Improving the internal control system at Company X: a qualitative approach

Master thesis Industrial Engineering and Management

UNIVERSITY OF TWENTE.

Public version

This is a public version. Sensitive information about the company is adjusted or intentionally left out.

November 27, 2018

Author:
M.J. Harmsen

Supervisors:
University of Twente
R.A.M.G. Joosten
B. Roorda

MANAGEMENT SUMMARY

The goal of this thesis is to improve the internal control system at Company X by developing a comprehensive risk control framework. Due to a fast-changing world and business environment, the complexity of risk has changed. This has urged the need for increased risk awareness and oversight, together with improved risk reporting. In this regard, traditional internal control systems may not be sufficient anymore to deal with the increased risk complexity.

Compared to traditional internal control systems, enterprise risk management (ERM) provides a more complete view of risk management. We use the '*COSO ERM: integrating with strategy and performance'* framework to develop a new risk control framework, for which we use the current risk overview as starting point. The new framework should provide better insight into the risks faced by the organisation and how these risks relate to the company's strategy and objectives. Moreover, we analyse whether residual risks align with risk appetites, and define specific actions and responsibilities regarding risk governance and oversight. Altogether, this should lead to the improvement of the current internal control system.

The development of the framework follows the five components for ERM as defined by COSO. In addition, each component comprises several principles of which the relevant ones are discussed. The five components are:

- Governance & Culture.
- Strategy & Objective-Setting.
- Performance.
- Review & Revision.
- Information, Communication & Reporting.

Although the effectiveness of ERM practices relates to the presence of all five components in an organisation and their interconnectedness, the component 'performance' receives most attention since it is concerned with the identification, assessment, and response to risks.

For the identification of relevant risks on an entity level, and their assessment, we use a qualitative approach consisting of interviews, the review of business plans and the annual report, and meetings with the risk project team. Consequently, we assess the risk appetite, impact, probability, inherent risk exposure, control effectiveness, and residual risk exposure, using classifications ranging from 'negligible' to 'high'. By using these classifications, the relative importance of risks is indicated. Ultimately, the residual risks should align with the risk appetites.

Twelve main risks are identified in this report, for which we describe the risk components and control processes. From the assessment of these risks, we conclude that for two of the twelve main risks, residual risks are not within risk appetites. These risks are reputation risk and people risk. It is currently neither desirable, nor cost-effective to increase mitigation measures for reputation risk, which is why the medium residual is retained despite of the low risk appetite. However, continued efforts are necessary for improvement of the mitigation measures for people risk, to bring the medium residual risk within the low risk appetite. Besides the twelve main risks, three opportunities are identified: ICT improvement, cross department initiatives, and the development of alternative business. Seizing these opportunities can also help to reduce the negative effects of the twelve main risks. In order to keep the

proposed framework up to date and effective, we present a process of maintenance, together with responsibilities and risk oversight activities for various internal stakeholders.

The main recommendations regarding the implementation of ERM are to create one clear focal point for risk management practices and to increase risk awareness throughout the organisation. By transforming the current risk project team into a risk committee, it becomes clear who is responsible for managing and supervising risks. By making risk management part of Company X’s culture, people across the organisation become aware that risks are a shared understanding and responsibility. Lastly, high commitment from management is crucial because without it, ERM will most likely not become part of the corporate strategy or will not be integrated in the decision-making process.

Concluding, the proposed framework in this report provides a more complete, and coherent, overview of risks compared to traditional internal control systems. The new framework considers risks on an entity level in relation to Company X's strategy and entity objectives, governance structure, and culture. This should help to bring residual risks within risk appetites and to achieve Company X's ambition of being the market leader in their focussed business direction.

PREFACE

I hereby present my master thesis: '*Improving the internal control system at Company X: a qualitative approach*'. This thesis is the result of a research I conducted over the course of six months at Company X and which concludes my master in Industrial Engineering and Management at the University of Twente. For me, this has been a great opportunity to apply the theoretical knowledge I acquired during my study in practice.

I would like to thank Company X for giving me the opportunity to get to know the organisation from the inside and improve my knowledge on the topic of risk management. In particular I would like to thank my supervisors at Company X for their continued support and feedback, and the other people at Company X who have made my stay pleasant, and contributed to my report. In addition, I want to thank my supervisors from the University of Twente, Reinoud Joosten as my first supervisor and Berend Roorda as second supervisor, for their guidance and feedback.

Baarn, November 2018

Michiel Harmsen

CONTENTS

1. INTRODUCTION

Chapter 1 introduces the research at Company X. Section 1.1 starts with a description of the company where after the problem is described in Section 1.2. Section 1.3 discusses the goal of the research and Section 1.4 defines the research questions. Lastly, Section 1.5 discusses the scope and limitations of the research after which Section 1.6 presents an overview of the report structure.

1.1 Company description

This sub section has been intentionally left out for confidentiality purposes.

1.2 Problem identification

In today's enterprises, managing risks is very important. Since the introduction of ERM, firms do not only see risk as something that needs to be reduced or eliminated anymore, but acknowledge that there are potential opportunities connected to these risks. This way, risk is seen as the effect of uncertainty on objectives (ISO, 2009), rather than only considering negative effects or financial loss. In this regard, connecting risk management to the strategic objectives of the enterprise is essential. Due to the competitive, complex and fast changing world Company X operates in, there is a need to keep developing risk management practices within the organisation. Not only do adequate risk management and internal control help with realising company objectives, they also help with the ability to implement the right strategy and the realisation of targets. In order to be able to deal with uncertainty, it is important to map the possible risks. The outcomes of these risks can be both positive and negative, but being aware of the scenarios is essential.

Currently, Company X is starting to give more attention to the risks associated with the organisation. An important first step in this regard is the identification of these risks, together with their probability of occurrence and impact. Mapping these risks is necessary to come up with a plan on how to control them, and to decide to what extent residual risks are allowed. Although the mapping of risks associated with the different divisions by a project team has resulted in an overview already, there is still a need to explore the risks in depth in order to embed risk management in the organisation.

The absence of a clear approach towards risk management can cause a suboptimal realisation of the organisation's targets and objectives (RIMS, 2012). This can be from a strategic perspective but might relate to operational performance as well. At this moment there is no clear document that provides a comprehensive framework of the risk management practices. Furthermore, there is insufficient translation of this information into concrete actions for relevant people in every layer of the organisation.

1.3 Research goal

Company X is aware that their business goals and corresponding strategic choices expose the organisation to risks. To deal with the uncertainty this implies, a comprehensive risk control framework needs to be developed to mitigate risks and manage exposure. The current overview of risks will be taken as a starting point. The goal is to create a comprehensive risk control framework that specifies and complements the components already identified in the overview, and to translate the framework to the everyday practice in the organisation. To do so, the already existing overview will be coupled to a theoretical ERM model to make sure that the eventual framework matches the standards of ERM models in the field. The framework has to show what the risk profile of the organisation looks like, what the elements of the risks are and whether these are related, and to what extent residual risks are acceptable. Finally, the framework needs to be translated into practice in order to connect risk management to the strategic objectives. It should become clear why specific elements are chosen and how they help with reaching company objectives. This final step might further include making everyone aware of their responsibility in the process by specifying concrete actions.

1.4 Research questions

Company X is looking for a way to improve internal control. A systematic approach is needed to define clear steps in the risk management process and to come up with concrete actions and maintenance processes that can be used by the relevant stakeholders. These stakeholders will be discussed in Chapter 4. The COSO ERM model is one of the most widely used frameworks (Olson & Wu, 2008) when it comes to internal control. It aims to identify the relationship between the risks facing the organisation and the internal control system. COSO (2017) defines five elements for control systems that should help with realising strategic objectives, operational efficiency, reliable reporting, and compliance with relevant laws and regulations. Such a model could provide a solid base for the development of a risk control framework at Company X.

Now that the problem has been identified and the research goal has been defined, a research question can be formulated. Based on the problem at hand and the desired result, the research question should contain a threefold of components:

1. It should refer to the improvement of the internal control system. The main improvement compared to the initial overview should be a more complete and more coherent overview of risks in the organisation.
2. The outcome should contain a framework with, among other things, a list of clear actions, which will help with the transition to practice.
3. Effective risk management contributes to reaching company goals and objectives (RIMS, 2012) The result should explain how this link can be achieved.

Combining these three component results in the following research question:

Main question

- How can Company X improve its internal control system by developing a framework that connects risk management to its strategic objectives?

Sub questions - current situation

The first step in the process of answering the main question is the mapping of the current situation. In this regard it is important to understand how risk management practices are currently performed in the organisation. This includes for instance the risk appetite of the company and who ensures that risk management is performed in a responsible way. In relation to the current situation, the following sub questions need to be answered:

- What does the governance structure for risk management look like?
- To what extent is Company X willing to take risk?
- What does the overview for risk management currently look like?

Sub questions - theory

Subsequently, a literature review will be performed to get more knowledge about what risk management is and how theoretical models can be used to develop a framework for Company X. This way, the developed framework will match standards used in the field. Related to this, the following theoretical sub questions are defined:

- What is ERM?
- What standards are available in theory for internal control?
- How can the governance structure be effectively organised?

Sub questions - solution

Based on the theory, the current risk management overview for Company X can be improved. Besides using standards from theory to improve the overview, aspects like the risk type, exposure and mitigation measures need to be specified and, if needed, expanded in order to develop a comprehensive framework.

- Which risks does the organisation face and how can these be categorised?
- What is the risk exposure?
- How can the risks be mitigated and which processes are already in place to do so?
- To what extent are residual risks acceptable?
- How can risk management be modelled comprehensively?

The developed framework should be self-containing and easy to understand, so that it can be used as a reference for risk control practices. An accompanying subsection should explain why a certain theoretical model is chosen and how this results in the presented framework.

Sub questions - application

Finally, the solution needs to be translated to practice. At this point, there should be a framework on paper, but people should become aware of their own responsibility to embed risk management in the organisation. In this part, I will discuss some concrete actions for the successful implementation of the framework. Therefore, the following questions need to be answered:

- How can the risk model be applied in practice?
- How can the model contribute to the strategic objectives of the company?
- What is needed to make everyone in the organisation aware of their role in ERM?

1.5 Scope and limitations

The goal is to present a framework that will help improve internal control. In this regard, the focus will primarily be on the risk factors that directly influence the organisation, and the ability to deal with those factors. The macro environment of the organisation might therefore be discussed to a lesser extent. Furthermore, the framework will be qualitative. Quantification of risks is out of the scope of this research.

1.6 Report structure

In this chapter, Company X is introduced, together with the problem the company is dealing with and the objectives this research aims to realise. Chapter 2 will be about the current situation. A look is taken at how risk management is currently organised. This includes the risk components that are already identified but also the way in which risk is governed and how responsibilities are assigned. Chapter 3 describes the theoretical framework of the research, including literature about risk management frameworks, ERM, governance and the elaboration of identified risk components. In Chapter 4, I propose a risk control framework for Company X which should function as a reference book for questions regarding risk management practices within the organisation.

Chapter 5 deals with the way the framework presented in Chapter 4 can be applied in practice. It concerns the implementation of the steps necessary to embed risk management in the organisation and the way in which employees become aware of their responsibility in this process. In Chapter 6 we conclude the research, where after we discuss the limitations and possibilities for further research in Chapter 7.

2. SITUATION DESCRIPTION

Chapter 2 discusses the current situation regarding risk management at Company X. In Section 2.1, we present the governance structure and Section 2.2 gives an overview of the components Company X considers in their risk management practices.

2.1 Governance structure

2.1.1 Organisational structure

This sub section has been intentionally left out for confidentiality purposes.

2.1.2 Authority and Responsibility

Corporate responsibility

Senior management ultimately holds the responsibility for risk management practices within the organisation. The board of directors advises and monitors senior management to make sure risk management practices are performed in a responsible manner.

Local Responsibility

On a local level, the responsibility for managing risk is delegated to the respective person(s) in charge. They are expected to give an overview of the main risks and opportunities for their departments in their business plans.

2.2 Risk overview

Across the organisation, several risk management practices are already conducted. However, a clear and practical overall framework is missing. The first step the company took to create such an overview was the establishment of a project team.

2.2.1 Risk identification

To get an idea about the risks in the organisation, interviews are conducted with people from different departments. Input from people in different functions is crucial to get a complete risk profile. The identification of risks should ultimately give better insights into how risks can affect the realisation of objectives and how business continuity can be guaranteed. Business continuity means that in case of an event with possibly serious operational consequences, the organisation should be able to (partly) carry on with delivering their service. Interviews with people from the different departments and business plans from these departments, will give various perspectives to create a complete overview of risks. The initial interviews are conducted by the members of the project team and resulting from this, they created the overview in Appendix B. Based on these interviews and the corresponding overview, conversations with the project team, and business plans from the departments, I composed a list of risks that are relevant on an entity level. These risks will be discussed in Section 2.2.3. The specific functions of the interviews with internal stakeholders are listed in Appendix A.

2.2.2 Risk categorisation

Before discussing the individual risks, risk categories are defined so the risks can be classified according to their nature. The current classification is based on the four categories as defined by the Treadway Commission (COSO, 2004) and is complemented with a financial category. Together, this results in the following five categories:

- **Strategic**: high-level goals, aligned with and supporting the mission
- **Operational**: effective and efficient use of resources
- **Reporting**: reliability of reporting
- **Compliance**: compliance with applicable laws and regulations
- **Financial:** risk regarding financial performance

2.2.3 Risk description

Interviews, group sessions and department business plans resulted in a list of eighteen risks. The individual risks will be discussed below, together with the initial categorisation of these risks by the task force.

Strategic

- **Critical employee positions**
  The risk of losing key employees with specific knowledge and capabilities.
- **Reputation (brand positioning)**
  The way in which Company X is generally seen or judged by (potential) customers.
- **Culture & behaviour**
  The norms and values in the organisation and the way people act in their working environments.
- **Market risk**
  The risk of changing market conditions (e.g. economic conditions, competition).

Operational

- **Purchasing & payable cycle (products and services)**
  The risk relating to the outsourcing of services and hiring external personnel.
- **IT performance**
  The availability and continuity of IT systems.
- **Cyberattack**
  A possible strike against the company's computer systems, causing theft of sensitive information or the falling-out of digital systems.
- **Quality and innovation of services**
  The degree to which the organisation is able to fulfil the needs of their customers, and the ability to adapt to changing requirements by providing new or improved services.
- **Internal control risks**
  Inadequate division of tasks, inefficient processes and control measures that do not function as intended or are absent.
- **Insufficient awareness of risk**
  Not being aware of all the risks facing the organisation, which makes it impossible to come up with effective mitigation measures.

Reporting

The risk that reports do not use the same standards, provide the same quality or reflect reality. Examples of reports are:

- **Corporate Social Responsibility - including media interest and transparency reporting**
- **Financial reporting**
- **Law and regulations requirements**

Compliance

- **Customer risk**
  The risk of getting into business with the wrong parties.
- **Joiner and leaver process (employees)**
  The risk of hiring new employees and ending employment in a responsible manner.
- **Professional development**
  Guaranteeing enough critical employee positions to make internal advancement possible and to keep the company attractive for future employees. Provide regular education and training for current employees.

Financial

- **Financing**
  Arrange sustainable financing to ensure long-term growth.
- **Profitability (margin)**
  The risk that the profit to revenue ratio is not high enough, causing the need for cost reduction which is undesirable.

2.2.4 Impact

The effect an individual risk can have on the organisation is defined as the risk impact. The higher the impact is, the higher the potential (negative) consequences are. The impact can be classified as *negligible*, *low*, *medium* or *high*. The actual meaning of these classifications depends on the impact category and was initially determined by the project team. In case of the financial risks, negligible (marginal) means a potential loss of under 25,000 euro, low between 25,000 and 100,000 euro, medium between 100,000 and 500,000 euro, and everything above 500,000 is considered a high impact. On the other hand, we have the remaining impact categories where the meaning of the classification is defined qualitatively, rather than quantitatively. The exact meaning of the classifications for every impact category is listed in Appendix C.

2.2.5 Control processes

Across the organisation there are different measures in place to deal with uncertainty. The control processes range from a trust person in case employees have a complaint that needs to be dealt with privately, to active customer screenings, and audits performed internally and externally. The project team defined the possible classifications for the control measures, which are *non-existent, low, medium* and *high.* In case there is an actual control mechanism in place to deal with a specific risk, the frequency is classified as *on-going, regular* or *ad-hoc*.

2.2.6 Residual risk

The control mechanisms are meant to mitigate risks and manage exposure. However, for some of the risks needs to be determined whether the control measures are sufficient to match the residual risk with Company X's risk appetite. Again, these residual risks can be defined as *negligible, low, medium* and *high.*

By putting the discussed aspects together, the project team created an overview which specifies for every risk to what category it belongs and what the potential impact might be. Furthermore, it specifies the control mechanisms in place for mitigation purposes and ends with the residual risk that remains. The overview can be found in Appendix B.

3. THEORETICAL FRAMEWORK

In this chapter, we discuss the theoretical framework. In Section 3.1, the focus will be on some core concepts related to risk management, including a definition of risk itself. Section 3.2 discusses ERM, where after a comparison is made between ERM frameworks in the literature in Section 3.3. This results in the elaboration of the COSO ERM framework in Section 3.4 and finally the three lines of defence model will be discussed in Section 3.5 with regard to the governance structure.

3.1 Core concepts

Relating to risk management practices, a lot of terms and definitions are used interchangeably or have a meaning that is rather vague. In this section, relevant terms and definitions will be discussed to clarify how they are used in this report.

3.1.1 Risk

Risk is a subject that has traditionally concerned many scholars and practitioners (Gahin, 1971). There are many definitions of risk of which the meaning is not always the same. When people think about risk, it is often regarded as a negative concept, but there might also be a potential upside connected to a risk. In an attempt to create a definition of risk that can be used consistently while still capturing the essence of what risk is about and how it occurs, the International Standards Organization (2009) defines risk as:

The effect of uncertainty on objectives.

Trying to achieve company objectives causes uncertainty since both internal and external factors are involved that cannot be controlled completely. This may cause the organisation to fail to achieve its objectives or may cause delay (Purdy, 2010). The objectives could also be achieved early or exceeded, which is why risk is neither positive nor negative by definition. With this definition, risk is a description of what could happen and how this influences the achievement of objectives, rather than just an event or consequence.

Risk is built up out of two components, probability and impact. Probability is the likelihood that an event occurs that influences the achievement of objectives. Impact is the degree to which the event affects the organisation. To describe the relation, the following risk formula can be used (Cox Jr., What's Wrong with Risk Matrices, 2008):

$$Risk = Probability * Impact$$

Likelihood is often used interchangeably with probability and frequency, and impact with severity and consequences. In this report, probability and impact will be used as defaults. In case the components cannot be defined quantitatively, it is also possible to assess the risks qualitatively. With a risk matrix, probability and impact can be represented graphically to show the relative importance of risks. The use of risk matrices has been supported by risk management standards (e.g. AS/NZS 4360:1999 (Standards Association of Australia, 1999)) and is now widely adopted by organisations and risk consultants, for instance in the field of ERM (Cox Jr., What's Wrong with Risk Matrices, 2008).

Table 1: Standard risk matrix.

Prob. Impact	Very low	Low	Medium	High	Very high
Very high	🟨	🟨	🟥	🟥	High
High	🟩	🟨	🟨	🟥	🟥
Medium	🟩	🟩	Medium	🟨	🟥
Low	🟩	Low	🟩	🟨	🟨
Very low	Negligible	🟩	🟩	🟩	🟨

Although risk matrices are widely adopted, there is little research as to how they actually improve risk management decisions. Since the inputs and resulting risk ratings are largely subjective, risk matrices should be used with caution, and with careful explanations of embedded judgements (Cox Jr., What's Wrong with Risk Matrices, 2008). Because the risk assessment in this report will be qualitative, a risk matrix can provide a simple overview of the relative importance of the risks.

3.1.2 Internal control

"Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance (COSO, 2012)." When comparing this definition with ERM, it can be seen that internal control neglects the strategic aspect, and a silo-approach is used instead of looking across the enterprise. The silo-approach means that risks are treated independently in different business units.

3.1.3 Risk exposure, appetite & tolerance

Risk exposure is the amount of risk Company X experiences. Risk appetite refers to the amount of risk Company X is willing to take in the pursuit of its strategy and objectives. This (partly) reflects the definitions used by ISO (2009) and COSO (2009). Risk appetite might be with respect to individual risks or aggregates, and can be expressed as being qualitative or quantitative. In case the risk appetite of a risk is high, Company X is willing to accept a high level of residual risk. When the appetite is averse, Company X aims to reduce the residual risk as much as possible.

COSO (2009) defines risk tolerance as "the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve". According to Purdy (2010) it should be avoided to get ensnared in the debate about risk appetite and risk tolerance, since the terms are often misused and confusing. In for instance the financial sector, there is no consensus on what the two terms actually mean and how they can be differentiated (Basel Committee on Banking Supervision., 2010). Therefore, this report will only make use of the definition for risk appetite.

3.1.4 Inherent, target & residual risk

In the process of assessing risks and determining to what extent these risks are acceptable, a distinction is made between inherent risk, target residual risk and residual risk. Inherent risk represents the amount of risk to the entity in case control measures are absent. This means that no actions are taken to alter the risk's probability or impact. Target residual risk on the other hand, is the desired level of residual risk, knowing that mitigation measures will be, or have been implemented and should fall within the organisational risk appetite. Residual risk refers to the amount of risk that actually remains after the entity's risk response which differ from the risk appetite.

3.2 Enterprise risk management

In the last decades, especially after the financial crisis in 2008, a more holistic view of risk management has replaced the traditional silo-approach (Oliviera et al., 2018). A growing number of firms show interest in this new and more complete view of corporate risk, which is commonly referred to as ERM (Oliviera et al., 2018).

According to the Treadway Commission (COSO, 2004), ERM can be defined in the following way: "ERM is a process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

In essence, ERM and the corresponding frameworks are concerned with identifying, analysing, responding to, and monitoring risks and opportunities in the enterprise environment. Typically, every organisation has its own departments or functions to map and deal with risks. Encountering risks in a competitive environment is inevitable, which makes it of utmost importance to deal with these risks in a correct manner. The actions taken to manage risk are generally classified into four categories:

1. *Avoidance*: stop with the activity causing the risk.
2. *Reduction*: take action in order to reduce impact of the risk or the likelihood of occurring.
3. *Transfer*: sharing or transferring risk, for instance by taking out insurance.
4. *Retain*: accept the risk as it is and take no action. Potential benefits outweigh the cost of mitigation.

The risks facing the enterprise can be either external or internal. External factors are often beyond the control of an organisation and can result from developments in the economic landscape, or due to changes in the political, legal, technological, and demographic environments (Olson & Wu, 2008). Internal factors on the other hand might include human errors, fraud and system failure. For internal risks it is often easier for organisations to develop procedures to control these risks.

When comparing ERM with traditional risk management, some differences can be noticed (Olson & Wu, 2008). Probably the most notable one is that ERM sees risk in the context of the business strategy, rather than individual hazards. Risk is treated as a portfolio instead of individual identification and assessment. The focus is primarily on the critical risks and risk is not only seen as something that must be mitigated or eliminated, but as something that needs to be optimised. Critical risks can for instance be determined by looking at whether residual risks align with the risk appetites. Instead of only setting risk limits, ERM results in a risk strategy where responsibilities are clearly defined and everyone in the organisation is aware of their role.

3.3 Comparison frameworks

With the increasing interest in (enterprise) risk management practices over the years, many frameworks appeared in an attempt to create a risk management standard. Among the first risk management standard is the first edition of AS/NZS 4630, originating in Australia and New Zealand (Moeller, 2007). Nowadays, over 80 frameworks exist with COSO's "*Enterprise Risk Management - Integrated*

Framework" and "*AS/NZS 4360"* as the ERM frameworks that are used most commonly (Olson & Wu, 2008; Moeller, 2007). Although the definitions and number of steps in these two frameworks differ, the principles seem fundamentally the same.

In 2009, the International Organization for Standardization (ISO) published ISO 31000:2009 "*Risk management - principles and guidelines".* The standard is aimed at creating a standard for managing risk in every organisation by creating one vocabulary, a set of performance criteria, one common process for identifying, analysing, evaluating and treating risks, and guidance on how this process should be integrated in the decision-making process (Purdy, 2010). According to Gjerdrum & Peter (2011), ISO provides a streamlined approach, where the COSO framework is rather complex and difficult to implement. However, since ISO largely adopts the process as defined by AS/NZS 4360:2004 (Purdy, 2010), one could argue that the underlying principles are still the same. Furthermore, in an attempt to create a standard that can be used in every organisation no matter the size or sector, ISO uses broad definitions and abstract language. Resulting from this, Leitch (2010) summarizes ISO 31000:2009 as unclear, impossible to comply with, not mathematically based, and causing illogical decisions.

Although there are different views on which framework to use, it can be argued that the different standards have more in common than in opposition (Gjerdrum & Peter, 2011). Ultimately, an additional standard may provide additional insight. The topic of risk management remains rather abstract and therefore requires a tailored and well-founded approach for every individual company. Since the COSO model is control and compliance based, and Company X is already familiar with certain aspects of the model, COSO will be used as the basis for the new risk management framework for Company X.

3.4 COSO ERM framework

One of the most widely used frameworks for ERM is the *'Enterprise Risk Management - Integrated Framework'*, developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In the section above, ERM was shortly introduced and a definition of ERM was given, as stated by COSO. With the underlying premise of ERM that every entity exists to provide value for its stakeholders, the definition reflects some core concepts (COSO, 2004); ERM is an ongoing process, affected by people in different levels of the organisation, throughout the entity. ERM should be taken into account when determining strategy, and risks should be managed from an entity-level portfolio view. Developing a portfolio view of risk means identifying risks that are severe on an entity level (COSO, 2017). It might for instance be acceptable that some operating units experience a higher level of risk than others, as long as the overall risk remains within the risk appetite. Possible events have to be identified to manage risk within the organisation's risk appetite, thereby providing assurance to the management and board of directors, and contributing to the achievement of entity objectives.

The link between ERM and the achievement of entity objectives is a recurring theme. Effective risk management helps with reaching objectives in the context of the entity's mission or vision. The COSO framework presents four categories in which the objectives can be put. By defining four categories, a distinct focus can be used for different objective types. A particular objective can however still fall into more than one of the four categories (COSO, 2004):

- Strategic: high-level goals, aligned with and supporting the mission
- Operations: effective and efficient use of resources

- Reporting: reliability of reporting
- Compliance: compliance with applicable laws and regulations

The way each category is managed is also connected to the degree the organisation is able to control the respective objectives. Reporting and compliance is an internal affair and therefore the organisation should be able to provide reasonable assurance that objectives in these categories will be achieved. Strategic and operational objectives on the other hand, are also subject to events in the external environment which cannot always be controlled and therefore might require a different approach. This requires the responsible parties to be aware of external events that might happen and being able to respond adequately in case such an event does occur. Events with a negative impact represent risks, whereas events with a positive impact represent opportunities.

Besides the four objective categories, the COSO framework defines eight interrelated components ERM consists of. The components should not be treated as a step-by-step plan, but as a process that is iterative and in which most components influence each other. The components are (COSO, 2004):

- *Internal environment* - The internal environment describes the culture and values in the organisation. It encompasses the way in which risk is viewed and addressed, to what extent the organisation is willing to bear risk, and the environment in which they operate.
- *Objective setting* - By defining entity objectives, potential events that might disrupt their achievement can be identified. A process must be in place to ensure the objectives are consistent with for instance the risk appetite.
- *Event identification* - Events that can affect the achievement of the entity objectives must be identified. These events can be internal or external, and represent a risk or opportunity. In case of an opportunity, these might be channelled back to the point where strategy is determined and objectives are being set.
- *Risk assessment* - This component is concerned with analysing the identified risks. Likelihood and impact of the risks are considered to come up with a plan on how these risks can be managed effectively.
- *Risk response* - Based on the risk assessment, a response strategy is chosen to align the risk with the risk appetite. As discussed in Section 3.2, possible risk responses are to avoid, reduce, accept (retain) or share (transfer) risk.
- *Control activities* - The policies and procedures that are in place to ensure the risk response strategies are carried out effectively.
- *Information and communication* - Relevant information is identified and communicated to make people aware of their responsibilities, as well as to spread the information throughout the organisation.
- *Monitoring* - Monitoring of ERM practices to ensure effective execution and improvements when necessary. This can be done by ongoing management activities, separate evaluations, or both.

Relationship

The relationship between the entity's objectives and the needed ERM components to achieve these objectives, can be represented in a three-dimensional matrix. The horizontal rows represent the eight ERM components, the vertical columns represent the four objective categories, and the third dimension are the entity's units. When combining the three dimensions graphically, the relationship can be shown in the form of a cube. It shows that the focus can be on the entirety of the entity's ERM, as well as on a specific component, unit, or objective category.

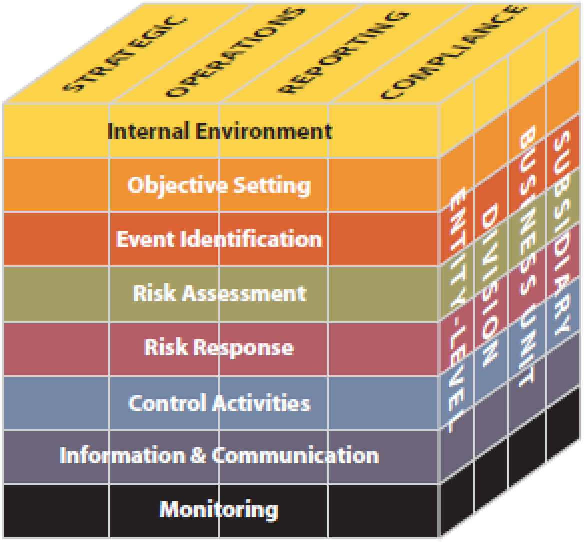


Figure 3.2: Relationship between objectives, components and units (COSO, 2004).

The effectiveness of the model largely depends on the judgement of whether the eight components are present and well-functioning. The components therefore also serve as criteria for the effectiveness of ERM.

Updated COSO framework

In 2017, a revised version of the *'Enterprise Risk Management - Integrated framework'* was presented by COSO. Since 2004, the complexity of doing business and the emergence of corresponding risks have changed. The updated framework, '*Enterprise Risk Management - Integrating with Strategy and Performance*' addresses the changes in ERM and how this influences the risk approach in the organisation. It clarifies the importance of ERM in strategic planning and embedding it throughout the organisation (COSO, 2017). Instead of using eight components, the updated framework uses five interrelated components, as shown in Figure 3.2, which are supported by a set of twenty principles.

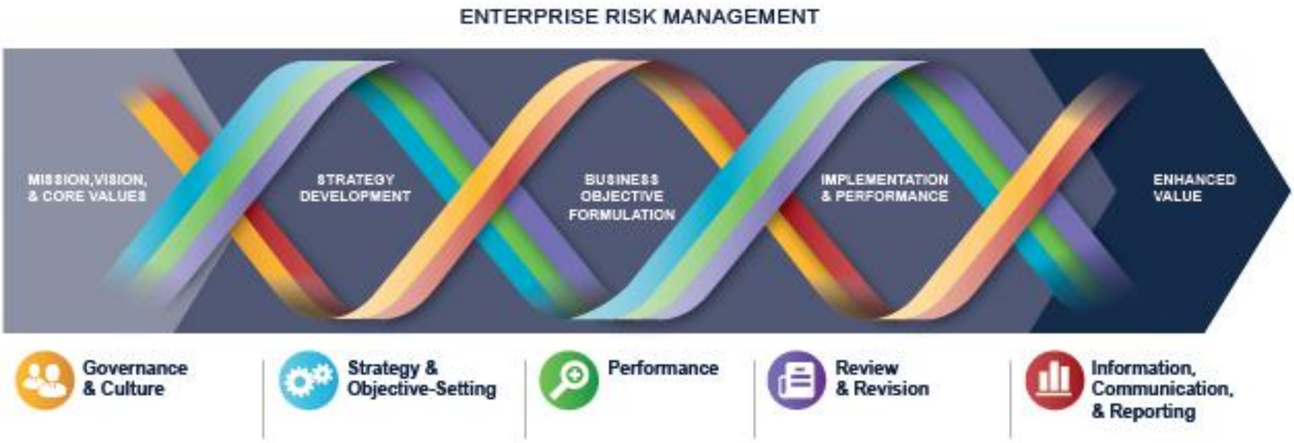

ENTERPRISE RISK MANAGEMENT
MISSION,VISION, & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

Figure 3.2: Risk management components (COSO, 2017).

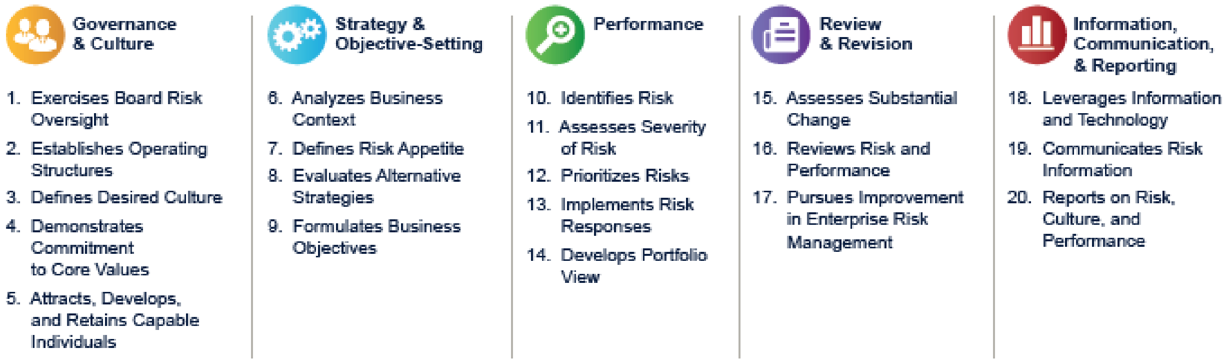
The Treadway Commission describes the five components in the following way (COSO, 2017):

- *Governance & Culture* - Governance and culture refers to the tone of the organisation, the way in which responsibilities are established and their importance in relation to ERM, and the culture. Culture is about desired behaviours, ethical values, and the understanding of risk.

- *Strategy & Objective-Setting* - Strategy and objective-setting are connected to ERM, and are therefore important in the strategic-planning process. This component is concerned with the establishment of risk appetite, setting up objectives, and alignment with the chosen strategy.
- *Performance* - Based on the strategy and objectives, risks are identified to assess their impact. The risks are prioritized and evaluated in relation to the risk appetite. Risk responses are selected and a portfolio view is taken of the amount of risk it has assumed. The outcomes are then reported to key risk stakeholders.
- *Review & Revision* - A review should be performed on how the ERM components are functioning and whether they are effective. Based on the review, revisions can be considered for improvement.
- *Information, Communication & Reporting* - Information regarding ERM needs to be communicated and reported. Obtaining and sharing information, from internal and external sources, is essential in the process of creating awareness across the entire organisation.

The principles associated with the components are represented in F*igure 3.3*. A short explanation of the individual principles is provided in Appendix D.

Figure 3.3: Risk management principles (COSO, 2017).



Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

3.5 The three lines of defence model

With the need to identify and manage risks properly, organisations more often have a diverse range of risk management functions. These functions can for instance be compliance officers, internal auditors, and ERM specialists and are increasingly being split over multiple departments and divisions. (IIA, 2013). To make sure there is an effective coverage of tasks and responsibilities, a well-coordinated approach is necessary. Although risk management frameworks can help with the identification of the specific risks an organisation should aim to control, there is little documentation on how risk functions should specifically be assigned and coordinated. The three lines of defence model, discussed by the institute of internal auditors (2013), "provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties". This model presents a guideline to improve the effectiveness of risk management within the organisation.

3.5.1 Three lines of defence

The three lines of defence model distinguishes three groups that are involved in effective risk management (IIA, 2013):

- Functions that own and manage risks.
- Functions that oversee risks.
- Functions that provide independent assurance.

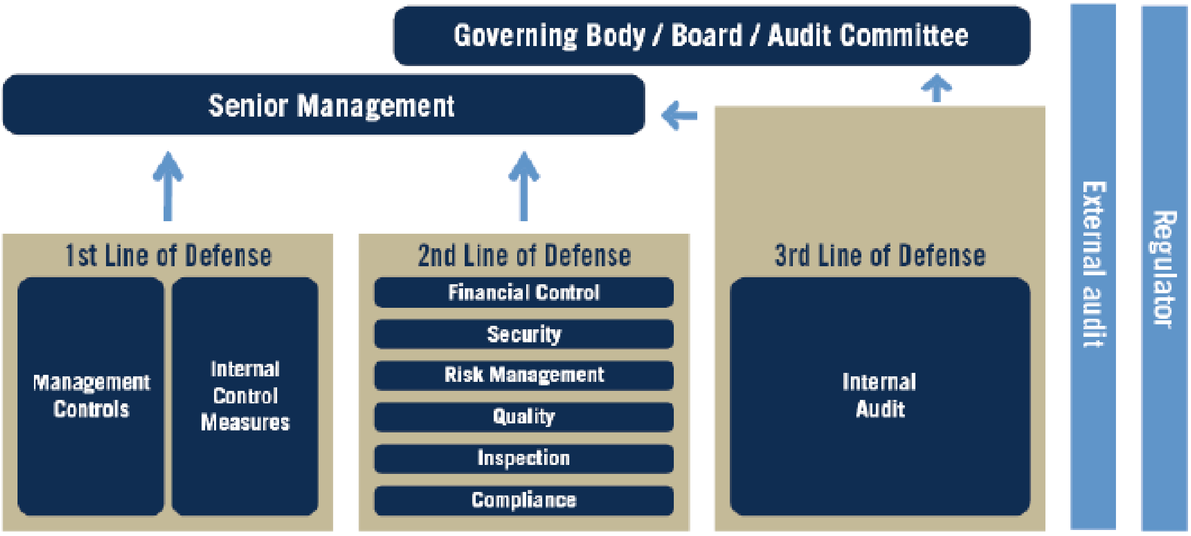


Figure 3.4: Three lines of defence model (IIA, 2013).

3.5.2 The first line of defence: operational management

One of the concepts behind the model is to assign the basic control and responsibilities to the first line of defence. These are often the staff and managers from the business units that generate revenues (BIS, 2015). This way, these staff members and managers own and manage the relevant risks. Operational management encounters the risks on a daily basis and is therefore the first line that "identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives". Their familiarity with the workflow corresponding to the daily business should enable them to identify weaknesses early and act appropriately.

3.5.3 The second line of defence: risk management and compliance functions

Only a single line of defence, especially in larger organisations, can often prove to be inadequate. Therefore, risk management and compliance functions are created to assist and control the first line of defence for if they become ineffective (BIS, 2015). According to the model, these functions can for instance be financial control, security, risk management, quality assessment, inspection and compliance. The second line is concerned with monitoring and reporting risk-related practices and information. Furthermore, they deal with issues regarding compliance and financial control. By doing so, these second line functions must ensure that the first line functions as intended. Although the second line functions offer some degree of independence, they are management functions by nature. Therefore, the analyses the second line provides cannot be truly independent regarding risk management and internal controls (IIA, 2013).

3.5.4 The third line of defence: internal audit

The third and last line of defence is the internal audit. This line is meant to give assurance to the governing body and senior management, with the highest level of independence (IIA, 2013). This can be for instance on the effectiveness of governance and internal control. This also includes the way in which the first and second line achieve their risk management objectives. In order for the function to be effective, the highest level of independence is needed. Therefore, the chief executive audit should be able to communicate with senior management and the board of directors directly (Arndorfer & Minto, 2015). The third line often comes down to a periodic risk assessment of categories with a high level of residual risk, rather than an ongoing risk assessment that is typical for the first line of defence (Arndorfer & Minto, 2015).

3.5.5 External control

The three lines of defence model is focussed on assigning control functions and risk management responsibilities within an organisation. There can however also be additional external levels of control that complement the first three lines. BIS (2015) mentions the financial sector as an example of an industry where specific regulatory bodies monitor whether organisations comply with the rules. Although this case is focussed on the financial sector, external audits might add an extra layer of control with a high level of independence in other regulated industries as well. However, the scope of risks addressed by external bodies is generally less extensive than the internal lines of defence (IIA, 2013).

3.5.6 Remarks

The three lines of defence model provides a clear structure for governance within an organisation, but the model also has weaknesses that should be addressed. Often, the first line of defence is seen as the most important since this is the line that encounters risks on a daily basis (Arndorfer & Minto, 2015). However, the first line also comprises the people that are responsible for the revenues in the organisation. When these people are also the risk takers in the organisation, there might be a conflict of interest when the risk is connected to the amount of revenue that is being generated.

When it comes to the second line of defence, a certain degree of organisational independence is required to ensure effective control. However, control functions in the second line sometimes lack this kind of independence (Anderson & Eubanks, 2015) which causes the control to be inadequate. In a formal structure, risk management functions report directly to the board. However, in daily practice it is more likely to go to management which causes the second line to become engaged with other control functions. The exchange of information resulting from this might cause the control units in the second line to adopt views that decrease their independence. Decreased independence might cloud the second lines' judgements, making the control ineffective. Even if organisational independence is guaranteed, this does not necessarily mean that the second line of defence has sufficient skills and expertise to control the first line of defence effectively.

Lastly, there is the third line of defence. For the internal audit to be effective, the annual risk assessment should be well planned and performed by internal auditors that have a good understanding of the risk profile of the organisation. In case internal auditors have insufficient skills and knowledge to identify the high-risk areas to be assessed in the periodic review, wrong risk areas will be highlighted and the effectiveness of the third line of defence will be undermined.

4. RISK CONTROL FRAMEWORK

In Chapter 4, I will elaborate the proposed risk control framework for Company X. The structure of the framework is based on the five components as defined by COSO (2017) and aims to cover the relevant principles as described in Appendix D. Section 4.1 describes the governance structure and culture. In Section 4.2, Company X 's strategy and objectives are presented, together with the degree to which the organisation is willing to accept risk. Section 4.3 zooms in on the individual risks and their qualitative assessment. Finally, in Sections 4.4 and 4.5, I will give examples of triggers for reassessment of the framework, together with the way in which the framework should be communicated.

4.1 Governance and culture

Company X's board has a significant role in risk governance, and influencing ERM. Defining a clear governance structure and culture are important so they reflect Company X's core values.

4.1.1 Risk governance

In Chapter 2, the current responsibilities regarding risk management are discussed. For the new risk control framework as discussed in this chapter, the three lines of defence model will be adapted to improve risk governance throughout the organisation.

Corporate responsibility

The board ultimately holds the responsibility that the overall risk profile of the organisation is in line with the risk appetite. The board of directors advices and monitors senior management to make sure risk management practices are performed in a responsible manner.

Three lines of defence

Although the board ultimately holds the overall responsibility for risk management, tasking them with carrying out major ERM practices would be very time consuming. By applying the three lines of defence model, essential roles and duties are appointed and clarified to enhance communication on risk and control.

The first line of defence: operational management

Basic control and responsibilities are assigned to the first line of defence. For Company X this means that on a local level, the responsibility for identifying, evaluating and managing risks is delegated to the department managers and the employees in those departments. Since operational management is expected to encounter risk on a daily basis as part of their workflow, they should be able to identify risks early and act appropriately.

The second line of defence: risk management and compliance functions

Because a single line of defence can often prove to be inadequate, risk management and compliance functions should assist and control the first line of defence to make sure they operate effectively. At Company X, second line of defence functions are compliance and financial control. Furthermore, a project team works towards the creation of a risk control framework. Altogether, the second line of defence is concerned with monitoring and reporting risk-related practices and information.

The third line of defence: internal audit

Internal audit should provide independent assurance to senior management and the board of directors regarding risk management practices. Internal audit performs checks at random and can be tasked with the periodic assessment of the main risks in the organisation. Since Company X does not have an internal audit function, there is no absolute independence. This is however compensated by the fact that an external audit is performed. Additionally, regulators oversee whether Company X abides laws and regulations.

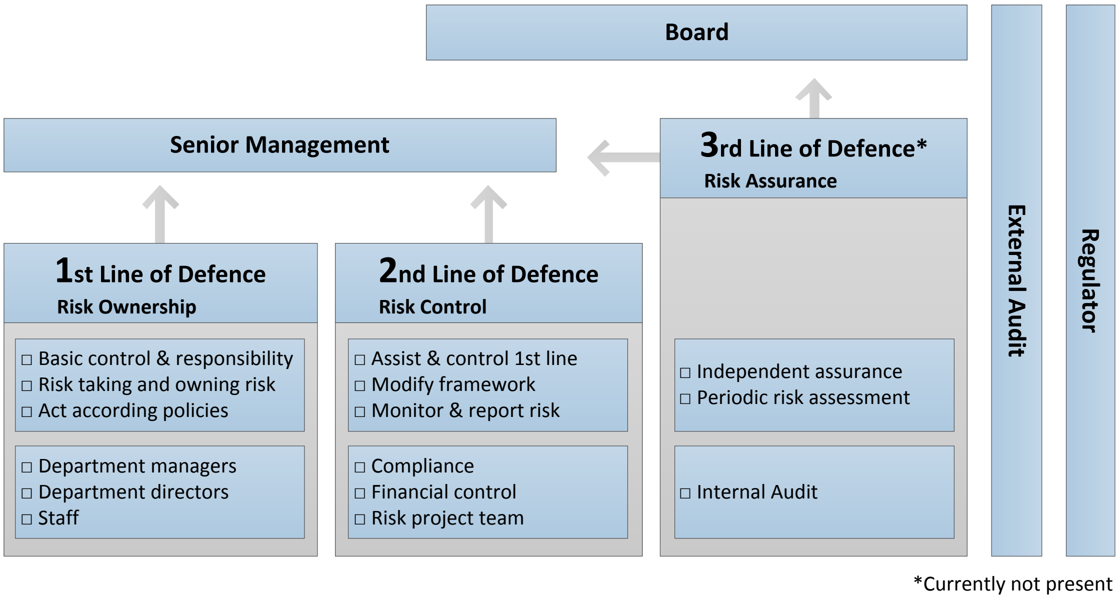


Figure 4.1: Three lines of defence Company X - Adapted from Figure 3.4 (IIA, 2013).

4.1.2 Culture

The ultimate goal regarding culture is the creation of a stimulating and inspiring environment where everyone is given the opportunity to reach their full potential. In this regard, Company X strives to stimulate a professional culture which is characterized by three objectives:

- Not only provide customers with expertise, but also to think from an entrepreneurial perspective where Company X is able to identify opportunities, and delivers real solutions based on a thorough understanding of their customer's business.
- Use of a collective approach based on teamwork to create added value by combining knowledge and building on each other's strengths instead of focussing on individual performance.
- Create openness through direct feedback, collective responsibility, and transparency. This should result in an open environment where questions can be asked, and the initiation of ideas is stimulated.

The organisational structure, and in particular the division between commercial people and others, causes a split in culture. Certain aspects of the desired culture, like being entrepreneurial in addition to providing expertise, are mainly applicable to the commercial people. Moreover, the fact that commercial people are engaged in customer contact, requires them to be more formal in certain aspects of their work. Regarding general internal behaviour, a positioning survey is performed on how people would describe Company X 's culture. Resulting from this survey, key words describing the internal behaviour are considerate, integer, friendly, and humane.

4.2 Strategy & objective-setting

The integration of ERM with strategy-setting, provides insight regarding the risk profile associated with strategy and business objectives (COSO, 2017). Understanding the business context, like trends and relationships that influence the organisation's current and future strategy and objectives, enables Company X to create a comprehensive risk profile.

4.2.1 Strategy & entity objectives

Company X 's ambition is to be the market leader in their focussed business direction. To realise this ambition, four main priorities are identified for 2017-2018 to realise progress:

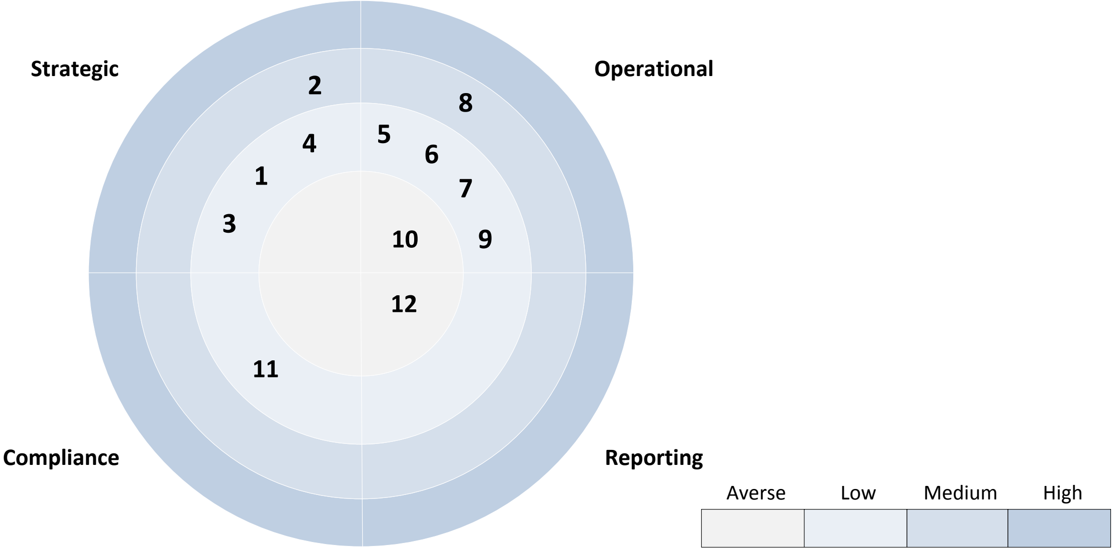
- ***Business direction***
  The development of a clear and shared market focus to prepare for sectors with growth opportunities, and to deepen the relationship with customers. Depending on the market of the individual offices, commercial employees are asked to participate in company-wide, strategic commercial activities, focussing on the most attractive customers, markets, and sectors.
- ***Authentic positioning***
  The implementation of authentic positioning is a five-phase process, to reposition Company X's brand distinctively. The gathering of information, and sessions with customers and employees resulted in a draft of five customer promises. The testing of these customer promises and the mapping of required resources, should ultimately result in the internal- and external roll-out of the final brand promise.
- ***Innovation***
  Transformation in the business of customers, mainly caused by digitalisation, requires Company X to keep developing their services and business model. In this regard, innovating is important to stay in touch with the needs of customers while staying focussed on Company X 's performance.
- ***Professional culture***
  By stimulating a professional culture as described in Section 4.1.2, Company X aims to fulfil their renewed brand promise, work on service improvement, and bring success in their focussed business direction.

Realising the strategy and corresponding four main priorities on an entity level, also require activities and projects on a business level. To achieve the ambitions, priorities are defined for daily practice in four categories: market, people, quality, and operational excellence. Examples of activities and projects are presented in Appendix E.

4.2.2 Define risk appetites

Company X acknowledges and accepts that their strategic choices and corresponding business goals and objectives expose the organisation to risk. The uncertainty this implies is inherent to doing business. The attitude towards individual risks depends on the characteristics of the risk category. Company X is relatively risk averse when it comes to for instance compliance and reporting risks since the degree to which the organisation should be able to control these risks is relatively high (COSO, 2004). On the other hand, market risk for instance also depends on the external environment (e.g. competitors, economy) and therefore, the organisation is not always able to provide the same level of assurance as to risks in the internal environment. This can cause the risk appetite for market risk to be higher.

To be able to assess the risks individually, the amount of risk Company X is willing to accept needs to be defined. In case the risk appetite of a risk is high, Company X's target residual risk is relatively high. When the appetite is averse, Company X's target residual risk is negligible. The risk appetites for the individual risks are determined in a session with the members of the project team and shown in Figure 4.2. The risk categories and corresponding individual risks are discussed in detail in Section 4.3.



Strategic	Operational	Compliance	Reporting
1) Reputation risk 2) Market risk 3) Financial risk 4) Culture risk	5) IT risk 6) Service risk 7) People 8) Customer risk 9) Control risk 10) Awareness risk	11) Compliance risk	12) Reporting risk

Figure 4.2: Risk appetites.

4.3 Performance

Identifying, assessing, and responding to risks is often a key part of risk management practices. By assessing risks, the actual performance regarding the identified risks for Company X can be determined by looking at whether residual risks are within risk appetites.

4.3.1 Risk identification

Resulting from multiple interviews with internal stakeholders (see Appendix A) and reports from different departments, the main risks for Company X have been identified. The initial categorisation and description of these risks have already been discussed in Section 2.2. The initial categorisation comprised five categories: financial, strategic, operational, compliance, and reporting. In the proposed risk control framework, 'financial' will not be treated as a separate category. Instead, I apply the categorisation as defined by COSO (2004) to Company X:

- ***Strategic***
  Company X should think of risk in relation to high-level goals, aligned with and supporting its mission. The uncertainty of changing market conditions requires Company X to create a professional environment where adaptability enables Company X to fulfil the need of their customers.
- ***Operational***
  Operational risk refers to Company X's risk in relation to operational practices, and the effective and efficient use of resources. Company X should think of people in relation to their capability in providing and improving services, and take the risk and opportunity associated with business decisions into consideration.
- ***Compliance***
  Company X's ability to abide relevant laws and regulations, which is important in providing services. Not doing so directly endangers Company X's integrity and reputation.
- ***Reporting***
  Company X should provide uniform reporting standards and guarantee reliability regarding the provision of information.

To keep the framework clear and accessible, I grouped together or renamed some of the risks as discussed in Section 2.2. This results in the definition of twelve main risks, which are divided into the respective categories based on their characteristics (see Figure 4.3). The division does not exclude that a risk can fall into more than one of the categories, but instead indicates in which category the risk fits best.

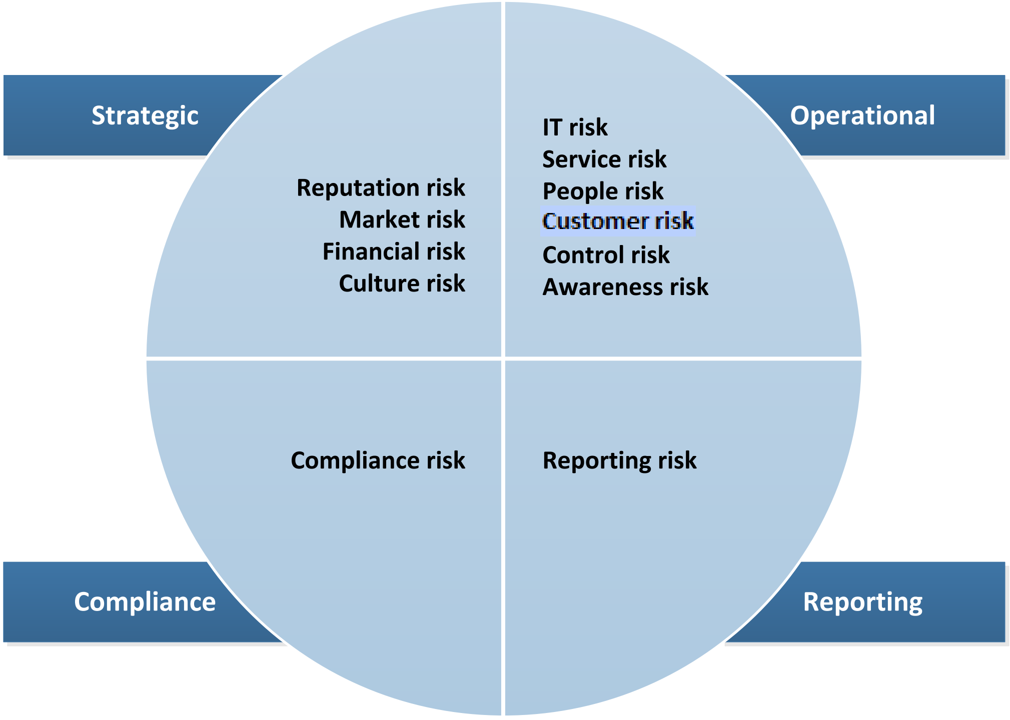


Figure 4.3: Risk categories and main risks.

Strategic

Reputation risk

Trend: Inherent to doing business is the risk of reputation damage. The reputation of Company X is founded on trust from its employees, customers, regulators and from the public in general. Isolated events can undermine that trust and negatively impact Company X's reputation as a whole. Creating a strong and reliable reputation should ultimately result in the realisation of Company X's ambition of being the market leader in their focussed business direction.

Impact: The reputation of Company X is crucial in realising their ambition. Reputation damage can cause disruption in establishing and keeping customer relations, and in attracting the best people.

Mitigation: Company X works together closely with customers to formulate clear customer promises. In 2015/2016, Company X started with gathering information from employees and customers to reposition the brand distinctively. This resulted in five customer promises that can be used as a starting point for customer dialogues. In 2017/2018, the specific resources needed for the positioning statement and promises were defined, so the authentic positioning can eventually be rolled out internally and externally. Employees are stimulated to operate according to these promises and Company X's values. Project A and a professional culture should align individual behaviour with Company X’s brand. In addition, Company X invests heavily in information security related to the ICT environment as well as to physical storage, which are audited regularly.

Market risk

Trend: After the crisis, companies have profited from the economic recovery. Developments like increasing digitalisation lead to new forms of services. While this presents exciting opportunities to differentiate from the competition, it also brings new risks with regards to innovation choices. Events like the Brexit show how unpredictable the market is and that disruption is always possible. Lastly, increasing competition causes margins to be under pressure.

Impact: Changing market conditions might cause Company X to pursue different customers, offer innovative services, and operate more efficiently. Moreover, new entrants offering digital services at a lower price might threaten profitability.

Mitigation: Closely monitoring the market enables Company X to spot opportunities and changing market conditions at an early stage. Project B must strengthen customer focus and collaboration. Lastly, striving for steady innovation must enable Company X to stay ahead of their competitors.

Financial risk

Trend: To stay in business and grow sustainably, Company X must operate profitably. Over the last years, the development of margins has been stable. However, it remains important to monitor developments in the markets Company X operates in to stay competitive and ensure profitability. In addition, the Finance department monitors Company X's liquidity and solvency. Company X should be able to meet its financial obligations, both on the short- and long-term. It is therefore important to keep paying attention to the management of working capital and to ensure financing by external parties.

Impact: Not being able to meet financial obligations can endanger Company X's continuity and its ability to do business.

Mitigation: Paying close attention to customer contracts must ensure Company X engages with customers on favourable terms. Monthly and quarterly reporting must provide a good overview of the financial situation. By making reports regularly, (negative) developments can be spotted easily. Besides the internal reporting, a regular external audit is performed. For the management of working capital, quick billing of expenses is important.

Culture risk

Trend: The culture and behaviour of Company X contribute to a stimulating working environment. By stimulating the professional culture of Company X, employees and contractors are enabled to develop, and an atmosphere of mutual trust is created. Developing this culture can be realised by focussing on entrepreneurship, a collective approach where teamwork is emphasized, and moving towards openness through direct feedback, shared responsibilities, and transparency.

Impact: By not creating a professional, open environment, people might not be able to reach their full potential. The development of culture helps with brand positioning and the improvement of services.

Mitigation: To create an open environment, Project A has been introduced. To build trust and create social control, there are whistleblower and trust regimes. Regular workshops and trainings must ensure that individual behaviour is aligned with the organisational culture.

Operational

Information technology risk

Trend: To further enable collaboration and supporting business intake within Company X, ICT services have been centralised and harmonised. This however increases the risk of critical ICT systems having restricted availability or being unavailable. Failing ICT systems will endanger the continuity of Company X. Data should be recoverable in the case of a risk event and employees should at all times be able to do their job. By storing documents in the cloud, Company X does not have to rely on a single physical storage. At the same time, digitalisation increases the risk of cyberattacks, since the information systems contain a lot of sensitive information about customers that should be protected. Improvement of the overall ICT infrastructure remains a point of attention.

Impact: The disability to withstand the loss of critical systems can come at a high cost. Studies suggest that companies losing critical systems for more than ten days quickly file for bankruptcy and companies suffering a catastrophic loss of data and equipment without a business continuity plan in place go out of business within 24 months of the loss (Krell, 2006). Relating to a cyberattack, different consequences may occur depending on the kind of attack. The company can have financial losses due to the theft of (confidential) company and customer information, or a disruption in business continuity. An attack can also damage customer trust and consequently Company X's reputation.

Mitigation: The ICT helpdesk is available to help solve general problems regarding the ICT infrastructure. The ICT department additionally defines for instance the maximum tolerable period in which data might be lost from an ICT service due to a major incident. Stress tests must show whether Company X is able to recover within this tolerable period. Additionally, Company X invests heavily in protection against cyberattacks.

Service risk

Trend: To be able to provide customers with the solutions they desire, the quality and innovation of services is essential. Transformations in the business of customers, primarily digitalisation, can cause current services to become ineffective, and at the same time offers opportunities for future business.

Impact: Quality and innovation of services are key in attracting and retaining customers. In case Company X is not able to provide the right service for the needs of their customers (in the future), this might result in a loss of business.

Mitigation: To stay in touch with the needs of their customers, regular customer satisfaction assessments are performed. Quality of service also means complying with relevant laws and regulations. In addition to the internal procedures, external supervision provides assurance that the quality of services is vouched for. Corresponding with the business objective of continuous innovation, ideas for new services, sectors, and themes are identified and prioritised. This must result in the development of cross department innovations.

People risk

Trend: People are key in offering services to customers. Therefore, attracting and retaining the best people, and giving them the opportunity to develop is important. The appointment of new board members must be well founded, taking into account individual capabilities as well as the size of the respective department. Continuity in critical partner and employee positions should remain monitored to ensure critical knowledge and capabilities are warranted in case of people leaving. Lastly, screening procedures for new employees have been intensified over the years.

Impact By not creating sufficient development possibilities for employees, Company X might fail to attract and retain the best people. Since employees are key in offering the best solutions to customers, not being able to attract the right people might have consequences for the success of doing business. With the disappearance of employees from critical positions of the organisation, knowledge and capabilities that are important for the business could potentially be lost. Furthermore, underutilisation can cause a decrease in quality of work, or result in health issues. Finally, the use of a flexible layer of personnel might cause safety risks regarding confidential information because of limited loyalty.

Mitigation: To ensure professional development, employees receive education and training. In addition, periodic reviews are conducted to assess individual performance and to discuss career path opportunities. Critical positions with corresponding knowledge and capabilities are monitored and mapped. Adequate back-ups for these critical positions must ensure a smooth transition in case of a sudden departure. Potential employees are screened intensively by an external party (i.e., certificate of conduct, references) before entering a working relationship.

Customer risk

Trend: Thorough selection of customers helps to determine whether Company X will be able to provide the quality of service customers demand and whether the customers satisfy the requirements from Company X.

Impact: Insufficient customer selection may lead to undesirable contracts, causing margins to be under pressure. Furthermore, it might negatively affect Company X's ability to get paid. By engaging in unfavourable contract, the customer base does not grow sustainably.

Mitigation: This sub section has been intentionally left out for confidentiality purposes.

Control risk

Trend: Unpredictable process environments in which control measures are inadequate or absent remain a point of attention. Reasonable deliberation regarding monitoring and control processes is required, while a high level of bureaucracy is undesirable.

Impact: As a result from insufficient internal control, process goals are not always well defined, ICT tools are utilized suboptimally and staff might not always be aware of their tasks and responsibilities, or might not possess the right capabilities. Control measures that are designed or implemented do not always work effectively. Consequently, this leads to inadequate separation of functions and inefficient processes.

Mitigation: The mapping of control measures must provide an overview to stakeholders about control processes. By paying attention to responsibilities, managers, employees and contractors are made aware of their tasks and roles in the internal control process.

Awareness risk

Trend: In the last few years, Company X has worked towards the creation of a complete risk overview. By composing a project team and proposing a risk control framework as a basis for risk management dialogues, Company X strives towards mapping the risks faced by the organisation to the best of its ability.

Impact: Not being aware of all the risks in the organisation makes it impossible to come up with appropriate mitigation measures or to seize opportunities. This might for instance have financial or reputational consequences. In addition, the reporting of the overall risk profile of the organisation might be incorrect.

Mitigation: The proposed risk control framework provides an overview of the risks Company X faces. Periodic assessment of the main risks and opportunities by departments, together with reviewing and discussing the risks in the framework, should result in a complete overview and increased risk awareness.

Compliance

Compliance risk

Trend: Company X does business in accordance with laws and (professional) regulations in the jurisdictions in which it operates. Company X notices that regulation in society is generally increasing. Although this offers opportunities for new business, Company X also increasingly needs to comply with applicable laws and regulations, whilst pressure in the market increases in terms of financial performance to develop the market position. A recent example of such regulation is the General data Protection Regulation (GDPR). Internal policies and codes of conducts are developed and implemented to help Company X reach this goal.

Impact: This sub section has been intentionally left out for confidentiality purposes.

Mitigation: The compliance office is observant when it comes to new developments in laws and regulations. They are responsible for monitoring and advising the board to implement new requirements in a timely manner.

Reporting

Reporting risk

Trend: With offices in different countries, unambiguous reporting is important. Written reports regarding financial statements, corporate social responsibility, and law and regulations requirements must provide the same quality and use of standards, reflecting the current state of the organisation.

Impact: Misstatements in reporting might cause disturbance internally or the need for rectifications externally. This might influence Company X's reputation by damaging their credibility.

Mitigation: Reports are checked and reviewed extensively by both the authors and management. Next to the internal control measures, the external auditor performs a quarterly review in the form of an external audit. Together, this should provide assurance that the reports provide a true and fair overview.

4.3.2 Risk assessment

In Section 4.3.1, twelve main risks for Company X have been identified. To understand Company X's exposure to these risks in relation to the achievement of its strategy and objectives, and risk appetite, they are assessed. Since it is neither practicable, nor cost-effective to obtain sufficient data for quantification, the risks will be assessed using a qualitative approach. Qualitative assessments are more efficient to complete, but the ability to identify correlation between the risks or perform a cost-benefit analysis is limited (COSO, 2017). The qualitative approach consisted of:

- Interviews with different internal stakeholders by the project team (see Appendix A).
- Review of the annual business plans from Company X's departments where they indicate their main risks and opportunities.
- Review of previous risk assessments (e.g. Appendix B).
- Sessions with the project team to discuss classifications of individual risks.

This way, the qualitative assessment takes into account different internal stakeholders:

- The departments and their employees.
- The second line of defence, consisting of the compliance office and financial control.
- A member of the executive committee.

For the assessment of the risks, I use the same classifications as in the initial overview of the project team (as described in Section 2.2): negligible, low, medium and high. By using these four categories, the relative importance of the risks can be easily represented. In addition, this classification is also similar to the way in which departments report their main risks in their annual business plans, so changing would be impractical. The global meaning of the different classifications is shown in Appendix C.

Prob. **Impact**	**Negligible**	**Low**	**Medium**	**High**
High	🟩	🟨 Service risk Customer risk	🟥 Market risk Culture risk People risk Compliance risk	🟥 Reputation
Medium	🟩	🟨 Reporting risk	🟨 IT risk Control risk	🟥
Low	🟩	🟩 Awareness risk	🟨 Financial risk	🟨
Negligible	🟦	🟩	🟩	🟩

Figure 4.4: Risk matrix.

Negligible inherent risk	🟦
Low inherent risk	🟩
Medium inherent risk	🟨
High inherent risk	🟥

Inherent risk

The risk appetites for the main risks are already described in Section 4.2.2. To determine the inherent risk exposure, a risk matrix is used. In the matrix, *probability* is the likelihood that an event occurs that influences the achievement of objectives. *Impact* is the degree to which the event affects the organisation. By using the described qualitative approach, the probability and impact of the twelve main risks are assessed, resulting in the risk matrix in Figure 4.4. The combination of probability and impact determines the inherent risk classification. The probability, impact, and inherent risk classifications are also represented in Appendix F (1/2).

Mitigation measures

For every main risk and its components, the (possible) control processes to mitigate the risk are listed (see Appendix F). For every control process, the effectiveness is assessed, together with the frequency in which these processes are conducted. The frequency can be none-existent, on-going, regular, or ad-hoc. Subsequently, I determine the overall control effectiveness of the mitigation measures which are represented in Table 4.2.

Residual risk

Where inherent risk indicates the amount of risk before mitigation measures are considered, residual risk is the risk that remains after mitigation. Company X's target is to bring the residual risk within the risk appetite. By considering the inherent risks and overall effectiveness of mitigation measures for the twelve main risks, I assess the residual risks which are represented in Table 4.2.

Table 4.2: Classification main risks.

Risk	Risk appetite	Inherent risk	Mitigation measures	Residual risk
1) Reputation risk	Low	High	Medium	Medium
2) Market risk	Medium	High	Low	Medium
3) Financial risk	Low	Medium	High	Low
4) Culture risk	Low	High	Medium	Low
5) IT risk	Low	Medium	Medium	Low
6) Service risk	Low	Medium	Medium	Low
7) People risk	Low	High	Medium	Medium
8) Customer risk	Medium	Medium	Medium	Low
9) Control risk	Medium	Medium	Low	Medium
10) Awareness risk	Averse	Low	Medium	Negligible
11) Compliance risk	Low	High	High	Low
12) Reporting risk	Averse	Medium	Medium	Negligible

When comparing the risk appetites with the residual risks, it can be noticed that for two of the twelve main risks, the residual risk is not within Company X's risk appetite. I will discuss these risks individually:

- **Reputation risk**
  Company X's risk appetite for reputation risk is low. By conducting business, Company X is inevitably exposed to this kind of risk on a daily basis. Despite the positioning project, Project A, and culture and behaviour, the possibility of losing a laptop, a customer being unsatisfied, or negative reporting about Company X remains. Therefore, the residual risk is still classified as medium. Although this is not within the risk appetite, it is neither desirable, nor cost-effective to prohibit for instance the use of personal laptops or to monitor the performance and behaviour of Company X's professionals more intensively. By defining a low risk appetite, Company X strives to keep improving current mitigation measures and to identify possible new ones as long as the benefits outweigh the downsides. For now, the residual risk is retained.
- **People risk**
  Company X's risk appetite towards people risk is low. The residual risk is however medium and therefore not within the risk appetite. People risk consists of several components (see

Appendix F). Over the last years, Company X has intensified screening procedures for new employees which increases the control effectiveness. However, departments still feel the risk of underutilisation is present, as well as limited back-ups for critical positions which might cause the loss of knowledge and capabilities in case of departure. Therefore, the current residual risk does not match Company X's risk appetite. Lining up critical positions more frequently and creating adequate back-ups can help to reduce the residual risk further. Otherwise, Company X might want to change its appetite.

4.3.3 Main opportunities

The main focus of this report is to identify downside risks and to come up with appropriate mitigation actions, rather than the identification of opportunities. In general, efforts to seize opportunities are limited compared to mitigation actions, although it could help to reduce the negative effects of risk (Oliviera et al., 2018). Therefore, I will list the main opportunities for Company X, resulting from the interviews (see Appendix A) and departments' business plans.

- **ICT improvement**
  Besides cyberattacks, many departments see ICT as an opportunity, rather than a risk. Improving the ICT infrastructure offers opportunities for the development of new tools, improving efficiency and monitoring performance.
- **Cross department initiatives**
  Increased collaborations between departments should enable Company X to reach more customers by developing new services and improving existing ones. Furthermore, inter-office cross selling by introducing, for instance, historical Dutch customers to Company X's international offices can increase business.
- **Alternative business**
  The identification of alternative, or fast-growing, business and service areas can help in creating a diverse portfolio of customers and sustainably grow the business. In this regard, it is important to attract relevant experts to increase Company X's knowledge on these topics.

4.3.4 Portfolio view

ERM aims to approach risk from an entity-wide, or portfolio, perspective (COSO, 2017). Such a portfolio view must enable Company X to think of risks in relation to strategy and objectives, and to each other. When Company X's strategy is to be the market leader in their focussed business direction, it is for instance important to think about this strategy in relation to attracting and retaining capable individuals, as well as to how compliance with laws and regulations can position Company X as a trustworthy business partner. Moreover, treating risks in so called "silo's" might enable individual business units to specialize their approach to reduce individual risks, but does not consider the organisation as a whole. At Company X, different departments experience different amounts of risk, for instance regarding competition. This is acceptable as long as the overall risk remains within Company X's risk appetite, which can only be assessed by using a portfolio view. Lastly, developing a portfolio view might help in showing how risks can offset each other. Strengthening the professional culture at Company X for example, helps in reducing reputation risk.

COSO (2017) distinguishes four levels of integration in the development of risk views. With minimal integration (risk view), only individual risks are considered. Limited integration (risk category view), allows for risks to be organised in categories, while partial integration (business objective view) also considers business objectives. Lastly, full integration (portfolio view) adds the layers where Company X's strategy and entity objectives are considered. This portfolio view for Company X is represented in Figure 4.4.

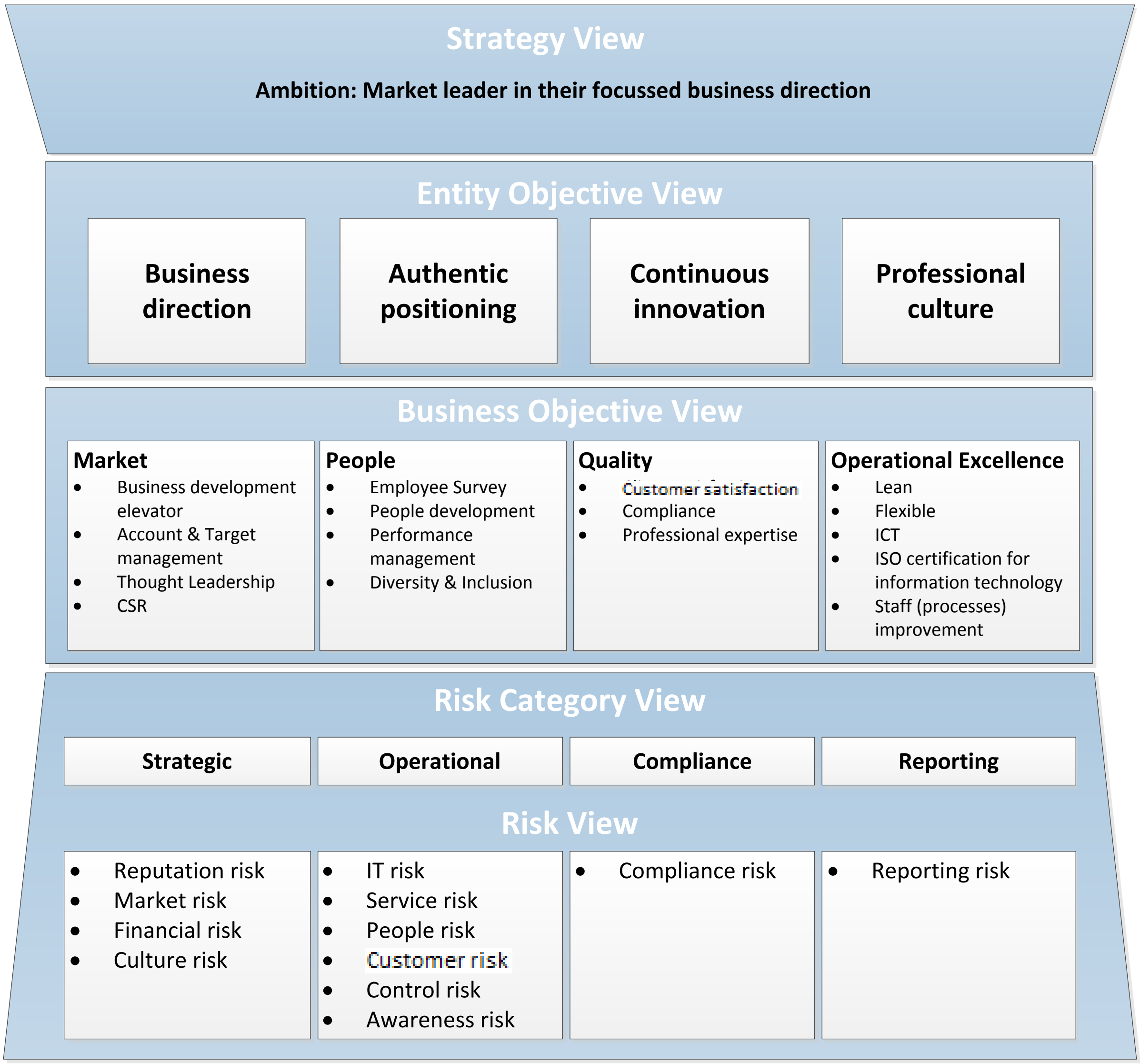


Figure 4.5: Portfolio view of risk - Adapted from COSO (2017).

4.4 Review & revision

Changes in the business context of the organisation might cause the need to revise the risk control framework and its corresponding practices. Therefore, it is important to identify triggers for reassessment to integrate reviews into business practices.

4.4.1 Assess substantial change

Organisations are usually able to anticipate changes in relation to strategy, culture and operational performance. However, attention should also be paid to substantial change in the underlying assumptions that make up the framework's components. According to COSO (2017), substantial internal and external changes related to the business context require identification because they might affect the entire attitude towards risk. Some examples will be discussed below.

Internal change

Leadership & staff: Change in leadership can affect the attitude towards risk management. A new leader might approach risk management differently by focussing on risk performance without linking it to risk appetite or organisational culture.

Innovation: The introduction of innovations might change risk responses or management's attitude towards risk. For example, staff might need training as a result of an innovation in the ICT environment. At the same time, such an innovation can increase management's ability to monitor performance.

External change

Market environment: Changes in the competitive environment, or political events like the Brexit can cause disruption in the way Company X does business. Besides the individual risks that are affected, the need to implement another strategy can also influence the entire risk appetite.

Laws & regulations: New laws and regulations may cause staff to work according to new policies, or force Company X to pursue other type of customers, resulting in a changing risk profile.

4.4.2 Review risk and performance

Besides the assessment of underlying assumptions that make up the framework, the risk mapping and risk performance need to be reviewed. To do so, questions that need to be answered are for instance whether the description of risks is complete, the risk classifications still representative, the level of residual risk matches the organisational risk appetite, and opportunities are pursued in the way they should? In case the answers to these questions are not within acceptable boundaries, Company X might want to review, and possibly revise, specific components of the risk control framework as discussed in this chapter.

4.4.3 ERM improvement

Assessing change, and reviewing risk and performance must ultimately contribute to the improvement of ERM practices within Company X. Management should pursue steady improvement at all levels by embedding evaluations into business practices, while pursuing opportunities to improve efficiency and usefulness of ERM (COSO, 2017). Improvements might further result from new technology, analysing shortcomings in dealing with risk events, or peer comparison. In Chapter 5, the application of ERM will be discussed more specifically.

4.5 Information, communication & reporting

Nowadays, organisations face an increasing amount of information they have to deal with. Technology has made it easier to collect, store and share this information, but this might also create an overload. Therefore, it is important to communicate the right information to the right people, to support decision-making in all layers of the organisation.

This chapter provides a portfolio view of risk. The main risks on an entity level are discussed, together with their severity and possible impact on the achievement of Company X's strategy and business objectives. In doing so, a high-level overview is created which provides the overall risk profile of the organisations to relevant stakeholders. Additionally, this report provides a structured basis for risk management dialogues. Chapter 5 will address how risk management practices can be communicated and reported, and how this results in the right information ending up with the right people.

5. APPLICATION

In Chapter 5, I discuss the application of the proposed risk control framework. In Section 5.1, I propose a maintenance process, where after critical success factors are discussed in Section 5.2. Chapter 5 ends with the definition of typical ERM activities and responsibilities for the board and risk committee in Section 5.3.

5.1 Maintenance process

The framework as discussed in Chapter 4 provides a comprehensive overview of the risks and (desired) risk management practices in the organisation. Keeping the framework up to date is important for risk management practices to be effective. Therefore, a process for maintenance is discussed in this section, together with the identification of specific triggers for reassessment of the framework.

Generally, the risks faced by Company X will be reviewed once a year. The departments, report the most important risks they encounter in their daily practice, together with opportunities that could be pursued. Until now, departments were asked to think about specific risks (e.g. market risk, operational risk, human resources risk). In the new situation, departments can use the risks from the proposed framework as reference and must be encouraged to think beyond the framework to spot new risks as well. In addition to naming the risks, the departments are asked to think about the possible impact and probability of occurrence. Impact and possibility ratings will consequently be used to determine the overall risk classifications. Lastly, the annual business plans of the departments are discussed in a meeting with all the department managers.

Based on the annual business plans of the departments, the framework must be updated to make sure it is a good representation of the current situation. The risk project team will incorporate significant changes, resulting from the business plans and department managers meeting, in the risk control framework. Subsequently, the updated framework is discussed in a meeting of the executive committee. They discuss for instance whether the framework represents the overall risk profile of the organisation, whether the control measures function as intended, and if appropriate actions are taken to deal with possible residual risks.

Identifying triggers for reassessment must enable Company X to review risk management practices in case of an event that might change the overall risk profile. Examples of triggers are the introduction of a new strategy or policy plan, change in the underpinning risk appetite, a significant increase/drop in revenue or margin, or innovations that might disrupt the industry. The overall process for maintenance and improvement of the risk control framework is represented in Figure 5.1.

5.2 Critical success factors in ERM implementation

Although more and more companies are embracing ERM in response to regulators calling for its adoption, its implementation remains poorly integrated (Arena et al., 2010). Oliviera et al. (2018) performed a literature review which identifies critical factors associated with ERM initiatives. The critical success factors (CSFs) are ranked based on a questionnaire that is conducted among risk management experts. The identified ten CSFs are discussed below, starting with the CSF that is ranked the highest (Oliviera et al., 2018).

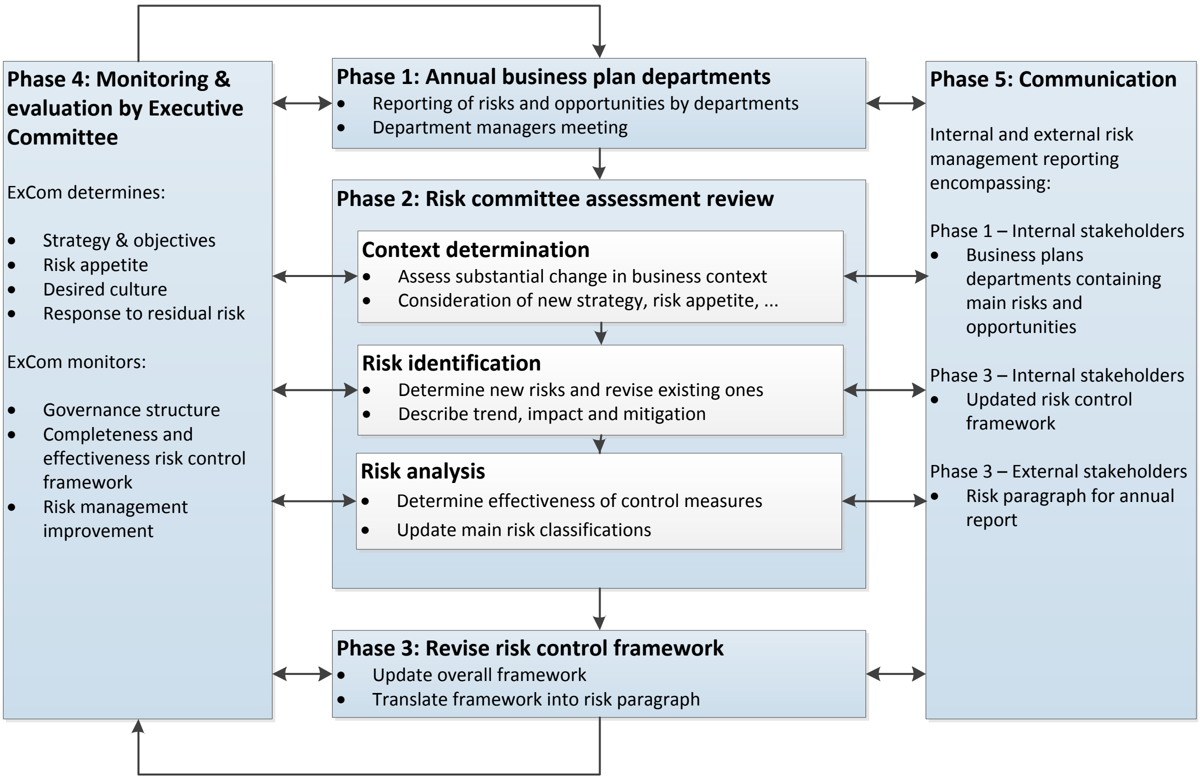

Phase 4: Monitoring & evaluation by Executive Committee
ExCom determines:
Strategy & objectives
Risk appetite
Desired culture
Response to residual risk
ExCom monitors:
Governance structure
Completeness and effectiveness risk control framework
Risk management improvement
Phase 1: Annual business plan departments
Reporting of risks and opportunities by departments
Department managers meeting
Phase 2: Risk committee assessment review
Context determination
Assess substantial change in business context
Consideration of new strategy, risk appetite, ...
Risk identification
Determine new risks and revise existing ones
Describe trend, impact and mitigation
Risk analysis
Determine effectiveness of control measures
Update main risk classifications
Phase 3: Revise risk control framework
Update overall framework
Translate framework into risk paragraph
Phase 5: Communication
Internal and external risk management reporting encompassing:
Phase 1 – Internal stakeholders
Business plans departments containing main risks and opportunities
Phase 3 – Internal stakeholders
Updated risk control framework
Phase 3 – External stakeholders
Risk paragraph for annual report

Figure 5.1 Process for maintenance and improvement - Adapted from risk-based approach according to ISO 31000.

- **High management commitment**
  A high commitment from management is important to make ERM a priority and essential to the organisation. Without it, ERM will most likely not become part of the corporate strategy or will not be integrated in the decision-making process (Oliviera et al., 2018).
- **Awareness and risk culture**
  Related to the first CSF to make ERM a priority in the organisation, is the creation of risk awareness and making ERM part of the organisational culture. This way, risks become a shared understanding and responsibility of all people. Therefore, Company X might want to make risk management part of their desired culture.
- **Risk identification, analysis and response**
  Risk identification, analysis and response are key components of many risk management frameworks like COSO ERM (2017), ISO 31000 (2009) and AS/NZS 4360 (1999). Including these actions in the proposed risk control framework helps with the identification of main risks, which improves the ability to come up with appropriate mitigation measures and reducing residual risk.
- **Focal point for ERM process**
  Although one could argue that the responsibility towards ERM is shared across organisations, Banham (2004) states the importance of having a responsible person to manage and supervise risks. Sometimes, organisations create a Chief Risk Officer position. Alternatively, Company X might want to make a senior executive or risk committee responsible for issues related to risk management.
- **Institution's compliance with laws and applicable regulations**
  Conforming to laws, regulations and internal policies stands out in literature as a relevant factor for ERM implementation (Oliviera et al., 2018), by contributing to the development of

ERM initiatives. At Company X, internal policies and compliance actions already reduce the exposure to risk in individual business units, as well as the general exposure to risk in the company.

- **Risk communication**
  Communicating information regarding risk management across Company X increases transparency and risk awareness. Moreover, it enables relevant stakeholders to use this information in decision-making (COSO, 2017).
- **Risk indicators, monitoring, review and improvement**
  Section 5.1 proposed a process for maintenance for Company X regarding the risk control framework. Monitoring and review must result in improvement of the framework so that it represents Company X's current situation. Identifying specific risk indicators for monitoring are beyond the scope of this research, but could possibly improve Company X's ability to monitor the main risks.
- **Tolerance and risk appetite**
  Risk appetite refers to the amount of risk Company X is willing to take in the pursuit of its strategy and objectives. The desired level (target) of residual risk must hereby fall within this risk appetite. As discussed in Section 3.1.4, this report does not use the concept of risk tolerance. Nonetheless, risk appetite and (target) residual risk are important components of risk management frameworks that balance the organisation's strategy and objectives, and the desired comfort level to achieve them (COSO, 2004).
- **Seizing opportunities**
  Often, the focus of risk management is on the mitigation of risks, while the effort to seize opportunities is limited. This is also reflected by the fact that seizing opportunities is among the least voted CSFs with very high influence in their research, which is remarkable since it could help to reduce negative effects of risk (Oliviera et al., 2018).
- **Resources availability**
  Resource availability, for instance qualified personnel, is important for Company X to improve risk management processes. However, since resource availability does not arouse risk awareness or incorporate ERM in the organisational culture, this CSF has less power compared to the other CSFs (Oliviera et al., 2018).

5.3 ERM activities & responsibilities

In Section 4.1.1, the governance structure for risk management was introduced, using the three lines of defence model to describe basic accountabilities for the various lines. In this section, risk oversight activities and responsibilities for senior management, the board of directors, and the risk committee are discussed in detail.

Senior management

Senior management is ultimately responsible for ERM and the overall culture, capabilities, and practices needed to achieve Company X's strategy and objectives. COSO (2017) defines responsibilities that typically belong to senior management:

- Defining Company X's core values, standards, expectations of competence, organisational structure, and accountability. Moreover, they provide leadership and direction to management functions.

- Evaluating different strategies, choosing one, and defining business objectives in line with this strategy. In setting these objectives, senior management should consider the business context, resources, and capabilities in relation to Company X's risk appetite.
- Overseeing the risks facing the organisation by directing management and staff to proactively identify, assess, prioritize, respond to, and report risks they encounter.
- Providing guidance to the development and performance of ERM practices across Company X, and delegating responsibilities to management functions.

Risk oversight

The board of directors is generally responsible for providing oversight, including oversight of risk management practices related to the proposed risk control framework. Since it is undesirable for the board of directors at Company X to hold complete risk oversight responsibility, specific tasks can be dedicated to the risk committee. By appointing two chairs from different departments, independence of the risk committee is stimulated. Both chairs discuss the topic 'risk' in their meetings with other managers and directors who are tasked with compliance and risk management to evaluate and improve risk management practices. The risk committee can be responsible for (COSO, 2017):

- Overseeing the proposed risk control framework, including the identification, assessment, prioritization, responding to, and reporting of risks.
- Communicating ERM practices to senior management and the board of directors Moreover, the risk committee escalates identified or emerging risk exposures.
- Acting as focal point for risk management, creating and maintaining relationships with those responsible for risk management practices in the different departments, and overseeing risk management ownership in the different lines of defence.
- Developing and improving the risk control framework by establishing new practices and policies to identify, assess and manage risks.
- Reviewing Company X's risk profile and whether residual risks are within Company X's risk appetites.

In addition, COSO (2017) identifies risk oversight activities for the board of directors related to the five components of the COSO framework, which are represented in Table 5.1. As mentioned, these activities can be (partly) dedicated to the risk committee.

Table 5.1: Board oversight activities (COSO, 2017).

ERM component	Risk oversight activities
Governance & Culture	• Assess the appropriateness of the Company X 's strategy, alignment to the mission, vision, and core values, and the risk inherent in that strategy. • Define the board risk governance role and structure including sub-committees for Company X. • Engage with management to define the suitability of ERM. • Oversee evaluations of the Company X's culture and that management remediates any noted gaps.

	• Promote a risk-aware mindset that aligns the maturity of Company X with its culture. • Oversee the alignment of business performance, risk taking, and incentives/compensation to balance short-term and long-term strategy achievement. • Challenge the potential biases and organisational tendencies of management and fulfil its independent and unbiased oversight role. • Understand Company X's strategy, operating model, industry, and issues and challenges affecting Company X. • Understand how risk is monitored by management.
Strategy & Objective-setting	• Set expectations for integrating ERM into the strategic management processes, including strategy planning, capital allocation, etc. • Discuss and understand the risk appetite and consider whether it aligns with its expectations. • Engage in discussions with management to understand the changes to the business context that may impact the strategy and its linkage to new, emerging, or manifesting risks. • Encourage management to think about the risks inherent in the strategy and underlying business assumptions. • Require management to demonstrate an understanding of the risk capacity of the entity to withstand large, unexpected events.
Performance	• Review Company X's strategy and underlying assumptions against the portfolio view of risk. • Set expectations for risk reporting, including the risk metrics reported to the board relative to Company X's risk appetite and external ERM disclosures. • Understand how management identifies and communicates the most severe risks as depicted by Company X's portfolio view. • Review and understand the most significant risks, including emerging risks, and significant changes in the portfolio view of risk and specifically what responses and actions management is taking. • Understand the plausible scenarios that could change the portfolio view.
Review & Revision	• Ask management about any risk manifesting in actual performance (both positive and negative). • Ask management about the ERM processes and challenge management to demonstrate the suitability and functioning of those processes.
Information, Communication & Reporting	• Identify information, underlying data, and formats required to execute board oversight. • Access internal and external information, and insights conducive to effective risk oversight.

	• Obtain input from external audit, and other independent parties regarding management perceptions and assumptions

6. SUMMARY AND CONCLUSIONS

This research project provides a clear approach towards risk management for Company X. We propose a comprehensive risk control framework to help Company X deal with the uncertainty the company inevitably experiences in the pursuit of its strategy and objectives. The main research question underlying this report was as follows:

How can Company X improve its internal control system by developing a framework that connects risk management to its strategic objectives?

By reviewing literature regarding risk management, it became clear that the traditional silo-approach associated with internal control in organisations is not sufficient anymore to deal with the fast-changing world Company X operates in. This traditional approach thinks of risks independent from each other, thereby neglecting the overall risk profile and strategic aspect. We have discussed the example of market risk, where departments experience a different level of competition. Resulting from this, these departments are exposed to different amounts of risk. These varying amounts of risks are acceptable as long as the overall risk for Company X remains within the risk appetite. This way, a negligible market risk exposure in one practice group can be offset by the high market risk exposure in another practice group. By using a holistic approach, Company X can see risks in relation to the company’s strategy and objectives, rather than individual hazards. This more complete view is commonly referred to as ERM.

The comparison of different ERM frameworks results in the adoption of the COSO ERM framework: *integrating with strategy and performance*. We adopt the five components of this framework to work out the proposed Company X risk control framework as described in Chapter 4. The effectiveness of ERM practices is related to the presence of the five components.

Twelve main risks have been identified, together with the control processes to mitigate these risks. We use a qualitative approach to determine whether the residual risks are within Company X's risk appetite. From this we conclude that residual risks are not within risk appetites for two of the twelve main risks. For reputation risk, it is neither desirable, nor cost-effective to increase mitigation measures at this time. Therefore, the medium residual risk is retained. For people risk however, continued efforts must make sure that the current medium residual risk will be reduced to match the low appetite. Literature also ranks risk identification, analysis and response as one of the most important factors for successful ERM implementation.

Other important factors for successful ERM implementation are commitment from management, awareness and risk culture, and a focal point for ERM. The proposed framework provides a clear approach towards risk management, but without commitment from senior management, it will not become a priority and essential to Company X. Furthermore, risk management should become part of Company X's culture to make it a shared understanding and responsibility of all people. I would therefore recommend adding risk management to Company X's culture. Lastly, by transforming the project team into a risk committee, one clear focal point for risk management practices is created. Besides being responsible for the effectiveness of the proposed framework and keeping it up to date, people across Company X can escalate identified and emerging risks to the risk committee apart from their direct manager.

Although the focus of this report is on managing downside risk, we present three main opportunities. Improvement of ICT must stimulate the creation of new tools, which can help to improve operational efficiency and monitor risk performance. In addition, continued efforts should go to cross department initiatives and the development of alternative business. Seizing these opportunities can also help to reduce the negative effects of risks.

With the help of the three lines of defence model, we define risk oversight activities and responsibilities for senior management, the board of directors, the risk committee, and staff. This way, people in every layer of the organisation are aware of their responsibilities. In addition, I propose a process of maintenance to keep the framework up to date and effective.

Altogether, the proposed risk control framework approaches risk from an entity-wide perspective, or portfolio view. This must enable Company X to think of risks in relation to its strategy and entity objectives, and to each other. In doing so, Company X's overall risk profile is considered instead of only mitigating risks in individual departments. Moreover, it provides insights in how some of the risks might offset each other. This should ultimately increase Company X's ability to bring residual risks within risk appetites, thereby providing reasonable assurance towards the achievement of Company X's strategy and objectives.

7. LIMITATIONS AND FURTHER RESEARCH

Limitations

The twelve main risks that are identified in this report are described from a high-level perspective so they represent the threats to Company X as a whole, rather than individual departments. Consequently, a qualitative approach has been used to classify Company X's risks, resulting in a global assessment of the residual risks Company X faces. Since quantification of the risks was undesirable and out of the scope of this research, the qualitative approach was an efficient way to assess the degree to which Company X is exposed to risks. At the same, this limits Company X's ability to identify correlation between risks or to perform a cost-benefit analysis. In the future, Company X might want to explore the possibility of increased risk quantification so that the risks can be assessed in more detail. This also improves Company X's ability to assess whether control processes function as intended. A quantitative approach might for instance encompass the definition of key performance indicators for the twelve main risks, or risk modelling. However, Company X first has to determine whether this is desirable and if the benefits of such a quantitative approach outweigh the costs.

We provide a comprehensive framework for risk management practices within Company X. However, the proposed framework is neither final, nor binding. Instead, this research aims to provide a clear approach towards risk management, including the assessment of risk appetites, probabilities, impacts, inherent risks, control processes, and residual risks, which can be used as a basis for further discussions and risk management dialogues. Although I believe that this report takes into account perspectives from various internal stakeholders, senior management still has to determine whether the proposed framework and corresponding risk assessments are representative for Company X as a whole. The current classifications might be partly subjective because they rely on personal interpretations and those of the project team (risk committee) members. This is also a result of the chosen qualitative approach.

Finally, the proposed framework still needs to be implemented. General responsibilities for senior management, the board of directors, risk committee, and staff have been defined, together with a process for maintenance to keep the framework up to date. However, this still needs to be applied to individual departments, for instance by appointing a focal point for risk management practices besides the risk committee. Perhaps the most important is that all people within Company X become aware that risk management is a collective responsibility. This might take time and requires continued efforts.

Further research

Although quantitative assessments are beyond the scope of this research, further research on this topic can help to improve risk management practices even more. The improvement of risk management in this research is primarily concerned with creating a comprehensive risk overview and increased risk awareness, whereas a quantitative approach also offers opportunities for risk monitoring and more specific risk assessments.

Quantitative assessment approaches allow for increased precision and support a cost-benefit analysis. Probabilistic models such as value at risk (VAR) can help to think of a range of possible risk events, together with the corresponding impact and probability of these events. Understanding how each risk factor could vary and impact the cash flow, for instance, allows management to better measure and manage risk (COSO, 2017).

In this research, we use the following risk formula to assess the twelve main risks (Cox Jr., 2008):

$$Risk = Probability * Impact$$

For the impact is defined when it is seen as negligible, low, medium, or high (see Appendix C). However, for probability we have not looked at which percentage corresponds to, for instance, the classification ‘negligible’. The risks with a very high impact and very low probability can be dangerous, since these could disrupt the whole organisation. Using VAR would require Company X to think about the probability (in percentages instead of qualitatively) of a potential loss and the height of that loss. When doing this for a range of possible events, VAR indicates the probability that a loss exceeds a certain amount over a period of time. The quantified potential loss for an individual risk event can be defined as the risk exposure, which is calculated by multiplying the probability with the potential loss. This also corresponds to the risk formula presented earlier. For Company X we have seen that a financial loss is high when it exceeds €500,000. An interesting question for further research might be for which probability Company X is willing to accept a loss of over €500,000 in a certain time period? However, to be able to determine this, quantification is required. Moreover, this raises the question to what extent it is beneficial to reduce the probability of such an event if this increases the cost of mitigation significantly. By using VAR, we ultimately want to make a statement like: “We are X percent certain that we will not lose more than V euros in time T” (Hull, 2015).

As mentioned, we assess the risk impact as negligible, low, medium, or high. For each classification, we define the meaning in Appendix C. A medium risk impact for instance, represents a monetary loss between €100,000 and €500,000. However, a risk event causing a loss of customers, media attention, a decrease in customer or employee satisfaction, or a change in competitive advantage can also be classified as medium. A loss of customers is relatively easy to express as financial loss compared to for instance media attention, since it directly decreases turnover. Then again, if this causes a loss between €100,000 and €500,000 the classification is medium, and if the loss exceeds €500,000 the classification is high. However, risk events like media attention, customer and employee satisfaction, and competitive advantage are much more difficult to express as a monetary amount. Instead, negative media attention might make it more difficult to attract new customers and consequently disables Company X to grow sustainably. Moreover, a decrease in employee satisfaction can cause these employees to be less productive. Although we cannot directly assign a monetary amount to these kind of risk events, there certainly is a loss of value. Thinking about this value quantitatively and how this affects Company X’s performance, might further improve risk management practices.

Another benefit of risk quantification is the increased ability to monitor risks. By defining key performance indicators (KPIs) for the main risks, it can be monitored whether risk performance is within acceptable variation. If we look for instance at financial risk, KPIs can for instance be the margin, solvability, and liquidity. These examples are already part of the periodic financial reporting at Company X, but KPIs could be useful for other risks as well.

IT risk is an example of a risk within Company X for which monitoring KPIs can be useful. Examples of possible KPIs are the number of events causing downtime, the actual downtime, and the number of cyberattacks. By using a dashboard to represent the KPIs graphically, Company X can easily see whether the KPIs are within acceptable boundaries, and how this performance relates to the same period in a different year. This way, Company X can also determine whether mitigation measures are effective and function as intended.

For people risk, KPIs might be the number of sick days per employee or the amount of trainings per time period. These examples also show that quantification does not mean that risks need to be expressed as a potential monetary loss. It differs per risk category how often certain risks arise and how quick they change. Operational and compliance risks are more likely to be experienced on a daily basis, whereas strategic risks like reputation risk and market risk are probably more difficult to measure, and more focussed on the long-term.

Concluding, there are enough opportunities for further research in the area of risk quantification. However, Company X first has to determine whether they think it is useful and if the increased efforts associated with quantification are beneficial from a cost-perspective.

REFERENCES

Anderson, D., & Eubanks, G. (2015). *Leveraging COSO across the three lines of defense.* New York: Committee of Sponsoring Organizations of the Threadway Commision.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society, 35*(7), 659-675.

Arndorfer, I., & Minto, A. (2015). *The "four lines of defence model" for financial institutions.* Basel: Bank for International Settlements.

Banham, R. (2004). Enterprising Views of Risk Management. *Journal of Accountancy, 197*(6), 65-72.

Basel Committee on Banking Supervision. (2010). *Consultative document: Principles for enhancing corporate governance.* Basel: Bank for International Settlements.

COSO. (2004). *Enterprise risk management - integrated framework; Executive summary framework.* New York: Committee of Sponsoring Organizations of the Treadway Commission.

COSO. (2009). *Strengthening Enterprise Risk Management for Strategic Advantage.* New York: Committee of Sponsoring Organizations of the Treadway Commission.

COSO. (2012). *Enterprise risk management - understanding and communicating risk appetite.* New York: Committee of Sponsoring Organizations of the Treadway Commission.

COSO. (2017). *Enterprise risk management - Integrating with strategy and performance.* New York: Committee of Sponsoring Organizations of the Treadway Commission.

Cox Jr., L. (2008). What's Wrong with Risk Matrices? *Risk Analysis, 28*(2), 497-512.

Gahin, F. (1971). Review of the Literature on Risk Management. *The Journal of Risk and Insurance, 38*(2), 309-313.

Gjerdrum, D., & Peter, M. (2011). The new international standard on the practice of risk management - A comparison of ISO 31000:20090 and the COSO ERM framework. *Risk management, 11*(21), 8-12.

Hull, J. C. (2015). *Risk Management and Financial Institutions.* Hoboken, New Jersey: Wiley.

IIA. (2013). *The three lines of defence in effective risk management and control.* Florida: The Institute of Internal Auditors.

ISO. (2009). *ISO 31000:2009 Risk Management - Principles and Guidelines.* Geneva: International Standards Organisation.

ISO. (2009). *ISO Guide 73: risk management - vocabulary.* Geneva: International Organization for Standardization.

Krell, E. (2006). *Management accounting guideline: Business continuity management.* Missisauga: CMA-Canada.

Leitch, M. (2010). ISO 31000:2009 - The new international standard on risk management. *Risk Analysis, 30*(6), 887-892.

Moeller, R. (2007). *COSO Enterprise risk management: Understanding the new integrated ERM framework.* Hoboken: Wiley.

Oliviera, K., Méxas, M., Meiriño, M., & Drumond, G. (2018). Critical success factors associated with the implementation of enterprise risk management. *Journal of Risk Research*, 1-16. doi:10.1080/13669877.2018.1437061

Olson, D., & Wu, D. (2008). *New frontiers in enterprise risk management.* Berlin: Springer.

Purdy, G. (2010). ISO 31000:2009 - Setting a New Standard for Risk Management. *Risk Analysis, 30*(6), 881-886.

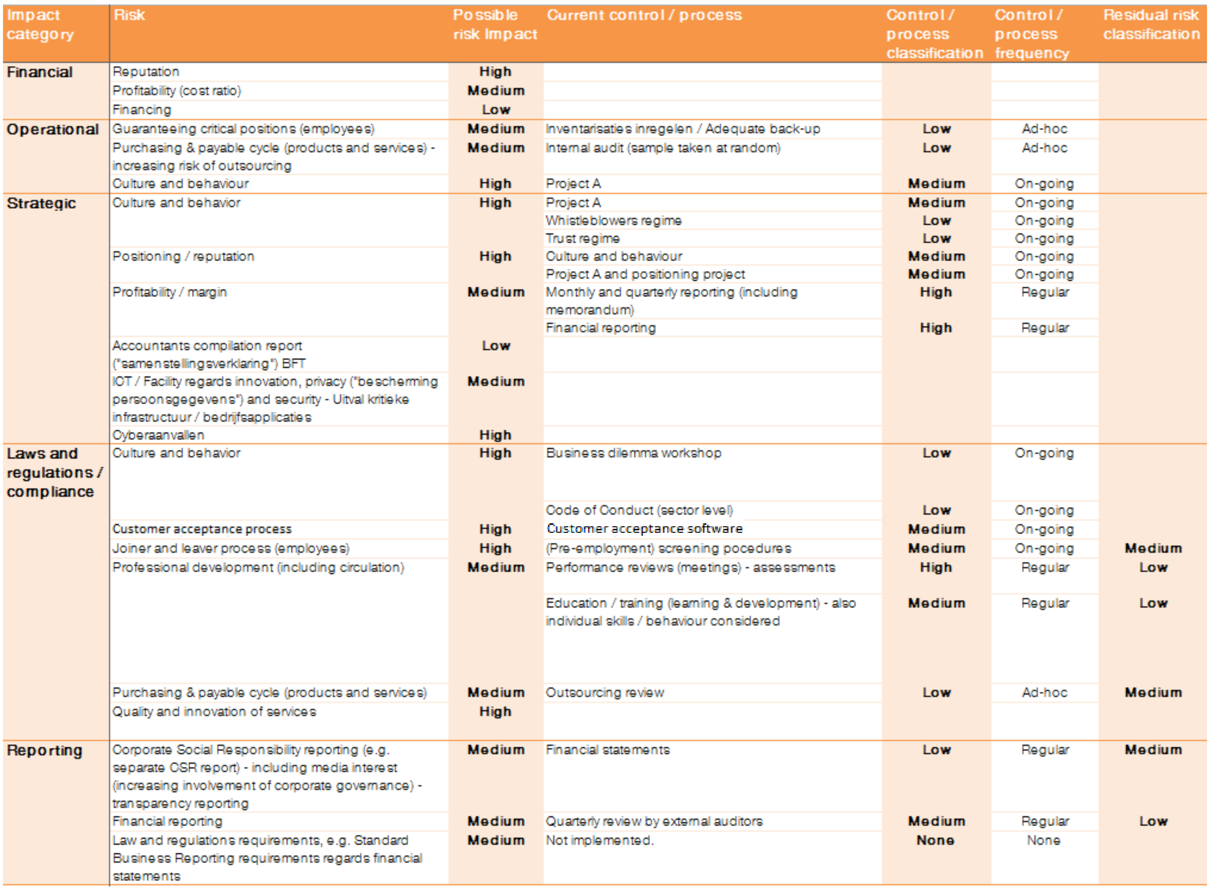
RIMS. (2012). *The Risk Perspective: Exploring Risk Appetite and Risk Tolerance.* New York: The Risk Management Society.

Standards Association of Australia. (1999). *AS/NZS 4360:1999 Risk Management.* Strathfied, NSW: Standards Australia.

APPENDIX A: FUNCTIONS PROJECT TEAM & INTERVIEWS

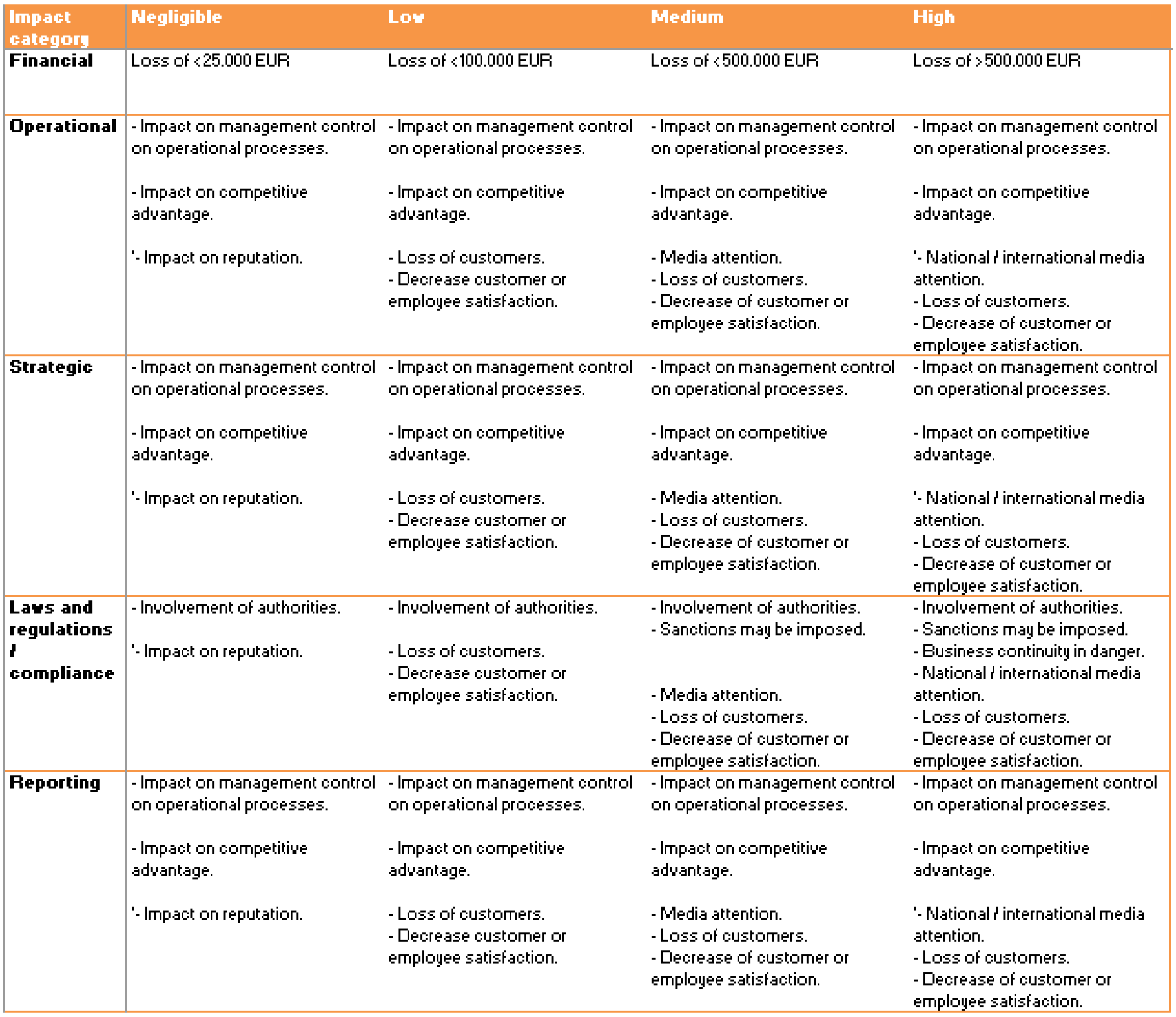
Appendix A is intentionally left out for confidentiality purposes.

APPENDIX B: INITIAL RISK OVERVIEW



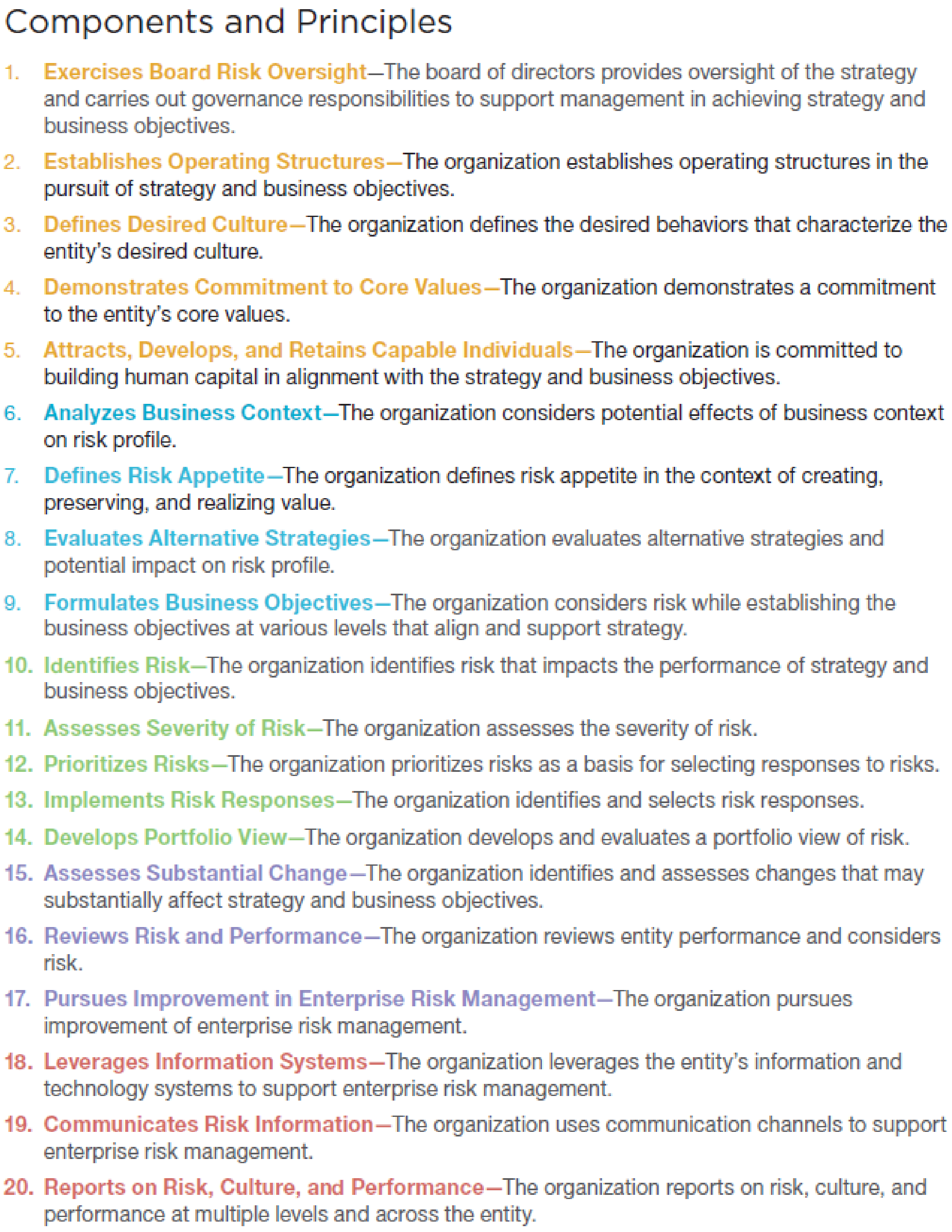
Impact category	Risk	Possible risk Impact	Current control / process	Control / process classification	Control / process frequency	Residual risk classification
Financial	Reputation	**High**				
	Profitability (cost ratio)	**Medium**				
	Financing	**Low**				
Operational	Guaranteeing critical positions (employees)	**Medium**	Inventarisaties inregelen / Adequate back-up	**Low**	Ad-hoc	
	Purchasing & payable cycle (products and services) - increasing risk of outsourcing	**Medium**	Internal audit (sample taken at random)	**Low**	Ad-hoc	
	Culture and behaviour	**High**	Project A	**Medium**	On-going	
Strategic	Culture and behavior	**High**	Project A	**Medium**	On-going	
			Whistleblowers regime	**Low**	On-going	
			Trust regime	**Low**	On-going	
	Positioning / reputation	**High**	Culture and behaviour	**Medium**	On-going	
			Project A and positioning project	**Medium**	On-going	
	Profitability / margin	**Medium**	Monthly and quarterly reporting (including memorandum)	**High**	Regular	
			Financial reporting	**High**	Regular	
	Accountants compilation report ("samenstellingsverklaring") BFT	**Low**				
	ICT / Facility regards innovation, privacy ("bescherming persoonsgegevens") and security - Uitval kritieke infrastructuur / bedrijfsapplicaties	**Medium**				
	Cyberaanvallen	**High**				
Laws and regulations / compliance	Culture and behavior	**High**	Business dilemma workshop	**Low**	On-going	
			Code of Conduct (sector level)	**Low**	On-going	
	Customer acceptance process	**High**	Customer acceptance software	**Medium**	On-going	
	Joiner and leaver process (employees)	**High**	(Pre-employment) screening pocedures	**Medium**	On-going	**Medium**
	Professional development (including circulation)	**Medium**	Performance reviews (meetings) - assessments	**High**	Regular	**Low**
			Education / training (learning & development) - also individual skills / behaviour considered	**Medium**	Regular	**Low**
	Purchasing & payable cycle (products and services)	**Medium**	Outsourcing review	**Low**	Ad-hoc	**Medium**
	Quality and innovation of services	**High**				
Reporting	Corporate Social Responsibility reporting (e.g. separate CSR report) - including media interest (increasing involvement of corporate governance) - transparency reporting	**Medium**	Financial statements	**Low**	Regular	**Medium**
	Financial reporting	**Medium**	Quarterly review by external auditors	**Medium**	Regular	**Low**
	Law and regulations requirements, e.g. Standard Business Reporting requirements regards financial statements	**Medium**	Not implemented.	**None**	None	

APPENDIX C: MEANING CLASSIFICATIONS



Impact category	Negligible	Low	Medium	High
Financial	Loss of <25.000 EUR	Loss of <100.000 EUR	Loss of <500.000 EUR	Loss of >500.000 EUR
Operational	- Impact on management control on operational processes. - Impact on competitive advantage. '- Impact on reputation.	- Impact on management control on operational processes. - Impact on competitive advantage. - Loss of customers. - Decrease customer or employee satisfaction.	- Impact on management control on operational processes. - Impact on competitive advantage. - Media attention. - Loss of customers. - Decrease of customer or employee satisfaction.	- Impact on management control on operational processes. - Impact on competitive advantage. '- National / international media attention. - Loss of customers. - Decrease of customer or employee satisfaction.
Strategic	- Impact on management control on operational processes. - Impact on competitive advantage. '- Impact on reputation.	- Impact on management control on operational processes. - Impact on competitive advantage. - Loss of customers. - Decrease customer or employee satisfaction.	- Impact on management control on operational processes. - Impact on competitive advantage. - Media attention. - Loss of customers. - Decrease of customer or employee satisfaction.	- Impact on management control on operational processes. - Impact on competitive advantage. '- National / international media attention. - Loss of customers. - Decrease of customer or employee satisfaction.
Laws and regulations / compliance	- Involvement of authorities. '- Impact on reputation.	- Involvement of authorities. - Loss of customers. - Decrease customer or employee satisfaction.	- Involvement of authorities. - Sanctions may be imposed. - Media attention. - Loss of customers. - Decrease of customer or employee satisfaction.	- Involvement of authorities. - Sanctions may be imposed. - Business continuity in danger. - National / international media attention. - Loss of customers. - Decrease of customer or employee satisfaction.
Reporting	- Impact on management control on operational processes. - Impact on competitive advantage. '- Impact on reputation.	- Impact on management control on operational processes. - Impact on competitive advantage. - Loss of customers. - Decrease customer or employee satisfaction.	- Impact on management control on operational processes. - Impact on competitive advantage. - Media attention. - Loss of customers. - Decrease of customer or employee satisfaction.	- Impact on management control on operational processes. - Impact on competitive advantage. '- National / international media attention. - Loss of customers. - Decrease of customer or employee satisfaction.

APPENDIX D: COMPONENTS AND PRINCIPLES COSO FRAMEWORK



Components and Principles

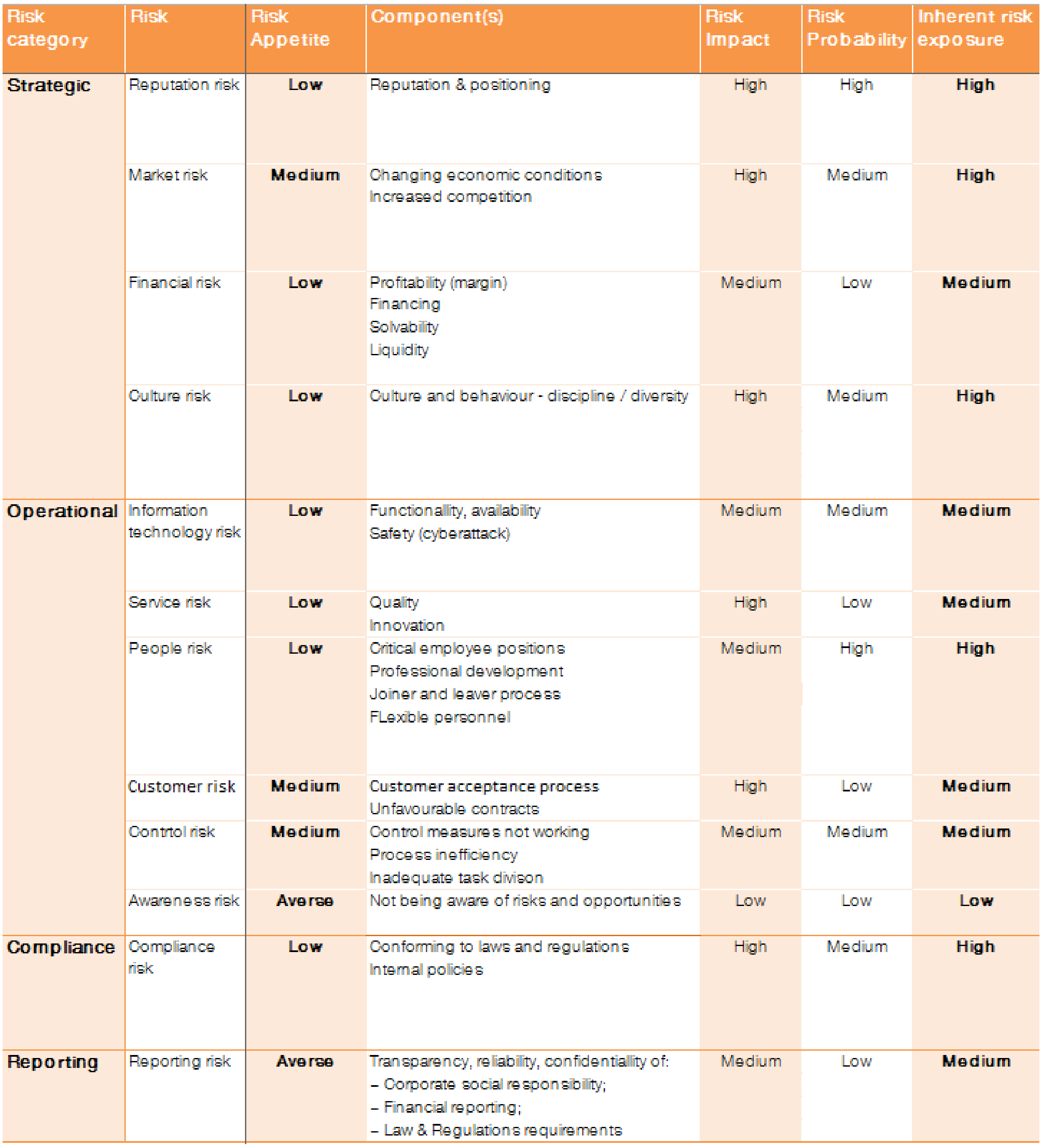
1. **Exercises Board Risk Oversight**—The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Operating Structures**—The organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Culture**—The organization defines the desired behaviors that characterize the entity's desired culture.
4. **Demonstrates Commitment to Core Values**—The organization demonstrates a commitment to the entity's core values.
5. **Attracts, Develops, and Retains Capable Individuals**—The organization is committed to building human capital in alignment with the strategy and business objectives.
6. **Analyzes Business Context**—The organization considers potential effects of business context on risk profile.
7. **Defines Risk Appetite**—The organization defines risk appetite in the context of creating, preserving, and realizing value.
8. **Evaluates Alternative Strategies**—The organization evaluates alternative strategies and potential impact on risk profile.
9. **Formulates Business Objectives**—The organization considers risk while establishing the business objectives at various levels that align and support strategy.
10. **Identifies Risk**—The organization identifies risk that impacts the performance of strategy and business objectives.
11. **Assesses Severity of Risk**—The organization assesses the severity of risk.
12. **Prioritizes Risks**—The organization prioritizes risks as a basis for selecting responses to risks.
13. **Implements Risk Responses**—The organization identifies and selects risk responses.
14. **Develops Portfolio View**—The organization develops and evaluates a portfolio view of risk.
15. **Assesses Substantial Change**—The organization identifies and assesses changes that may substantially affect strategy and business objectives.
16. **Reviews Risk and Performance**—The organization reviews entity performance and considers risk.
17. **Pursues Improvement in Enterprise Risk Management**—The organization pursues improvement of enterprise risk management.
18. **Leverages Information Systems**—The organization leverages the entity's information and technology systems to support enterprise risk management.
19. **Communicates Risk Information**—The organization uses communication channels to support enterprise risk management.
20. **Reports on Risk, Culture, and Performance**—The organization reports on risk, culture, and performance at multiple levels and across the entity.

APPENDIX E: BUSINESS OBJECTIVES

Appendix E is intentionally left out for confidentiality purposes.

APPENDIX F: RISK OVERVIEW

(1/2)

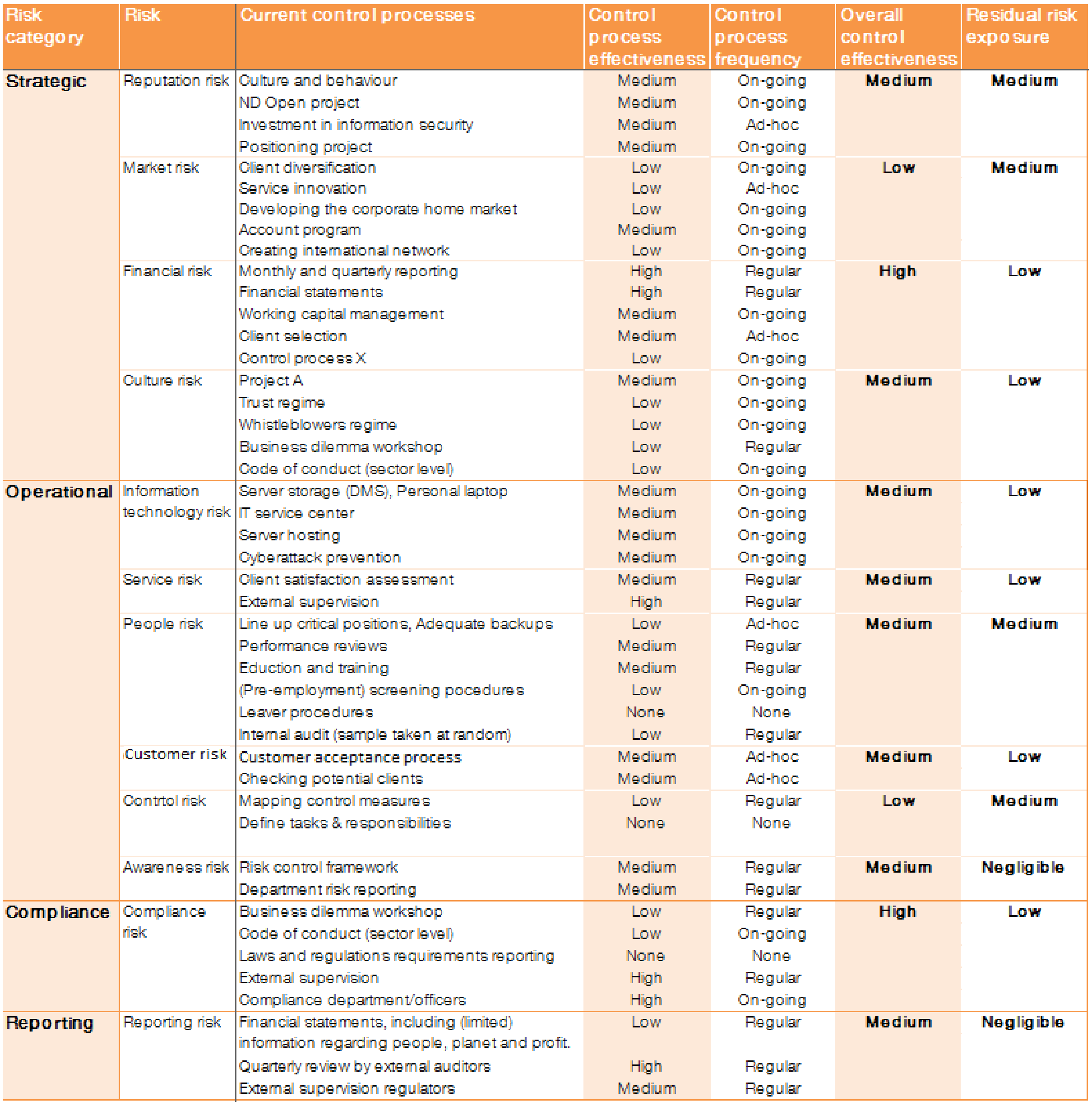


Risk category	Risk	Risk Appetite	Component(s)	Risk Impact	Risk Probability	Inherent risk exposure
Strategic	Reputation risk	**Low**	Reputation & positioning	High	High	**High**
	Market risk	**Medium**	Changing economic conditions Increased competition	High	Medium	**High**
	Financial risk	**Low**	Profitability (margin) Financing Solvability Liquidity	Medium	Low	**Medium**
	Culture risk	**Low**	Culture and behaviour - discipline / diversity	High	Medium	**High**
Operational	Information technology risk	**Low**	Functionality, availability Safety (cyberattack)	Medium	Medium	**Medium**
	Service risk	**Low**	Quality Innovation	High	Low	**Medium**
	People risk	**Low**	Critical employee positions Professional development Joiner and leaver process FLexible personnel	Medium	High	**High**
	Customer risk	**Medium**	Customer acceptance process Unfavourable contracts	High	Low	**Medium**
	Contrtol risk	**Medium**	Control measures not working Process inefficiency Inadequate task divison	Medium	Medium	**Medium**
	Awareness risk	**Averse**	Not being aware of risks and opportunities	Low	Low	**Low**
Compliance	Compliance risk	**Low**	Conforming to laws and regulations Internal policies	High	Medium	**High**

Reporting	Reporting risk	**Averse**	Transparency, reliability, confidentiality of:
			– Corporate social responsibility;
			– Financial reporting;
			– Law & Regulations requirements
				Medium	Low	**Medium**

APPENDIX F: RISK OVERVIEW

(2/2)



Risk category	Risk	Current control processes	Control process effectiveness	Control process frequency	Overall control effectiveness	Residual risk exposure
Strategic	Reputation risk	Culture and behaviour	Medium	On-going	**Medium**	**Medium**
		ND Open project	Medium	On-going		
		Investment in information security	Medium	Ad-hoc		
		Positioning project	Medium	On-going		
	Market risk	Client diversification	Low	On-going	**Low**	**Medium**
		Service innovation	Low	Ad-hoc		
		Developing the corporate home market	Low	On-going		
		Account program	Medium	On-going		
		Creating international network	Low	On-going		
	Financial risk	Monthly and quarterly reporting	High	Regular	**High**	**Low**
		Financial statements	High	Regular		
		Working capital management	Medium	On-going		
		Client selection	Medium	Ad-hoc		
		Control process X	Low	On-going		
	Culture risk	Project A	Medium	On-going	**Medium**	**Low**
		Trust regime	Low	On-going		
		Whistleblowers regime	Low	On-going		
		Business dilemma workshop	Low	Regular		
		Code of conduct (sector level)	Low	On-going		
Operational	Information technology risk	Server storage (DMS), Personal laptop	Medium	On-going	**Medium**	**Low**
		IT service center	Medium	On-going		
		Server hosting	Medium	On-going		
		Cyberattack prevention	Medium	On-going		
	Service risk	Client satisfaction assessment	Medium	Regular	**Medium**	**Low**
		External supervision	High	Regular		
	People risk	Line up critical positions, Adequate backups	Low	Ad-hoc	**Medium**	**Medium**
		Performance reviews	Medium	Regular		
		Eduction and training	Medium	Regular		
		(Pre-employment) screening pocedures	Low	On-going		
		Leaver procedures	None	None		
		Internal audit (sample taken at random)	Low	Regular		
	Customer risk	Customer acceptance process	Medium	Ad-hoc	**Medium**	**Low**
		Checking potential clients	Medium	Ad-hoc		
	Contrtol risk	Mapping control measures	Low	Regular	**Low**	**Medium**
		Define tasks & responsibilities	None	None		
	Awareness risk	Risk control framework	Medium	Regular	**Medium**	**Negligible**
		Department risk reporting	Medium	Regular		
Compliance	Compliance risk	Business dilemma workshop	Low	Regular	**High**	**Low**
		Code of conduct (sector level)	Low	On-going		
		Laws and regulations requirements reporting	None	None		
		External supervision	High	Regular		
		Compliance department/officers	High	On-going		
Reporting	Reporting risk	Financial statements, including (limited) information regarding people, planet and profit.	Low	Regular	**Medium**	**Negligible**
		Quarterly review by external auditors	High	Regular		
		External supervision regulators	Medium	Regular		