national or local. By developing the external context it is important to ensure that objectives and concerns of external stakeholders are taken into account.¹²⁶

A company has to fulfil some certain legal requirements depending on their legal form and size as shown in chapter 2.2. An intentional or careless violation of these requirements can harm the company's objectives, management and employees. Despite all legal and normative requirements, whether national or international, the determination of insufficient executions of these requirements is necessary.¹²⁷

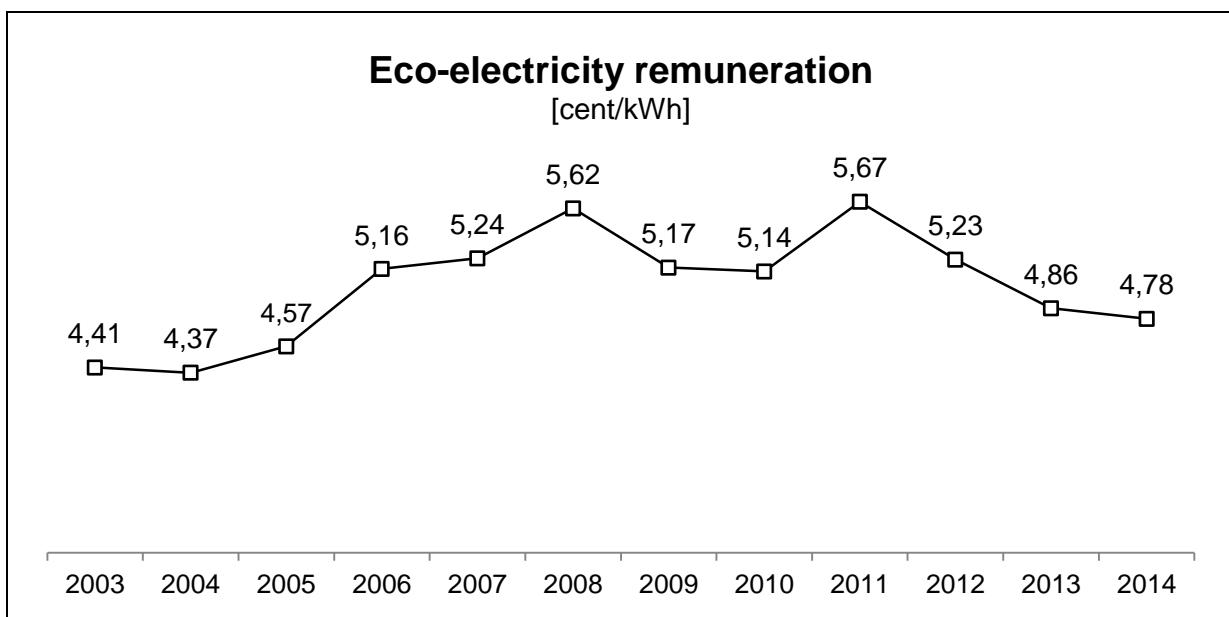


Figure 10: Eco-electricity remuneration of small hydro generating stations¹²⁸

An important source of risk is the economic environment in which a company is operating. The choice of a proper location can decide whether a company is competitive or not. This strongly depends on legal certainty, law enforcement, taxes and tariffs or social security contributions of the chosen country.¹²⁹ In Austria the Austrian Green Electricity Law 2012 (aÖSG 2012) regulates among others the specifications of eco-electricity plants, the validity period and the amount of feed-in tariffs. An eco-electricity plant is defined according to §5 aÖSG 2012 as a plant that produces electricity exclusively out of renewable energy sources. Furthermore, a small hydro generating station has to be based on renewable energy sources with a bottleneck capacity of up to 10MW. This bottleneck capacity is specified as the highest possible electrical continuous output of the worst performing part of

¹²⁶ Cf. ONR 49001:2014, p. 18.

¹²⁷ Cf. BRÜHWILER, B. (2011), p. 104 f.

¹²⁸ Cf. ENERGIE-CONTROL AUSTRIA (2009).

¹²⁹ Cf. BRÜHWILER, B. (2011), p. 105.

the plant. If the small hydro generating station fulfils the requirements of aÖSG 2012 the green power settlement agency (*OeMAG*) is obligated to pay a predefined feed-in tariff. The *Ökostrom-Einspeisetarifverordnung 2012 (ÖSET-VO 2012)* specifies the feed-in tariff depending on the amount of electricity fed by the power plant operator. This feed-in tariff is guaranteed for 13 years according to §16 aÖSG 2012.¹³⁰ Figure 10 shows the average remuneration per year paid by *OeMAG* for small hydro generating stations in Austria. As the remuneration has been declining for the last couple of years, investments in new or revitalising old small hydro generating stations have become less interesting for power plant operators.

The success of many companies depends on available natural resources like fossil oil, natural gas, coal and minerals. Furthermore, mountains, shores and natural reserves are very important for tourism. Scarcity of these resources can threaten the means of existence of many industries.¹³¹ As EFG's products strongly depend on water, a water scarcity could arise to an existentially threatening risk. Due to the fact that EFG's majority of projects are done in Austria, water scarcity should not evolve into a problem in the next decades.

2.3.1.2 Establishing the internal context

The internal context is the internal environment in which a company tries to accomplish its objectives. Therefore, the risk management process is tailored to a company's culture, processes, structures and strategies. The internal context considers anything within a company that influences the process of managing risks. In order to perform the risk management process in a proper way it is important to understand the internal context which takes the governance, organisational structure, roles, capabilities, standards and guidelines into consideration.¹³²

Supply and demand determines the price for products and services and is steered by competitors. A company has to compare the customer satisfaction of their products with the customer satisfaction of their competitors. A high divergence can lead to a loss of customers due to quality issues, too expensive products and services or delayed deliveries.¹³³

Classical financial risks of private companies are capital procurement and liquidity generation. Risk capacity of private companies is defined by the available equity. The procurement of equity capital and profits out of operating activities can increase the risk capacity of companies. Medium- and long-dated debt capital is normally used for financing means of production. Changes in interest, exchange rates, procurement goods and real estates can cause additional financial risks.¹³⁴ Hydropower plant manufacturers often deal with contractual penalties concerning delayed deliveries or efficiencies. Furthermore, a common practice is the splitting of the order value depending on the size of order into three or five transactions. Typically, EFG's projects are divided into three transactions. The first

¹³⁰ aÖSG 2012 *BGBI I* 2011/75.

¹³¹ Cf. BRÜHWILER, B. (2011), p. 106.

¹³² Cf. *ONR 49001:2014*, p. 19.

¹³³ Cf. BRÜHWILER, B. (2011), p. 108.

¹³⁴ Cf. BRÜHWILER, B. (2011), p. 110.

transaction takes place after placing the order while the second one is executed after the start of on-site assembling. The customer transfers the final amount after the hydropower plant is put into service. As these projects have usually durations of several months, companies need enough liquid assets to finance purchased parts in advance until they receive the next transaction.

Work and development of a company strongly depends on the competences of its employees. The employees provide labour to the company and produce new products and offer services. The support and continuing education of employees are chances to expand the professional competence. Any company that neglects the support of employees creates risks and threatens the company's existence.¹³⁵

2.3.1.3 Defining risk criteria

Companies have to define criteria for the evaluation of identified risks. Those criteria represent values, objectives and resources of a company and can contain legal requirements and regulations. Furthermore, criteria have to be defined at the beginning of the risk management process and continuously reviewed. During the definition of risk criteria factors, such as nature of causes and consequences, definition of likelihood, determination of risk level or tolerable risk level should be taken into consideration.¹³⁶

The classification of each risk criterion regarding likelihood and consequences has to be individually defined for each company. By using the expected value (see chapter 2.1.1) a comparison of different risks is possible. Many companies use simple rating systems for the determination of likelihood and consequences.^{137,138}

Level	Frequency
Frequently	once every month or more often
Likely	between once every month or once every quarter
Rarely	between once every quarter or once every year
Very rarely	between once every year or once every three years
Unlikely	more seldom than once every three years

Table 6: Risk criteria – likelihood (high frequency)¹³⁹

¹³⁵ Cf. BRÜHWILER, B. (2011), p. 111.

¹³⁶ Cf. ONR 49001:2014, p. 20.

¹³⁷ Cf. ROMEIKE, F. [b] (2003), p. 183 f.

¹³⁸ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN, H. (2006), p. 26.

¹³⁹ Adapted from ONR 49002-2:2014, p. 25.

Level	General	Health	Image	Finances
Insignificant	Due to company's size the risk is neglectable; customers are barely affected.	Personal damage with minor injuries and no loss of working hours.	Occasionally complaints and reclamations.	Financial loss is barely noticeable in the budget.
Minor	Risk creates disturbances and additional costs; single customers are unsatisfied.	Personal damage with healable injuries and loss of working hours.	Critical media reports lead to public emotions against activities, products and services.	Financial loss leads to deviations from budget.
Noticeable	Risk harms performance. Single operational functions are affected; this results in delayed deliveries.	Lightly and permanent damage to health; quality of living is affected.	Criminal investigations with charges are initiated because of grossly omission, gross negligence or violations against laws and values.	Financial results are visibly affected; revenue and liquidity are affected.
Critical	The company's capability is affected; customer losses increase.	Severe and permanent damage to health; quality of living dramatically decreases.	Criminal investigations lead to long-range and widely loss of trust which can only be compensated with large effort.	Financial result gets permanently affected; damage increases up to an annual result; tight liquidity.
Catastrophic	Risk affects the whole company; market position gets lost; company's continuation is questioned.	Personal damage with lethal consequence or serious invalidity.	Heavy violations against safety regulations and retirement of responsible people; it will be hard to recover from the damage.	Financial consequences of the risk exceed the annual result and leads to losses of equity; threat of bankruptcy.

Table 7: General risk criteria – consequences¹⁴⁰

ONR 49002-2:2014 provides different recommendations concerning risk criteria for different application areas. Some of these qualitative recommendations concerning likelihood and consequences are displayed in Table 6 and Table 7. Besides the usage of qualitative criteria the evaluation of consequences can also be done with quantitative criteria. Therefore, literature suggests the usage of earnings before interest and taxes (EBIT) or equity of a company. EBIT allows the evaluation of the operational business independent of variations of interest and taxes as well as extraordinary business transactions. In consultation with EFG's accountant as quantitative criteria for the evaluation of consequences the EBIT was chosen. By using a combination of qualitative and quantitative criteria for the evaluation of risks a context between the different criteria has to be established as displayed in Table 8.^{141,142}

¹⁴⁰ Cf. ONR 49002-2:2014, p. 24.

¹⁴¹ Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 106.

¹⁴² Cf. SCHWAB, A. (2010), p. 127.

Consequences		
Qualitative		Quantitative
Insignificant	...	0–5% of EBIT
Minor	...	5% of EBIT
Major	...	25% of EBIT
Severe	...	100% of EBIT (Risk can get the company in the red)
Catastrophic	...	Height of equity

Table 8: Risk criteria context – consequences¹⁴³

In principle it is possible to distinguish between nominal, ordinal and proportion scales. The nominal scale enables to a pure qualitative evaluation. Risks with identical characteristics are matched with identical numbers or adjectives. A ranking of risks can be accomplished by using ordinal scales. The usage of an ordinal scale makes possible a comparison of different risks concerning their likelihood and consequences and can be applied for qualitative evaluations. However, a statement about various risk levels of identified risks is not possible. Proportion scales enable to an evaluation of risk levels by using numerical values and are preferably used for quantitative evaluations. The chosen evaluation scale has to provide the highest possible accuracy based on available information. Based on this knowledge a combination of an ordinal and proportion scale (see Figure 11) was developed for EFG.¹⁴⁴

2.3.1.4 Risk criteria at EFG

In co-operation with EFG's top management and accountant risk criteria based on recommendations of *ONR 49002-2:2014* (Table 6 and Table 7) were defined. Furthermore, the context between qualitative and quantitative risk criteria for the evaluation of identified risks was established. This enables the risk manager and risk owners of EFG either to evaluate an identified risk qualitative or quantitative with a specific amount of money related to their EBIT. Before each risk evaluation the EBIT has to be updated by the risk manager. Figure 11 shows correlations of the risk criteria evaluation scale between qualitative and quantitative risk criteria. Furthermore, Table 6 and Table 7 are used to link the qualitative risk criteria adjectives with the scale in Figure 11 in order to establish a consistent understanding during risk assessment.¹⁴⁵ On the left-hand side of each scale the percentage of the risk matrix (see Figure 17) is plotted. The right-hand side of the scale illustrates corresponding risk criteria either qualitative or quantitative. For example, in case of consequences the qualitative value catastrophic is displayed as a range between 80% and 100%. For the calculation of the risk matrix in the risk management tool (RMT) a specific percentage for each qualitative risk criteria is deposited. For example, catastrophic is set to 90%, which can be adjusted later on in the settings of the RMT. The entered EBIT, which is for data

¹⁴³ Adapted from DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 106.

¹⁴⁴ Cf. DAHMEN, J. (2003), p. 36 ff.

¹⁴⁵ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN, H. (2006), p. 27.

protection reasons not allowed to publish, is equivalent to 100% of the quantitative risk criteria scale.

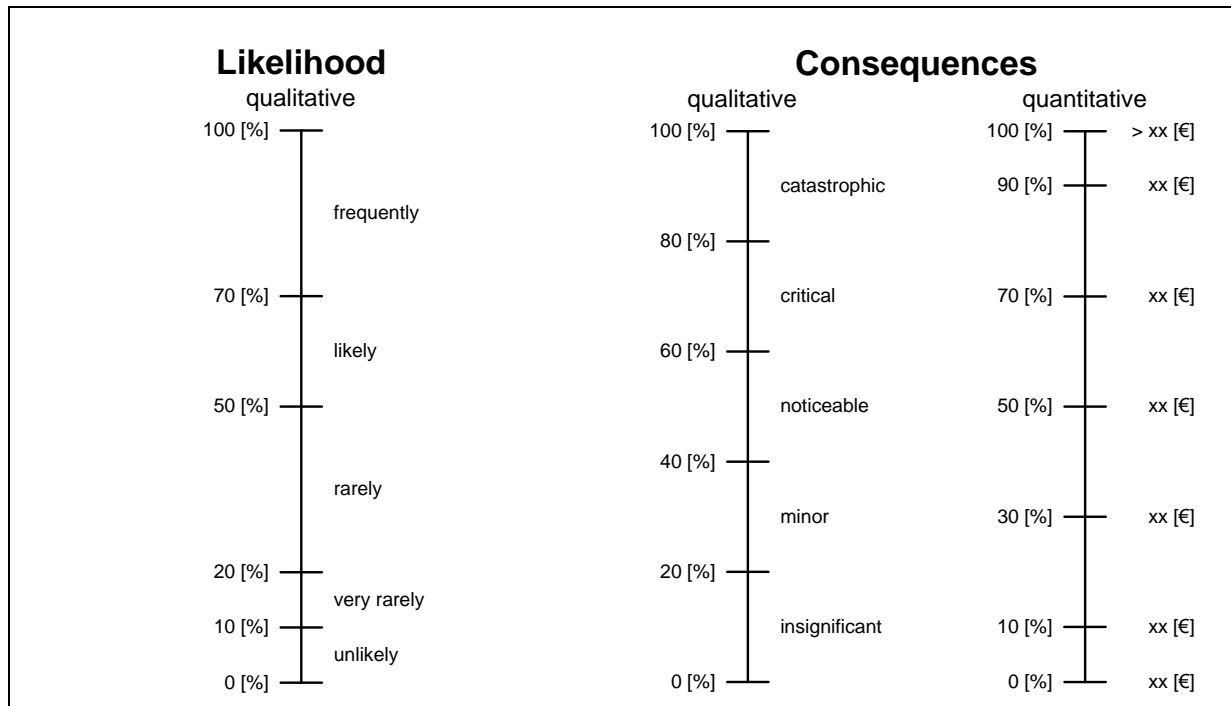


Figure 11: Risk criteria context at EFG¹⁴⁶

2.3.2 Risk assessment

Risk assessment is made up of the following process steps: risk identification, risk analysis and risk evaluation as displayed in Figure 2. Below each process step is theoretically analysed as well as linked to a practical context by applying to EFG. Therefore, the process step's outcome is described.

2.3.2.1 Risk identification

The first step of the risk assessment process is the identification of risks. The company has to identify causes and potential consequences, sources of risks, areas of impacts and events. The aim of this process step is to generate a comprehensive list of risks. This list should be as complete as possible because not identified risks will not be included in further process steps. The identification should also include risks whether or not their source or cause is under company's control.¹⁴⁷ The possibility to influence risks can be distinguished into three different circles (see Figure 12). The circle in the centre – circle of control – includes all internal company processes and risks. Due to independency of third parties, companies have the most influence on these parameters. In the middle circle – circle of influence – the influence of companies decreases due to dependency on external parties or factors. The last circle – circle of concern – contains external factors, which cannot be

¹⁴⁶ Adapted from DAHMEN, J. (2003), p. 38.

¹⁴⁷ Cf. ONR 49001:2014, p. 21.

influenced by a single company. One external factor of this circle would be the price for electricity, which cannot be influenced by EFG.¹⁴⁸

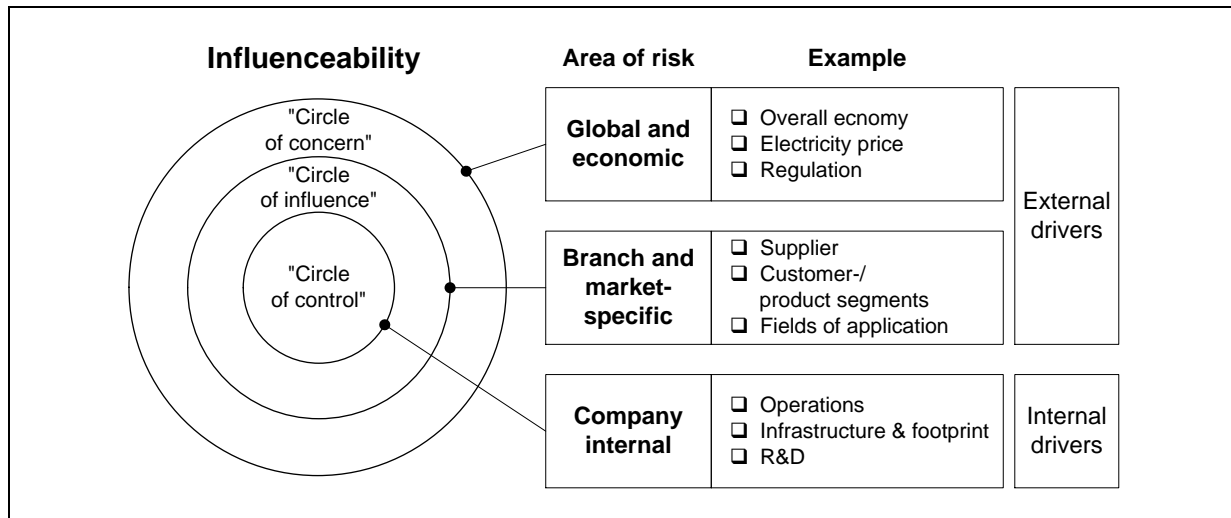


Figure 12: Circles of influence and risk sources¹⁴⁹

Objectives and capabilities of chosen risk identification tools and methods should be appropriate for occurring risks. Background information as well as relevant and up-to-date information is essential for this process step.¹⁵⁰

Identification methods according to *ONR 49002-2:2014* from Table 13 can be divided into collection and search methods displayed in Figure 13. Collection methods are used for existing or obvious risks. Checklists, interviews and questionings are the most frequently used collection methods. Experience and expertise of questioners and interviewed people have a high influence on the outcome of conducted methods. Search methods can further be divided into analytical and creativity search methods. The aim of analytical search methods is to identify future and until now unknown company risks. Some of the listed methods like FMEA were established for the application in quality management, but due to suitability adapted for the usage in risk management. Creativity methods like brainstorming are based on creative processes. These methods are characterised by divergent thinking and lead relatively fluent and flexible to innovative ideas and solutions.¹⁵¹ Latest studies point out that the choice of used identification methods strongly depend on the company's size and maturity of their risk management. Especially small companies make use of the brainstorming method, which is easily and cheaply applicable. Large companies with necessary financial background tend to use interviews with experts.¹⁵²

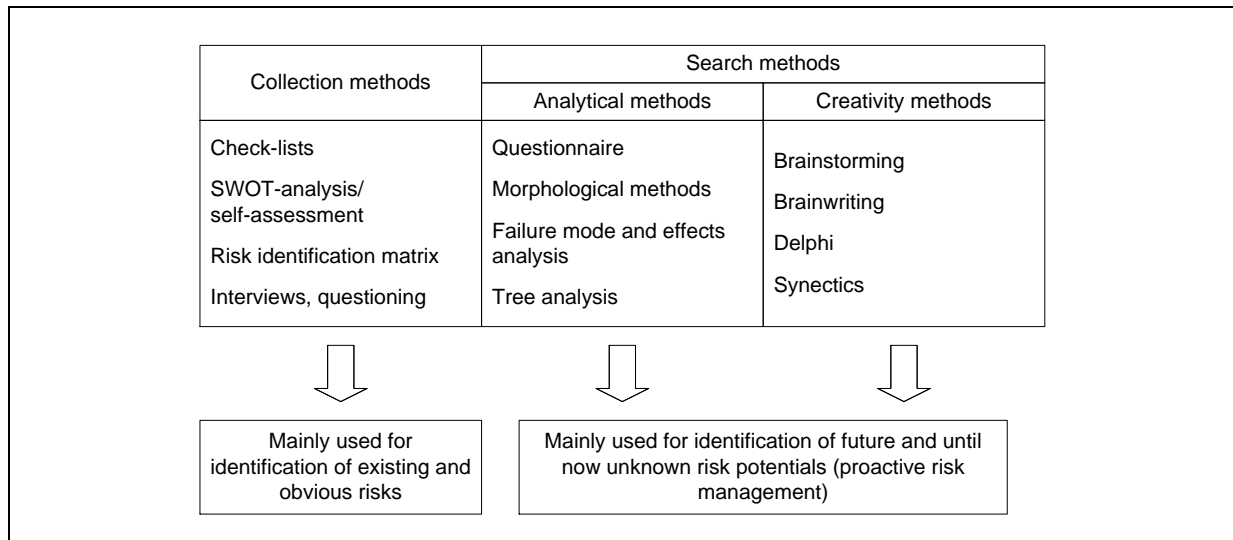
¹⁴⁸ Cf. SCHEEL, O.; FRANK, B. (2014), p. 37.

¹⁴⁹ Adapted from SCHEEL, O.; FRANK, B. (2014), p. 36.

¹⁵⁰ Cf. *ONR 49001:2014*, p. 21.

¹⁵¹ Cf. ROMEIKE, F. [a] (2003), p. 174 ff.

¹⁵² Cf. NORELL, E.; MONTAGNE, E.; THOMIK, M.; BOUTELLIER, R.; ETH ZÜRICH (2014), p. 37 f.

Figure 13: Risk identification methods¹⁵³

At the end of this process step all identified risks are entered in a risk catalogue for documentation. Therefore, risk categories and groups have to be precisely defined. Due to complexity the definition of risk categories and groups can sometimes be a very complicated and time-consuming task. Besides categorizing risks the catalogue includes also a short but meaningful risk explanation. The catalogue mirrors the outcome of this first very important process step in a compressed form. A proper documentation ensures a permanent and from employees' independent functionality of the risk management process.^{154,155} Table 9 displays the hierarchical structure of the chosen risk catalogue, which consists of three levels.

1. Level	2. Level	3. Level	Example
Risk category			Operational risks
	Risk group		Personnel risk
		Risk	Risks of employee qualification

Table 9: Hierarchical structure of the risk catalogue¹⁵⁶

The first level risk category provides an overview and is used as a rough categorisation of identified risks. The second level risk group provides further categorizing to sort identified risks. The first and second levels need to be adjusted according to the company's needs. Each risk category contains several risk groups. This layout ensures easy and flexible adjustments of categories and groups later on. Finally, the third level risk contains the identified risks.¹⁵⁷

¹⁵³ Cf. ROMEIKE, F. (2004), p. 109.

¹⁵⁴ Cf. ROMEIKE, F. [a] (2003), p. 179.

¹⁵⁵ Cf. ROMEIKE, F. (2004), p. 110.

¹⁵⁶ Cf. SEIDEL, U. (2005), p. 33.

¹⁵⁷ Cf. SEIDEL, U. (2005), p. 33.

2.3.2.2 Risk identification at EFG

During the risk identification process at EFG the earlier described combination of the top-down and bottom-up approach was used. This ensures the identification of as many risks as possible within EFG. After an analysis of EFG's structure with top management, risk categories and groups for the risk catalogue were defined. The adjusted risk catalogue (see Figure 14) is based on the elaborated one of Mr Weißensteiner, which was part of his diploma thesis. The final risk catalogue consists of 18 risk groups, which are sorted into four risk categories. By taking the elaborated risk catalogue into account, meetings with employees from different departments and hierarchical levels were conducted.

A combination of collective and search methods, displayed in Figure 13, was used. As part of this master thesis a literature research was conducted. Results of the literature research slipped in interviews and brainstorming meetings. This combination has helped to identify current and until now unknown risks because outsiders often see risks, which are common practice for people involved. To meet the spirit of the top-down and bottom-up approach blue-collar workers, managers, top managers and stakeholders from EFG have attended these meetings.

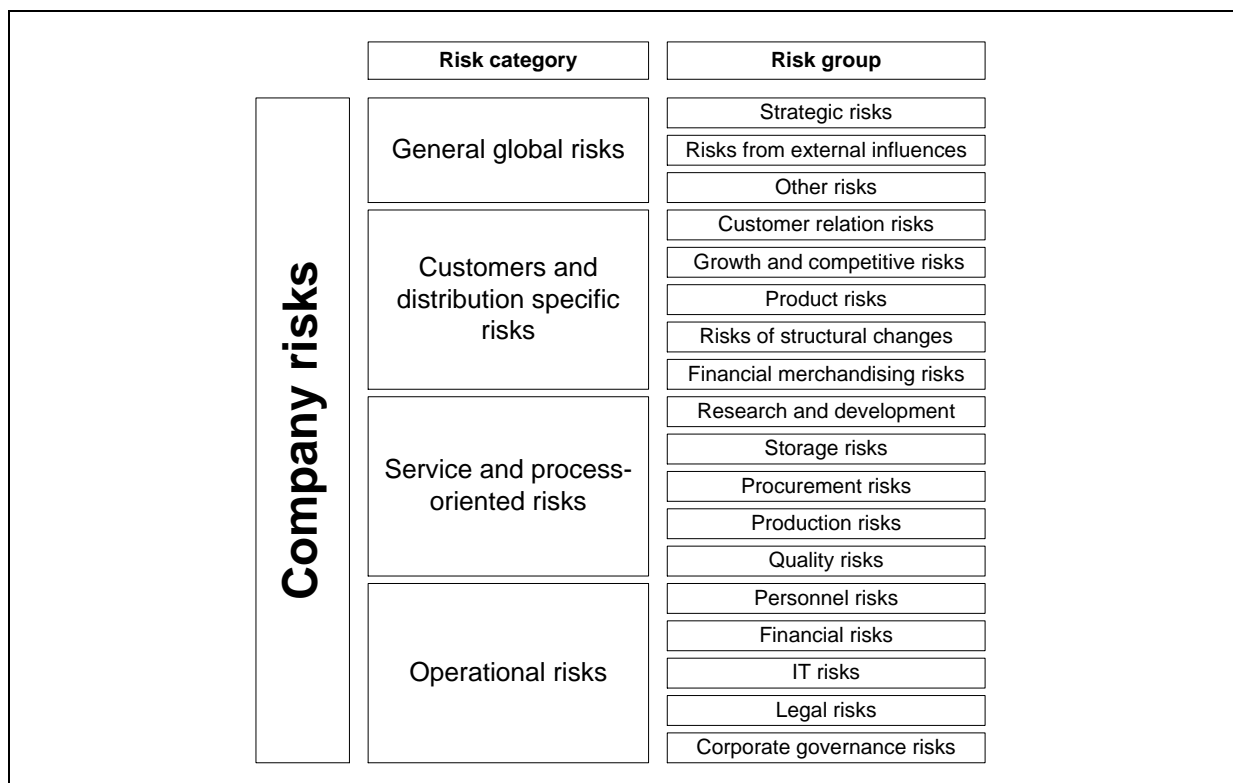


Figure 14: Hierarchical structure of EFG's risk catalogue¹⁵⁸

¹⁵⁸ Adapted from WEIßENSTEINER, C. (2007), p. 21.

In the course of this process step approximately 75 current and potential risks have been identified and documented in the risk catalogue. During the next process step identified risks are briefly described, prioritised and finally, depending on their risk level selected for further evaluation.

2.3.2.3 Risk analysis

The purpose of the third process step is to establish an understanding for identified risks. Furthermore, this step includes a detailed description of risks as well as the estimation of likelihood and consequences. Tables and scales from chapter 2.3.1.3 provide the necessary assistance for a proper estimation of likelihood and consequences. Risk owners and risk managers need to understand sources and causes of risks, positive and negative likelihoods and consequences in order to evaluate them in the next process step. Gathering these information helps to decide if risk treatment is necessary or not.^{159,160}

After gathering this information, it is possible to display all company risks in a risk matrix by calculating an expected value. It is possible to distinguish between a two-part risk matrix with a risk tolerance limit and a risk matrix with three tolerance ranges (see Figure 15). In each case likelihood (consequences) is (are) plotted on the vertical (horizontal) axis. The tolerance limit divides the matrix into tolerable and not tolerable risks. The matrix with three tolerance ranges adds an additional option, which represents partly tolerable risks. In both cases not tolerable risks should not be tolerated and in case of a risk matrix with three tolerance ranges partly tolerable risks have to be minimised.^{161,162}

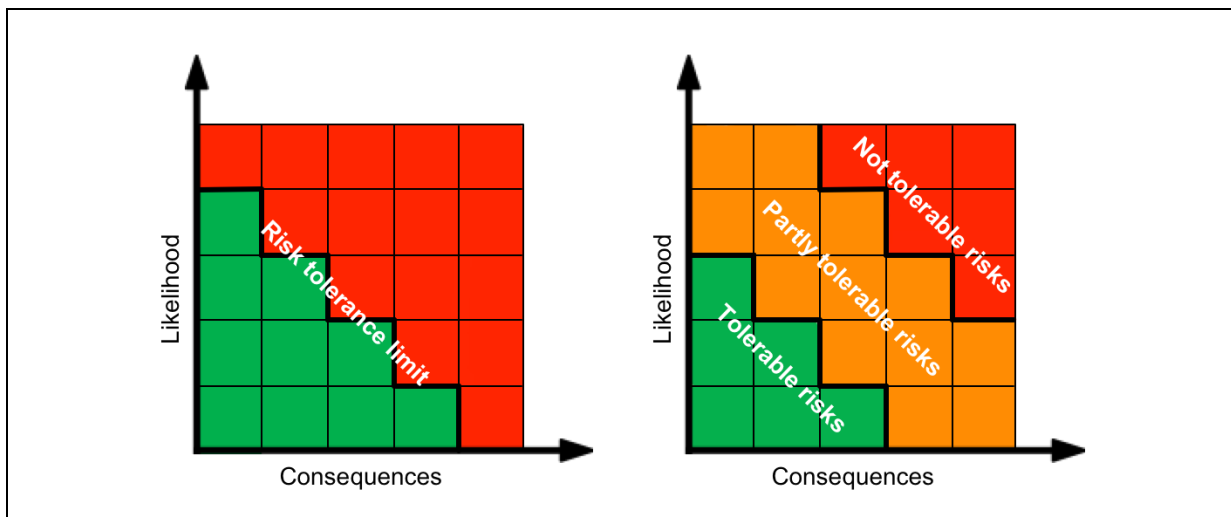


Figure 15: Risk matrix with tolerance limit and tolerance ranges¹⁶³

Entering risks in the risk matrix helps to understand correlations between different risks. The usage of a table enables a systematic approach by determining and revealing dependencies

¹⁵⁹ Cf. BRÜHWILER, B. (2011), p. 124.

¹⁶⁰ Cf. ONR 49001:2014, p. 21.

¹⁶¹ Cf. ONR 49001:2014, p. 22 f.

¹⁶² Cf. BRÜHWILER, B. (2011), p. 119.

¹⁶³ Cf. ONR 49001:2014, p. 22.

between them. Furthermore, it is possible to determine if a risk is a cause or a partial cause of another risk. Also key risks, which are influenced by many other risks, can be determined. For example risk 2 and risk 3 in Table 10 are heavily influenced by each other, whereas the influence between risk 1 and risk 2 is very weak. In this table a zero means that risks are not correlated. In reality understanding and determination of correlations can be very difficult because often an obvious cause-effect chain is difficult to identify. The key point is to realise how risks influence each other.^{164,165}

	Risk 1	Risk 2	Risk 3	Risk 4
Risk 1		--	0	--
Risk 2	--		+++	++
Risk 3	0	+++		0
Risk 4	--	++	0	

Table 10: Mutual risk dependencies¹⁶⁶

Figure 16 summarises the approaches of risk identification and risk analysis. The usage of suitable identification methods in combination with employees from different hierarchical level and departments ensures a successful identification of many risks. Afterwards identified risks are captured and briefly described. The established risk catalogue sorts risks into risk categories and groups. This helps involved people to understand those risks. During documentation further details are gathered like likelihood and consequences. These details enable the creation of a risk matrix, which reflects the company's risk landscape. Prioritizing all identified risks helps to concentrate on the most important ones. All identified risks are taken into consideration but only not tolerable and partly tolerable risks are treated further on in order to increase the efficiency of the risk management process. Tolerable risks are monitored and reviewed on a continuous basis in order to detect changes in their likelihood and consequences.¹⁶⁷

¹⁶⁴ Cf. BRÜHWILER, B. (2011), p. 130.

¹⁶⁵ Cf. ONR 49001:2014, p. 22 f.

¹⁶⁶ Cf. ONR 49001:2014, p. 23.

¹⁶⁷ Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 102.

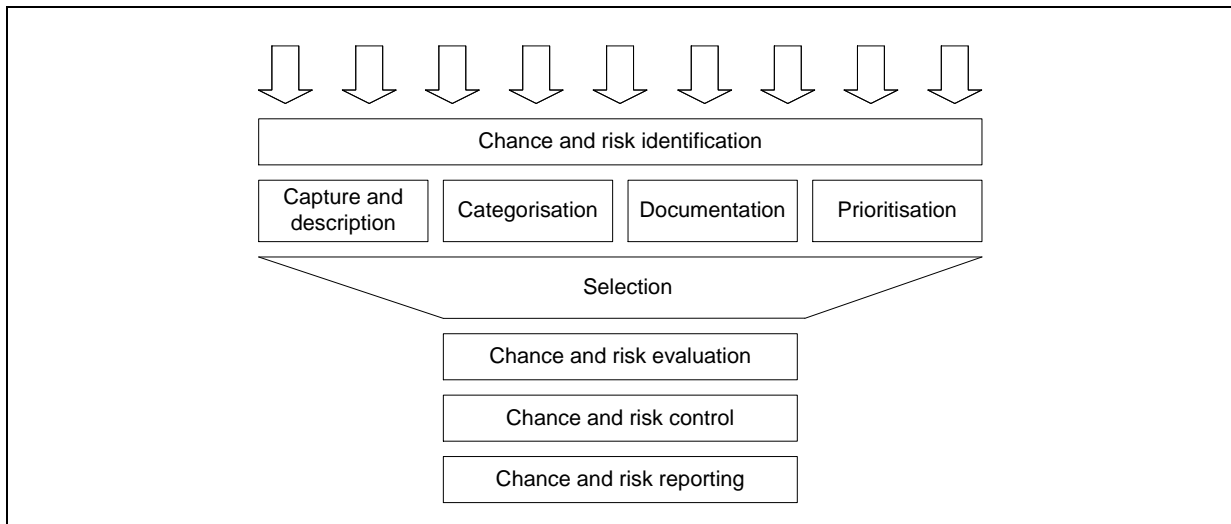


Figure 16: Documentation approach of risk identification results¹⁶⁸

2.3.2.4 Risk analysis at EFG

The success of the entire risk management process is based on the quality and completeness of the earlier created risk catalogue. Unidentified risks are not taken into consideration in further process steps. In several meetings with EFG's management the risk catalogue was reviewed twice. During these meetings some documented risks were combined and others classified as optimizations. A few of them were combined because they were targeting finally the same cause. Other risks could be written off as optimizations due to the fact that these selected risks do not represent a threat to EFG. After this second review 48 risks remained for capturing, documenting and prioritising them in the developed risk management tool. The development of this RMT is the second defined main goal.

On a second pass the 48 remaining risks were entered in the RMT together with employees who identified the individual risks. Most of the time qualitative adjectives were used for the estimation of likelihood and consequences because a quantitative estimation of consequences is very difficult without necessary data. Especially, doing a risk analysis for the first time.

The RMT provides a clearly and straightforward designed input screen (see Figure 39). Among other things the date of record, risk category and group, risk description, likelihood and consequences have to be determined. Figure 44 and Figure 45 show a risk assessment template, which helps to estimate the likelihood and consequences of risks by summarizing earlier defined risk criteria and risk scale. At the beginning of the risk analysis the risk manager has to enter the current EBIT on the second page of this template in order to update the quantitative values of the risk scales. Furthermore, she/he is able to adjust the weighting of qualitative adjectives to the company's needs. During this process step, perspectives of likelihood and consequences from different employees concerning one risk were taken into account. The divergence of different perspectives regarding likelihood and

¹⁶⁸ Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 102.

consequences was surprisingly low. This indicates a consistent risk awareness of all participating employees.

No.	Main risk	Likelihood [%]	Consequences [%]
1	Lack of knowledge exchange	70	70
2	Uncontrollable cost allocation	85	50
3	Outsourcing of production parts	85	50
4	Product liability risk	60	70
5	Drop in sales/decline in sales	70	50
6	Insufficient production planning	70	50
7	Contemporary management style	50	70
8	Contractual penalties/warranties	35	90
9	Insufficient qualified CAD/CAM staff	35	90

Table 11: Identified main risks at EFG

At the end of this process step a prioritised list of all 48 risks has been evolved. The ranking is based on the expected value of each risk. Some of the identified main risks are listed in Table 11 with the corresponding risk matrix displayed in Figure 17. In case of EFG a risk matrix with three tolerance ranges was chosen. The initial gradient of the risk matrix is divided into three equally sized parts. It is possible to adjust the gradient in the settings screen of the RMT (see Figure 36). This enables EFG to modify the gradient according to their needs afterwards. By lowering for example the upper threshold, the not tolerable risk range moves down and further risks become categorised as not tolerable and vice versa.

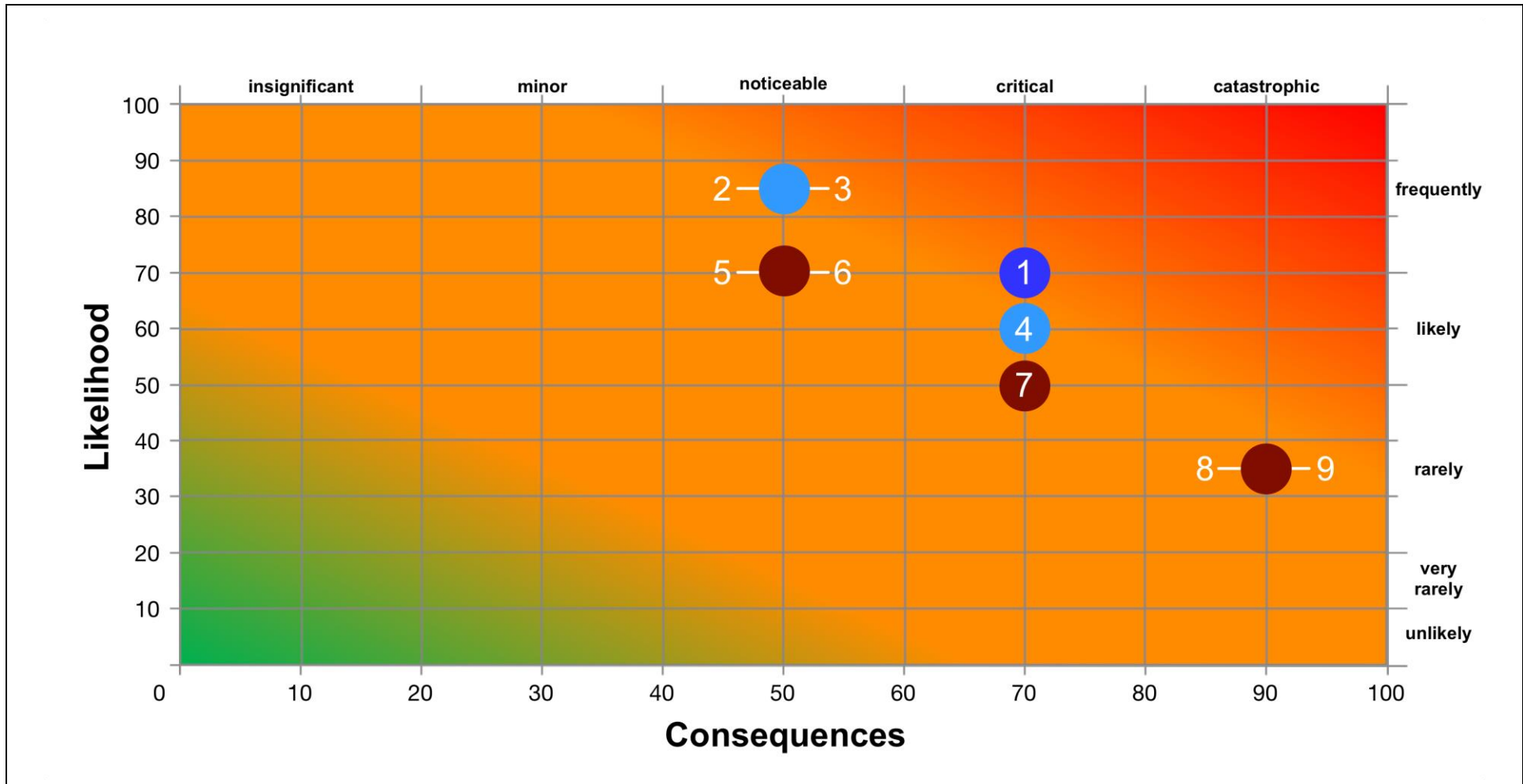


Figure 17: EFG's risk matrix with main risks

To sum up, three main risks have been identified during the risk assessment process at EFG. It is advised to focus on the management of these risks. In the following these three main risks are described and a possible approach in order to reduce the risk level is developed.

Lack of knowledge exchange

The updated ISO 9001:2015 version demands from its members besides risk management in addition the implementation of knowledge management. The defined knowledge cycle is based on the earlier described PDCA cycle and consists of the following elements in sequential order:^{169,170}

- Determining necessary knowledge
- Considering existing knowledge
- Acquiring necessary knowledge (intern/extern)
- Sharing and making knowledge available
- Maintaining knowledge

The requirement of knowledge management is based on the experience that the knowledge of the whole company matters not only the knowledge of single employees. Knowledge is not just a collection of information. The usefulness strongly depends on the linkage of information regarding the context.¹⁷¹

In order to meet the requirements from ISO 9001:2015 different methods and tools can be used. For example, *Offensive Mittelstand* provides check-lists especially for SMEs. Check-lists are provided for various topics and enable SMEs to evaluate themselves in order to establish an action plan.¹⁷²

A cheap but also very effective method is the determination and implementation of a properly adjusted folder structure on servers. This measure helps employees by searching and finding documents quickly. Due to different ways of working and mind-sets employees find it very difficult to orientate themselves to foreign folder structures and file names. Therefore, folder structures and file names have to be unified throughout departments. A good folder structure enables users to quickly find documents with only a few clicks. The name of folders and documents should start with the highest information content and abbreviations should be self-explaining. Upper levels of the structure hierarchy should be consistent throughout the whole company. Lower levels can be adjusted to the needs of each department but have to follow certain rules. This enables employees to easily find documents even if they are not used to that. Suitable naming conventions of documents allow users to easily find the right document within complex folder structures. The folder structure strongly depends on the area a company is operating in. It can be project, process, product, department or customer based. An approach for determining a folder structure can be as follows. At the beginning the

¹⁶⁹ Cf. NORTH, K.; BRANDNER, A.; STEININGER, T. (2015), p. 21.

¹⁷⁰ Cf. ORTH, R.; KARCHER, P. (2015), p. 27.

¹⁷¹ Cf. NORTH, K.; BRANDNER, A.; STEININGER, T. (2015), p. 21.

¹⁷² Cf. *OFFENSIVE MITTELSTAND* (-).

folder structure depending on the company's needs, for example project based, has to be defined. Afterwards, upper levels and naming conventions have to be established. A refinement of lower levels can be done if necessary. During a test, mode defined folder structures are implemented and evaluated based on user reviews and user friendliness. At the end maintenance plans and responsibilities have to be created. Folders of the structure should not either be empty or contain too many files. An ideal number of documents within a folder is approximately seven. A properly designed folder structure enables companies to store, share and use their gained knowledge.¹⁷³

Another tool suggested by literature are so called wiki-systems. They are similar to Wikipedia but especially adjusted to the needs of companies. They are structured like a website where all employees have read and write permissions. This enables a knowledge exchange and collaboration possibilities for employees. These systems are relatively cheap and easy to implement. The selection of the right wiki-system "Wikimatrix" (<http://www.wikimatrix.org>) allows companies to compare various wiki-systems by showing their different features. The success strongly depends on the contribution of employees as well as the defined content structure. Using additional modules can extend the basic functionality of wiki-systems. This enables the wiki-system to grow in an organic way. A wiki consists of several pages, which are linked to each other and support full-text search. Employees can add and edit single pages. In order to prevent mistakes most wiki-systems provide versioning and logging functions, which store the complete page history. When adding or editing pages documents, graphics and links can be inserted. Wiki-systems can be used for various tasks like:^{174,175}

- Knowledge management
- Quality management
- Standard management
- Project management
- Provisioning of check-lists, instruction sheets and manuals

Outsourcing of production parts

In the course of producing products most companies are forced to outsource parts of the final product to other companies. This may be due to the fact that capacities are limited, lack of necessary know-how or financial reasons. Even EFG is forced to outsource the production of single parts for their hydropower plants. Below some advices are given in order to avoid the transfer of detailed information to outsider.

During the process of outsourcing, important knowledge is transferred to the supplier. In order to minimise transferred knowledge companies should add most of the value of a product within their own company. This helps keeping transferred knowledge at a minimum level. In case information is transferred, rules for this process have to be established. Information can be passed on either paper-based or in an electronically way. A person

¹⁷³ Cf. VOIGT, S. (2009), p. 69 ff.

¹⁷⁴ Cf. ORTH, R. (2009), p. 75 ff.

¹⁷⁵ Cf. ULRICH, A. (2015), p. 32 f.

responsible for the approval of transferred information should be defined. Her/his task is to verify if internal and external people are allowed to receive information.¹⁷⁶

Long-term-employees with valuable knowledge gathered in the course of time are the most important knowledge database. In order to avoid those employees from changing to competitors interesting tasks and training opportunities have to be provided by the company, individually adjusted to the employees' needs. Another common possibility of committing important employees to the company are providing an attractive salary, employee benefits or binding their families also to the company or location. Companies have to provide instructions concerning knowledge exposure, knowledge drain and knowledge protection. This promotes the awareness of a proper information handling.¹⁷⁷

Knowledge transfer can be restricted or blocked by following different rules. For example taking pictures in sensitive areas can be prohibited in order to prevent industrial espionage. The IT department is able to block external volumes and lock computer ports for external volumes. Notebooks and USB sticks have to be encrypted in case they get lost.¹⁷⁸

The selection of proper suppliers for companies plays an important role. Suppliers with a low understanding of systems should be picked. Choosing suppliers with deep knowledge in specific technology sectors can reduce knowledge drain. Due to that fact the supplier is not able to become a competitor. Only essential information for the production process should be provided to suppliers. Also a diversification reduces the creation of a system understanding within suppliers.¹⁷⁹

Another possibility for reducing the knowledge transfer is the development of products with low tolerances or the usage of materials which are difficult to analyse. Employees can be forced to sign confidentiality statements due to the fact that illegal activities are greater barriers than moral scruples. Some confidentiality statements can be applied to customers and suppliers in order to prevent knowledge from getting transferred. Economic dependence of suppliers and negative consequences in case of unwanted knowledge transfer caused by the supplier is a further possibility to prevent knowledge transfer. The offering of product based services, maintenance agreements and replacements forces customer loyalty, and competitors are not assigned with the maintenance of products. Successful and long-term based business connections minimise the opportunity chances of knowledge transfer due to the fact that suppliers feel obliged to act morally. Following the rules outlined minimises the opportunity of unwanted knowledge transfer caused by third parties.¹⁸⁰

¹⁷⁶ Cf. LINDEMANN, U.; MEIWALD, T.; PETERMANN, M.; SCHENKL, S. (2012), p. 87.

¹⁷⁷ Cf. LINDEMANN, U.; MEIWALD, T.; PETERMANN, M.; SCHENKL, S. (2012), p. 89 f.

¹⁷⁸ Cf. LINDEMANN, U.; MEIWALD, T.; PETERMANN, M.; SCHENKL, S. (2012), p. 92 f.

¹⁷⁹ Cf. LINDEMANN, U.; MEIWALD, T.; PETERMANN, M.; SCHENKL, S. (2012), p. 94 f.

¹⁸⁰ Cf. LINDEMANN, U.; MEIWALD, T.; PETERMANN, M.; SCHENKL, S. (2012), p. 97 ff.

Insufficient production planning

Production planning involves all measures, which are necessary for the manufacturing of products. It includes the preparation of documents and operating means arising during planning, control and monitoring of the production process. The purpose of production planning is the optimisation of production in order to reach an optimum economical work result. An insufficient production planning can cause among others following risks: delivery delay, incorrect capacity planning and unnecessary ways during production. Tasks of production planning are:^{181,182,183}

- Transforming customer orders in manufacturing orders
- Preparation of documents (bill of material, task schedule, allocation of drawings)
- Capturing of personnel and material capacities
- Material specification and work instructions
- Monitoring of production activities

Production planning can be divided into work scheduling and work control. The first one contains all onetime measures like design of products, manufacturing preparation, planning as well as allocation of equipment and approval for production. The second one, work control consists of measures, which are necessary to conduct the work. It supervises procedures especially within manufacturing.^{184,185}

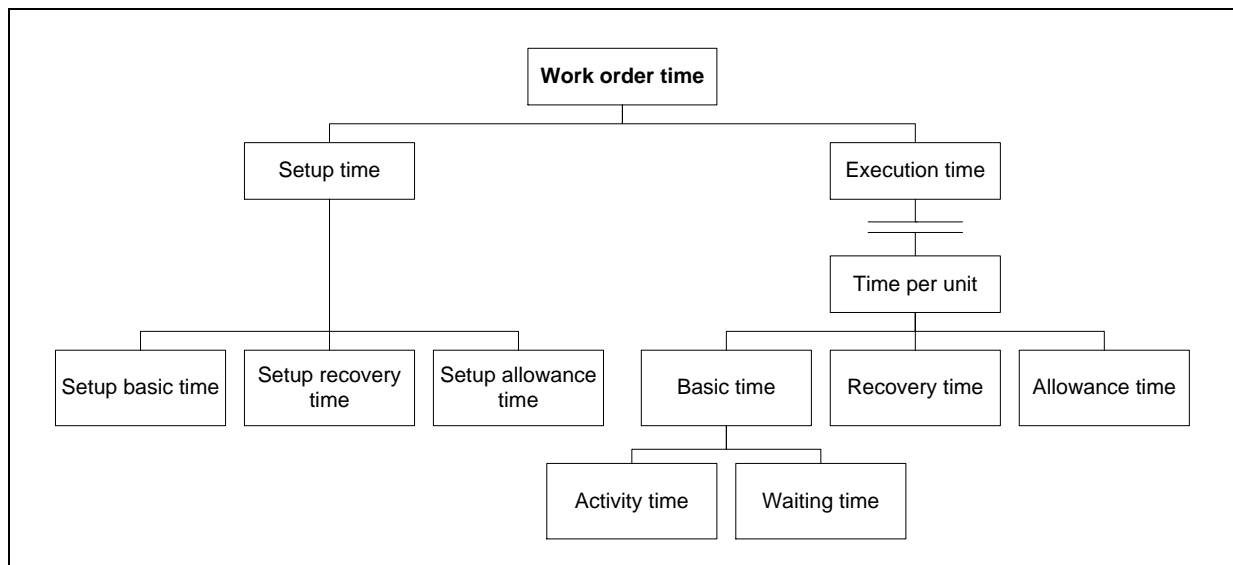


Figure 18: Time structure for work order time¹⁸⁶

An essential component of production planning is time tracking of working steps in order to calculate the capacity utilisation. For an accurate time tracking the working steps should be

¹⁸¹ Cf. WESTKÄMPER, E. (2014), p. S133.

¹⁸² Cf. WANNENWETSCH, H. (2007), p. 440.

¹⁸³ Cf. ARNDT, K. (2015), p. S41.

¹⁸⁴ Cf. WESTKÄMPER, E. (2014), p. S133.

¹⁸⁵ Cf. WESTKÄMPER, E. (2014), p. S135 f.

¹⁸⁶ Adapted from WESTKÄMPER, E. (2014), p. S135.

structured into process sections and illustrated in a written work order. The time for the execution of each defined working step can be determined either through timetables provided by *REFA* or timing devices. Figure 18 illustrates the structure for the calculation of the work order time according to *REFA*. The work order time results from the addition of the setup time and the execution time. These times can be further divided into basic time, recovery time and allowance time as pictured above. In course of the preparation of the working order, the work order time should be determined for each defined working step. Setup time and execution time of each working step should be determined only for the first time. Afterwards determined execution times have already been available for further usage. In course of the introduction of automated time and attendance systems for recording the working time, determined execution times of the different working steps can be verified for their correctness. At the beginning of a task employees get their work orders from a terminal. A work order contains among others the following information like part name, material, type of order, time per unit, setup time and operational means. After a working step is completed an employee verifies the successful accomplishment at a terminal and gets the next work order. After an introduction phase companies should have gained a large amount of accurate data for planning their capacities. Furthermore, upper hierarchical levels like top management and project managers are able to see the progress of projects as well as the current status of each single part.¹⁸⁷

2.3.2.5 Risk evaluation

This process step is based on the outcome of the risk analysis and supports the process of decision-making whether a risk has to be treated or not. In practice this term is often misunderstood and used for determination of likelihood and consequences. The risk level of the risk analysis is compared with established risk criteria. Based on that comparison risk manager and risk owners decide whether a risk needs to be treated or not. The outcome of this process step can either be that a further risk analysis is necessary or that set countermeasures are sufficient. It is possible to distinguish between a dogmatic and a pragmatic problem solving approach. The dogmatic one implies that each risk, which exceeds the risk tolerance limit, has to be treated. If a risk exceeds the risk tolerance limit and countermeasures are not sufficient, a justification will be necessary. Therefore, positive aspects of a risk have to prevail against negative ones. Decision makers should reveal and document their assumptions and information sources for traceability reasons.^{188,189}

Figure 19 distinguishes between top-down and bottom-up approach, which are finally divided into qualitative and quantitative risk evaluation methods. Quantitative evaluation approaches are based on mathematical-statistical methods and can be used if a large amount of data is available. On the other hand, qualitative evaluation approaches are primarily based on subjective and experimental ratings. These methods are suitable for SMEs, where large amounts of data, required resources and detailed knowledge are not available. The top-down approach focuses on the consequences of risks, which the company is aware of. This

¹⁸⁷ Cf. WESTKÄMPER, E. (2014), p. S134 f.

¹⁸⁸ Cf. *ONR* 49001:2014, p. 23 f.

¹⁸⁹ Cf. BRÜHWILER, B. (2011), p. 133.

approach investigates the fluctuation of earnings, costs and operating income based on internal and external historical data. All qualitative and quantitative top-down methods are conceptually very easy, quick and affordable to implement but do not provide many new perceptions. In contrast to bottom-up methods, which start with causes of risks and try to identify and evaluate the potential consequences caused by those risks. For a successful application of bottom-up methods, relevant processes have to be analysed in detail and continually verified. All qualitative and quantitative bottom-up methods are compared to top-down methods quite expensive but provide a higher motivation for innovations and behaviour changes. This helps to build a strong foundation of a company-wide risk culture.^{190,191}

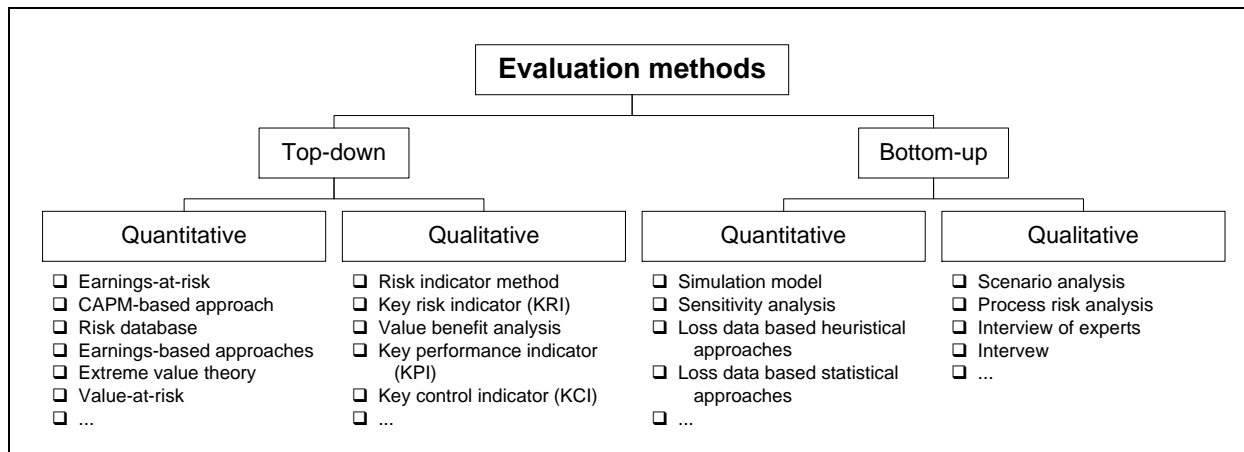


Figure 19: Risk evaluation methods¹⁹²

SMEs like EFG often do not have the required personnel resources, budget and knowledge for the application of the more cost extensive quantitative risk evaluation methods. Risk management should be tailored to company's needs and size. The key of success is the right choice of the level of detail regarding their implemented risk management. SMEs should use appropriate evaluation methods like qualitative ones, which can be performed with less effort and deliver useful results. The level of detail can be distinguished into three levels of detail like qualitative, qualitative/quantitative and quantitative risk management, which differentiate in their applicability, result, assessment, effort and periodicity (see Table 12).¹⁹³

¹⁹⁰ Cf. ROMEIKE, F. [b] (2003), p. 183 ff.

¹⁹¹ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN. H. (2006), p. 26.

¹⁹² Cf. ROMEIKE, F. [b] (2003), p. 185.

¹⁹³ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN. H. (2006), p. 26.

	Applicability	Result	Assessment	Effort	Periodicity
Level 1 Qualitative RMGT Level area/process	SMEs, which try to reduce their most important company risks with minimal effort.	<ul style="list-style-type: none"> ▪ Risk inventory on company level ▪ Significant risk areas in firm ▪ Assessed measures per risk area 	<u>Qualitative:</u> <ul style="list-style-type: none"> ▪ Incidence ▪ Consequence 	<ul style="list-style-type: none"> ▪ 2 workshops each 3 hours ▪ Participants: Management and administrative board 	Annual or semi-annual
Level 2 Qual./quant. RMGT Level area/process	SMEs, which try to get a comprehensive picture of their company risks and response with adequate measures.	<ul style="list-style-type: none"> ▪ Risk inventory on area/process level ▪ Significant risks per area/process ▪ Assessed measures per risk 	<u>Qualitative:</u> <ul style="list-style-type: none"> ▪ Incidence <u>Quantitative:</u> <ul style="list-style-type: none"> ▪ Consequence (% of EBIT) 	<ul style="list-style-type: none"> ▪ 3-5 workshops each 3 hours ▪ Participants: Management and department managers 	Semi-annual or quarterly
Level 3 Quantitative RMGT Level company	Large concerns, with necessary resources to deal intensively with occurring risks.	<ul style="list-style-type: none"> ▪ Detailed risk inventory ▪ Significant risks with detailed scenario ▪ Assessed measures 	<u>Quantitative:</u> <ul style="list-style-type: none"> ▪ Incidence/likelihood ▪ Consequence (% of EBIT) 	<ul style="list-style-type: none"> ▪ One or more risk manager ▪ Data modelling ▪ Simulation ▪ Value-at-Risk model 	Online Monitoring

Table 12: Level of detail of risk management¹⁹⁴

Qualitative risk management – level 1 – is the simplest form of risk management. Its objective is to quickly gain an overview over different risk areas within a company. At first a three-hour workshop with the top management and the administrative board is enough to get a good insight of the current situation. This workshop aims at the identification and determination of causes and consequences of risks. Risks are evaluated by the usage of a predefined risk scale as shown in Figure 11 and their corresponding risk criteria. Adjectives have to be suitable for the particular purpose. The qualitative explanation (Table 6 and Table 7) ensures a consistent understanding of risks. The aim of the evaluation is to prioritise and graphically display identified risks. In the second workshop attendees try to find suitable measures to reduce identified risks. The outcome is an implementation plan, which contains the defined person in charge and dates set for the control of measures. On an annually or semi-annually basis companies should invest these six hours to identify arising risks in an early state and verify set countermeasures.¹⁹⁵

A combination of qualitative and quantitative risk management – level 2 – is appropriate if also the process level will be taken into account. In a first step top management, administrative board and involved employees are questioned in detail. Employees from investigated departments contribute with their detailed knowledge about occurring risks.

¹⁹⁴ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN, H. (2006), p. 27.

¹⁹⁵ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN, H. (2006), p. 27.

Since financial and personnel resources in SMEs are limited, only most important risk areas should be taken into consideration. Risk management on level 2 focuses on single risks within defined departments. In a second step after identifying risks on a department basis the above described qualitative risk management procedures of level 1 are applied. An implementation plan for each department is created with countermeasures, people in charge are identified and dates are set. This enables the top management to set appropriate actions.¹⁹⁶

Quantitative risk management – level 3 – tries to get a comprehensive overview of the current company's risk situation. This approach is mostly suitable for large companies. The analysis and description of different scenarios helps to gather information to conduct further stochastic distribution functions and simulations. The level of detail and effort increases compared to level 1 and level 2. This is the reason why only life-threatening risks, which passed level 1 and level 2, should be managed with quantitative methods.¹⁹⁷

2.3.2.6 Risk evaluation at EFG

Due to EFG's company size and lack of financial and personnel resources as well as the limited amount of available data, the implemented risk management approach is based on the earlier described level 1 and level 2 approach. A combination is described of the top-down and bottom-up approach in chapter 2.3. On the one hand this ensures the identification of most important risk areas and on the other hand employees, knowledge, experience and perceptions are included. Below, some strongly applicable risk evaluations methods from Table 13 are described in order to provide EFG tools with a high cost-benefit-ratio.¹⁹⁸

Failure mode and effects analysis (FMEA)

FMEA is used to analyse complex technical systems, components or processes in order to increase quality and functional reliability. It is possible to distinguish between design, process and system FMEA (see Figure 20). Therefore, during a system analysis the entire system is split into subsystems, subassemblies or processes depending on the needed detail of information. Functions are described in detail and possible failures as well as causes are identified. After the identification of possible malfunctions, the risk priority number ($RPN = P \times SEV \times D$) is determined. It is the product of likelihood of failure (probability), consequences of failure (severity) and ability to detect a problem (detection). According to the defined evaluation criteria (usually between 1 and 10) the RPN is calculated. The value of the RPN can be between 1 (no risk) and 1000 (maximum risk). By exceeding a defined value, countermeasures should be defined in order to reduce the RPN to the lowest possible level. The FMEA method is suitable for product development. New or changed construction plans are approved for production if all identified risk from the design FMEA are successfully reduced. Applying a bottom-up approach on a detailed level can increase safety and quality

¹⁹⁶ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN, H. (2006), p. 27 f.

¹⁹⁷ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN, H. (2006), p. 28.

¹⁹⁸ Cf. BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN, H. (2006), p. 28 f.

of technical systems. The top-down approach is not applicable for a company wide risk analysis and evaluation.^{199,200}

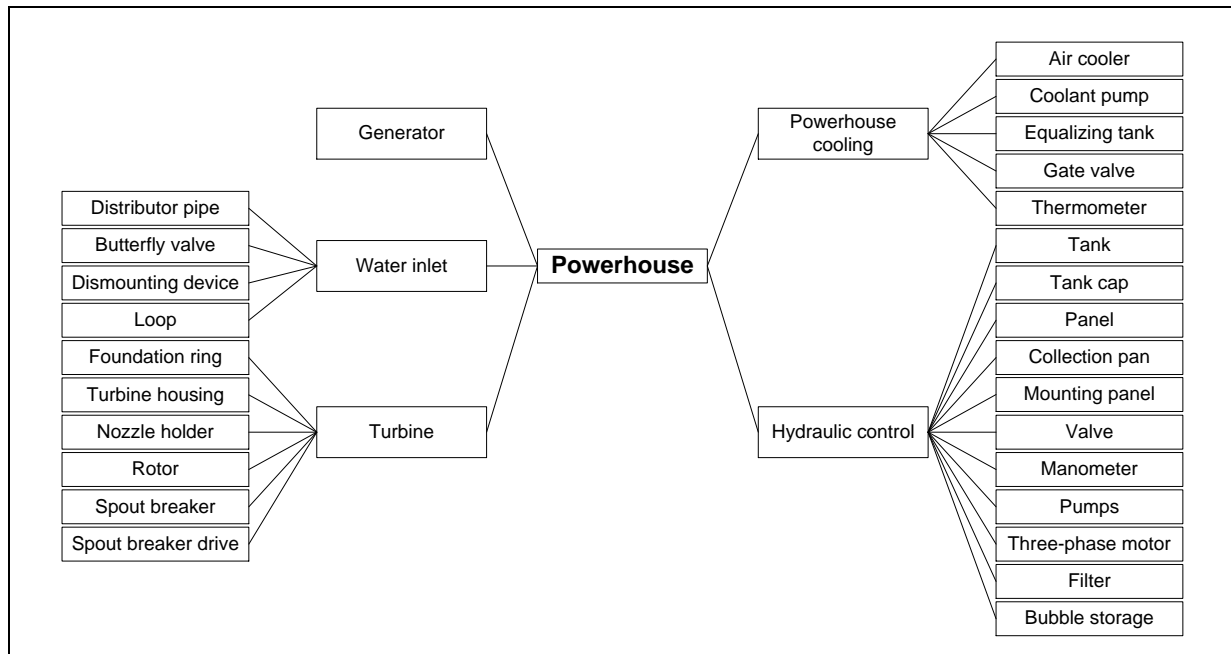


Figure 20: Design FMEA for a Pelton turbine²⁰¹

Scenario analysis – Cause-and-effect analysis – Ishikawa diagram

This risk evaluation method is used to identify causes of single occurring damaging events. Due to the simplicity of this method it is widespread and quite popular. The goal is to avoid similar events from happening and it can be used for minor and major damaging events. Causes and influencing factors of damaging events on technical or organisational systems are determined. Identified causes are divided into main cause and sub-causes. Figure 21 shows the main causes for the manufacturing industry: machines, methods, materials, measurements, mother nature (environment) and manpower (people, operators). At the beginning of this analysis the course of events is required to be determined. As damaging events are mostly negative accusations, they should be avoided in order to get objective results. A cause analysis has to identify all possible sources of accidents as well as prioritise them. The Ishikawa diagram is appropriate for illustrating the context between all relevant and identified causes. If the effect of a damaging event could have been worse, it is important to analyse the effect more detailed.^{202,203}

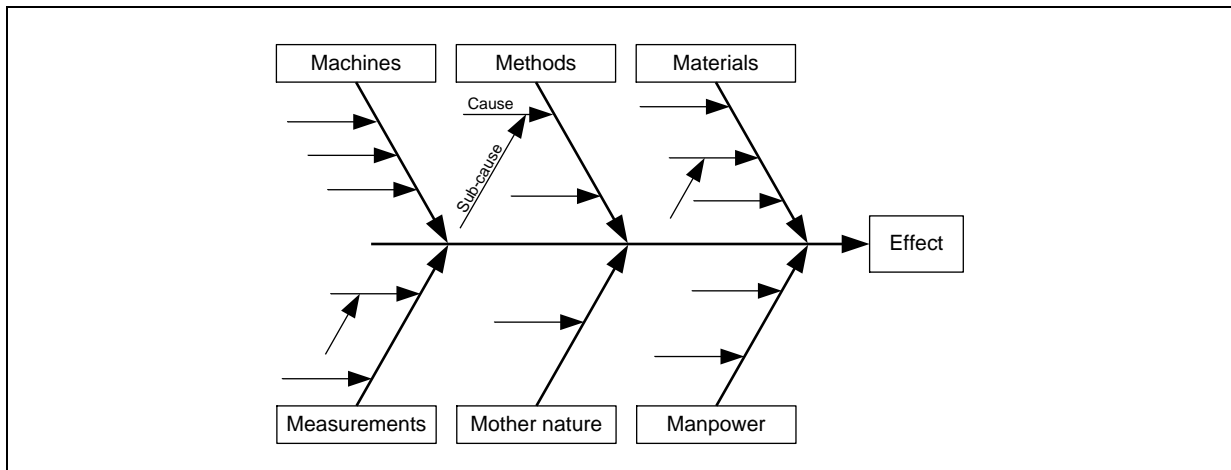
¹⁹⁹ Cf. ONR 49002-2:2014, p. 16 f.

²⁰⁰ Cf. BRÜHWILER, B. (2011), p. 182 ff.

²⁰¹ Adapted from ONR 49002-2:2014, p. 17.

²⁰² Cf. ONR 49002-2:2014, p. 8.

²⁰³ Cf. BRÜHWILER, B. (2011), p. 162 ff.

Figure 21: Ishikawa diagram²⁰⁴

Fault and event tree analysis

The starting point of this analysis is a damaging event, called top event. The fault tree analysis shows possible previous causes of top events, whereas the event tree analysis points out scenarios of effects caused by top events. Causes and effects of technical systems are determined by using a combination of both analyses (see Figure 22). An evaluation of one or more depending or partially depending top events is possible. This analysis follows the sequential steps of the risk management process. Very important for this analysis is a proper identification of the top event. The top event is a prior state, which can cause a catastrophe under unfavourable circumstances. For example, the top event of an airplane crash is the moment when the pilot loses control of the airplane. The top event can arise to a catastrophe but with the right countermeasures it can be avoided. Determination of causes and scenarios of effects increases the understanding of risks. The fault tree analysis uses AND, OR and NOT gates to structure identified causes, whereas the event tree analysis only uses OR gates. The output of AND gates occur if all input events are true. By OR gates only one input needs to be true in order to enable the output.^{205,206}

²⁰⁴ Adapted from ONR 49002-2:2014, p. 8.

²⁰⁵ Cf. ONR 49002-2:2014, p. 10 f.

²⁰⁶ Cf. BRÜHWILER, B. (2011), p. 167 ff.

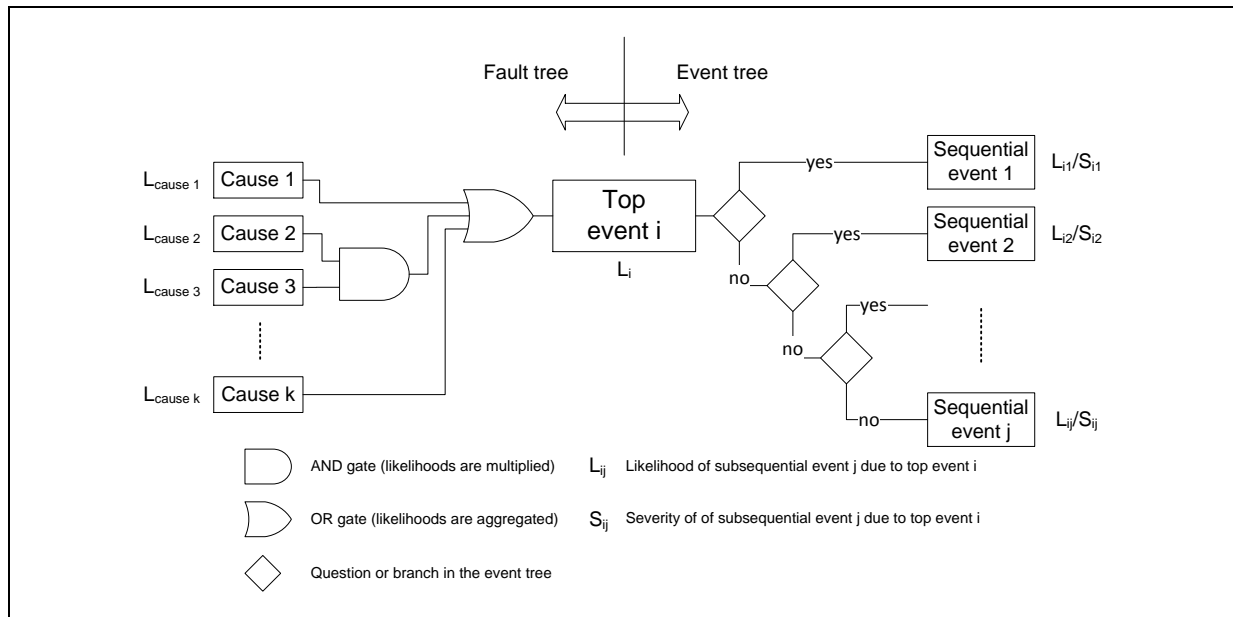


Figure 22: Fault and event tree analysis²⁰⁷

2.3.3 Risk treatment

The purpose of this process step is the selection and implementation of one or more risk treatment options in order to reduce the risk level. Risk treatment is a cyclical process and consists of the following stages:²⁰⁸

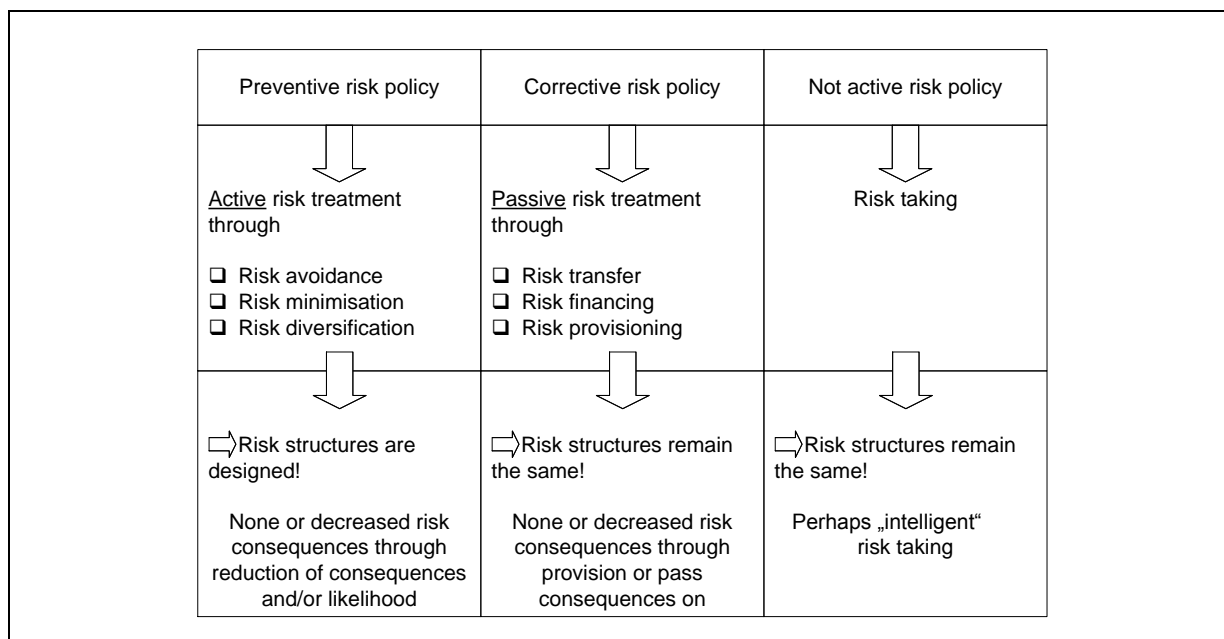
- Risk treatment assessment
- Determination of tolerable risk level
- In case of a not tolerable risk, development of net measures
- Assessment of risk treatment efficiency

Risk treatment will meet its objectives if implemented optimisations increase a company's value. This can be achieved by using preventive, corrective or not active risk policies (see Figure 23). A preventive risk policy tries to reduce causes of risks either through avoiding, minimisation or diversification, whereas a corrective risk policy accepts risks and takes risk provisioning measures in order to avoid or reduce consequences.²⁰⁹

²⁰⁷ Adapted from BRÜHWILER, B. (2011), p. 168.

²⁰⁸ Cf. ONR 49001:2014, p. 24.

²⁰⁹ Cf. ROMEIKE, F. [c] (2003), p. 235 ff.

Figure 23: Overview of risk treatment strategies²¹⁰

Risk avoidance is the easiest and most obvious strategy for reducing risk levels. However, a risk stands for the negative and positive deviation of the expected value. Therefore, risk avoidance also jeopardises a potential chance. In other words it is necessary to consider simultaneously possibilities and threats of a risk. The aim of risk avoidance is either to completely eliminate the likelihood or the consequences of a risk. For the first avoidance strategy the possibilities to influence risk causes plays a very important role by either deciding to eliminate the likelihood or the consequence of a risk. An advantage is that it delivers a clear solution to problems because risks do not arise anymore. A successful elimination of the likelihood or consequence of risk 1 and risk 2 is displayed in Figure 24. This strategy is suitable for companies with a minor risk bearing ability. An example for EFG would be the rejection of a project, which is identified as profitable but dangerous.^{211,212,213}

Risk minimisation describes passing risks onto third parties or preventing risks from happening by implementing technical and organisational measures. The purpose is to reduce the likelihood and/or the consequences of a risk to an acceptable risk level. It is possible to distinguish between cause-oriented minimisation of likelihood and effect-oriented minimisation of consequences. Causes-oriented minimisation is for example maintenance of EFG's IT infrastructure in order to enhance the reliability of their CNC machines. An example of an effect-oriented minimisation is the decrease of fixed costs through outsourcing. This measure reduces consequences of drops in sales. Risk 3 in Figure 24 illustrates a combination of both minimisation approaches.^{214,215,216}

²¹⁰ Cf. ROMEIKE, F. [c] (2003), p. 236.

²¹¹ Cf. ROMEIKE, F. [c] (2003), p. 235 f.

²¹² Cf. GLEISSNER, W. (2008), p. 158.

²¹³ Cf. DIEDERICHS, M. (2010), p. 189 f.

²¹⁴ Cf. ROMEIKE, F. [c] (2003), p. 237.

²¹⁵ Cf. GLEISSNER, W. (2008), p. 159 f.

²¹⁶ Cf. DIEDERICHS, M. (2010), p. 190.

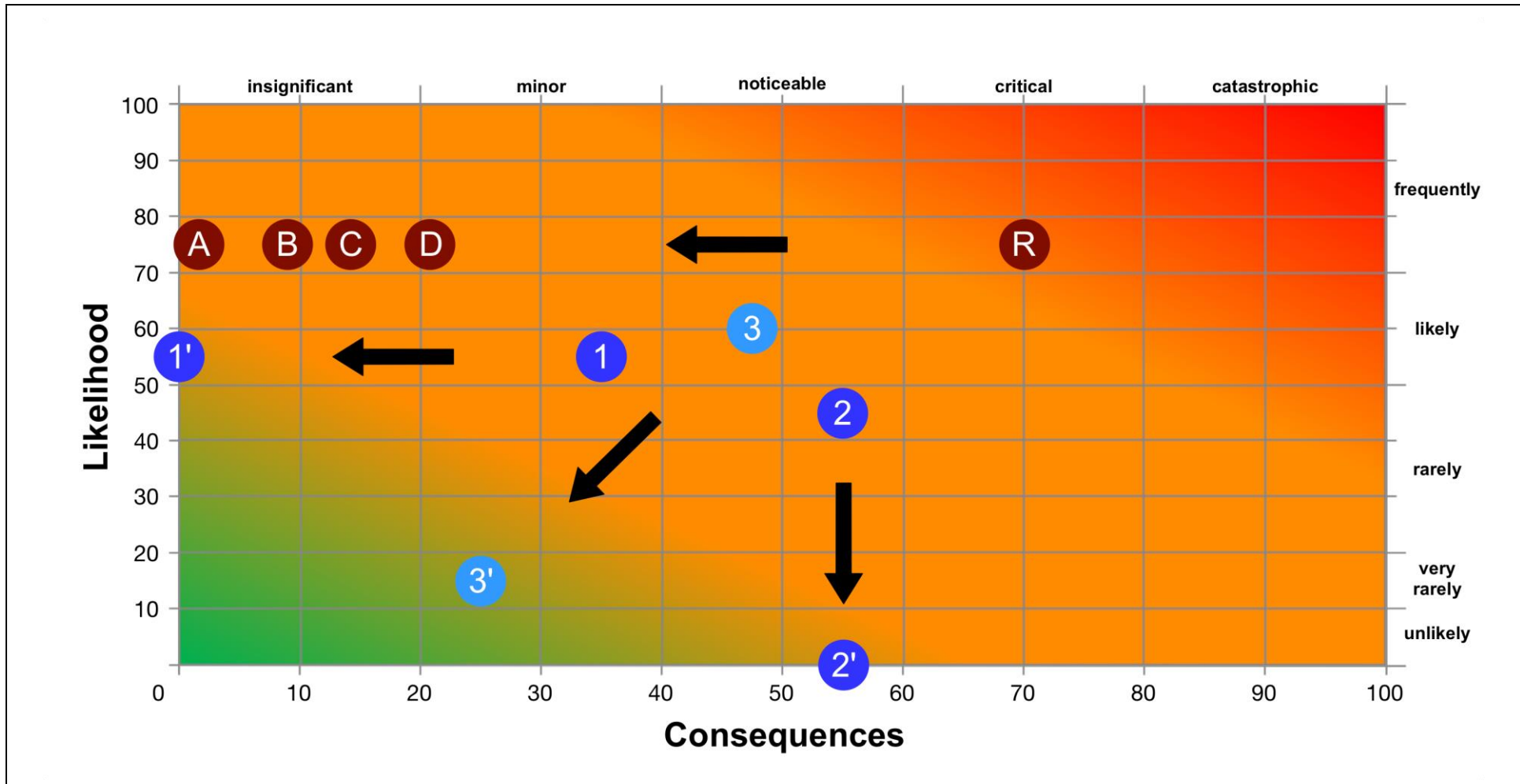


Figure 24: Risk treatment through risk avoidance, minimisation and diversification²¹⁷

²¹⁷ Adapted from ROMEIKE, F. [c] (2003), p. 237 ff.

The third active strategy is called risk diversification. Especially large companies benefit from this strategy. It describes the approach of spreading risks and can be applied to independent local, object-related or individual-related risks. Risk diversification is an affordable risk minimisation method for independent risks with the purpose of dividing one high risk into several risks with lower risk levels. For example, EFG uses several subcontractors for important parts of their hydropower plants instead of only one. Figure 24 displays the diversification of risk R into four minor risks with the same likelihood but decreased consequences. This enables EFG in case of quality problems or delivery delays of switching to another subcontractor. Personal-related risks concerning employees in charge of key positions can be minimised by using separate company vehicles or airplanes during business trips.²¹⁸

A corrective risk policy contains risk transfer, risk financing and risk provisioning as risk treatment strategies. Risk transfer describes the strategy of transferring risks onto third parties especially risks, which exceed the financial resources of a company. Instead of eliminating risks, risks are normally transferred onto insurance companies or contractual partners. Paying an insurance rate enables companies to transfer their risks onto insurance companies. The amount of the insurance rate depends on possible consequences, personal contributions in the event of risk occurrence and countermeasures taken by the company. In the event of damage insurance companies have to pay an amount of money predefined in advanced. As in the introduction mentioned, only actual risks can be insured, whereas an insurance of speculative risks is normally not possible. EFG's insurance policies have already included all kinds of various insurances like property, indemnity and personal insurances. Risk transfer onto contractual partners can be achieved by using special contract terms. The risk transfer level strongly depends on the negotiating power of a company. The negotiating power increases by the number of subcontractors, who are competing for an order. In the course of this master thesis EFG's general business terms were reviewed and compared with the competitors' general business terms. Afterwards the finally updated general business terms were presented to a lawyer for verification.^{219,220}

The purpose of risk financing is to gather financial capital in order to compensate occurring losses. Transferring risks onto third parties as described above can be seen as a risk financing method in the broadest sense. Risk provisioning aims at a premature creation of financial provision. This financial capital can be composed of earnings, (hidden) reserves gathered over several periods of time. It is important to start creating this financial capital in advance before risks occur.²²¹

²¹⁸ Cf. ROMEIKE, F. [c] (2003), p. 238 ff.

²¹⁹ Cf. ROMEIKE, F. [c] (2003), p. 240 f.

²²⁰ Cf. DIEDERICHS, M. (2010), p. 192 f.

²²¹ Cf. ROMEIKE, F. [c] (2003), p. 240 f.

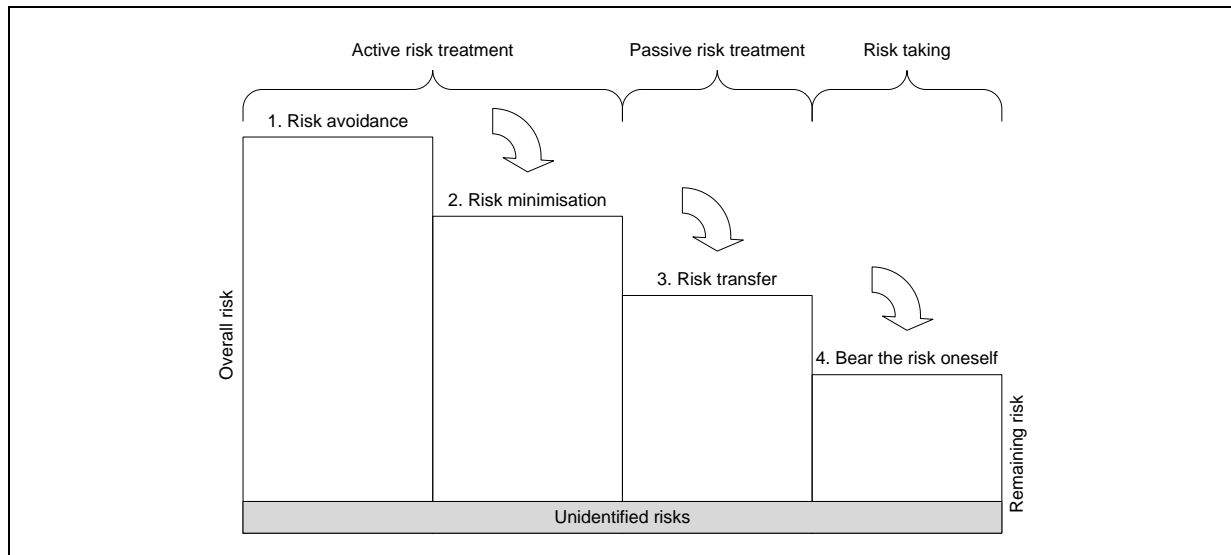


Figure 25: Risk treatment options²²²

Besides preventive and corrective risk policies, companies can also decide to accept a risk or not. Figure 25 summarises different risk treatment options from above. It displays the decreased risk level by implementing different strategies. It is possible to influence each individual risk by using one or a combination of different risk treatment options. At the end some remaining risks have to be accepted by the company, especially core risks. For being a successful company it is essential to create success potentials. Therefore, risks have to be taken. EFG's core competences are its knowledge and manufacturing skills regarding hydropower plants. They should work continuously on their success potentials to always be a step ahead of competitors. Because of that EFG invests into research and development. A separation of main and secondary risks is necessary in order to decide whether a risk should be taken or not. Secondary risks should be transferred at acceptable costs to third parties. This action enables companies to establish new success potentials by taking and focusing on core risks.^{223,224,225,226}

2.3.4 Communication and consultation

Another important part of the risk management process is communication and consultation. Information exchange should take place between internal and external stakeholders during all process steps. The development of communication and consultation plans should be initiated at the early beginning of the risk management process establishment. These plans address issues concerning risks, causes, consequences and taken countermeasures. It ensures that all people involved have the same basic knowledge of the necessity of particular countermeasures. The different perceptions of people involved concerning values, needs, assumptions and concepts have to be taken into account during the decision making

²²² Adapted from ROMEIKE, F. (2004), p. 117.

²²³ Cf. ROMEIKE, F. [c] (2003), p. 241.

²²⁴ Cf. GLEISSNER, W. (2008), p. 39 f.

²²⁵ Cf. GLEISSNER, W. (2008), p. 161.

²²⁶ Cf. DIEDERICHS, M. (2010), p. 194.

process. Risk communication during crisis according to *ONR 49002-3:2014* will be described later on.²²⁷

Risk communication within the company takes place between risk managers and risk owners. A risk owner, who is in charge of a risk, can influence it by deciding on its priority and execution of countermeasures. The task of the risk owner is to communicate the progress of each risk internally. A risk manager supports a risk owner as an expert but does not take responsibilities due to the lack of decision-making authority. Contents of communication can be methods, resources, assessments, priorities and other subject matters concerning risks. Authorities and responsibilities have to be defined during establishing the context.²²⁸

A risk dialogue with stakeholders during all process phases encourages the establishment of a communication culture according to *AS/NZS 4360*. The management is required to accept that it treats risks in an open and dynamic environment instead of a closed one. Considering coherences on objective, subjective and social levels can increase their trustworthiness. The “objective” level of risk management tries to understand technical and organisational systems. This understanding helps by controlling these systems and increases their reliability in order to reduce risks. The “subjective” level reduces risks from anxiety and aggression by taking emotions of involved people into consideration. Communication influences perceptions of risks, which are taken into consideration by the social levels of risk management. The goal is to start a discussion on risks and their benefits on technologies or systems.²²⁹

2.3.5 Monitoring and review

As displayed in Figure 2 monitoring and review is a continuous process in risk management. These processes take place periodically or if an event requires it in case of emergency. Furthermore, responsibilities for monitoring and reviewing have been defined during the establishment of the context. Risk monitoring is an ongoing process to observe remaining risks and searching for trends. The purpose is to detect trends of risks as well as prevent unidentified risks. Risk review focuses on implementing the earlier described risk treatment strategies. Countermeasures, deadlines and responsibilities are set in order to reduce the risk level of not tolerable and partly tolerable risks. The efficiency of defined measures is evaluated. In terms of the PDCA cycle risks of an increasing risk level pass the process steps of risk assessment once again.^{230,231}

²²⁷ Cf. *ONR 49001:2014*, p. 17 f.

²²⁸ Cf. BRÜHWILER, B. (2011), p. 150 f.

²²⁹ Cf. BRÜHWILER, B. (2011), p. 153 f.

²³⁰ Cf. *ONR 49001:2014*, p. 29.

²³¹ Cf. BRÜHWILER, B. (2011), p. 154 f.

2.4 Risk reporting at EFG

The developed RMT is besides assessing risks also applicable for risk reporting. Increased demands in modern times require information systems, which provide information in suitable quality and quantity to avoid wrong decisions. Due to increased complexity decision makers' are not able to keep up with all areas. Therefore, they need support provided by information systems. Figure 26 illustrates the level of information before and after the usage of information systems. Information needs of decision makers' can be divided into objective and subjective information needs. Objective information need is based on the tasks, which should be accomplished, whereas subjective information need is made up of information which seems relevant to specific types of problems. The level of information is determined by the intersection of objective information needs, information demands and information supplies. Created transparency minimises complexity and helps decision makers' to understand problems. Another positive effect is the increase of information offers caused by effective and quick information provision.²³²

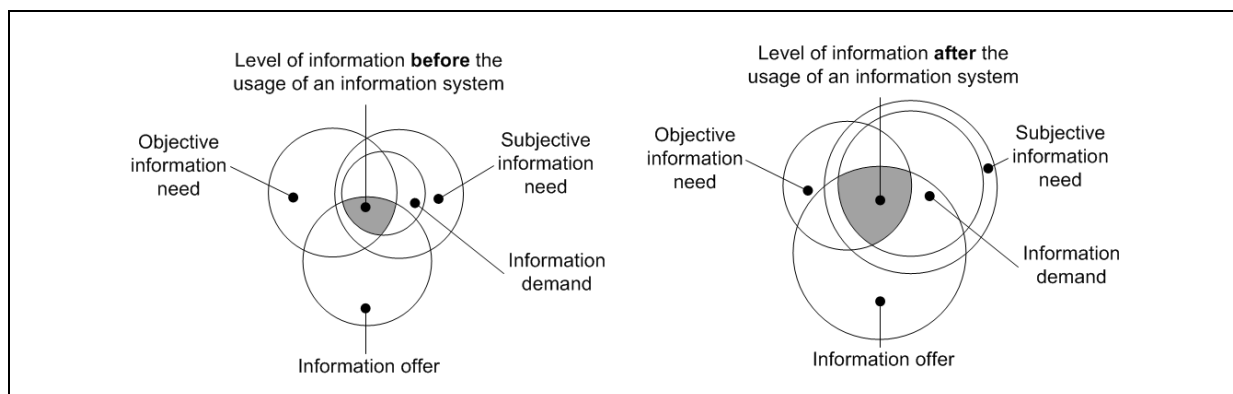


Figure 26: Level of information of decision makers²³³

The ISO 9001:2015 process description (see Appendix 4) displays defined risk reporting procedure within EFG. It starts with identifying and recording risks in the RMT. While recording risks, a revision interval is required to define. This periodicity should prioritise risk reports depending on their importance. This increases efficiency and avoids a flood of unnecessary reports. Based on recommendations in literature it is possible to choose between yearly, quarterly, monthly, weekly and ad hoc revision intervals. Besides regular revision intervals ad hoc reporting can be used for new arising and existence-threatening risks. This ensures a quick respond to threats by selecting appropriate countermeasures in order to avoid major losses.^{234,235} Based on the chosen interval, the next revision date for risk reporting or risk updating is displayed on the start screen of the RMT. Risk owners can save risks as PDF files for reporting reasons. The risk manager is able to see upcoming risk evaluations on the start screen. Saved reports contain all information recorded up to now

²³² Cf. ERBEN, R.; ROMEIKE, F. (2003), p. 277 f.

²³³ Cf. ERBEN, R.; ROMEIKE, F. (2003), p. 278.

²³⁴ Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 138 f.

²³⁵ Cf. MOTT, B. (2001), p. 221.

regarding each risk. To simplify matters, saved reports are structured similarly to the RMT, which is described later on in more detail. Risk management within EFG is implemented near top management, which will be described in chapter 2.6.3. The EFG's risk manager is able to inform the top management in case of an emerging threatening risk any time.

Besides these standard reports the current risk matrix is presented on an annual basis. This presentation is illustrated as risk reporting in the ISO 9001:2015 process description. During this meeting risk inventory is tested for completeness as well as a presentation of most important risks is conducted. Attendees are the EFG's risk manager and risk owners. Risk owners present their assigned risks starting from the upper right to lower left of EFG's risk matrix. This approach ensures the discussion of the most important risks. Previous measures, estimated likelihoods and consequences as well as assessments of the current situation and further course of actions are presented for each risk to up-date all involved.

At this point a recommendation to EFG for further risk management expansion possibilities is given. This master thesis deals with the basic knowledge for a company-wide application of risk management. After the establishment of a basic risk culture an expansion of the existing risk management to RFG's projects is recommended. Therefore, the bottom-up approach is expanded by EFG's projects. Figure 27 illustrates a company-wide top-down and project-related bottom-up approach. During the lifecycle of each project the techniques and methods from above can be applied. Risk identification collection methods like check-lists take identified risks from earlier projects into account. Interviews with internal and external experts consider perspectives concerning their areas. Analytical methods like FMEA or fault tree analysis help to systematically identify threats of existing systems. Creativity methods like brainstorming or the Delphi method help to identify risks in a chaotic way. During the risk analysis phase an expected value based on likelihood and consequences is calculated for each identified project risk. Therefore, the earlier described risk assessment template with predefined scales can be used. Single risks of each project are combined in order to calculate an overall risk level for each project. For example, for each project a newly, adapted Excel file of the RMT can be created. This contains all identified risks related to the project. Risk categories and groups can be changed in order to meet project phases. This enables EFG to display risks separately for each project phase in the risk matrix. Furthermore, the arithmetic average can be used as overall project's risk level. If this arithmetic average exceeds a predefined value the project's feasibility should be reconsidered. The functionality of the RMT will be described more detailed in chapter 3 later on.²³⁶

²³⁶ Cf. BECKER, W.; EBNER, R.; FISCHER-PETERSOHN, D.; RUHNAU, M. (2015), p. 26 ff.

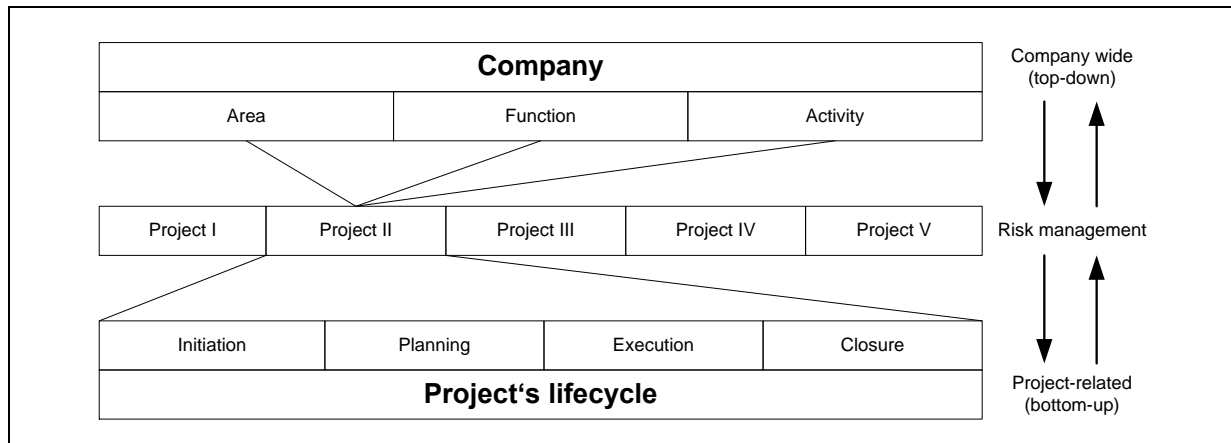


Figure 27: Expansion of risk management to project risk management²³⁷

This stepwise risk management integration in EFG ensures a stable base for further implementations. The risk management process steps of risk assessment are simple to integrate into planning processes. EFG's project managers should review their assumptions during the planning phase. This forces them to reconsider their thoughts, which enhances the quality of planning in the long run.²³⁸

2.5 Crisis management

The purpose of *ONR 49002-3:2014* is to prepare companies for the management of risk scenarios, which can suddenly occur even if countermeasures are set. Despite all preventive measures companies have to take certain risks, which have low likelihoods but in case of occurrence high consequences. These risks are often operational and impact companies' performance. The purpose of emergency, crisis and continuity management is the reduction of material and immaterial consequences of risks. Investigating EFG's risk portfolio proves that risk 7 and risk 8 (see Figure 17) are risks with relatively low likelihood but high consequences.²³⁹

Figure 28 illustrates the different stages of emergency, crisis and continuity management after an event. In the first step after a damaging event the emergency management goes into action. If more than one department is affected, the emergency management becomes the crisis management. The aim of the emergency and crisis management is a fast implementation of countermeasures in response to an event in a structured order. The continuity management's purpose is the rapid rebuilding of damaged structures in order to get operations back to work.²⁴⁰

Besides minor disturbances, companies are asked to establish criteria, which label localised damaging events as a company-wide crisis. Furthermore, counteractions concerning

²³⁷ Cf. HENSCHER, T. (2010), p. 52.

²³⁸ Cf. BÖCKMANN, D.; HENDRICKS, F. (2006), p. 166.

²³⁹ Cf. *ONR 49002-3:2014*, p. 4.

²⁴⁰ Cf. *ONR 49002-3:2014*, p. 5.

different identified scenarios are required. These scenarios are identified and analysed by using the above described risk management process. As a preferred risk evaluation method a combination of the worst-case scenario analysis and the top-down approach is recommended. This should ensure that only crucial risks are identified. Therefore, causes and consequences of identified scenarios are estimated. The worst but still plausible scenario of a risk from the risk catalogue is chosen and described. Causes and effects as well as likelihoods and consequences are taken into consideration. A combined danger list from various organisations with regard to EFG includes the following scenarios:^{241,242}

- Internal damaging events
- Natural disasters
- Environmental incidents
- IT breakdowns
- Technical failures
- Legal challenges
- Loss of key personnel

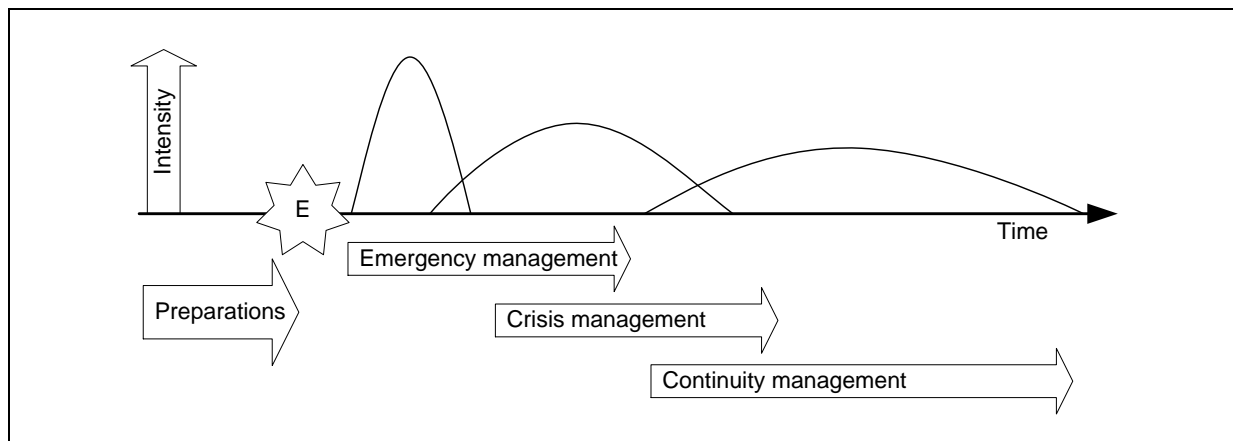


Figure 28: Emergency, crisis and continuity management²⁴³

Top management and managers should carry out preparations and process flows for emergency and crisis management. During the establishment of action plans the absence of key personnel should be taken into account. Therefore, established action plans are designed in order to be flexible, robust and independent from personnel. People involved in emergency and crisis plans should be able to identify and analyse occurring scenarios. It is recommended to practise defined procedures. The ability of a quick reaction of people involved in real situations is very important. In case of an emergency the following steps should be done: After triggering the emergency alarm immediate actions like evacuations are initiated. Besides gathering information and assessing the situation, a connection to action forces and authorities needs to be established. Defined countermeasures should be put in motion to avoid or reduce damages as well as to continue operations. A reliable internal and external crisis communication is necessary during the entire crisis. The desired outcome is

²⁴¹ Cf. ONR 49002-3:2014, p. 6 f.

²⁴² Cf. ONR 49002-2:2014, p. 11 f.

²⁴³ Cf. ONR 49002-3:2014, p. 5.

the establishment of normal conditions. Smaller organisations like EFG are not required to differentiate between emergency and crisis management. They can use a combination of emergency and crisis management.²⁴⁴

Due to limited financial resources SMEs should make efforts to find the right balance of risk and crisis management as displayed in Figure 29. Risk management uses proactive measures in order to reduce the likelihood of risks, whereas the crisis management implements reactive measures to decrease consequences. Proactive risk identification methods are illustrated in Figure 13. On the one hand risk reacting costs increase when preventive measures are neglected in a company. On the other hand risk preventing costs increase by providing a higher reliability. Threshold values of minimum costs vary from company to company and should be individually defined for each company. Skilled companies combine risk and crisis management in a way that cumulated costs are minimised. To sum up it is necessary to identify risks at a very early stage and set countermeasures in order to keep costs at a minimum.²⁴⁵

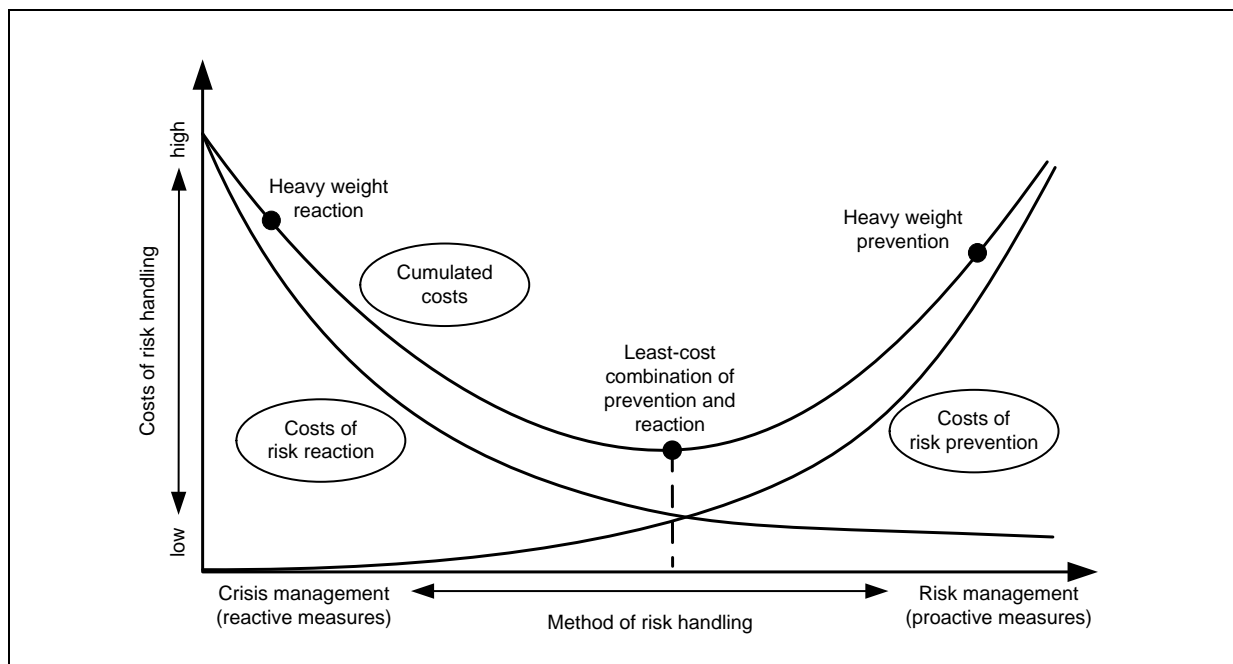


Figure 29: Context of risk and crisis management²⁴⁶

The purpose of continuity management is to ensure a reduction of operation disruptions by using suitable measures. Furthermore, a quality decrease of products and services should be avoided as well as required costs should be kept at a minimum. Suitable measures for continuity management are capacity reserves, inventory holdings and replacement procurements. Capacity reserves in terms of production plants, infrastructures and resources are the most suitable but also most expensive measures for the continuity management. A well-equipped inventory of resources and semi-finished products enables companies to bridge disruptions and keep their operations running. Consequences can be minimised with

²⁴⁴ Cf. ONR 49002-3:2014, p. 8 f.

²⁴⁵ Cf. BOUTELLIER, R.; MONTAGNE, E.; BARODTE, B. (2007), p. 45 f.

²⁴⁶ Cf. BOUTELLIER, R.; MONTAGNE, E.; BARODTE, B. (2007), p. 45.

a quick procuring of replacements like resources, goods and information. Furthermore, planning and preparations for this type of continuity management can be done in advance.²⁴⁷

In periodic time intervals the functionality of the emergency and crisis management needs to be tested. Therefore, scenarios are simulated and effectiveness of procedures is evaluated. It is recommended to hold trainings with the crisis committee on a quarterly or semi-annually basis. Furthermore, simulated mission exercises should be done every three or four years. Afterwards exercises are analysed and evaluated in order to optimise defined action plans.²⁴⁸

2.6 Organisational structures of risk management systems

After a detailed explanation of the risk management process the following chapter investigates in detail various organisational implementation possibilities of existing company structures. Furthermore, tasks, required competences and responsibilities of people involved at EFG are described.

2.6.1 People involved in risk management

Based on organisational principles of quality management the chain of commands (see Figure 30) starts with the company's owners or representatives. Their task is the instruction of an internal or external auditor in order to verify set objectives and review involved people. The appointed auditor should be an independent person regardless if she/he is a company internal or external employee. The auditor never tests himself. Her/his main task is to evaluate the top management which delegates organisational responsibilities to risk managers, risk responsible people and finally risk owners. Results concerning achieved objectives and occurring divergences are presented to her/his employer. Illustrated terms of Figure 30 are described below.²⁴⁹

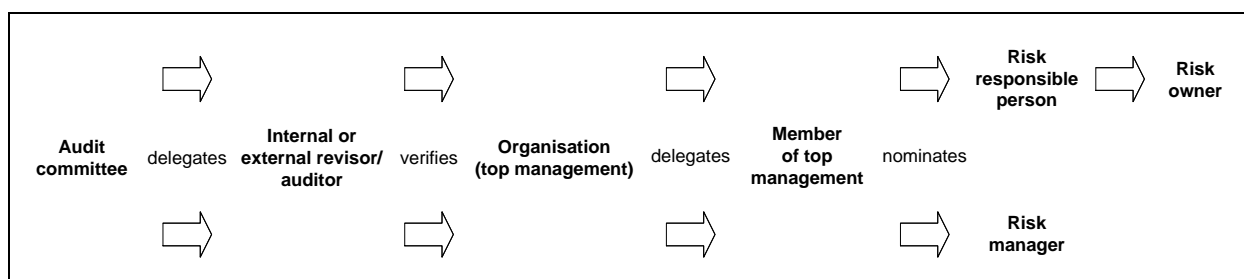


Figure 30: Chain of commands in risk management²⁵⁰

²⁴⁷ Cf. ONR 49002-3:2014, p. 16 f.

²⁴⁸ Cf. ONR 49002-3:2014, p. 18 f.

²⁴⁹ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 137 f.

²⁵⁰ Adapted from ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 138.

The revision department

Especially large companies instruct internal revision, which directly reports to top management or executive board, for verification of their implemented risk management and internal control systems. Due to the fact that internal revision is also evaluating the performance of the executive board, an independence from evaluated divisions as well as the board has to be guaranteed. Besides, evaluation of processes and compliance with all legislation as well as standards of internal revision and auditors are also responsible for the creation of inspections plans, recommendations and realistic reporting. Both, internal revision and auditors, have similar supervision and verification functions. Nevertheless their approaches used differ from each other. Internal revision evaluates effectiveness and functionality of defined controls by using tests of real business cases, whereas auditors follow a predefined schema. At the beginning they consider formal basics. Afterwards they concentrate on the practical implementation. Due to similar tasks and resulting synergy effects, a mutual organisational wide revision and audit program can be established.²⁵¹

The audit committee

According to § 92(4a) *aAktG* and § 30g(4a) *aGmbHG* companies, which match § 271a *aUGB* are legally obliged to implement an audit committee. This committee consists of members of the supervisory board and is also appointed by them. In case of a renunciation of this committee the supervisory board is in charge of terms regarding risk management. The purpose of the audit committee is to supervise financial reporting, effectiveness of risk management- and internal control systems as well as compliance of laws and standards.^{252,253,254,255}

The top management

ONR 49000:2014 defines top management as high-level people or a group of people that lead and steer companies. Furthermore, they are allowed to delegate powers and provide necessary resources within the company. The top management has to stand behind actions set during the risk management process in order to be trustworthy. Legal requirements and standards have to be practised and demonstrated on a daily basis by the top management. Objectives are among others communication of requirements to increase risk awareness, implementation of guidelines, further development of systems and supply of necessary resources. A contact person within the top management should be defined to act like an interface between the company's owners or representatives and the risk manager. In many cases people from top management occupy the risk manager's position.^{256,257}

²⁵¹ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 140 ff.

²⁵² *aAktG BGBI 1965/98* as amended *BGBI I 2012/35*.

²⁵³ *aGmbHG RGBI 1906/59* as amended *BGBI I 2008/70*.

²⁵⁴ *aUGB dRGBI 1897/219* as amended *BGBI I 2008/70*.

²⁵⁵ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 139 f.

²⁵⁶ Cf. *ONR 49000:2014*, p. 16.

²⁵⁷ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 143 f.

The risk manager

According to *ONR 49000:2014* the risk manager is a person who applies the risk management process and implements it within a company. As above mentioned a company's employee or an external consultant can occupy this position. She/he is the key element of risk management and is responsible for establishing and further developing a risk management system. A certified risk manager should be able to pass through the risk management process steps and apply these steps to companies, sub-areas and systems. Furthermore, she/he should be familiar with the structure of *ONR 4900x:2014* series (see Figure 7) and continues her/his education regularly in order to stay up-to-date.^{258,259,260}

Concerning *ONR 49000:2014* risk managers are asked to point out objectives and benefits of risk management to risk owners and people involved within a company. One requirement is the proper usage and understanding of risk management terms and basics. They should specify application areas within the company as well as the right implementation of the risk management into existing structures. *ONR 49001:2014* demands from risk managers the ability to establish the context concerning a risk management adjusted to the company's needs. Another important competence is the understanding of needs and expectations of people involved, such as the top management, managers, blue-collar workers and stakeholders. This standard expects from risk managers the knowledge as well as the ability to apply and implement the previously described risk management process steps. In addition *ONR 49002-1:2014* requires also from risk managers the understanding of a bigger picture in order to implement and establish connections between the risk management process and existing management systems. Furthermore, the risk managers should present the best way of regulating competences and responsibilities to the top management. According to *ONR 49002-2:2014*, risk managers need to be able to identify risks within the company or systems and select as well as apply suitable risk evaluation methods. *ONR 49002-3:2014* requests a basic knowledge of emergency, crisis and continuity management from risk managers. They should be able to identify and analyse most important emergency, crisis and continuity management scenarios and establish suitable action plans. Documentation is very important as well as making adjustments to occurring changes.²⁶¹

The risk responsible person

Managers within a company often fill this position. This person is responsible for steering processes concerning threats within a department. She/he helps to introduce the risk management into her/his assigned areas and evaluate the implementation of activities. Furthermore, tasks of a risk responsible person are the identification, analysis, evaluation and treatment of risks, creation of a risk catalogue and monitoring respectively reviewing costs of set counteractions. It is advisable to appoint a line manager for this position in order to avoid leadership conflicts.²⁶²

²⁵⁸ Cf. *ONR 49003:2014*, p. 4 ff.

²⁵⁹ Cf. *ONR 49000:2014*, p. 13.

²⁶⁰ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 144 f.

²⁶¹ Cf. *ONR 49003:2014*, p. 4 ff.

²⁶² Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 145 f.

The risk owner

A risk owner is defined according to ISO Guide 73:2009 as a “person or entity with the accountability and authority to manage a risk.”²⁶³ A risk owner is confronted with risks on a daily basis and embodies the executive power. She/he assists in the identification, analysis and evaluation of risks and performs risk reducing activities as well as applied countermeasures. The ultimate goal of selected actions should be a reduction of the risks’ likelihood and consequences.²⁶⁴

2.6.2 Implementation possibilities of the risk management

As described above one of the risk manager’s task is the implementation of a risk management system tailored to the company’s needs. The risk management can be established within – internal – an organisation or as a separate – external – unit. External located risk management units emphasize the importance of the risk management within the organisation. Members of these units are well-trained and focus on an organisational wide proper implementation of the risk management. Furthermore, this approach ensures an independent control and supervision. Crucial problems that can occur are for example inappropriate information exchange and interface problems between the organisation and external units. Internal located risk management units enable the usage of existing structures with minor adjustments. There is a need to clarify whether additional tasks and obligations can be added to existing tasks of employees. This increases the efficiency as people involved have more detailed information, which is necessary to make the right choices concerning risk management. Furthermore, additional administrative efforts can be avoided. Below, some internal risk management implementation possibilities are described.²⁶⁵

Risk management implemented as part of the top management

The left picture in Figure 31 shows the integration of risk management within the executive board or top management. This enables the top management to act as a role model and represent the risk management according to their ideas. Independent from the located position of risk management final decisions are done by the top management. Possible downsides of this approach are the delegation of operational tasks and the guarantee of providing enough resources for the risk management phases.²⁶⁶

Risk management implemented as executive department

The right picture in Figure 31 illustrates the implementation approach of using an executive department. This combines the advantages of a near to top management located risk management as well as an independent position of the risk manager. Existing executive departments can be extended or new ones created. This has the advantages of a close relationship to the top management, bundling various tasks in one position; and the risk manager can concentrate on essential parts. Furthermore, executive departments are neutral against other line functions and risk managers are able to gain an overall picture.

²⁶³ ISO GUIDE 73:2009, chap. 3.5.1.5.

²⁶⁴ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 147 f.

²⁶⁵ Cf. DIEDERICHS, M. (2010), p. 208 f.

²⁶⁶ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 148 f.

Disadvantages are demanded requirements from leadership as well as the fact that executive departments only serve as consultants and have no decisional power. Implementing a risk management the in quality management or other executive departments can bring about advantages to SMEs like EFG in terms of a better utilization of existing personal resources but can cause a process oriented risk management.^{267,268}

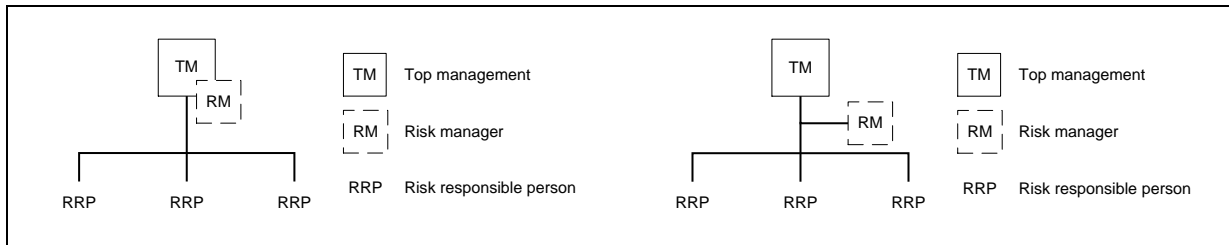


Figure 31: Risk management as part of top management and executive department²⁶⁹

Risk management implemented as line function

With the increasing growth of a company it is getting more likely to implement a risk management as a separate unit within the company (see Figure 32, left picture). This department is equal to other departments like procurement or research and development in terms of obligations and duties. Other departments perceive and acknowledge the risk management department as part of the company. However, this can lead to an isolated thinking between the different departments. Furthermore, equalisation of departments prevents the risk management of making decisions.²⁷⁰

Risk management implemented within different business areas

The right picture in Figure 32 describes the organisational implementation of a department-specific risk management within the organisation. This approach is used for organisations with heavily varying business areas. Upsides are the equalisation of risk managers with risk responsible persons. Furthermore, risk managers can entirely focus on their business area. Due to the lack of a higher authority who is responsible for risk managers the big picture of the company's risk landscape is not overseen and business areas can develop in opposite directions.²⁷¹

²⁶⁷ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 149 f.

²⁶⁸ Cf. DENK, R.; EXNER-MERKELT, K.; RUTHNER, R. (2008), p. 248 ff.

²⁶⁹ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 148 f.

²⁷⁰ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 150.

²⁷¹ Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 150 f.

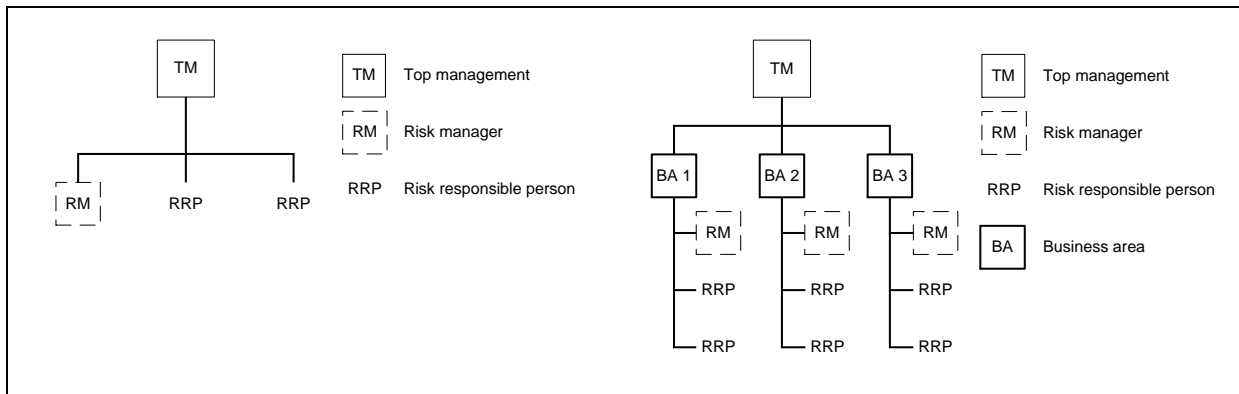


Figure 32: Risk management as line function and within different business areas²⁷²

2.6.3 Risk management implementation at EFG

Risk management integration strongly depends on existing management systems within companies. Many companies like EFG are part of the ISO 9000 family, which is suitable for implementing risk management. *ONR 49002-1:2014* provides an implementation suggestion for combining the *ONR 4900x:2014* series with ISO 9000 (see Figure 33). ISO 9000 is aligned to fit customer requirements and should finally lead to satisfied customers as well as stakeholders. Risk management is part of the management responsibility and contains of the actions: communication and consultation, establishing the context, risk assessment, risk treatment and monitoring and review of risks.²⁷³

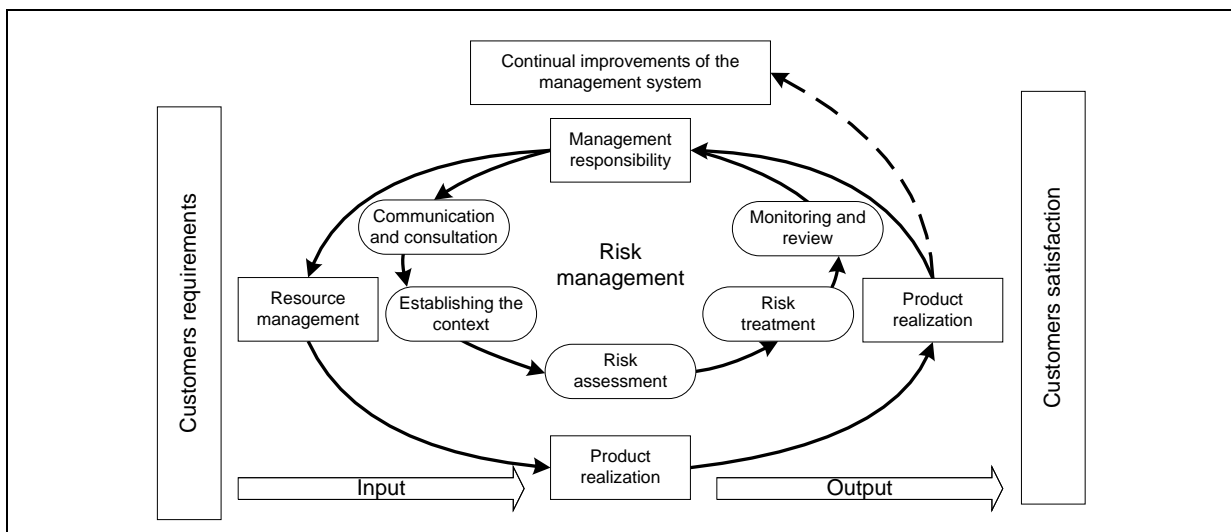


Figure 33: ÖNORM EN ISO 9000 with implemented risk management process²⁷⁴

Based on the different implementation possibilities explained in the previous chapter, a suitable solution for EFG has to be selected. The task is to choose an implementation structure, which fits to their existing company structure. In view of the existing situation it does not make any sense to create an executive department for the risk manager, who will

²⁷² Cf. ILLETSCHKO, S.; KÄFER, R.; SPATZIERER, K. (2014), p. 150 f.

²⁷³ Cf. *ONR 49002-1:2014*, p. 5.

²⁷⁴ Cf. *ONR 49002-1:2014*, p. 5.

exclusively devote himself to risk management. Instead, the nominated risk manager gets, in addition to her/his daily tasks, the supervision of risk management. She/he is contact for questions concerning risk management and responsible for a proper implementation of the risk management process. Figure 34 illustrates the selected risk management implementation for EFG. The risk manager is in the centre located near the top management in order to allocate enough resources for the process as well as to act like a role model to establish a company-wide risk culture. Using this approach instead of a line function gives the risk manager the ability make decisions. Furthermore, the appointed risk manager has a detailed knowledge of company processes and procedures to keep an overview during the risk management process.

Besides, the risk responsible persons of each department report to the risk manager, which is displayed in Figure 34. These risk responsible persons act at the same time as risk owners and conduct risk treatment strategies. However, they have the executive power to delegate others to perform countermeasures in order to reduce the company's risk level. As in this case risk responsible persons and risk owners are the same, terms are unified and the term risk owner is used in this master thesis. In addition to her/his risk reducing tasks, each risk owner presents her/his risks which she/he is responsible for. During the annual or semi-annual risk matrix presentation risk owners present their risks to the risk manager in order to keep him up-to-date.

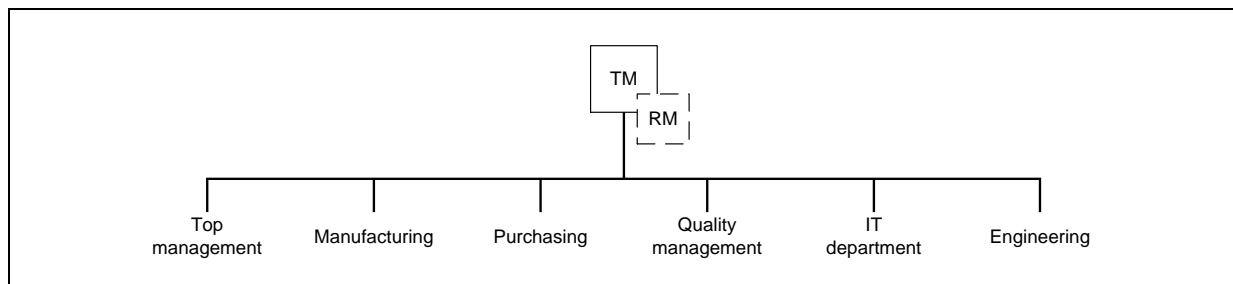


Figure 34: Risk management implementation at EFG

3 Structure of the risk management tool

The following chapter describes the risk management tool developed in Microsoft Excel in order to accomplish the second main goal. This tool is tailored to EFG's needs and enables them to document, monitor and present their identified risks.

Figure 35 illustrates the start screen of the developed RMT. The three buttons in the upper half lead to the corresponding screens, which will be discussed later on. On the left-handed side within the frame, all identified risks are summed up and distinguished according to their position in the risk matrix. As earlier described, a risk matrix with three tolerance ranges is used. This enables EFG's risk managers and risk owners to see how many risks are in each tolerance range. Furthermore, successfully reduced risks are archived and summed up, too. On the right-hand side within the frame, all entered risks are sorted dependent upon their due date for their next revision. Double-clicking on a risk leads to a more detailed risk overview screen.

The gear icon in the lower left corner opens the settings screen (see Figure 36). This settings screen is password protected in order to prevent unauthorised users from entering and changing settings. The button besides the gear icon leads to a screen, where potential risks can be entered. Potential risks are not worth to be entered in the tool at the moment and sorted out at the first decision element from the process description for ISO 9001:2015 (see Figure 42).

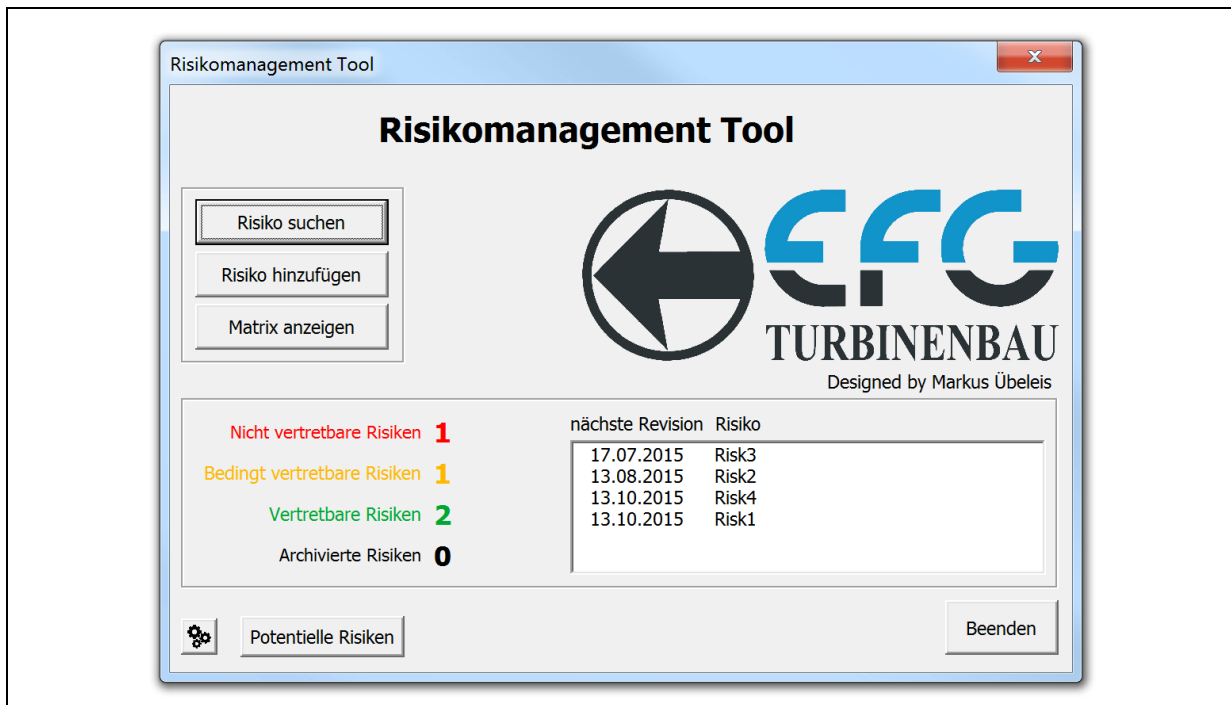


Figure 35: Risk management tool – start

The settings screen of the RMT is displayed in Figure 36. Adjustments in the settings screen are possible in order to provide EFG a degree of flexibility. Values within the frame in the

upper left corner are used to define the upper and lower threshold for the tolerance ranges of the risk matrix. Changing these two values enlarges or reduces the three tolerance ranges. Positions of risks remain the same but tolerance ranges get shifted. The middle frame on the left-hand side is relevant for EFG's risk manager. Periodically the risk manager has to update the EBIT according to EFG's economic development. The lower left frame is used to change the password, which has to be entered for accessing the settings screen and deleting risks.

The frame on the right-hand side enables EFG to adjust the context between qualitative and quantitative risk criteria of likelihood and consequences (see Figure 11). At the first start of this tool the storage path of the risk matrix background has to be defined in order to display the risk matrix. Furthermore, an edit mode is implemented for making changes or adjustments to this tool.

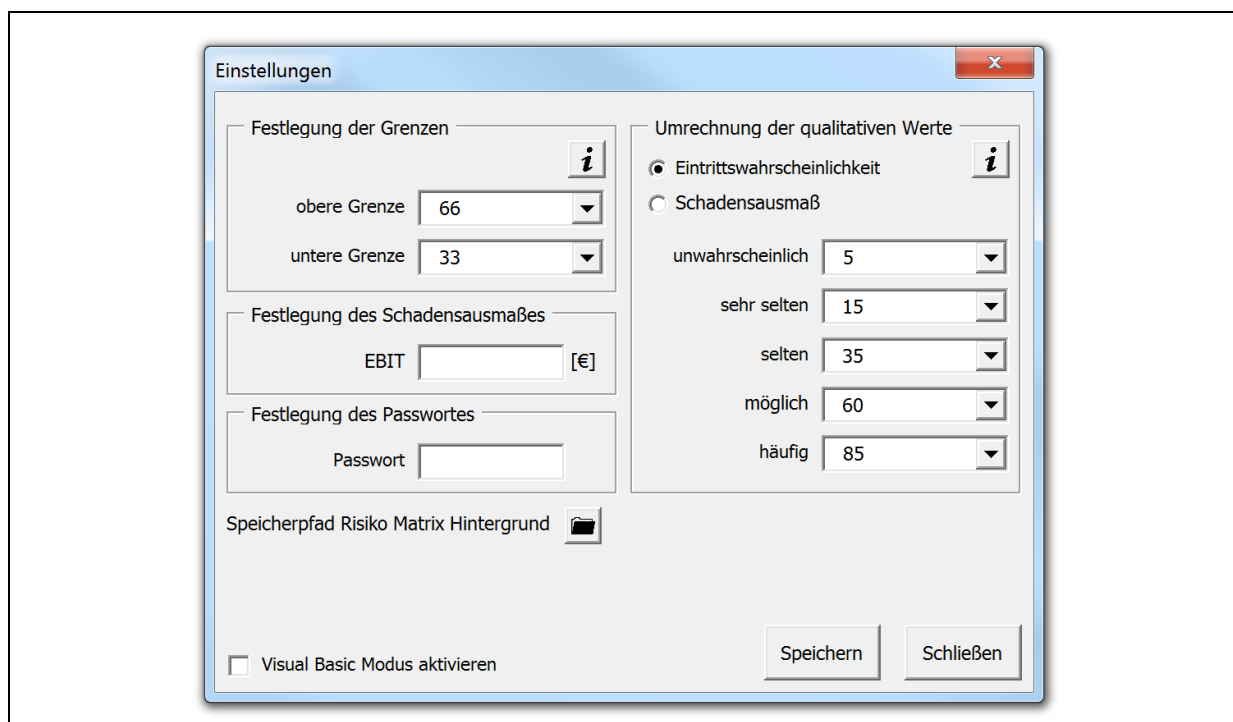


Figure 36: Risk management tool – settings

The search screen of Figure 37 can be reached from the start screen and provides comprehensive search possibilities. For each risk the current likelihood, consequences, risk category and group as well as the risk name are listed. Recorded risks are sorted according to their current expected value in a descending order. A search can be performed by choosing a risk category. Furthermore, selecting a risk group can narrow search results down. Risk owners are able to pick their area of responsibility and assigned risks get displayed. This enables them to quickly display and access their risks for further revisions. Entering a keyword into the search box, lists risks which contain the keyword in their names. Clicking search risk without entering a keyword displays all risks recorded in the RMT.

The search screen provides like the start screen a possibility to add a new risk. Selecting a risk from the list enables the user to display, edit or update the risk. The structure of these

screens will be explained later on. Furthermore, it is possible to delete risks and display archived ones, which were successfully reduced.

The screenshot shows a window titled 'Risiko suchen' with a search interface. It includes several input fields and buttons for managing risks.

Search Filters:

- Risikokatalog
- Risikokategorie (dropdown)
- Risikogruppe (dropdown)
- Verantwortlich (dropdown)
- Risiko suchen (text input)

Action Buttons:

- Risiko hinzufügen
- Risiko bearbeiten
- Risiko löschen
- Risiko anzeigen
- Risiko aktualisieren
- Archivierte Risiken
- Schließen

Risk Data Table:

EW	SA	Risikokategorie	Risikogruppe	Risiko
85	kritisch	Kunden- und absatzspezifische Risiken	Produkttrisiken	Risk2
möglich	kritisch	Allgemeine globale Risiken	Strategische Risiken	Risk1
selten	gering	Kunden- und absatzspezifische Risiken	Finanzielle Absatzrisiken	Risk4
sehr selten	gering	Operationale Risiken	Finanzwirtschaftliche Risiken	Risk3

Figure 37: Risk management tool – search, add, edit, display and update risks

Figure 39 displays the screen for adding a new identified risk. All edit, display and update screens have for the sake of convenience nearly the same structure. Due to the fact that the edit and update screen are basically the same screen as the adding of a new risk screen, it will not be discussed any further (see Figure 46 and Figure 47). The only difference is that the edit screen contains the option for archiving risks. On the left-hand side information concerning the risks have to be entered. The right-hand side contains information concerning assessment and further countermeasures of the risk. At the beginning of a recording the risk detection date and person have to be entered, followed by the risk category and group. The short risk description is used for the search of risks. Below, a more detailed risk description has to be filled in. Besides the risk owner, risk causes and interdependencies have to be entered.






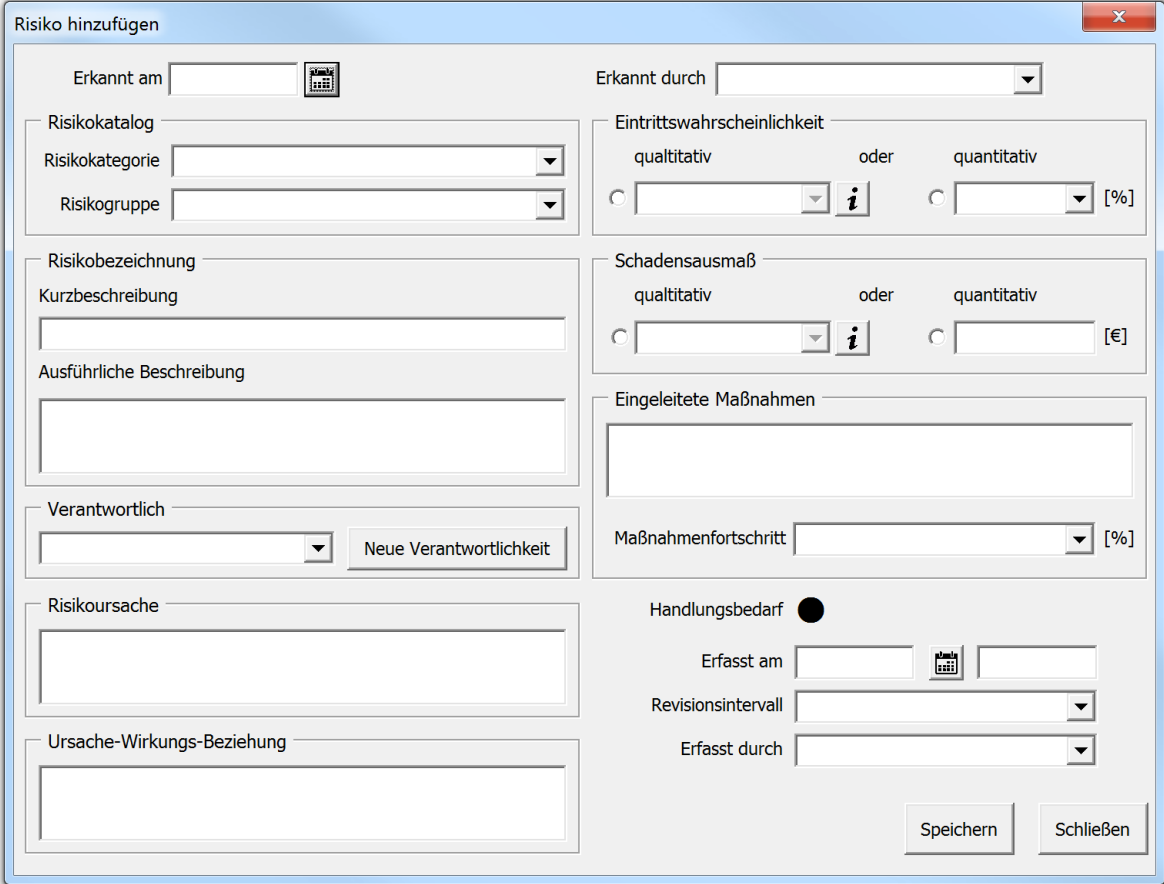
Handlungsbedarf  Kein Handlungsbedarf	Tendenz	Noch kein Trend erkennbar!
Handlungsbedarf  Präventivmaßnahmen setzen	Tendenz 	Risiko erfolgreich verringert!
Handlungsbedarf  Sofortmaßnahmen setzen	Tendenz 	Risiko unverändert!
	Tendenz 	Risiko gestiegen!

Figure 38: Legend of demand for action and risk tendency

On the right-hand side during the risk analysis phase estimated likelihood and consequences have to be entered either in a qualitative or quantitative way (see Figure 11). Based on the expected value of likelihood and consequences the demand for action is calculated. Depending on the risk's position in the risk matrix the black circle changes the colour and displays if actions have to be taken (see Figure 38). For example, the circle turns red which suggests taking countermeasures if the expected value is within the not tolerable range of the risk matrix. In addition, applied actions and their progress need to be entered. At the end the entry date and person as well as the revision interval has to be selected. It is possible to choose between yearly, quarterly, monthly, weekly and ad hoc revision intervals. Depending on the picked revision interval the next revision due date for the start screen is calculated and displayed.



The screenshot shows the 'Risiko hinzufügen' (Add Risk) dialog box. It contains the following fields and controls:

- Erkannt am:** A date picker field.
- Erkannt durch:** A dropdown menu for the person who identified the risk.
- Risikokatalog:**
 - Risikokategorie:** A dropdown menu.
 - Risikogruppe:** A dropdown menu.
- Risikobezeichnung:**
 - Kurzbeschreibung:** A text input field.
 - Ausführliche Beschreibung:** A larger text input area.
- Verantwortlich:** A dropdown menu with a 'Neue Verantwortlichkeit' button.
- Risikoursache:** A text input field.
- Ursache-Wirkungs-Beziehung:** A text input field.
- Eintrittswahrscheinlichkeit:**
 - Radio buttons for 'qualitativ' and 'quantitativ'.
 - Input fields for values and a percentage sign [%].
 - An information icon (i).
- Schadensausmaß:**
 - Radio buttons for 'qualitativ' and 'quantitativ'.
 - Input fields for values and a Euro symbol [€].
 - An information icon (i).
- Eingeleitete Maßnahmen:** A text input area for listing measures.
- Maßnahmenfortschritt:** A dropdown menu with a percentage sign [%].
- Handlungsbedarf:** A radio button (currently selected).
- Erfasst am:** A date picker field.
- Revisionsintervall:** A dropdown menu.
- Erfasst durch:** A dropdown menu.
- Buttons:** 'Speichern' (Save) and 'Schließen' (Close).

Figure 39: Risk management tool – add new risk

The basic structure of the screen for displaying risks (see Figure 40) is almost the same as the previous one. Information on this screen is not editable for users. The upper right-hand side displays information concerning the last risk's revision and below the current risk status is shown. At the bottom the risk tendency is displayed, which is the comparison of the last and current expected value (see Figure 38). Furthermore, each single risk can be saved as PDF file including the entire risk history.

Figure 40: Risk management tool – display risk

EFG's risk landscape (see Figure 41) can be accessed through the start screen. For each risk the name, likelihood, consequence and tendency is listed in order to provide a quick overview. Risks can be displayed by selecting a risk category and group. Risk owners are able to select her/his area of responsibility and get her/his risks, which she/he is responsible for, displayed in the risk matrix. This function is useful for the annual or semi-annual risk matrix presentation, where risk owners present their risks as well as countermeasures and further actions. Each area of responsibility has its own colour in order to help risk owners quickly identify their own risks when all risks are illustrated. Furthermore, all risks, top 10 risk and all risks including an arithmetic average can be displayed. The arithmetic average helps EFG quickly to compare their current risk landscape with the risk landscape of the past

couple of years. Like saving single risks the entire risk matrix and their corresponding risk can be saved as PDF.

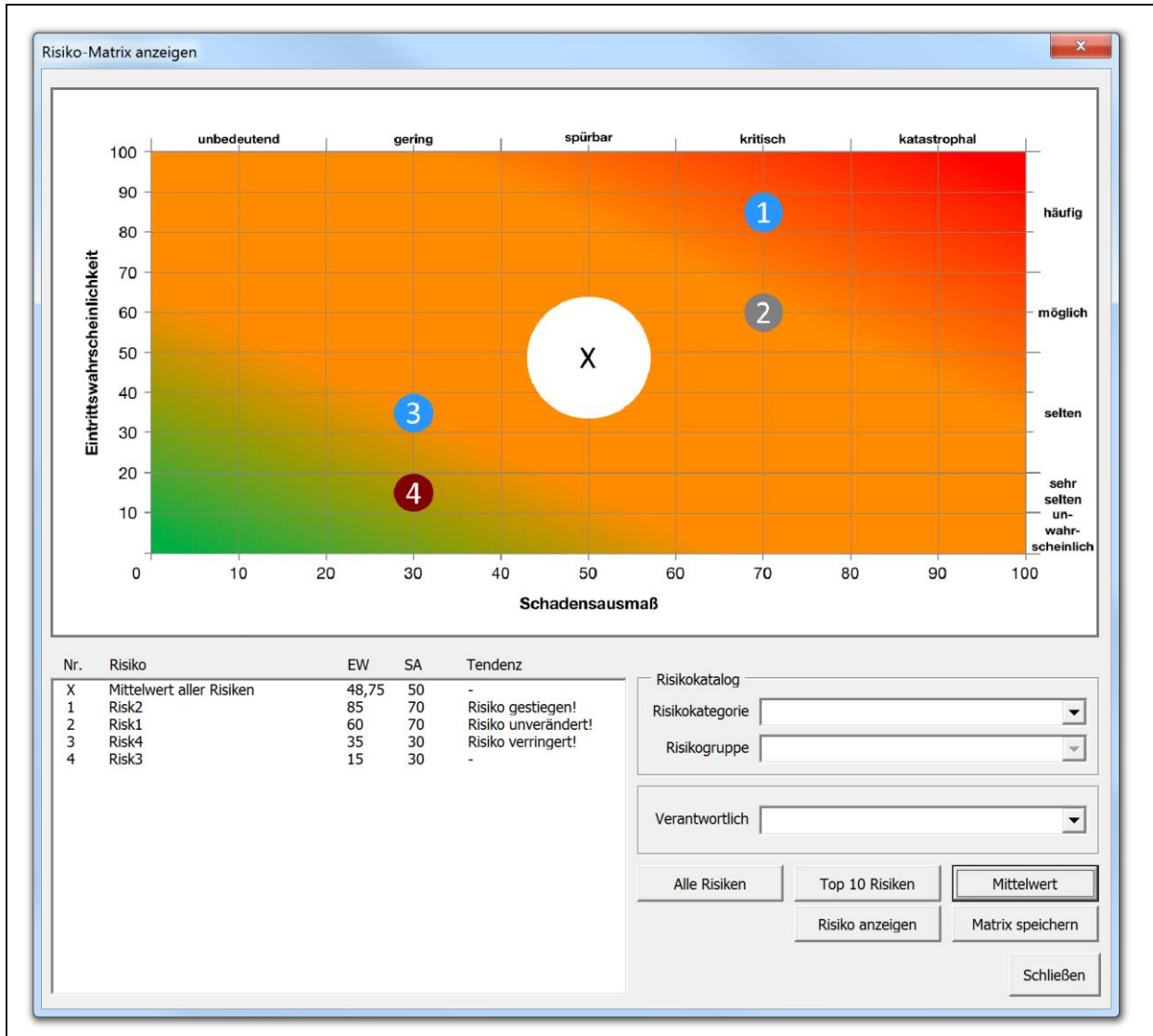


Figure 41: Risk management tool – risk matrix

4 Practical example of ISO 9001 process description

The following chapter describes the procedure of the ISO 9001:2015 process description by means of a use case. It should help EFG and other companies to properly perform the risk management process in case new risks arise. Therefore, knowledge and expertise gained during this master thesis are applied in this use case. It is assumed that a risk management system is already in place and the company's risk manager as well as risk owners are familiar with their obligations and duties. Furthermore, the process stage of establishing the context is already completed. Figure 42 illustrates a simplified but for this use case sufficiently enough risk management process description, which fits to the developed RMT described in the previous chapter. The use case presented is fictitious but tries to get as close as possible to reality.

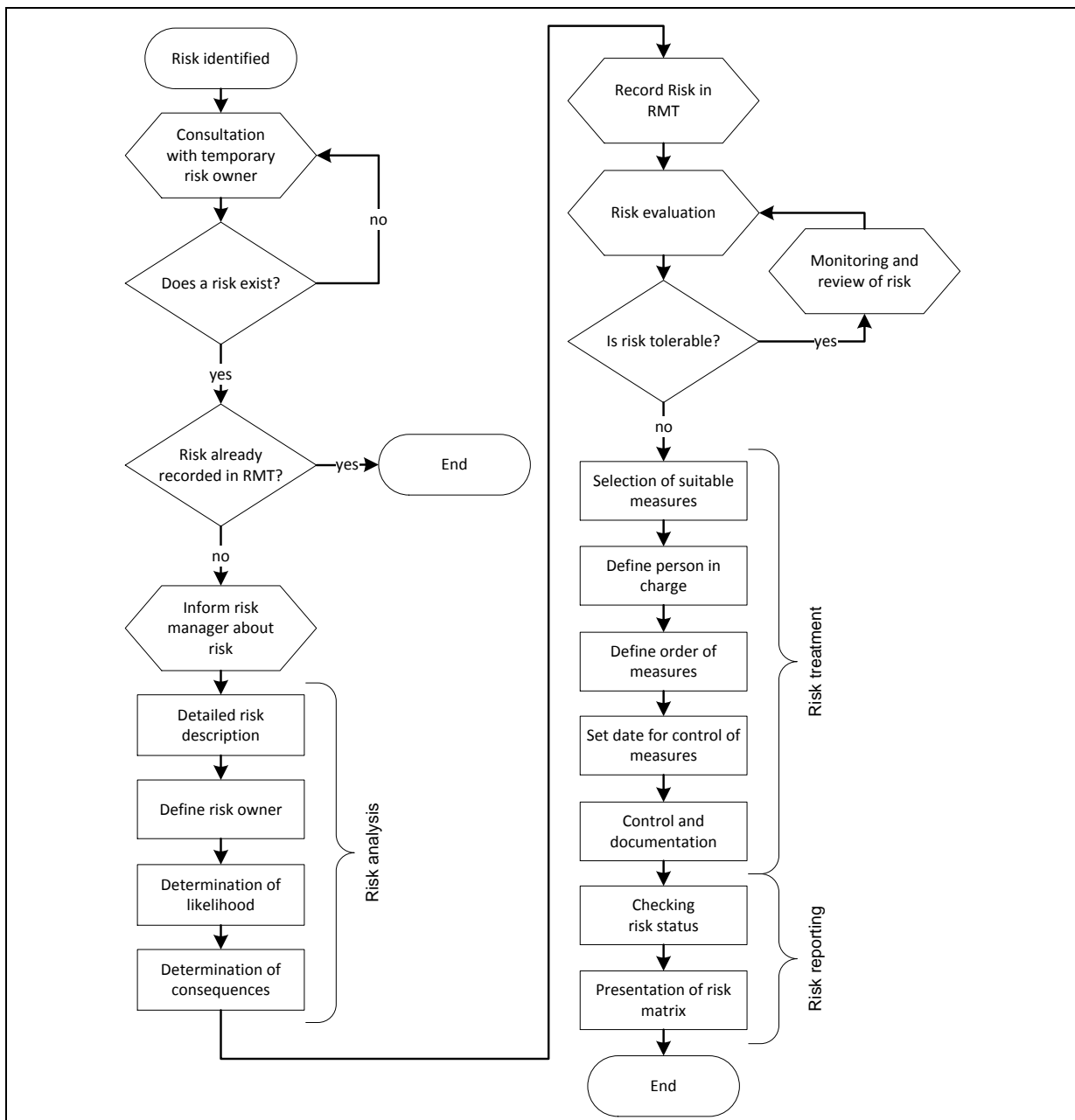


Figure 42: Simplified ISO 9001:2015 process description

The process description according to Figure 42 is initiated by an identified risk. In this use case a power plant operator passes her/his power plant by chance and notices unusual noises. Upon closer inspection of turbine housing and monitoring screen she/he realizes a breakdown of the Pelton turbine and immediately activates the kill switch in order to prevent something worse from happening.

After a few phone calls EFG’s management visits the power plant to get a first overview. At a first glance it seems like a bearing failure of the rotor. As a result of this bearing failure the rotor was damaged due to vibrations and imbalance. In consultation with management, project manager and power plant operator they decide to disassemble the damaged Pelton turbine and transport it into EFG’s headquarters. In the meantime, the risk manager checks the RMT for similar breakdowns. As this is happening for the first time, records concerning similar situations are not listed in the tool.

For the risk analysis a task force is appointed, consisting of top management, risk manager, quality manager, project manager and construction. During this process step the Pelton turbine is disassembled into their components in order to investigate causes of failure. Quality manager, project manager and construction are part of this investigation team. The appears from construction plans show that this power plant is equipped with an automatic lubrication system as well as a monitoring system, which should shut down the plant in case of an emergency. Disassembling reveals a partially destroyed rotor and turbine housing. This results from the totally destroyed bearings, which caused vibrations and imbalance to the rotor. For this reason the rotor tumbled and grazed the turbine housing. After further investigations the task force detects a lack of sufficient lubrication inside the bearings. It was caused by a broken oil pump; and unfortunately the rotation sensor of the oil pump of the monitoring system failed, too. In the course of the risk analysis likelihood and consequences within the RMT have to be defined with the help of the risk assessment template. Upon consultation with the task force the EFG’s risk manager selects unlikely and catastrophic risk criteria from for qualitative ones in order to enter the risk in the RMT.

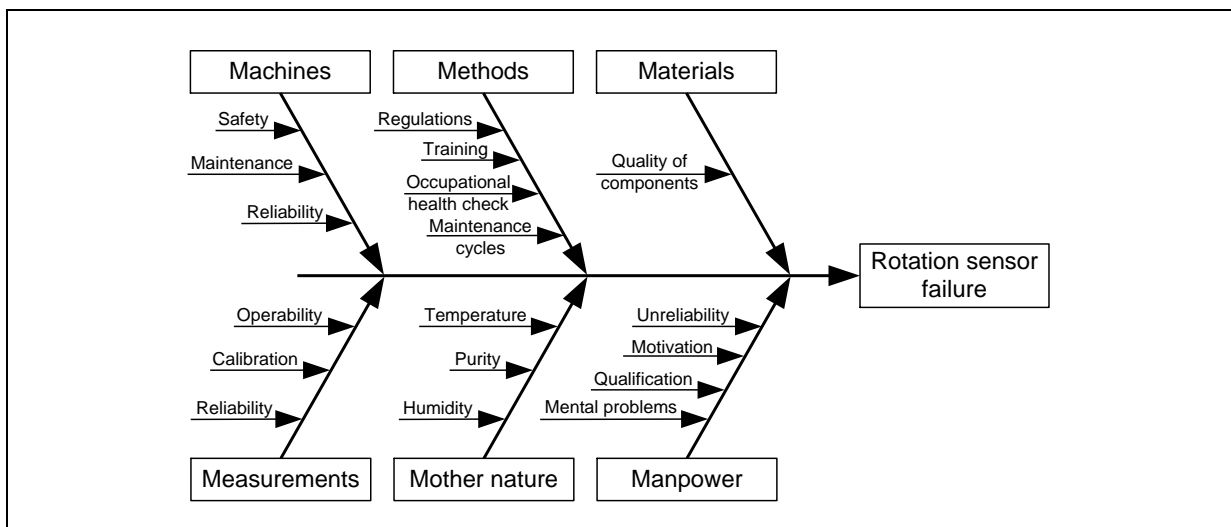


Figure 43: Ishikawa diagram for a rotation sensor failure

Since the beginning of the event EFG's task force applied the cause-and-effect analysis described in chapter 2.3.2.6. This scenario analysis is, according to Table 13, suitable throughout the whole risk management process. The outcome is illustrated in Figure 43. Based on this analysis they narrowed down the cause to a quality issue of the rotation sensor. The starting point of this event was the broken rotation sensor which was not able to detect the failure of the oil pump. This consequently caused the bearing failure and the demolished rotor. The task force decided not to tolerate that risk concerning quality problems of purchased components and initiated the risk treatment process phase.

During risk treatment measures, persons in charge and control dates were set. The task force agreed upon it as a first measure to consult the company, which delivered the monitoring system in order to check if that failure was common. In the meantime, the active risk treatment strategy of risk diversification can be applied by searching for subcontractors with equivalent monitoring systems. Quality manager and procurement are in charge of these measures and are responsible for meeting set deadlines. Failure safety can be increased with the active risk treatment strategy of risk minimisation by monitoring the lubrication flow in lubrication pipes with a redundant monitoring system. On the one hand the lubrication flow is monitored with the general monitoring system and on the other hand a visual independent monitoring system can be installed.

Risk reporting is the last phase of the ISO 9001:2015 process description. Earlier phases are applied for each single occurring risk. This phase is decoupled from previous phases and takes place once or twice a year depending on the company's necessity. During this meeting each risk owner presents her/his risks to the rest by means of the RMT. Therefore, she/he can use the function of showing risks depending on the respective risk owner in the RMT. Each risk owner presents her/his risks starting from the upper right to the lower left of the risk matrix. This approach ensures at least the treatment of important risks. By means of the status update risk manager and other risk owners should achieve the same level of knowledge.

5 Summary and outlook

Risk management in practise is often seen as an unnecessary, complex and bureaucratic effort. In reality it is a core task of the management and it should be a matter of concern that employees within the company understand the necessity of risk management. As described in this master thesis, several legal standards which often result from various crises, require risk management instruments for establishing and maintaining a sustainable company. For example, ISO 9001 gives certified members a three-year transition period for implementing a risk management in their companies required by the new revision. Most standards do not provide specific risk implementation plans, they offer guidance to companies implementing risk management systems according to their needs instead. Companies have to take risks in order to compete with competitors and be successful. The outcome of taking risks can either be positive or negative. In order to prevent or minimise negative risks, the risk management provides necessary tools and methods.

The intention of this master thesis is to give a detailed description of *ONR 4900x:2014* series in order to provide EFG with the knowledge to perform a risk management. Therefore, the first chapter briefly explains each risk management process step as well as EFG's history. The second chapter starts with an explanation of basic risk management terms to enhance the understanding of risk management. Afterwards voluntary and mandatory legal requirements are described. Besides *ONR 4900x:2014* series, interesting laws and standards for EFG are *aGmbHG*, *aUGB*, ISO 9001 and ACCG with regard to their provisions of reporting obligations and obligations of the top management. The last sub chapter is about the risk management process according to *ONR 4900x:2014* series. This contains a detailed literature research as well as recommendations concerning practical implementation possibilities for EFG. Furthermore, suitable risk evaluation methods for EFG are described. The third chapter explains the usage of the developed risk management tool, which is based on knowledge gained during literature research. Functionality and screens are described for users in detail. The fourth chapter shows an application example of the developed process description for ISO 9001:2015. It simulates the identification of a risk and passes through the established process description in order to give guidance to EFG's risk manager and risk owners for future arising risks.

This master thesis is the foundation for establishing a risk culture within EFG and increases risk awareness of employees. Their early involvement during all process stages is meant as an initial spark for establishing a risk culture. EFG's top management and risk manager have to be confident and stand behind the risk management approach in order to convince employees from all different hierarchical levels about arising risk and possibilities enabled by risk management. In today's world a working and efficient risk management as well as a lived risk culture within a company evolve to the key success factors of companies.

References

ARNDT, K.: *Arbeitswissenschaft*, in: BÖGE, A. (ed.): *Handbuch Maschinenbau*, Wiesbaden 2015, p. S24-S70

AS/NZS 4360:2004 – Risk management

AUSTRIAN CODE OF CORPORATE GOVERNANCE – as amended in January 2015

AUSTRIAN FEDERAL MINISTRY OF FINANCE: Solvency II, <https://english.bmf.gv.at/financial-sector/solvency-II.html>, accessed: 29.05.2015, status: 2015

AUSTRIAN FINANCIAL MARKET AUTHORITY: Basel III, <https://www.fma.gv.at/de/sonderthemen/basel-iii.html>, accessed: 29.05.2015, status: 22.01.2015

BARRIGA F.: Industry Report, in: The Economist Intelligence Unit Limited, -. Vol., 6/2014

BECKER, W.; EBNER, R.; FISCHER-PETERSOHN, D.; RUHNAU, M.: *Projektrisikomanagement im Mittelstand*, 1st Edition, Wiesbaden 2015

BÖCKMANN, D.; HENDRICKS, F.: *Risikomanagement – Schrittweise Integration von Risikomanagement-Systemen in den Planungs- und Managementzyklus*, in: ControllerNews, 10. Vol., 5/2006, p. 164-166

BOUTELLIER, R.; FISCHER, A.; PFUHLSTEIN, H.: *Das Risikomanagement an die Unternehmensgrösse anpassen*, in: io new management, 75. Vol., 11/2006, p. 26-29

BOUTELLIER, R.; MONTAGNE, E.; BARODTE, B.: *Die Risiken für KMU – und wie sie damit umgehen können*, in: io new management, 76. Vol., 11/2007, p. 43-46

BRÜHWILER, B.; ROMEIKE, F.: *Praxisleitfaden Risikomanagement*, 1st Edition, Berlin 2010

BRÜHWILER, B.: *Risikomanagement als Führungsaufgabe*, 3rd Edition, Bern, Stuttgart, Wien 2011

BRÜHWILER, B.: *Risikomanagement nach ISO 31000 und ONR 49000*, 2nd Edition, Berlin 2012

BUNDESMINISTERIUM DER FINANZEN [a]: Basel II, <http://www.bundesfinanzministerium.De/Web/DE/Service/Glossar/Functions/glossar.html?lv2=84618&lv3=175876#lv3>, accessed: 29.05.2015, status: 2015

BUNDESMINISTERIUM DER FINANZEN [b]: Basel III, <http://www.bundesfinanzministerium.De/Web/DE/Service/Glossar/Functions/glossar.html?lv2=84618&lv3=169496&lv3=169496&lv2=84618#doc169496bodyText1>, accessed: 29.05.2015, status: 2015

DAHMEN, J.: *Risiken systematisch identifizieren und bewerten*, in: *io new management*, 72. Vol., 9/2003, p. 34-42

DENK, R.; EXNER-MERKELT, K.; RUTHNER, R.: *Corporate Risk Management*, 2nd Edition, Wien 2008

DENK, R.; EXNER-MERKELT, K.; RUTHNER, R.: *Risikomanagement im Unternehmen – Ein Überblick*, in: *WIRTSCHAFT UND MANAGEMENT*, 3. Vol., 4/2006, p. 9-39

DIEDERICHS, M.: *Risikomanagement und Risikocontrolling*, 2nd Edition, München 2010

EBERT, C.: *Risikomanagement kompakt*, 2nd Edition, Berlin, Heidelberg 2013

ELLER, R.; HEINRICH, M.; PERROT, R.: *Kompaktwissen Risikomanagement*, 1st Edition, Wiesbaden 2010

ENERGIE-CONTROL AUSTRIA: *Ökostrom-Einspeisemengen und Vergütungen*, <http://www.e-control.at/de/statistic/oeko-energie/oekostrommengen>, accessed: 15.06.2015, status: 2009

ERBEN, R.; ROMEIKE, F.: *Risikoreporting mit Unterstützung von Risk Management-Informationssystemen (RMIS)*, in: ROMEIKE, F.; FINKE, R. (eds.): *Erfolgsfaktor Risiko-Management*, Wiesbaden 2003, p. 275-297

EUROPEAN COMMISSION [a]: Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361>, accessed: 19.05.2015, status: 20.05.2003

EUROPEAN COMMISSION [b]: The new SME definition – User guide and model declaration, http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_en.pdf, accessed: 19.05.2015, status: 29.03.2005

EUROPEAN COMMISSION [c]: What is an SME?, http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm, accessed: 13.05.2015, status: -

GASTL, R.: *Kontinuierliche Verbesserung im Umweltmanagement*, 1st Edition, Zürich 2005

GLEISSNER, W.: *Grundlagen des Risikomanagements*, 1st Edition, München 2008

HENSCHER, T.: *Erfolgreiches Risikomanagement im Mittelstand*, 1st Edition, Berlin 2010

HOYLE, D.: *ISO 9000 quality systems handbook*, 6th Edition, Amsterdam; Boston; London 2009

ILLETSCSKO, S.; KÄFER, R.; SPATZIERER, K.: *Risikomanagement*, 1st Edition, München 2014

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *ISO 9001 Quality Management Systems Revision*, http://www.iso.org/iso/home/standards/management-standards/iso_9000/iso9001_revision.htm, accessed: 01.06.2015, status: -

ISO 31000:2009 – Risk management — Principles and guidelines

ISO Guide 73:2009 – Risk management – Vocabulary

KOCH, S.: *Einführung in das Management von Geschäftsprozessen*, 2nd Edition, Berlin, Heidelberg 2015

KROLAK, T.; MORZFELD, K.; REMMEN, J.: *Financial Covenants als Instrument der Krisenfrüherkennung und der normierten Krisenbewältigung*, in: *Der Betrieb*, 62. Vol., 27/2009, p. 1417-1422

LINDEMANN, U.; MEIWALD, T.; PETERMANN, M.; SCHENKL, S.: *Know-how-Schutz im Wettbewerb*, 1st Edition, Berlin, Heidelberg 2012

MOTT, B.: *Organisatorische Gestaltung von Risiko-Managementsystemen*, in: GLEISSNER, W. (ed.): *Wertorientiertes Risiko-Management für Industrie und Handel*, Wiesbaden 2001, p. 199-232

NORELL, E.; MONTAGNE, E.; THOMIK, M.; BOUTELLIER, R.; ETH ZÜRICH: *RISIKEN einfacher abschätzen und vorbeugen*, in: *IM+io Fachzeitschrift für Innovation, Organisation und Management*, -. Vol., 03/2014, p. 36-41

NORTH, K.; BRANDNER, A.; STEININGER, T.: *Die neue ISO 9001:2015 – Wissensmanagement wird Pflicht!*, in: *Wissensmanagement*, 17. Vol., 2/2015, p. 20-23

OFFENSIVE MITTELSTAND: *Praxishilfen*, <http://www.offensive-mittelstand.de/praxishilfen/>, accessed: 31.07.2015, status: -

ÖNORM S 2410:2010 – Chancen- und Risikomanagement – Analyse und Maßnahmen zur Sicherung der Ziele von Organisationen

ONR 49000:2014 – Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen

ONR 49001:2014 – Risikomanagement für Organisationen und Systeme – Risikomanagement

ONR 49002-2:2014 – Risikomanagement für Organisationen und Systeme – Teil 2: Leitfaden für die Methoden der Risikobeurteilung

ONR 49002-2:2014 – Risikomanagement für Organisationen und Systeme – Teil 2: Leitfaden für die Methoden der Risikobeurteilung

ORTH, R.; KARCHER, P.: *Der Faktor Wissen: Die ISO 9001 beschreitet neue Wege*, in: *Wissensmanagement*, 17. Vol., 2/2015, p. 27-29

ORTH, R.: *Wissensmanagement mit Wiki-Systemen*, in: MERTINS, K.; SEIDEL, H. (eds.): *Wissensmanagement im Mittelstand*, Berlin 2009, p. 75-81

ÖVE/ÖNORM EN 31010:2010 – Risikomanagement Verfahren zur Risikobeurteilung

REINEMANN, H.; BÖSCHEN, V.: *Corporate Governance – Werte schaffen und bewahren*, http://www.deloitte.com/assets/Dcom-Germany/Local%20Assets/Documents/de_R_Corporate_Governance_D_240108.pdf, accessed: 11.02.2015, status: 2008

ROMEIKE, F. [a]: *Risikoidentifikation und Risikokategorien*, in: ROMEIKE, F.; FINKE, R. (eds.): *Erfolgsfaktor Risiko-Management*, Wiesbaden 2003, p. 165-180

ROMEIKE, F. [b]: *Bewertung und Aggregation von Risiken*, in: ROMEIKE, F.; FINKE, R. (eds.): *Erfolgsfaktor Risiko-Management*, Wiesbaden 2003, p. 183-198

ROMEIKE, F. [c]: *Der Prozess der Risikosteuerung und -kontrolle*, in: ROMEIKE, F.; FINKE, R. (eds.): *Erfolgsfaktor Risiko-Management*, Wiesbaden 2003, p. 235-243

ROMEIKE, F.: *Lexikon Risiko-Management*, 1st Edition, Weinheim 2004

SARBANES-OXLEY ACT: SOX, <http://www.sec.gov/about/laws/soa2002.pdf>, accessed: 15.08.2015, status: 30.07.2002

SCHEEL, O.; FRANK, B.: *Wachsende Komplexität treibt Risiken*, in: KNOLL, T.; DEGEN, B. (eds.): *Praxis des Risikomanagements*, Stuttgart 2014, p. 33-56

SCHWAB, A.: *Managementwissen*, 1st Edition, Berlin, Heidelberg 2010

SEIDEL, U.: *Risikomanagement*, 1st Edition, Kissing 2005

SOX-ONLINE: Sarbanes-Oxley Essential Information, <http://www.sox-online.com/basics.html>, accessed: 29.05.2015, status: 2012

TÜF SÜD AMERICA: ISO 9001:2015 Revision Factsheet, <http://www.tuv-sud-america.com/uploads/images/1405633108397773521586/iso-9001-2015-revision-factsheet-us.pdf>, accessed: 01.06.2015, status: 2014

ULRICH, A.: *Wissens- & Qualitätsmanagement mit Wikis vereinen*, in: *Wissensmanagement*, 17. Vol., 2/2015, p. 32-33

VOIGT, S.: *Selbsterklärende Ordnerstrukturen*, in: MERTINS, K.; SEIDEL, H. (eds.): *Wissensmanagement im Mittelstand*, Berlin 2009, p. 69-74

WANNENWETSCH, H.: *Integrierte Materialwirtschaft und Logistik*, 3rd Edition, Berlin 2007

WEIßENSTEINER, C.: *Konzeption und Implementierung eines Risikomanagementsystems*, diploma thesis, Graz 2007

WESTKÄMPER, E.: *Fertigungs- und Fabrikbetrieb*, in: GROTE, K.; FELDHUSEN, J. (eds.): *Dubbel*, Berlin 2014, p. S124-S145

WIRTSCHAFTSKAMMER ÖSTERREICH: *Ergebnisse der Leistungs- und Strukturstatistik 2012 nach Beschäftigtengrößengruppen*, http://wko.at/Statistik/kmu/LSE_BbisN_S95.pdf, accessed: 26.06.2015, status: 2012

WIRTSCHAFTSKAMMER ÖSTERREICH: *Klein- und Mittelbetriebe in Österreich – KMU-Definition*, https://www.wko.at/Content.Node/Interessenvertretung/ZahlenDatenFakten/KMU_Definition.html#MA, accessed: 19.05.2015, status: 19.12.2013

WIRTSCHAFTSKAMMER ÖSTERREICH: *KMU-Daten für Österreich*, <http://wko.at/Statistik/kmu/WKO-BeschStatK.pdf>, accessed: 26.06.2015, status: 2014

List of Figures

Figure 1: Area of investigation	3
Figure 2: Risk management system according to <i>ONR 49000:2014</i> and <i>ÖVE/ÖNORM EN 31010:2010</i>	4
Figure 3: Chance and risk management system according to <i>ÖNORM S 2410:2010</i>	5
Figure 4: Sources of risks	10
Figure 5: Overview of institutional frameworks	13
Figure 6: Legislative initiatives with effect on risk management	13
Figure 7: Structure of <i>ONR 4900x:2014</i> series	20
Figure 8: The PDCA cycle	21
Figure 9: Top-down and bottom-up approach	24
Figure 10: Eco-electricity remuneration of small hydro generating stations	25
Figure 11: Risk criteria context at EFG	30
Figure 12: Circles of influence and risk sources	31
Figure 13: Risk identification methods	32
Figure 14: Hierarchical structure of EFG's risk catalogue	33
Figure 15: Risk matrix with tolerance limit and tolerance ranges	34
Figure 16: Documentation approach of risk identification results	36
Figure 17: EFG's risk matrix with main risks	38
Figure 18: Time structure for work order time	42
Figure 19: Risk evaluation methods	44
Figure 20: Design FMEA for a Pelton turbine	47
Figure 21: Ishikawa diagram	48
Figure 22: Fault and event tree analysis	49
Figure 23: Overview of risk treatment strategies	50
Figure 24: Risk treatment through risk avoidance, minimisation and diversification	51
Figure 25: Risk treatment options	53
Figure 26: Level of information of decision makers	55
Figure 27: Expansion of risk management to project risk management	57
Figure 28: Emergency, crisis and continuity management	58
Figure 29: Context of risk and crisis management	59
Figure 30: Chain of commands in risk management	60

Figure 31: Risk management as part of top management and executive department.....	64
Figure 32: Risk management as line function and within different business areas.....	65
Figure 33: ÖNORM EN ISO 9000 with implemented risk management process.....	65
Figure 34: Risk management implementation at EFG.....	66
Figure 35: Risk management tool – start.....	67
Figure 36: Risk management tool – settings.....	68
Figure 37: Risk management tool – search, add, edit, display and update risks.....	69
Figure 38: Legend of demand for action and risk tendency.....	70
Figure 39: Risk management tool – add new risk.....	70
Figure 40: Risk management tool – display risk.....	71
Figure 41: Risk management tool – risk matrix.....	72
Figure 42: Simplified ISO 9001:2015 process description.....	73
Figure 43: Ishikawa diagram for a rotation sensor failure.....	74
Figure 44: Risk assessment template (1).....	90
Figure 45: Risk assessment template (2).....	91
Figure 46: Risk management tool – edit risks.....	92
Figure 47: Risk management tool – update risk.....	93
Figure 48: ISO 9001 process description (1).....	94
Figure 49: ISO 9001 process description (2).....	95
Figure 50: ISO 9001 process description (3).....	96
Figure 51: ISO 9001 process description (4).....	97

List of Tables

Table 1: Definition of SMEs [m...million].....	11
Table 2: Important paragraphs of a <i>UGB</i>	14
Table 3: Important paragraphs of a <i>AktG</i> and a <i>GmbHG</i>	16
Table 4: Important paragraphs of <i>KonTraG</i>	17
Table 5: Important paragraphs of <i>ACCG</i>	18
Table 6: Risk criteria – likelihood (high frequency).....	27
Table 7: General risk criteria – consequences.....	28
Table 8: Risk criteria context – consequences.....	29
Table 9: Hierarchical structure of the risk catalogue.....	32
Table 10: Mutual risk dependencies.....	35
Table 11: Identified main risks at EFG.....	37
Table 12: Level of detail of risk management.....	45
Table 13: Summary of methods for the risk management process.....	89

List of Abbreviations

<i>(d)RGBI</i>	<i>(deutsches) Reichsgesetzblatt</i>
a	Austrian
ACCG	Austrian Code of Corporate Governance
AG	<i>Aktiengesellschaft</i>
<i>AktG</i>	<i>Aktiengesetz</i>
AS/NZS	Australian/New Zealand Standard
AWU	Annual Work Unit
BA	Business area
BCBS	Basel Committee on Banking Supervision
BGBI	<i>Bundesgesetzblatt</i>
C	Consequences
CAD	Computer aided design
CAM	Computer-aided manufacturing
CE	Comply or explain
CNC	Computerized numerical control
D	Detection
EBIT	Earnings before interest and taxes
EC	European Commission
EFG	<i>Turbinen- und Kraftwerksanlagenbau EFG – Energieforschungs- und Entwicklungsgesellschaft m.b.H. & Co. KG.</i>
<i>EN</i>	<i>Europäische Norm</i>
EU	European Union
FMEA	Failure mode and effects analysis
g	German
<i>Ges.m.b.H. & Co. KG</i>	<i>Gesellschaft mit beschränkter Haftung & Compagnie Kommanditgesellschaft</i>
<i>GmbH</i>	<i>Gesellschaft mit beschränkter Haftung</i>
<i>GmbHG</i>	<i>Gesellschaft mit beschränkter Haftung – Gesetz</i>
<i>HGB</i>	<i>Handelsgesetzbuch</i>
i	Running index from 1, ..., I
IAS	International Accounting Standards
IFRS	International Financial Reporting Standards
IRÄG	<i>Insolvenzrechtsänderungsgesetz</i>

ISO	International Organization for Standardization
IT	Information technology
j	Running index from 1, ..., J
<i>KonTraG</i>	<i>Gesetz zur Kontrolle und Transparenz im Unternehmensbereich</i>
kWh	Kilowatt hour
L	Likelihood
LR	Legal requirement
m	Million
MW	Megawatt
<i>OeMAG</i>	Green power settlement agency
<i>ÖNORM</i>	<i>Österreichische Norm</i>
<i>ONR</i>	<i>Österreichisches Regelwerk</i>
<i>ÖSET-VO 2012</i>	<i>Ökostrom-Einspeisetarifverordnung 2012</i>
<i>ÖSG 2012</i>	Austrian Green Electricity Law 2012
<i>ÖVE</i>	<i>Österreichischer Verband für Elektrotechnik</i>
P	Probability
PDCA	Plan-Do-Check-Act
PDF	Portable Document Format
R	Risk
<i>RÄG</i>	<i>Rechnungslegungsänderungsgesetz</i>
REC	Recommendation
REFA	<i>Verband für Arbeitsgestaltung, Betriebsorganisation und Unternehmensentwicklung</i>
RM	Risk manager
RMGT	Risk management
RMT	Risk management tool
RPN	Risk priority number
RRP	Risk responsible person
S	<i>Sonstige Normengebiete</i>
SEV	Severity
SEC	Securities and Exchange Commission
SME	Small and medium-sized enterprises
SOX	Sarbanes-Oxley Act
SWOT	Strengths, weaknesses, opportunities, threats analysis
TM	Top management

U.S.	United States
UGB	<i>Unternehmensgesetzbuch</i>
URÄG	<i>Unternehmensrechts-Änderungsgesetz</i>
URG	<i>Unternehmensreorganisationsgesetz</i>
US-GAAP	United States Generally Accepted Accounting Principles

List of Translations

German terms

(deutsches) Reichsgesetzblatt
Abwicklungsstelle für Ökostrom AG
Aktiengesellschaft
Aktiengesetz
Bundesgesetzblatt
Geschäftsführung
Gesellschaft mit beschränkter Haftung
Gesellschaft mit beschränkter Haftung - Gesetz
Gesellschaft mit beschränkter Haftung & Compagnie Kommanditgesellschaft
Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
Handelsgesetzbuch
Insolvenzrechtsänderungsgesetz
Kapitalgesellschaft
Ökostromgesetz 2012
Prüfungsausschuss
Rechnungslegungsänderungsgesetz
Risikoeigner
Risikoverantwortlicher
Unternehmensgesetzbuch
Unternehmensrechts-Änderungsgesetz
Unternehmensreorganisationsgesetz

English Terms

(German) Imperial Law Gazette
 Green power settlement agent
 Public Limited Company
 Law on Public Limited Company
 Federal Law Gazette
 Top management
 Austrian Limited Liability Company
 Law on Limited Liability Company
 Limited Liability Company & Limited Partnership
 Corporate Sector Supervision and Transparency Act
 Commercial Code
 Insolvency Law Reform Act
 Company Limited by Shares
 Austrian Green Electricity Law 2012
 Audit committee
 Law on Changes in Accounting
 Risk owner
 Risk responsible person
 Austrian Business Code
 Company Law Amendment Act
 Business Reorganisation Law

List of Symbols

§	Article
=	Equal sign
€	Euro
%	Percentage

List of Appendices

Appendix 1: Risk management process methods	89
Appendix 2: Risk assessment template.....	90
Appendix 3: Risk management tool.....	92
Appendix 4: ISO 9001 process description	94

Appendix 1: Risk management process methods

Process risk management					
Method	Identification	Assessment			Evaluation
		Consequence	Likelihood	Level of risk	
Brainstorming	+++	+	+		+
Delphi	++	++	++		++
World Café	+++	+	+		
Citizen conference	+++	++	+		+
Failure analysis	++	+	+		+++
London-protocol	+++	+			+++
Fault and event tree analysis		++	+++	+	++
Scenario analysis	+++	+++	++	++	+++
CIRS (Critical Incident Reporting System)	+++		+		++
CBRM (Change Based Risk Management)	+++	+		++	
FMEA (Failure Mode and Effects Analysis)	+++	++	++	+	+++
Hazard analysis	++	+++	++	++	+++
HAZOP (Hazard and Operability Study)	+++	+++	++	+	+++
HACCP (Hazard and Critical Control Point)	++	++			+++
Standard deviation		++	+++	++	
Confidence interval		++	+++	++	
Monte Carlo simulation	+	++	+++	++	
+ not applicable ++ applicable +++ strongly applicable					

Table 13: Summary of methods for the risk management process²⁷⁵

²⁷⁵ Cf. ONR 49002-2:2014, p. 5.

Appendix 2: Risk assessment template



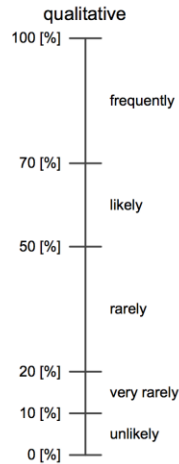
	TURBINEN- UND KRAFTWERKSANLAGENBAU EFG Energieforschungs- und Entwicklungsgesellschaft m.b.H. & Co. KG.																															
<h3>Risk assessment template</h3>																																
Likelihood qualitative																																
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%;">Level</th> <th>Frequency</th> </tr> </thead> <tbody> <tr> <td>Frequently</td> <td>once every month or more often</td> </tr> <tr> <td>Likely</td> <td>between once every month or once every quarter</td> </tr> <tr> <td>Rarely</td> <td>between once every quarter or once every year</td> </tr> <tr> <td>Very rarely</td> <td>between once every year or once every three years</td> </tr> <tr> <td>Unlikely</td> <td>more seldom than once every three years</td> </tr> </tbody> </table>	Level	Frequency	Frequently	once every month or more often	Likely	between once every month or once every quarter	Rarely	between once every quarter or once every year	Very rarely	between once every year or once every three years	Unlikely	more seldom than once every three years																				
Level	Frequency																															
Frequently	once every month or more often																															
Likely	between once every month or once every quarter																															
Rarely	between once every quarter or once every year																															
Very rarely	between once every year or once every three years																															
Unlikely	more seldom than once every three years																															
Consequence qualitative																																
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">Level</th> <th style="width: 20%;">General</th> <th style="width: 20%;">Health</th> <th style="width: 20%;">Image</th> <th style="width: 25%;">Finances</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Insignificant</td> <td>Due to company's size the risk is neglectable; customers are barely affected.</td> <td>Personal damage with minor injuries and no loss of working hours.</td> <td>Occasionally complaints and reclamations.</td> <td>Financial loss is barely noticeable in the budget.</td> </tr> <tr> <td style="text-align: center;">Minor</td> <td>Risk creates disturbances and additional costs; single customers are unsatisfied.</td> <td>Personal damage with healable injuries and loss of working hours.</td> <td>Critical media reports lead to public emotions against activities, products and services.</td> <td>Financial loss leads to deviations from budget.</td> </tr> <tr> <td style="text-align: center;">Noticeable</td> <td>Risk harms performance. Single operational functions are affected; this results in delayed deliveries.</td> <td>Lightly and permanent damage to health; quality of living is affected.</td> <td>Criminal investigations with charges are initiated because of grossly omission, gross negligence or violations against laws and values.</td> <td>Financial results are visibly affected; revenue and liquidity are affected.</td> </tr> <tr> <td style="text-align: center;">Critical</td> <td>The company's capability is affected; customer losses increase.</td> <td>Severe and permanent damage to health; quality of living dramatically decreases.</td> <td>Criminal investigations lead to long-range and widely loss of trust which can only be compensated with large effort.</td> <td>Financial result gets permanently affected; damage increases up to an annual result; tight liquidity.</td> </tr> <tr> <td style="text-align: center;">Catastrophic</td> <td>Risk affects the whole company; market position gets lost; company's continuation is questioned.</td> <td>Personal damage with lethal consequence or serious invalidity.</td> <td>Heavy violations against safety regulations and retirement of responsible people; it will be hard to recover from the damage.</td> <td>Financial consequences of the risk exceed the annual result and leads to losses of equity; threat of bankruptcy.</td> </tr> </tbody> </table>	Level	General	Health	Image	Finances	Insignificant	Due to company's size the risk is neglectable; customers are barely affected.	Personal damage with minor injuries and no loss of working hours.	Occasionally complaints and reclamations.	Financial loss is barely noticeable in the budget.	Minor	Risk creates disturbances and additional costs; single customers are unsatisfied.	Personal damage with healable injuries and loss of working hours.	Critical media reports lead to public emotions against activities, products and services.	Financial loss leads to deviations from budget.	Noticeable	Risk harms performance. Single operational functions are affected; this results in delayed deliveries.	Lightly and permanent damage to health; quality of living is affected.	Criminal investigations with charges are initiated because of grossly omission, gross negligence or violations against laws and values.	Financial results are visibly affected; revenue and liquidity are affected.	Critical	The company's capability is affected; customer losses increase.	Severe and permanent damage to health; quality of living dramatically decreases.	Criminal investigations lead to long-range and widely loss of trust which can only be compensated with large effort.	Financial result gets permanently affected; damage increases up to an annual result; tight liquidity.	Catastrophic	Risk affects the whole company; market position gets lost; company's continuation is questioned.	Personal damage with lethal consequence or serious invalidity.	Heavy violations against safety regulations and retirement of responsible people; it will be hard to recover from the damage.	Financial consequences of the risk exceed the annual result and leads to losses of equity; threat of bankruptcy.		
Level	General	Health	Image	Finances																												
Insignificant	Due to company's size the risk is neglectable; customers are barely affected.	Personal damage with minor injuries and no loss of working hours.	Occasionally complaints and reclamations.	Financial loss is barely noticeable in the budget.																												
Minor	Risk creates disturbances and additional costs; single customers are unsatisfied.	Personal damage with healable injuries and loss of working hours.	Critical media reports lead to public emotions against activities, products and services.	Financial loss leads to deviations from budget.																												
Noticeable	Risk harms performance. Single operational functions are affected; this results in delayed deliveries.	Lightly and permanent damage to health; quality of living is affected.	Criminal investigations with charges are initiated because of grossly omission, gross negligence or violations against laws and values.	Financial results are visibly affected; revenue and liquidity are affected.																												
Critical	The company's capability is affected; customer losses increase.	Severe and permanent damage to health; quality of living dramatically decreases.	Criminal investigations lead to long-range and widely loss of trust which can only be compensated with large effort.	Financial result gets permanently affected; damage increases up to an annual result; tight liquidity.																												
Catastrophic	Risk affects the whole company; market position gets lost; company's continuation is questioned.	Personal damage with lethal consequence or serious invalidity.	Heavy violations against safety regulations and retirement of responsible people; it will be hard to recover from the damage.	Financial consequences of the risk exceed the annual result and leads to losses of equity; threat of bankruptcy.																												
1 of 2																																

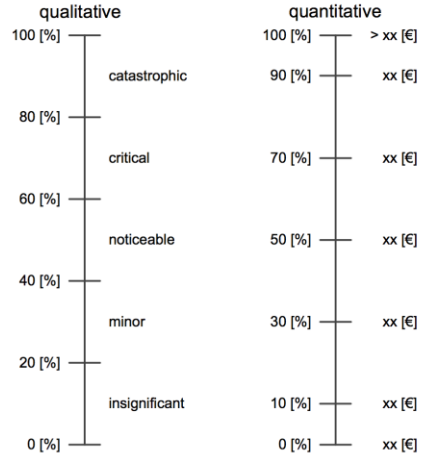
Figure 44: Risk assessment template (1)



Likelihood



Consequences



EBIT

Likelihood		Consequence		
qualitative		qualitative		quantitative
	[%]		[%]	[€]
frequently	85	catastrophic	90	€ 0,00
likely	60	critical	70	€ 0,00
rarely	35	noticeable	50	€ 0,00
very rarely	15	minor	30	€ 0,00
unlikely	5	insignificant	10	€ 0,00

Legend

Input field



Figure 45: Risk assessment template (2)

Appendix 3: Risk management tool

The screenshot shows a software window titled "Risiko bearbeiten" (Edit Risk). The interface is organized into several sections:

- Identification:** "Erkannt am" (Discovered on) with a date picker, and "Erkannt durch" (Discovered by) with a dropdown menu.
- Risikokatalog (Risk Catalog):** Includes "Risikokategorie" (Risk category) and "Risikogruppe" (Risk group), both with dropdown menus.
- Risikobeschreibung (Risk Description):** Contains "Kurzbeschreibung" (Short description) and "Ausführliche Beschreibung" (Detailed description), each with a text input field.
- Verantwortlich (Responsible):** A dropdown menu and a button labeled "Neue Verantwortlichkeit" (New responsibility).
- Risikoursache (Risk Cause):** A text input field.
- Ursache-Wirkungs-Beziehung (Cause-Effect Relationship):** A text input field.
- Eintrittswahrscheinlichkeit (Occurrence Probability):** Radio buttons for "qualitativ" (qualitative) and "quantitativ" (quantitative), with a dropdown menu and an information icon. The unit is "[%]".
- Schadensausmaß (Extent of Damage):** Radio buttons for "qualitativ" and "quantitativ", with a dropdown menu and an information icon. The unit is "[€]".
- Eingeleitete Maßnahmen (Initiated Measures):** A text input field.
- Maßnahmenfortschritt (Measure Progress):** A dropdown menu with the unit "[%]".
- Handlungsbedarf (Action Required):** A radio button that is currently selected.
- Erfasst am (Recorded on):** A date picker.
- Revisionsintervall (Revision Interval):** A dropdown menu.
- Erfasst durch (Recorded by):** A dropdown menu.
- Buttons:** "Risiko archivieren" (Archive risk), "Speichern" (Save), and "Schließen" (Close).

Figure 46: Risk management tool – edit risks

The screenshot shows a software window titled "Risiko aktualisieren" (Update Risk). The window contains the following fields and controls:

- Erkannt am**: Text input field.
- Erkannt durch**: Text input field.
- Risikokatalog**: Section header.
- Risikokategorie**: Text input field.
- Risikogruppe**: Text input field.
- Eintrittswahrscheinlichkeit**: Section header with radio buttons for "qualitativ" and "quantitativ". The "quantitativ" option is selected, followed by a dropdown menu and an information icon (i), and a "[%]" label.
- Schadensausmaß**: Section header with radio buttons for "qualitativ" and "quantitativ". The "quantitativ" option is selected, followed by a dropdown menu and an information icon (i), and a "[€]" label.
- Risikobeschreibung**: Section header.
- Kurzbeschreibung**: Text input field.
- Ausführliche Beschreibung**: Text input field.
- Eingeleitete Maßnahmen**: Section header.
- Maßnahmenfortschritt**: Dropdown menu with a "[%]" label.
- Verantwortlich**: Text input field.
- Handlungsbedarf**: Radio button (selected).
- Erfasst am**: Date input field with a calendar icon.
- Revisionsintervall**: Dropdown menu.
- Erfasst durch**: Text input field.
- Risikoursache**: Text input field.
- Ursache-Wirkungs-Beziehung**: Text input field.
- Buttons**: "Letzte Revision", "Speichern", and "Schließen".

Figure 47: Risk management tool – update risk

Appendix 4: ISO 9001 process description

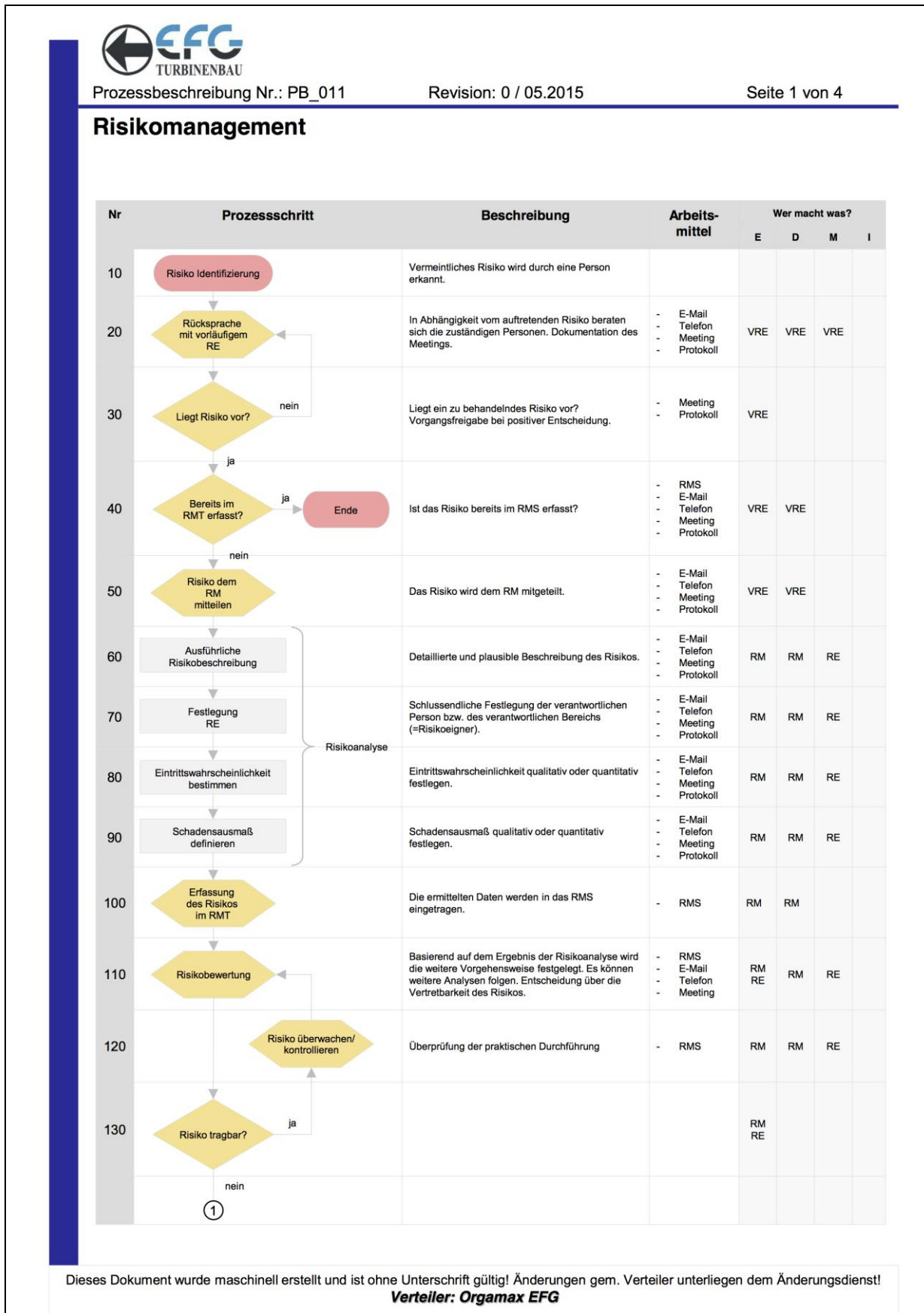


Figure 48: ISO 9001 process description (1)



Risikomanagement

Nr	Prozessschritt	Beschreibung	Arbeitsmittel	Wer macht was?			
				E	D	M	I
	①						
140	Auswahl geeigneter Maßnahmen	Auswahl geeigneter Maßnahmen bezogen auf deren Kosten und Nutzen.		RM	RM RE	RE	
150	Festlegung Umsetzungsverantwortlicher	Auswahl einer Person, die für die Umsetzung der gewählten Maßnahmen verantwortlich ist.	- RMS - Meeting	RM	RM RE	RE	
160	Festlegung Maßnahmenreihenfolge	Festlegung der Maßnahmenreihenfolge innerhalb des Maßnahmenplans.	- RMS	RM	RM RE	RE	
170	Termin für Maßnahmenkontrolle						
180	Kontrolle und Dokumentation	Fortlaufende Kontrollen und Dokumentation.	- RMS	RM	RM RE	RE	
190	Statusüberprüfung der Risiken	Hauptkontrolltermin für die Überprüfung sämtlicher Risiken in der Risiko Matrix (z.B.: halbjährlich).	- RMS	RM	RM RE	RE	
200	Präsentation der Risiko Matrix						
210	Ende						
220							
230							
240							
250							

Dieses Dokument wurde maschinell erstellt und ist ohne Unterschrift gültig! Änderungen gem. Verteiler unterliegen dem Änderungsdienst!

Verteiler: Orgamax EFG

Figure 49: ISO 9001 process description (2)



Prozessbeschreibung Nr.: PB_011

Revision: 0 / 05.2015

Seite 3 von 4

Risikomanagement

2. Begriffe und Abkürzungen:

Abkürzungen			
E	Entscheidungsverantwortung	I	wird informiert
D	Durchführungsverantwortung	M	Mitarbeit
()	bei Bedarf	↗	Risiko im Prozessschritt
GF	Geschäftsführer	ZP	Zuständige Person
FE	Fertigung - Leitung	RM	Risikomanager
EK	Einkauf	RMT	Risikomanagement-Tool
QS	Qualitätssicherung	RE	Risikoeigner
VRE	Vorläufiger Risikoeigner		

Risikoeigner			
GF	Geschäftsführer	FE	Fertigung - Leitung
QS	Qualitätssicherung	EDV	EDV-Abteilung
EK	Einkauf	T	Technik

3. Prozesskennzahlen:

Prozesskennzahl 1: Risikohöhe = Eintrittswahrscheinlichkeit * Schadensausmaß

4. ↗ Risiko

5. Zuständigkeiten, Verantwortlichkeiten, wichtige Hinweise

6. Änderungshinweise

Neuausgabe

7. Mitgeltende Unterlagen

Erstellt und Geprüft	In Kraft gesetzt

Dieses Dokument wurde maschinell erstellt und ist ohne Unterschrift gültig! Änderungen gem. Verteiler unterliegen dem Änderungsdienst!

Verteiler: Orgamax EFG

Figure 50: ISO 9001 process description (3)



Risikomanagement

Übergabenachweis

Datum:

X **Neuausgabe**

Geänderte Ausgabe

übergeben an:

Die Prozessbeschreibung „PB_011 wurde dem/der Leiter(in) des Prozesses übergeben. Die/der Leiter(in) des Prozesses ist verantwortlich für den Austausch der geänderten und die Vernichtung der ungültigen Version, sowie für die Weiterleitung, Schulung und Dokumentation der neuen Ausgabe an alle bzw. aller betreffenden MitarbeiterInnen gem. Verteiler in der Fußzeile.

Name (BLOCKBUCHSTABEN)	Unterschrift	Datum	Schulung / Info / Unterweisung durch	Kurz- zeichen

Figure 51: ISO 9001 process description (4)