University of Stavanger

A guide on how to apply an uncertainty-based perspective in Enterprise Risk Management

Master Thesis autumn 2020
University of Stavanger

Paniz Golrang, 215197

University of Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme/specialisation: Risk Management	~~Spring/~~ Autumn semester, 2020 Open / ~~Confidential~~
Author: Paniz Golrang, 215197	
Supervisor: Professor Terje Aven	
Title of master's thesis: A guide on how to apply an uncertainty-based perspective in Enterprise Risk Management	
Credits: 30	
Keywords: COSO, ERM, risk management, beginner maturity, uncertainty	Number of pages: 61 + supplemental material/other: 16 Oslo, 13.12/2020

Acknowledgements

This thesis is the result of my two-year master's program in Risk Management at the University of Stavanger. I have gained insight in the implementation of an all-around risk management framework, and as a result, been appointed my dream job.

I wish to express my appreciation to my advisor, professor Terje Aven, who helped me put a name on the ideas I had regarding a beginner risk management guide which incorporated the entity as a whole, namely enterprise risk management. I would also thank Aven for the (nearly) countless books and materials he has published which has truly enhanced the risk industry.

I want to thank Statnett SF for believing in my abilities, letting me take inspiration from the day to day work I do here, as well as giving me the time off needed to write this thesis. I also want to thank all the fantastic risk professionals from Statnett, KPMG, and Equinor who have listened to my ideas, suggestions and helped me with questions and enquiries, and in that way help me with becoming a better risk manager.

Lastly, I want to thank Einar, who has been on my side cheering me on every minute of every day. I owe you the world.

Paniz Golrang

Oslo // 12.12.2020

Abstract

The purpose of managing and mitigating risks has long been a way of securing an entity's assets or values. Today, more and more businesses are opening their eyes to using risk management to create, preserve, and realise value by implementing enterprise risk management (ERM). One of the most recognised frameworks for ERM are COSO's *Enterprise Risk Management – Integrating with Strategy and Performance*.

COSO's framework, however, is both very comprehensive, and requires the need for several risk professionals working in the entity. In addition to this, COSO (2017) mentions the importance of being aware of uncertainties regarding risks but fails to give methods in how to acquire sufficient knowledge to manage said risks. This thesis presents a guide for an entity in the beginner maturation state of implementing ERM, where they are demonstrated an activity plan based on COSO (2017), with extra emphasis on uncertainties.

This thesis consists of six chapters, with the first chapter introducing the background and objectives of the work. Secondly, a review of COSO (2017) is presented with a discussion on the limitations of COSO (2017) as a framework. The guide is demonstrated in chapter three, following the same structure as COSO (2017) ending in an activity plan. Chapter four presents an application example based on the *performance* component of the guide. The discussion chapter compares COSO (2017) to the guide presented earlier with the help of the application example. Lastly, the thesis is concluded in chapter six.

Discussions show that the guide is beneficial for smaller or medium sized entities who experience various degrees of uncertainties, and desire to implement an ERM process in order to help create, preserve, and realise their values by assessing risks that threaten the entity's objectives and strategy.

Terminology

Below is a list of terminology used in this thesis, based on COSO (2017) and the SRA Glossary list (2015).

Core value	The entity's beliefs and ideals about what is good or bad, acceptable or unacceptable, which influence the behaviour of the organisation. (COSO, 2017)
Entity	A broad term that can encompass a wide variety of legal structures including for-profit, not-for-profit, and governmental entities (COSO, 2017).
Mission	The entity's core purpose, which establishes what it wants to accomplish and why it exists (COSO, 2017).
Precautionary principle	An ethical principle expressing that if the consequences of an activity could be serious and subject to scientific uncertainties, then precautionary measures should be taken, or the activity should not be carried out (SRA, 2015).
Resilience	Resilience is the ability of the system to sustain or restore its basic functionality following a risk source or an event (SRA, 2015).
Risk aggressive	Taking risk in order to gain more opportunities.
Risk appetite	Amount and type of risk an organisation is willing to take on risky activities in pursuit of values or interests (SRA, 2015).
Risk assessment	Systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge (SRA, 2015)
Risk averse	Disliking or avoiding risk (SRA, 2015).
Risk capacity	The maximum amount of risk the entity can procure.
Risk tolerance	An attitude expressing that the risk is judged tolerable (SRA, 2015).
Robustness	The degree to which a system is unaffected by a risk source or agent (SRA, 2015).
Uncertainty	Imperfect or incomplete information/knowledge about a hypothesis, a quantity, or the occurrence of an event (SRA, 2015).
Vision	The entity's aspirations for its future state or what the organisation aims to achieve over time (COSO, 2017).

Table of contents

List of Figures

List of Tables

1 Introduction

1.1 Background

In the last several decades, risk management has gone from protecting companies with the use of derivatives, to protecting the company's values by implementing preventative measures and, at the same time, expanding business developments. According to the Society for Risk Analysis (SRA) risk management is defined as all measures and activities carried out to manage and govern risk, balance developments and opportunities, while at the same time avoid losses, accidents and disasters. (Aven et al., 2018) Profit-maximising enterprises apply different types of strategic management models and frameworks to achieve their goals, for example Enterprise Risk Management (ERM).

Enterprise risk management is derived from risk management and has the overall objective to maximise an enterprise's value without compromising health and safety by focusing its structure on the entity's business objectives. A very much used framework for ERM is *Enterprise Risk Management – Integrated Framework* by The Committee of Sponsoring Organizations of the Treadway Commission (COSO) which was created to fulfil the need for a management framework; presenting key principles and concepts, a common language and guidance in how to not only create, but also preserve, erode and realise value. It did so by introducing its five risk management components, divided into 20 principles each entity should apply to achieve effective enterprise risk management (COSO, 2017).

The framework assesses the situation of determining how much risk an enterprise is prepared to take and accept, in the path of creating value. One of the shortcomings of the framework is the lack of addressing risks when uncertainties and variations are high, which is a common challenge many entities experience.

The book *Enterprise risk management – Advances on its foundation and practice* (Aven & Thekdi, 2019) was written using the newest and most fundamental concepts in risk science, especially within an uncertainty-based perspective on risk. Aven and Thekdi succeeds in merging ERM and innovative risk science together into a broader concept which can aid in managing risks and opportunities an entity may experience.

A taxonomy of ERM maturity is also introduced by Aven and Thekdi, in view of the fact that not all entities have the time and resources to implement an entire ERM framework for all personnel. Having ERM maturity levels may make it easier for entities to implement and use ERM for the first time, and then upgrade the maturity level when they are ready.

The guide presented in this thesis will try to merge the book (Aven & Thekdi) and the framework (COSO) to benefit the various components found in *Enterprise Risk Management*

(COSO, 2017) by making a beginner ERM guide or procedure to help entities implement an ERM process with the addition of regarding uncertainty.

As a result of this thesis, the writer hopes to help entities implement ERM in an easier way by executing a step by step process which highlights the positive opportunities an entity may experience, but also the uncertainties that may originate from risks and negative surprises.

1.2 Objective

The purpose of this thesis is to develop a guide on how to apply an uncertainty-based perspective on risk in ERM, written towards the entity who aspire to utilise ERM but is in need of more guidance on the implementation of COSO's framework on ERM. By applying a broader sense of risk management to the enterprise risk management of an entity, the entity will be able to reduce the possibility of an event occurring, but also to manage the impact when or if it does occur.

1.3 Approach and Methodology

The guide will be presented in a qualitative manner, focusing mostly on the holistic part of risk management, achieved by documentary analysis of scientific literature and frameworks. *Enterprise Risk Management – Integrating with Strategy and Performance* (COSO, 2017) and *Enterprise Risk Management – Advances on its foundation and practice*s (Aven/Thekdi, 2019) as well as other publications stands for the base of this guide. A series of application examples are conducted to test the usability of the finished product.

1.4 Thesis Outline

This thesis will consist of 6 main parts, as well as an appendix. This thesis is organised as follows:

Chapter 1 introduces the idea for the thesis. It presents and covers the background, objective, and methodology of the thesis. Chapter 2 introduces the ERM and uncertainty principles. One is familiarised with the books and frameworks from *Enterprise Risk Management – Integrating with Strategy and Performance* (COSO) and *Enterprise Risk Management – Advances on its foundation and practice*s (Aven/Thekdi, 2019). Chapter 3 presents the guide composed to aid in the use of the COSO framework. Chapter 4 consists of an application example of parts of the guide. Chapter 5 will feature a discussion related to the application example, differences between the guide and the original COSO (2017) framework, and usability of the guide. Chapter 6 will present final conclusions.

2 A review of COSO and their take on ERM

2.1 The establishment of the Committee of Sponsoring Organizations of the Treadway Commission

The option of paying insurance companies were for many years a way for companies to transfer risks as a mean to protect the entity in case of large accidents, events, or disasters. The insurance companies did not, however, cover all risks an entity would experience. Human errors, certain natural catastrophes and fraud were examples of events less covered by the insurers, resulting in entity management having to look for substitutes to procuring insurance plans which could be managed and financed by the entity itself. (Dickinson, 2001)

In later years, in the 1970s, American companies started to pay more attention to financial risks and its management, both for negative risks as well as looking at positive opportunities coming from risk. A recession, caused amongst other things by the significant increase in oil prices after the Iranian Revolution of 1979, characterised the early 1980s high interest rates and inflation (UC Berkeley, 2011). The recession resulted in vast enterprise financial failures and closures. Some entities tried to save their company with counterfeit reporting, which sparked the interest of the US congress, but congress was not successful in making a legislation to correct these audits. Instead, a private group by the name of the National Commission on Fraudulent Financial Reporting (NCFFR) was constituted to investigate the reporting, sponsored by five US financial organisations: AICA, IIA, FEI, AAA, and IMA. The group was later appointed the name The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (R.Moeller, 2011)

The *Internal Control – Integrated Framework* (COSO) was first published in 1992 and provided a framework for entities to establish systems of internal control to, amongst others, detect and prevent fraud. In 2001 PWC was commissioned to make a framework which could define the essentials of risk management and propose a shared language for risks that could impact a whole enterprise as well as their activities. This was the first publication of Enterprise Risk Management. (R.Moeller, 2011)

2.2 COSO on defining ERM and its benefits

There is still no standardised definition of enterprise risk management, but COSO has produced their own definition on the matter:

> *"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (COSO, 2017)*

COSO's definition states that enterprise risk management (hereby on denoted as ERM) is a method for the entirety of an entity to make risk informed decisions by identifying and managing potential events. The definition also indicates that ERM follows a top down

hierarchy, where all employees, as well as the board of directors and management are to follow the principles of ERM as risk owners of the entity. The entity's objectives are to be the driving force of the company, and their risk appetite is their guideline in the case of how to tackle the risks the entity may encounter. COSO also emphasises identifying potential events which can affect the entity without the use of words like hazardous, harmful, or dangerous. This shows that they also mean potential events in a positive sense, which can help the entity thrive in achieving their objectives.

The definition above composes a set of 5 main benefits presented below in which ERM offers when combined with strategy-setting and performance management practices. (COSO, 2017)

1. "Increase the range of opportunities"(COSO, 2017)

By examining both the positive and negative features of all risks identified, the management will be able to recognise opportunities the entity can use, either now or in the future, to achieve their objectives. The objectives are divided into four different categories: strategic, operations, reporting and compliance, which are all treated equally when recognising opportunities in the entity (COSO, 2017).

2. "Increase positive outcomes and advantages while reducing negative surprises" (COSO, 2017)

ERM does not give its whole attention to negative (or pure) risks, but also gives emphasis to the positive risks or opportunities the entity can take advantage of. When identifying risks, the management spends time identifying both negative and positive risks by including speculative risks into their business strategies, setting up suitable risk responses which can boost positive results while at the same time minimise negative surprises affecting the entity objectives.

3. "Identify and manage entity-wide risks" (COSO, 2017)

ERM helps entities to identify and manage risks that may originate in one part of the entity, but affect another, in addition to making it easier to see interdependencies between different risks on the entity.

4. "Reduce performance variability"(COSO, 2017)

By identifying, evaluating, planning, and managing a full range of risks, the entity may foresee risks that can affect their performance and choose to implement measures for the entity to get back to normal operation quicker and more effectively.

5. Improve resource deployment"(COSO, 2017)

By managing a full range of risks and at all operational units, the entity can maintain their focus on their governing systems and performance in a manner which benefits share and stakeholders. The entity is more adept at planning in advance and will therefore manage retentions more efficiently, as well as managing growth and allocating capital and wealth.

2.3 COSO's frameworks on ERM

In 2017 PWC updated the COSO framework *internal control framework* by request from COSO's board of directors. The new framework was called *Enterprise Risk Management – integrating with strategy and performance,* and told to benefit entities by expanding the entity's opportunities, positive outcomes and benefits while reducing harmful surprises, identifying and managing risks while reducing performance variation and improve allocation of resources. (COSO, 2017)

The framework is divided into five components: governance and culture, strategy and objective-setting, performance, review and revision, and information, communication and reporting, whereas the three components in the middle are common process, and the first and last components are deemed as supporting, but also necessary, components. (COSO, 2017) Each component has a set of fundamental principles corresponding to each component.

Chapter 2.3.2 – 2.3.6 will consist of an overview of the different sub-components or principles in the performance component. Furthermore, a presentation of the limitations in the implementing of the different principles in regard to uncertainties will be provided in chapter 2.4.

2.3.1 Introduction to the framework

COSO's first publication for ERM – *enterprise risk management – integrated framework* (2004) presented their model in the shape of a cube (Figure 1). The top part of the cube represents the entity's objectives, while the eight components symbolise the road to achieving said objectives. On the side of the cube are the organisational units, showing that the entity as a whole will have to address the different objectives in addition to each individual unit.

Figure 1 - ERM component cube 2004 (COSO, 2014) Copyright © 1985-2020 The Committee of Sponsoring Organizations of the Treadway Commission. All rights reserved. Reproduced with permission. Please see Appendix 7.1 A for further information.

In the updated framework – *integrating with strategy and performance (2017),* COSO revised their cube into the loop introduced in Figure 2.

Figure 2 - ERM components 2017 (COSO, 2017) Copyright © 1985-2020 The Committee of Sponsoring Organizations of the Treadway Commission. All rights reserved. Reproduced with permission. Please see Appendix 7.1 A for further information.

The loop represents the strategy an entity must use to gain enhanced value, with mission, vision, and core values as its main driving force. The components below are the same components mentioned in the previous section. The main difference between the two models is that the event identification, risk assessment and risk response are now incorporated into the performance component, making the other planning, revision, and control-based components more important when viewing the components together as a whole.

The new and updated framework emphasises two aspects of ERM which the former did not, namely strategy and performance. The ultimate goal of the framework is to find a strategy, business objectives and business performance to obtain enhanced performance, which will later develop into enhanced value for the entity. Creating a solid foundation of mission, vision, and core values helps the entity to set strategies and make business objectives that are aligned with each other so that they can set their desired risk profile in a position that can take positive opportunities, but at the same time avoid events that are harmful to the entity in relations to cost or objectives. A positive trending risk profile corresponds to the performance levels the entity are operating, which also comes with its negative risks, and it is the board of directors and management who are responsible to choose how risk aggressive or aversive the entity is to be based on their chosen vision and objectives.

Is it common for entity's with high levels of uncertainty to have positive trending risk profiles. An example is oil and gas companies exploring in more complex and hard-to-reach areas when trying to acquire more oil or gas. Further complex pursuing of petroleum carries with it more risk in their attempt to locate resources.

A presentation of the five components in COSO's framework will be presented in the following, with special attention given to component number 3: Performance, where the principles will also be introduced.

2.3.2 Governance and Culture

The first component of the framework emphasises on the need of having a board of directors who provide full risk oversight in order to challenge and support the management when trying to obtain entity strategy and business objectives. Attention is given to a top-down hierarchy, where the board has to fully understand and agree on the entity's strategy and business objectives with the intention of increasing value in the entity. Operating structures are formed, where all personnel are trained in and embraces making risk-based decisions in correspondence to their level of authority. Full openness is advised to create a culture and easy discussion platform to consider risks faced in day-to-day operations, where adherence to core values are rewarded by the entity.

2.3.3 Strategy and Objective-Setting

In the second component of the framework, the entity chooses its strategy in order to support its mission, vision, and core values. The board of directors decides upon a risk appetite for the entity to obtain and establishes business objectives which supports the entity strategy of enhancing value. The strategy and business objectives chosen are the basis for assessing and responding to risks the entity may encounter.

2.3.4 Performance

The sub-components of the Performance-part of the COSO framework shows their version of a risk analysis process, consisting of principles 10 to 14. The first principle in the performance component is principle 10: *Identifies Risk*, where one identifies new, emerging, and current changing risks to create a risk inventory which results in the management being able to respond appropriately in advance. Principle 11: *Assesses Severity of Risk* selects severity measures and assessment approaches for the risk inventory created previously in principle 10. The management distributes funds and labour to the operational units according to the severity of the risks for the purpose of keeping the risk within their risk appetite. The risks are prioritised in principle 12: *Prioritises Risk*. The different organisational units allocate appropriate risk responses in principle 13: *Implements Risk Resources* by determining whether they choose to accept, avoid, pursue, reduce, or share the risks analysed. Lastly, the entity creates a portfolio view of risks to better understand connections between different risks and performance in principle 14: *Develops Portfolio View*. (COSO, 2017)

Principle 10: Identifies Risk

According to COSO (2017), ERM is sufficiently integrated when management is able to keep risks (new, emerging and changing) up do date during normal day-to-day operations. The risks can be grouped in different ways so that the entity may find risks that also affect the

enterprise as a whole. Some examples of risk groups are risks occurring because of a change in business objectives (e.g. new strategy) or business context and changes in regulations. Another grouping mentioned are risks that have previously been unknown but often rise in the case of changes in business context because of unknown external changes, for example new technology, labour shortages or depleting natural resources. In these situations, COSO states the importance of also being able to identify opportunities in the unknown changes.

The identified risks are then categorised into groups and sub-groups to provide common definitions for different risks as well as saving managements time and resources. All risks are to be evaluated by all organisational units in order to recognise both risks and opportunities across the whole entity in the same language, describing only the risk itself, rather than what caused it. The evaluation methods suggested by COSO are cognitive computing, data tracking, interviews, key indicators, process analysis and workshops, where data tracking and process analysis are the two methods proposed not to use when identifying emerging risks.

Principle 11: Assesses severity of risk

COSO describes the severity assessments as a process proceeding at all organisational levels, where each unit assesses the risks for their own unit as well as the unit below, resulting in for example the entity level also assessing the risks towards entity business objective level to assess if the risk is also of entity level interest. The recommended assessment approaches are qualitative, via interviews, workshops and surveys, suggested for simple risks and opportunities or quantitative assessments, using either probabilistic models (e.g. value at risk or cash flow at risk) or non-probabilistic models (e.g. sensitivity or scenario analysis) to be used for modelling, decision trees or Monte Carlo simulations for more complex risks and opportunities. The management may rely on knowledge and expertise when performing the assessment depending on the entity's complexity, with their assumptions clearly assigned. The severity measures are divided in to rating or impact type and likelihood, which is presented in a heat map or risk matrix. The heat map identifies signals or triggers that may change the entity's business context or risk appetite. COSO also describes bias in assessments when it comes to risks with high likelihood and low impact versus risks with high impact and low likelihood because they would both have the same results in the heat map.

Principle 12: Prioritises Risk

The entity's risk appetite, strong relevance to business objectives, as well as severity, are the main drivers for the prioritisation of risks identified, and priority criteria are to be decided beforehand to aid in order of priority. Examples described of prioritisation criteria are adaptability, complexity, velocity, persistence, and recovery are considered, together with the intensity of the risk in comparison to the entity's risk appetite.

Principle 13: Implement Risk Responses

The chosen risk owners for each organisational unit are accountable for prioritising and choosing suitable risk responses in light of both business objectives and performance. COSO recommends five risk responses to manage identified risks: accept, avoid, pursue, reduce, and share, conducted with business objectives, -context, performance, and risk appetite in mind. If the entity sees a greater opportunity in a risk than loss, they can choose to surpass their risk appetite, but if this happens too often the entity should consider modifying their risk appetite to suit their new levels. Many factors must be considered by the management when distributing risk responses. COSO suggests looking at their business context, obligations and expectations, risk appetite, -severity and the prioritisation provided by the risk owners. Connecting the prioritisation and severity with cost and benefits are especially highlighted as a factor. For new and unfamiliar risks, the management should also decide upon a degree of effectiveness and validity to the response they choose to take, as well as a note to look upon further in case of new opportunities not reviewed at an earlier time. The entity must evaluate if the benefits towards the strategy and business objectives exceed the cost of implementation.

Principle 14: Develops Portfolio View

The portfolio view is made to see if the risk appetite the entity has chosen is reflected in their risk profile. The risk appetite may be subject to change if they exceed their appetite, or the management may choose to inform organisational units to accept greater risks in specific areas to increase the entity's value. When analysing the portfolio view, the management may choose to do this quantitatively, with regression models and statistical analysis, or qualitatively, by applying scenario analysis or benchmarking. The analysis will help the management study the validity of the assumptions made under the severity of the identified risks, how the individual risks are conducted under stressed conditions, interdependencies between individual risks and how effective the various risk responses are, and thus identifying other possible risks or modify risk responses.

2.3.5 Review and Revision

Responses to assesses risks are reviewed and changed considering changes in the entity. This can be for example sudden growth of the entity, changes in leadership, and personnel or changes in regulations. These potential changes are identified and evaluated, while the response to the risks will be considered as lessons which can be applied in the future. The lessons, or reviews of past risks and responses are then incorporated into business practises for the entity to consider and change if deemed necessary. In the end, COSO advises to use these reviews to improve the entity's ERM to ensure continual growth.

2.3.6 Information, Communication, and Reporting

Lastly, the entity is required to work continually to obtain and share relevant information with internal and external stakeholders, as well as feed out non-relevant or low-quality information, which is both of less use for the entity, but also clogs up the information system. The information deemed relevant to strategy, business objectives and value enhancing are categorised in risk information groups chosen by the entity. Special attention is given to reporting and flow of information to notice key risk indicators more quickly, changes in frequency or quality.

2.4 Discussion

ERM – Integrating with strategy and performance appears to be written for an entity who is already risk aware, has a risk policy, or have one (or several) risk managers. This is clear when looking through the framework as it has plenty of information about what to remember when implementing ERM, but not how an entity is supposed to implement these measures. COSO does state in the end of chapter 1 that there is no one-size-fits-all approach for all entities, and many have constructed guides to how to include COSO ERM into their field. Some examples are guidance in Cyber Risk and ESG (environmental, social, and governance-related risks) (COSO, 1985-2020), but none of the guides feature an elevated emphasis on uncertainties even though it is highlighted in the second benefit of applying ERM by COSO.

Surprises, both positive and negative, are events that can happen which are not accounted for in the entity's risk assessments. These events or activities bring along a level of uncertainty, as well as assumptions and beliefs which may or may not happen. These uncertainties can affect the risk profile the entity has set for themselves by increasing and decreasing the relationships of risk vs. performance.

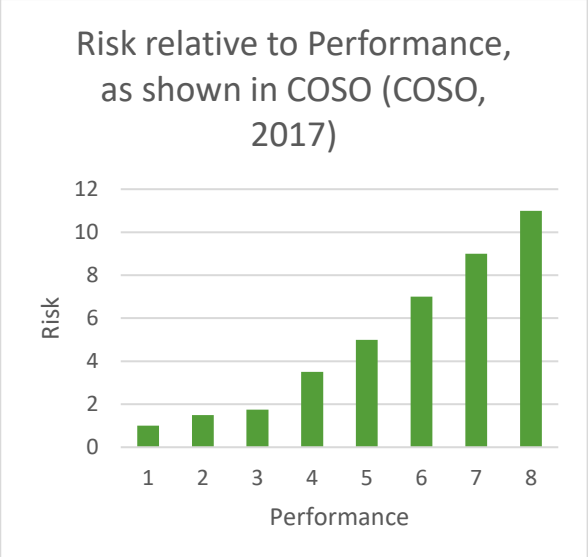


Figure 4 - Risk relative to Performance (inspired by COSO, 2017).

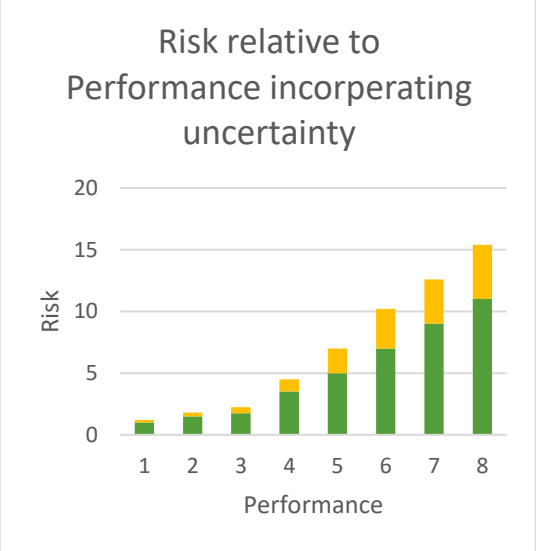


Figure 3 - Risk relative to Performance incorporating uncertainty (inspired by COSO, 2017 and own knowledge of uncertainty to state an example)

As an example, imagine an entity working on exploring new oil and gas reservoirs. With increased performance, they must search in more isolated areas or use more advanced (or hazardous) methods of extraction (e.g. fracking). These developments bring more risk in to the entity, hence the upwards trending curve in Figure 4. Based on the strategy of the entity, the management chooses a target performance at level 5, which gives a corresponding risk level at 5. The entity has set their risk capability at level 6, which gives their chosen performance level as acceptable. However, the risk picture the entity has produced is an assumption of the beliefs and judgements of whomever developed their scale. The assumptions come with uncertainties. In Figure 3 an extra measure of uncertainty is added to the graph, which may increase the risk factor significantly. The entity does not know if the risks of added performance will equal to the top or the bottom of the uncertain areas, but they know that they may be somewhere between the numbers 5 and 7, which is right above or below their risk capacity, ergo it is uncertain.

The addition of a measure of uncertainty to the risk profile and in the COSO framework in general encourages the entity to be more aware of variations and the possibility of unknown or little-known hazards that can affect the entity's objectives and value-creation. Inserting a measure of uncertainty into the company's risk profile may aid in making the entity more aware of the uncertainties of their labour. COSO mentions in principle 9 in the framework that some variations may appear which can be used to establish or modify tolerance levels, but these statements appear to be common-cause variations and not the whole spectrum of uncertainties (i.e. the addition of special-cause variations). With improved understanding of uncertainties and variations, the entity may notice signs or signals that can foreshadow events which the entity can mitigate or deflect if necessary.

The consideration to costs and benefits is a central part to COSO, especially in principle 13, where it is stated that the different risk responses are decided upon with the influence of the management's costs and benefits analyses. COSO does not suggest transforming all attributes to monetary value per se which is common practice when using cost-benefit analysis, but do imply to give monetary values to costs and, if needed, more subjective based responses to benefits (Aven & Thekdi, 2019) and (COSO, 2017). In the cases where subjective responses are preferred, the entity is to assess the benefits from the achievement of strategy and business objectives point of view. When considering ERM and performance management, the entity can often experience uncertainties and a lack of a sufficient amount of populations of similar systems, henceforth, the usage of expected values cannot be justified. Aven and Thekdi (2020) suggests supplementing quantitative approaches with strength of knowledge judgements to support the probabilities as well as adding the knowledge which the strength of knowledge and probabilities are based on. This ensures that the judgement made by the risk manager or expert is reported, communicated in a "good" way, and is supported by well documented knowledge (Aven & Thekdi, 2019).

Aven and Thekdi (2020) suggests a taxonomy of ERM maturity based on the three maturity levels: Beginner, Intermediate and Advanced. This promotes simplicity in the application of ERM, as well as giving the entity an opportunity to grow with the implementation of ERM. The table is separated into characteristics in four parts: resources, expertise, culture, and practices, and may be found in Appendix 7.2 B.

2.5 Conclusions

It may be concluded that COSO's framework on ERM would benefit from a few modifications in order to make it more user friendly, especially for entities who are in the early stages of implementing ERM. Several contributors have produced specialised frameworks or guides, but none that are developed with the beginner entity in mind. A thorough and simple how-to manual would benefit smaller entities by cutting costs and making for less confusion when starting the implementation. Secondly, many entities are highly affected by uncertain events happening within their field as well as around them, for instance natural disasters, oil prices or economic recessions. Adding a measure of uncertainty may make the entity better suited for these events by having, among other things, different or larger buffers and emergency procedures for black swan type of situations. Lastly, increasing the amount of knowledge, both the strength of knowledge to support probabilities, and the knowledge which it is based upon, works to provide more awareness and information about potential uncertain events.

Based on these conclusions, in the following chapter, we will provide a guide for an entity at the Beginner maturity level for ERM in which there is an emphasis on uncertainty and strength of knowledge. The guide will be based on COSO ERM, and thus divided in the same way to ensure complete comprehension when comparing to the original framework.

3 Guide

3.1 Set up and how to use the guide

The guide is set up based on the COSO ERM Framework (2017) and encompasses a beginner version of ERM, perfect for the entity implementing ERM for the first time. In addition to the information and guidance provided by COSO, there is also an added component of uncertainty and strength of knowledge incorporated based on the books of Aven and Thekdi (2020).

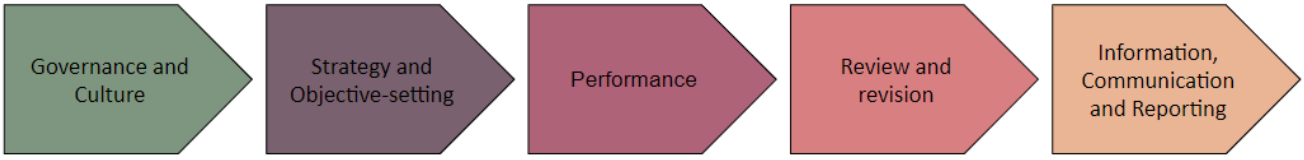


Figure 5 - COSO ERM Components and Principles (inspired by COSO 2017) Produced in Google Drawings.

1.Exercises Board Risk Oversight
2.Establishes Operating Structure
3.Defines Desired Culture
4.Demonstrates Commitment to Core Values
5.Attracts, Develops, and Retains Capable Individuals
6.Analyses Business Context
7.Defines Risk Appetite
8.Evaluates Alternate Strategies
9.Formulates Business Objectives
10.Identifies Risk
11.Assesses Severity of Risk
12.Prioritises Risk
13. Implements Risk Responses
14.Develops Portfolio View
15.Assesses Substantial Change
16. Reviews Risk and Performance
17.Pursues Improvement in Enterprise Risk Management
18. Leverages information and Technology
19.Communicates Risk Information
20.Reports on Risk, Culture, and Performance

The guide is divided into the same components as the COSO ERM Framework itself. It consists of five components with various principles. The guide has also an added number of activities in order to simplify the experience for the entity implementing ERM for the first time. The activities are collected in a project plan which is found in the end of the guide.

3.2 Governance & Culture

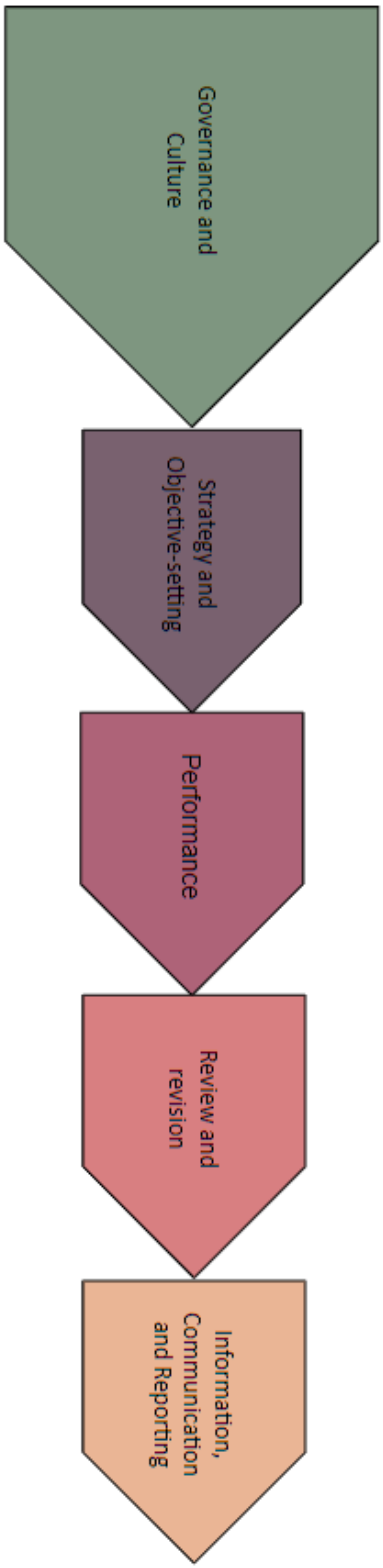


Figure 6 - Components: Governance and Culture. Produced in Google Drawings.

The first section of the COSO loop, governance, and culture, sets the tone for the entity both when it comes to the board of directors (henceforth called the board) and their role, as well as establishing a risk aware culture throughout the whole entity (COSO, 2017). While it is important that all personnel share the same view on risk, it should be noted that in this beginner guide to the COSO framework, not every employee will be trained on risk management practices as COSO narrates. This section of the guide is composed of five principles, based on COSO ERM Framework on Governance and Culture:

Principle 1: Exercises Board Risk Oversight: The board supports the management in the fulfilment of the entity's strategy and business objectives by providing strategies and conducting governance responsibilities (COSO, 2017).

Principle 2: Establishes Operating Structures: Operating structures are determined for achieving the entity's desired strategy and business objectives (COSO, 2017).

Principle 3: Defines Desired Culture: The entity implements a defined manner of behaviour which complements the entity's desired culture (COSO, 2017).

Principle 4: Demonstrates Commitment to Core Values: The entity shows full commitment to its core values (COSO, 2017).

Principle 5: Attracts, Develops, and Retains Capable Individuals: The entity commits to support and develop personnel who align with the entity's strategy and business objectives (COSO, 2017).

The sub-chapter contains the following activities:

Principle 1: Exercises Board Risk Oversight:

- Ensure all board members fully understand the industry of the entity and keep themselves updated at all time of changes in business context.
- Ensure the board is made up of independent professionals to avoid conflicts of interest.
- Review periodically that the board consist of a group with relevant skills and knowledge in order to provide entity oversight.

Principle 2: Establishes Operating Structures:

- Define the entity's regulatory and non-regulatory risk and safety guidelines.
- Consider a range of factors when developing the entity's operating structure.
- Establish an ERM committee to get insight on risks developing from different organisational units.

Principle 3: Defines Desired Culture:

- Assess internal and external factors to shape the entity's culture.
- Produce a simple visual representation which can function as a helpful guide to employees.
- Periodically assess the entity's risk culture after major changes in the entity.
- Produce clear and detailed definitions on various risk strategies (cautionary principles, robustness-, resilience-, and discursive strategies).
- Ensure compliance from the leaders top down by communicating the entity's desired culture and working as role models.

- **Principle 4: Demonstrates Commitment to Core Values:**
  Promote openness and transparency with regard to risk related subjects.
- Create a system for which personnel can easily send deviations and improvement suggestions anonymously.
- Encourage personnel to speak up about all hazardous behaviour in a polite manner no matter the level of the wrongdoer.

Principle 5: Attracts, Develops, and Retains Capable Individuals:

- Establish a system to provide personnel with guidance and motivation to show that the entity is committed to their welfare.
- Create a system for periodic reviews of every personnel's well efficiency, education, and wellbeing.

3.2.1 Exercises Board Risk Oversight

The board, being of the highest level in the entity, should provide the management with risk oversight while the management are assigned to carry on the entity's day-to-day activities. Asking the correct questions to support, but also challenge, the management to always improve regarding strategy, business objectives, and performance targets, is one of the board's responsibilities. The board should consist of individuals with appropriate skills, expertise, and business knowledge for the entity to easier define and stay informed on relevant concerns (COSO, 2017).

However, the board must be aware of factors which can impede the board's independence, for example if a board members holds a financial interest in the entity or has donated a significant amount of money in the entity, holds a financial interest in a third party service provider which has a material business relationship with the entity, individuals who have personal relationships with key stakeholders, as well as individuals who have organisational biases towards risk or numbers. The factors mentioned previously may impede with the board's capability of being objective in evaluating performance or the entity's advancement to value creation (COSO, 2017).

3.2.2 Establishes Organising Structures

For an entity to develop a transparent and multiway dialogue on ERM, a precise definition of the operating structure with responsibilities and reporting lines is essential to minimise unnecessary drag and labour consummation (COSO, 2017). When developing the entity's operating structure, some factors should be considered:

- The entity's strategy and business objectives.
- The entity's business nature, size, and geographic allocation.
- The entity's authoritative assignment, and responsibility in all organisational units.
- The entity's reporting lines and channel of communication.
- Local and industry specific regulations, and non-regulatory risk and safety guidelines.

A committee may be formed of some senior employees trained on how to practice risk management to aid the management with information on how risks associated with strategy and business objectives arises within the organisational units of the entity (COSO, 2017).

3.2.3 Defines Desired Culture

Culture and Desired Behaviours

The entity's culture is defined as the desired behaviours and understanding about risk which influences the judgements made by the management and personnel reflecting the entity's mission, vision, and core values. It is critical for the entity's success in achieving strategy and business objectives that all personnel adopts the entity's determined culture (COSO, 2017).

Deciding on a view of risk in the culture spectrum is a simple, visual representation of the entity's acceptance of risks in the accomplishment of its strategy and business objectives (see Figure 7 - Culture Spectrum (Inspired by COSO, 2017)Figure 7). An entity who chooses to be on the risk aggressive side of the spectrum are more accepting of assorted varieties and quantities of risk in order to achieve its business objectives, whiles the risk averse entity decides on a path with lower risk (COSO, 2017). There exists many factors the entity should assess before deciding upon its main culture, presented below Figure 7 of the culture spectrum.

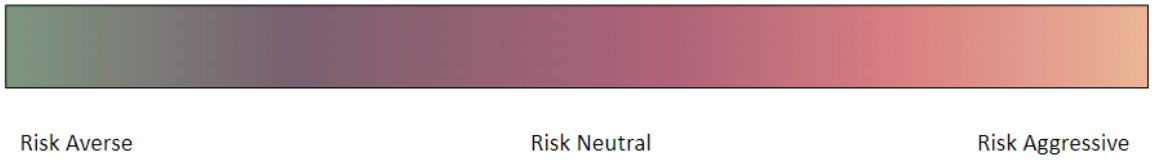


Figure 7 - Culture Spectrum (Inspired by COSO, 2017) Produced in Google Drawings.

Internal and external factors that can shape the entity's culture, and therefore should be assessed according to how the entity is run are factors like (COSO, 2017):

- The entity's standards and rules.
- The collaboration between personnel and their managers.
- The entity's reward and penalty system.
- Regulatory requirements.
- The expectations of customers, investors, and other stakeholders.

Changes in the entity, for example when acquiring new leadership, may cause the entity's culture to change, and thereof shift the entity's mission and vision leading to a change in how the entity views risk. It is therefore beneficial to assess the entity's risk culture after any major change in the entity to secure the achievement of strategy and business objectives (COSO, 2017).

In addition to the factors affecting culture, the entity must also produce a clear definition the entity's stance on various risk strategies, for example (Aven & Thekdi, 2019):

- Cautionary/precautionary principles
- Robustness strategies
- Resilience strategies
- Discursive strategies

The Importance of Aligning Core Values, Decision-Making, and Behaviours

The entity's approach to effectively achieving its desired strategy and business objectives may be blocked when the behaviours and judgements of the entity, or the entity's management or personnel, does not align with the entity's core values. A misalignment of core values and behaviours can lead to losing stakeholder's trust, inconsistency in day-to-day operations and lower performance (COSO, 2017). COSO (2017) has listed a number of reasons for an offset in core values and behaviours, some of them presented below:

- The tone at the top management does not communicate fitting expectations.
- The middle management do not align with the entity's mission, vision, and strategy.
- When strategy-setting or business planning, risk is seen as an afterthought.
- Management or personnel chooses not to comply with the entity's core values intentionally.

3.2.4 Demonstrates Commitment to Core Values

Embracing a Risk-Aware Culture

The tone of the entity demonstrates how core values are communicated across the entity. A steady tone defines a normal and mutual agreement of the core values, and desired behaviours of all stakeholders, including personnel and management (COSO, 2017). COSO (2017) describes a risk-aware culture to be an entity which:

- Sustains a strong leadership as the driver of change.
- Encourages personnel to take part in discussing strategy and business objectives.
- Holds personnel accountable for all actions, both positive and negative.
- Considers risks when making business decisions.
- Uses open, transparent, and timely risk communication about risks affecting the entity.
- Encourages viewing risk as one of all personnel's daily obligations.

Keeping Communication Open and Free from Retribution

The management can foster open and transparent communication by sending clear messages to personnel on the importance of risk being everyone's responsibility when achieving the entity's strategy and business objectives. By having open communication about risk, where no subject is too small and no individual is more important or free from responsibilities, the entity promotes personnel and management to speak up when experiencing activities that might be considered outside of the entity's risk culture. By having individuals openly question deviations from regulations, the entity can avoid small risks or hazards becoming large problems (COSO, 2017).

3.2.5 Attracts, Develops, and Retains Capable Individuals

For an individual to respect, follow and embrace entity's risk culture, it is important for them to feels as if the entity is committed to care about them, their safety, welfare, and constant growth. An entity with a low turnover both attracts, trains, mentors, evaluates and, in the end, retains its personnel by constantly measuring, providing guidance and motivation to the individual. An open dialogue during guidance gives the entity an opportunity to identify behaviours that are not consistent with entity standards or core values earlier, which therefore gives the entity an opportunity to correct said behaviours in a timely manner (COSO, 2017).

3.3 Strategy & Objective-Setting

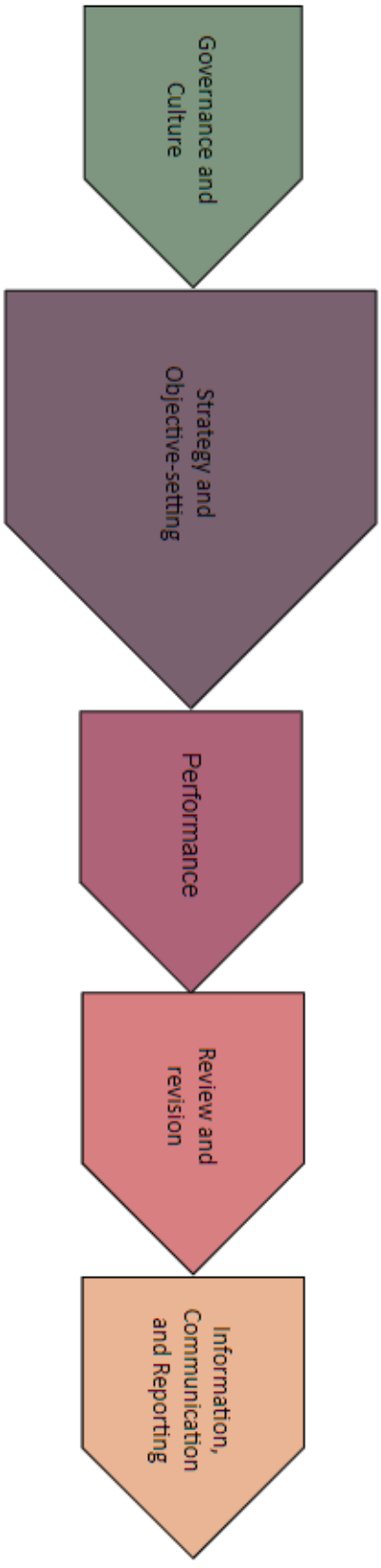


Figure 8 - Components: Strategy and Objective-setting. Produced in Google Drawings.

Strategy and objective-setting is the second section of the COSO loop and considers the entity's strategy, business objectives and business context. The entity sets its risk appetite aligned with its strategy and business objectives (COSO, 2017). This section of the guide is composed of four principles, based on COSO ERM Framework on Strategy and Objective-setting:

Principle 6: Analyses Business Context: The entity reviews the effects of their business context on the entity's risk profile (COSO, 2017).

Principle 7: Defines Risk Appetite: The entity establishes a risk profile corresponding to their risk culture in the achievement of creating, preserving, and realising value (COSO, 2017).

Principle 8: Evaluates Alternative Strategies: The entity reviews alternative strategies in their risk profile according to entity's resources and capabilities (COSO, 2017).

Principle 9: Formulates Business Objectives: The entity stablishes business objectives and reviews related risks at different levels (COSO, 2017).

The sub-chapter contains the following activities:

Principle 6: Analyses Business Context:

- Use external and internal environment characteristics to realise and establish the entity's business context.

Principle 7: Defines Risk Appetite:

- Create a risk to performance ratio, risk profile, to gain a rough draft for describing the entity's risk appetite.
- Use the risk culture decided upon previously to see how much variation the entity is willing to undergo in regard to value creation.
- Find the entity's target level and risk capacity to create a risk appetite for the entity.
- Define a total knowledge approach used for classifying knowledge throughout the ERM process.

Principle 8: Evaluates Alternative Strategies:

- Choose a strategy that reflects the entity's risk appetite, based on the strength of knowledge of the strategies in question.
- Set up periodical strategy-setting evaluations to keep an overview of short-term and long-term strategies

Principle 9: Formulates Business Objectives:

- Use the entity's strategy and risk appetite to formulate specific, measurable, attainable, and relevant business objectives.

3.3.1 Analyses Business Context

Understanding Business Context

The entity's business context is referenced by COSO (2017) to factors, like trends and relations, which impacts or can impact present and future strategy and business objectives. The business context can be described with one word as COSO has done (COSO, 2017):

- Dynamic: a business context with ever changing risks which may interrupt the entity's performance flow.
- Complex: the entity has many regulations to abide by, as well as many interconnections and interdependencies across the entity.
- Unpredictable: the entity experiences rapid and unpredicted changes.

To find the entity's business context, one can apply a broader sense of business context within, by dividing considered factors affecting the entity into categories, to see how the business context of the entity is defined in certain areas. COSO divides factors into external and internal environment categories and characteristics (COSO, 2017). Table 1 shows an example of internal and external environment categories and characteristics which may be used for the entity describing their business context.

Table 1 - Internal and external environment categories and characteristics for describing business context.

Category	External Environment Characteristics	Business Context
Political	Degree of government interference (tax policy, labour law, tariffs etc).	Dynamic
Economic	Interest rates, inflation, currency exchange rates, etc.	Complex
Social	Customer expectations and needs.	Dynamic
Technological	Digitalisation, R&D activity, etc.	Dynamic
Legal	Laws, regulations, and industry standards.	Dynamic
Environmental	Environmental disasters, climate change, and changes in energy consumption.	Unpredictable
Category	**Internal Environment Characteristics**	**Business Context**
Capital	Assets.	…
People	Knowledge, expertise, and culture.	…
Process	Changes in activities, assignments, policy, and procedures.	…
Technology	New or changed technology	…

Note - Categories and characteristics retrieved from COSO (2017)

3.3.2 Defines Risk Appetite

Defining Risk Appetite

COSO (2017) defines risk appetite as the willingness an entity has to create, preserve, and realise value, connected to the desired risk culture the entity previously set (COSO, 2017). The entity starts with setting its risk capacity, the maximum amount of risk the entity can procure, defined either by regulations or by the entity's ability to return to normal operations. When the risk capacity is set, risk appetite and target is set to get appropriate risk to performance ratio based on the strategy and business objectives, as well as the entity's risk culture. The target performance is set dependent on the willingness of the entity to encounter variation or uncertainties (w. COSO, 2018). For an entity with large uncertainties, typically a lower target is preferred to avoid reaching the set risk capacity. Figure 9 shows an example of an entity's risk profile presenting risk appetite, risk capacity and target performance.

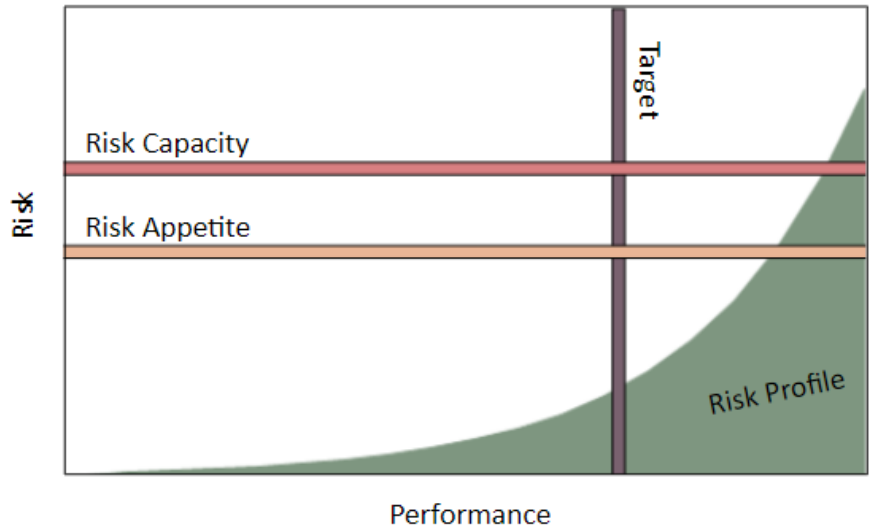


Figure 9 - Risk Profile showing risk appetite and risk capacity (Inspired by COSO 2017) Produced in Google Drawings

At an early stage of implementing ERM, setting a risk profile qualitatively with words like "positive or negative trending" risk profile may give the entity time to shape its risk profile, and thus risk appetite, in a dynamic way when the entity has gained more knowledge (COSO, 2017).

Defining Total Knowledge

Based on the entity's risk profile, the management sets a general way of judging the strength of knowledge of information attained by the entity. The total strength of knowledge approach chosen by the entity influences the decision-making when it is time for assessing and prioritising risk (Aven & Thekdi, 2019). Please see Appendix 7.3 C for methods of assessing strength of knowledge. Table 2 shows a suggestion of approaches and assumptions by Aven and Thekdi (2018):

Table 2 - Approaches to total knowledge

Approach	Assumptions that total knowledge is:
Conservative	"strong" if all classifications across criteria are strong. "weak" if all classifications across criteria are weak. "medium" otherwise.
Optimistic	The highest strength assigned among all criteria.
Pessimistic	The lowest strength assigned among all criteria.
Selective	"strong" if all classifications of entity deemed most important criteria are strong. "medium" if some of the classifications of the entity deemed most important criteria are strong. "weak" otherwise.

Note - Approaches and assumptions retrieved from Aven and Thekdi (2018).

3.3.3 Evaluates Alternative Strategies

Understanding and Aligning Strategy

As a part of strategy-setting, the entity should assess options from two different points of view: either that the strategy does not reflect the mission, vision, and core values of the entity, or impacts made from the entity's chosen strategy. A misalignment of strategy may increase distrust in stakeholders due to the entity's choices not reflecting its mission, vision, and core values (COSO, 2017). The management and board decides upon the strategies to adopt depending on the entity's risk appetite, as well as the strength of knowledge of the information (including assumptions) supporting the strategy (Aven & Thekdi, 2019). Please see Aven and Thekdi (2020) for details about strength of knowledge.

Making Changes to Strategy

The entity should hold strategy-setting sessions occasionally in order to have an overview of both short-term and long-term strategies. The currently used strategy should be changed if the entity deems the current strategy to fail in creating, preserving, or realising value, if the business context changes to such an extent that the entity has surpassed its risk appetite and nearing risk capacity, or the current strategy is requiring more resources and abilities than the entity is able to provide (COSO, 2017).

3.3.4 Formulates Business Objectives

The entity should create specific, measurable, or observable, attainable, and relevant business objectives related to areas of the entity in the achievement of its strategy. Areas that business objectives may relate to are, amongst others, financial performance, customer expectations, operational quality, compliance commitments, efficiency, or innovations. The entity can choose to have business objectives in every area for the whole entity, or choose as they wish for different organisational units, as long as the business objectives are fully aligned with the strategy in achieving the entity's mission and vision in addition to the entity's risk appetite. This means that if the entity is unable to develop business objectives supporting the entity's strategy, while keeping within the entity's risk appetite or capabilities, and representing its mission and vision, a study should be considered to change either the entity's strategy or risk profile (COSO, 2017).

3.4 Performance

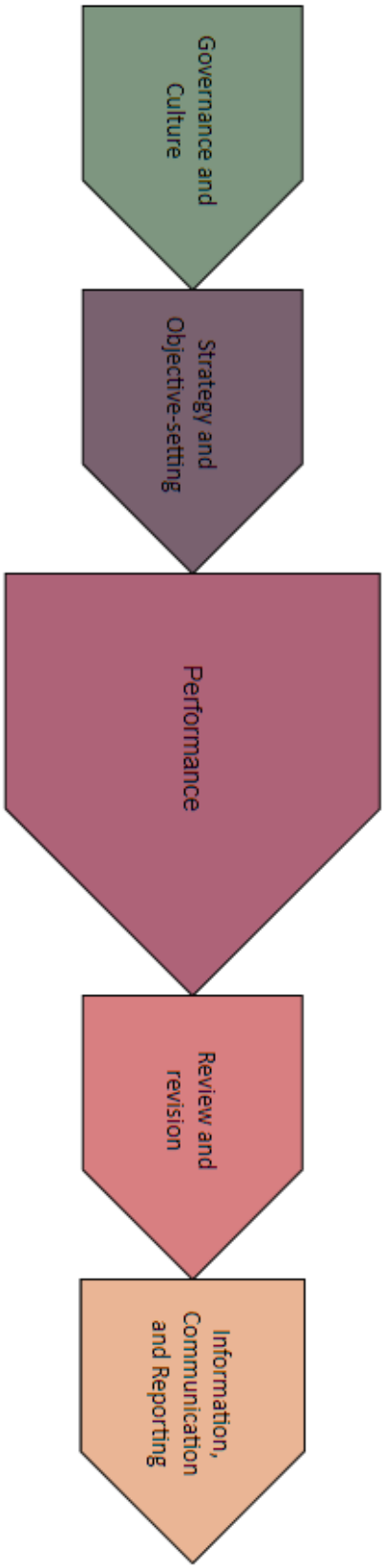


Figure 10 - Components: Performance. Produced in Google Drawings.

Performance is the next section of the COSO loop, which focuses on some processes during a classic risk assessment. The principles are produced to support the entity with knowledge which should be used to make decisions with regards to the entity's strategy and business objectives. The performance section is composed of five principles, based on COSO ERM Framework on Performance:

Principle 10: Identifies Risk: The entity identifies threats, hazards, and opportunities that may impact the entity's strategy or business objectives (COSO, 2017).

Principle 11: Assesses Severity of Risk: The entity analyses the severity of threats, hazards, and opportunities as well as its related uncertainties and strength of knowledge (COSO, 2017).

Principle 12: Prioritises Risk: The entity prioritises previously identifies threats, hazards, and opportunities as a foundation for risk response evaluation (COSO, 2017).

Principle 13: Implements Risk Responses: The entity evaluates risks and chooses to accept, avoid, pursue, reduce, or share threats, hazards, or opportunities (COSO, 2017).

Principle 14: Develops Portfolio View: The entity produces a portfolio view of threats, hazards, and opportunities (COSO, 2017).

The sub-chapter contains the following activities:

Principle 10: Identifies Risk:

- Select categories of risk which resonates with your entity
- Create a designated group of employees trained on risk management and practitioners to identify new, emerging, and changing risks.
- Utilise and continually update the entity's risk inventory to determine new, emerging, and changing risks several time each year.
- Identify threats/hazards/opportunities that can impact the entity's strategy and business objectives.
- Establish and use an entity sentence structure to precisely define risks.
- Use cause analysis to find the risk drivers threatening the entity's strategy or business objectives.
- Employ a specialised approach to cause analysis emphasising knowledge and surprises to risks with higher levels of uncertainties.

Principle 11: Assesses Severity of Risk:

- Classify the impacts affecting the entity by grouping into classifications in which the entity values.
- Analyse likelihoods qualitatively or quantitatively by referencing the strategy and business objectives of the entity.
- Enhance likelihoods and reduce uncertainty by including strength of knowledge and where the total knowledge comes from.
- Create an extended risk picture for an overall look of all identified risks.
- Display uncertain risks in an extended risk matrix to provide further judgement when prioritising and reviewing risks.

Principle 12: Prioritises Risk

- Create a set of risk criteria in order to compare the identified risks to the entity's risk appetite.
- Evaluate and prioritise risks at the level where the risk is owned.

Principle 13: Implements Risk Responses:

- Decide upon risk responses based on the entity's business context, obligations, regulations, risk appetite, severity, and prioritisation.
- Use a layered approach to assess which measures to implement based on cost and uncertainties.

Principle 14: Develops Portfolio View:

- Periodically evaluate how risks owned by different organisational units can affect strategy and business objectives.

3.4.1 Identifies Risk

Using a Risk Inventory

It is common for an entity to have a risk inventory of the risks they face. The entity selects appropriate categories of risk, where the most common categories for ERM are strategic, operational, financial and compliance (COSO, 2017). The risk inventory can also include more detailed units, for example impacts and risk owner.

In many cases when reviewing the risk inventory, it is easy to copy risks from previous analyses, so special caution must be given to not overlook special aspects or new features (Aven, 2015). See Table 3 for an example of a risk inventory with the associated risk owner.

Table 3 - Example of risk inventory

Strategic	**CEO**	**Operational**	**CTO**	**Financial**	**CFO**	**Compliance**	**CFO/HR**
• **Mergers and acquisitions** • **Technology** • **Competition** • **Political environment** • **Strategic Plan alignment** • **Labour Market**		• Supply chain disruption • Accidental events • Security related events • Customer satisfaction • Supervision		• Interest rates • Credit issues • Liquidity/Solvency issues • Reliance on funding • Stock prices		• Regulations • Fraud • Tax status change • Insurance and liability • Criminal activities	

Note - Examples inspired by COSO, & wbcsd. (2018)

Approaches to Identifying Risk

The entity can use a variety of methods to identify threats, hazards, and opportunities, but the process is generally the same. The risk owners, managers, leading practitioners, or other personnel responsible for risk bring in their input, which is the basis for the threat, hazard, or opportunity identification, resulting in a list of undesirable events or opportunities (Aven, 2015). See Table 4 for an example of a hazard or opportunity identification process.

Table 4 – Example HAZID

Input	**Process**	**Output**
• **Brainstorming** • **General experience** • **Inspections** • **Databases** • **Assumptions**	• SWIFT • HAZOP • Checklist • Guidewords • Process analysis • Reliability analysis • FMEA • Data tracking • Cognitive computing	List of undesirable event or opportunities

Note - Examples inspired and retrieved by Aven (2015) and COSO, & wbcsd. (2018)

When conducting an identification process, one is to be mindful of incorporating new, emerging, and changing risks relating to strategy and business objectives. This can be achieved by asking questions in the end of or during the process (COSO, 2017):

- How can this threat/hazard damage the entity's strategy or objectives?
- What kind of threat/hazard/opportunity can change the entity's business objectives or business context?
- How can this threat/hazard develop further in the future?
- What kind of opportunities can the entity salvage from previously identified threats/hazards?
- What kind of unlikely threats/hazards can the entity face?
- What kind of unknown threats/hazards can the entity face?
- How can emerging technology, depleting resources, mobility, changes in stakeholders, shifts in lifestyles or labour changes affect the entity's strategy or objectives?

Describing Risks with Precision

The risks should be described precisely, using a homogeneous language, and set up, in order to see the risks more effectively from different angles. Each risk should be considered throughout every organisational unit, and it is therefore recommended to describe the risk itself instead of potential impacts or root causes of said risk. Neutralising risks with precise risk identification can help the entity reduce risk bias when framing in a positive or negative manner. A neutral risk identification can also help the entity understand interdependencies between risks, strategy, business objectives and operational units (COSO, 2017).

COSO recommends the organisation describing risk by using an entity standard sentence structure, for example:

- The possibility of *[describe potential threat/hazard/opportunity]* and the associated impacts on *[describe specific business objective set by entity]* (COSO, 2017).
    - Example: The possibility of customer unsatisfaction and the associated impacts on revenue.
- The risk to *[describe category set by entity]* relating to *[describe possible threat/hazard]* and *[describe related impact].* (COSO, 2017)
    - Example: The risk to operational performance relating to a possible change in customer satisfaction and the impact on revenue.

Cause analysis

It is beneficial for the entity to understand the reasons for initiating events to occur to gain more knowledge on the different drivers of the entity's risks on strategy and business objectives (w. COSO, 2018). There exists several methods to determine root causes to identified risks (Aven, 2015):

- Brainstorming
- Fault tree analysis
- Bayesian networks
- Five whys (COSO & wbcsd, 2018)
- FMEA

In addition to techniques mentioned previously, the personnel performing the analysis should also choose an approach which emphasises knowledge and surprises which is described in depth in Aven (2014, p. 128).

- Anticipatory failure determination (AFD)
- Red Teaming
- Actor network theory (ANT)
- Scenario analysis

3.4.2 Assesses Severity of Risk

Assessment Approaches - Impact

Specified consequences for each identified risk should be conducted for each organisational unit in the entity. The reason for this being that the same risk can impact differently at multiple levels in the entity (COSO, 2017). At the same time, the severity of multiple risks groups may also have greater impact when happening together. It is beneficial to identify impacts according to different aspects or groups that they might affect, for example operations, human life, environment, and public perception (W. Røed, lecture "Risk assessment techniques 1, pp.25, 20.01.20).

Suggested methods for consequence analysis are:

- Event tree analysis (Aven, 2015)
- Analysing interdependencies (COSO, 2017)
- Multi attribute analysis (Aven & Thekdi, 2019)

See Table 5 for an example of impact classifications (Paladin Risk Management Service, 2017) and Table 6 for impact levels:

Table 5 - Impact classifications

Classification	Impact	
1 – insignificant	No injuries, public interest, environmental or operational impact.	
2 – low	a. Human life b. Public perception c. Environment d. Operations	Small injuries. Interest raised but reduced. Easily managed impact. Potential slowdown.
3 – moderate	a. Human life b. Public perception c. Environment d. Operations	Moderate injuries. Interest raised, not reduced. Repairable impact on site. Slowdown.
4 – high/catastrophic	a. Human life b. Public perception c. Environment d. Operations	Severe injuries or fatalities Public insecure Significant impact. Major idle time or stoppage.

Note - Inspired by W. Røed, personal communication, 20.01.20

Table 6 - Impact levels

Identified risk	Impact group	Impact level
1 – Gas leak not detected inside LPG module	a. Human life	2
	b. Public perception	2
	c. Environment	2
	d. Operations	2
2 - small gas explosion inside LPG module	a. Human life	3
	b. Public perception	3
	c. Environment	3
	d. Operations	4

Note - Example retrieved from report written by Golrang et al. (2020)

Assessment Approaches - Likelihood

Probabilities related to the likelihood of the threat/hazard/opportunities occurring are subject to strength of knowledge, are added nonetheless, either qualitatively, quantitatively, or both. A qualitative approach would be the entity setting its own reference categories for a high, medium, and low level (or similar), dividing risks across each level. For a quantitative approach, probabilities and imprecise interval probabilities can be assigned as likelihood but should have a note of both strength of knowledge and the knowledge all your information is based on. (Aven & Thekdi, 2019)

After the likelihoods are determined, the analysts should also consider the unknowns. In situations where the entity only suffers one type of consequence, for example number of fatalities, they can decide to use a quantitative method, applying an uncertainty interval, which estimates the degree of uncertainty to a particular risk (Aven, 2014).

Judging Strength of Knowledge

The likelihoods identified earlier are based on some knowledge gathered by relevant data acquisition categories, classified while analysing as strong, medium, or weak level (Aven & Thekdi, 2019). The categories for consideration of data acquisition are assumptions, data availability, data integrity, consensus, and system understanding. Conditions for classification levels can be found in Aven and Thekdi (2020). See Table 7 for data acquisition categories (Aven & Thekdi, 2019). The total knowledge strength is discovered within the entity's approach found earlier in the Strategy component.

Table 7 - Data acquisition categories

Data acquisition category	Strong classification implying…	Example
Assumptions	knowledge is justified.	There is strong support for assumptions associated with construction levels increasing with an increased number of personnel.
Data availability	accessible and available knowledge.	There is strong data availability associated with building specifications of certain factories.
Data integrity	relevant and appropriately analysed knowledge.	There is strong data integrity for information sourced from employee surveys.
Consensus	expert agreement on appropriateness of knowledge.	There is strong expert agreement for productivity levels being affected by employee satisfaction.
System understanding	well understood system with befitting models.	There is strong understanding of the systems needed for the construction of a certain product.

Note - Categories and classifications retrieved from Aven and Thekdi (2020)

Make an Extended Risk Picture

A qualitative presentation of the risk picture can help the management to see a more complete, and coherent overview of the analysis by combining the identified risk, impact, and likelihood levels, as well as uncertainty levels, and total strength of knowledge (SoK) (Aven & Thekdi, 2019). Table 8 displays a presentation of an extended risk picture.

Table 8 - Extended risk picture

Identified risk	Impact group	Impact level	Likelihood	Uncertainty	Total SoK
1 – Gas leak not detected inside LPG module	a. Human life	2	Very low (0,05%)	Low	Strong
	b. Public perception	2		Low	Medium
	c. Environment	2		Medium	Medium
	d. Operations	2		Medium	Strong
2 - Small gas explosion inside LPG module	a. Human life	3	Low (0,70%)	Medium	Strong
	b. Public perception	3		Medium	Weak
	c. Environment	3		High	Medium
	d. Operations	4		High	Medium

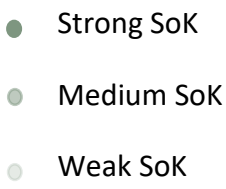
Note - Table inspired by Aven and Thekdi (2020) Example retrieved from report written by Golrang et al. (2020)

Make an Extended Risk Matrix

Risks that are scored higher than low on uncertainty or lower than strong SoK, can be further examined visually by creating an extended risk matrix for those particular risks. Table 9 presents an example of an extended risk matrix applied to risk 2: *small gas explosion inside LPG module*.

Table 9 - Extended risk matrix

Likelihood	≥ 0.90				
	0.50-0.90				
	0.10-0.50				
	0.01-0.10				
	≤ 0.01				
		Very low	Low	Medium	High
	Impacts				



Note - Table inspired by W. Røed, personal communication, 20.01.20

3.4.3 Prioritises Risk

Establishing the Criteria

The management prioritises risks based on the judgement made in the previous risk analysis, as well as a few criteria which the entity can make up themselves to compare the identified risks more easily to the entity's risk appetite (COSO, 2017). COSO (2017) gives the following examples for risk criteria:

- Adaptability: the entity's capacity to adapt and respond to risk.
- Complexity: the difficulty to establish an accurate prediction model of the risk.
- Velocity: the speed at which the risk can impact the entity.
- Persistence: the length of the impact the risk makes to the entity.
- Recovery: the entity's capacity to return to a tolerated risk level.

In addition, a measure of uncertainty and variance should be included in all entities to gain more awareness of uncertain risks (Aven & Thekdi, 2019).

- Uncertainty and variance: the entity's knowledge of the risk and large variances in impact.

Using Risk Appetite to Prioritise Risk

Management uses the risk criteria established, the extended risk picture, as well as the various extended risk matrices to make judgement upon the prioritisation of the identified risks. As an example, if there are risks approaching the entity's risk appetite in a specific business objective, it should be a given a higher priority (COSO, 2017).

Risks are to be prioritised at the level where the risk is owned. This means that a risk which is considered high priority by authorised risk personnel in a certain operational unit, should have the authority to help the management select a risk response which is appropriate even though the risk is not highly prioritised at higher levels. This results in a more consistent and cohesive risk response because it hinders risks at other organisational units evolving and becoming unmanageable at a later time (COSO, 2017).

Bias in Prioritisation

It is not unusual to find dominant or stubborn personalities in a managerial group using different techniques in terms of bias when prioritising risk. This may, among many, be using peer pressure, over confidence, a tendency to be extremely risk avoiding or extremely risk taking or relying too much on expected numbers. It is important for the management to look upon risks in a neutral manner and have uncertainty and knowledge in the back of their minds in order to ask appropriate questions and conclude with suitable risk responses (COSO, 2017).

3.4.4 Implements Risk Responses

Choosing Risk Responses

The management chooses a way to respond to identified risks within 5 categories (COSO, 2017):

- Accept: retain the risk by defining it manageable in accordance with the entity's risk appetite.
- Avoid: the risk is not tolerated, and action is taken to remove the risk.
- Pursue: the entity chooses to accept increased risk in order to optimise value generation.
- Reduce: the risk is too severe for the entity's risk appetite, and action is taken to reduce the risk.
- Share: the entity chooses to reduce the severity of the risk by transferring it or sharing a part of the risk by for example outsourcing the risk to insurance companies.

In addition to these responses, management may find themselves in a position where both business objectives and strategy has to be reviewed and revised if the threatened risk is large or extensive enough (COSO, 2017).

Considering Costs and Benefits of Risk Responses

Implementing expensive responses to risk which provides poor results is not beneficial for an entity's value creation. For that reason, it is important to consider the costs and benefits of the risk responses which are to be implemented. At the same time, keeping personnel and products safe should be on the top of an entity's priority list. Therefore, the management should use a layered approach to assess which measures to implement, based on costs, uncertainties, and ALARP, suggested by Aven (2017) (See Figure 11).

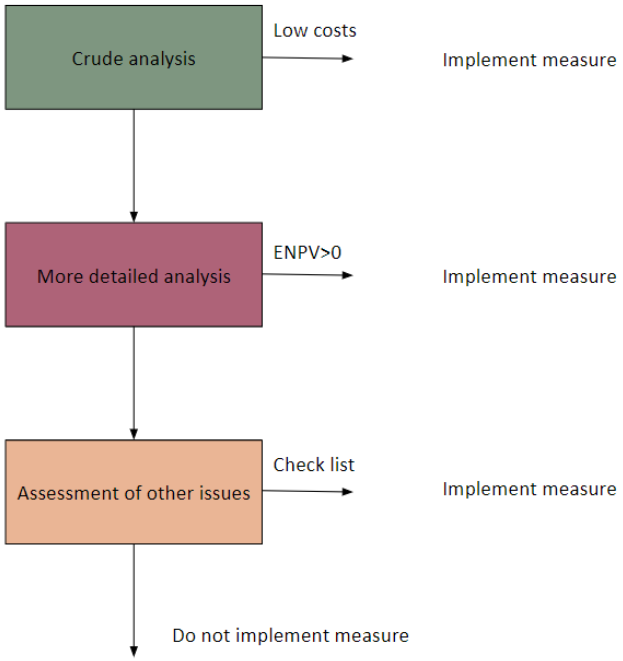


Figure 11 - Layered approach for implementing ALARP. Inspired by Aven (2017). Produced in Google Drawings.

Step 1: if the cost of the safety measure is low, the measure should be implemented if it is considered to have a positive impact on business objectives or values.

Step 2: if the costs of the safety measure is large, one should assess relevant in more detail, using for example cost-benefit-methods or similar, as long as the expected numbers are calculated with care. If the results of the more detailed analysis are positive, the measure should be implemented.

Step 3: if the expected numbers are measured to be too high, one has to assess other issues of interest, for example considering if the measure benefits the risk by decreasing uncertainties, reinforcing knowledge, or increasing robustness and resilience in view of strategy and business objectives.

3.4.5 Develops Portfolio View

Developing a Portfolio View

The entity can use a portfolio view to easily consider the risks in their risk (threat/hazard/opportunity) inventory, however it is important to note that a portfolio view should not set up a basis to determine how many of the individual risks identified can be tolerated into the entity's risk appetite. The reason for this is that the uncertainties are easily ignored, and the entity could potentially face a sum of larger risks than what their risk appetite can withstand (Aven, 2015).

The portfolio view should be used as a means to see how risks owned by different organisational units can affect the entity as a whole, as well as giving the management a means to determine if the entity's residual risks after risk responses are implemented are aligned with the entity's risk appetite (COSO, 2017).

The entity chooses their own way to organise the risks in portfolio view, for example emphasising risk categories across their operational units or the entity overall (COSO, 2017). The entity should also consider how much and what kind of knowledge is needed to better manage these risks in the future (COSO & wbcsd, 2018).

3.5 Review & Revision

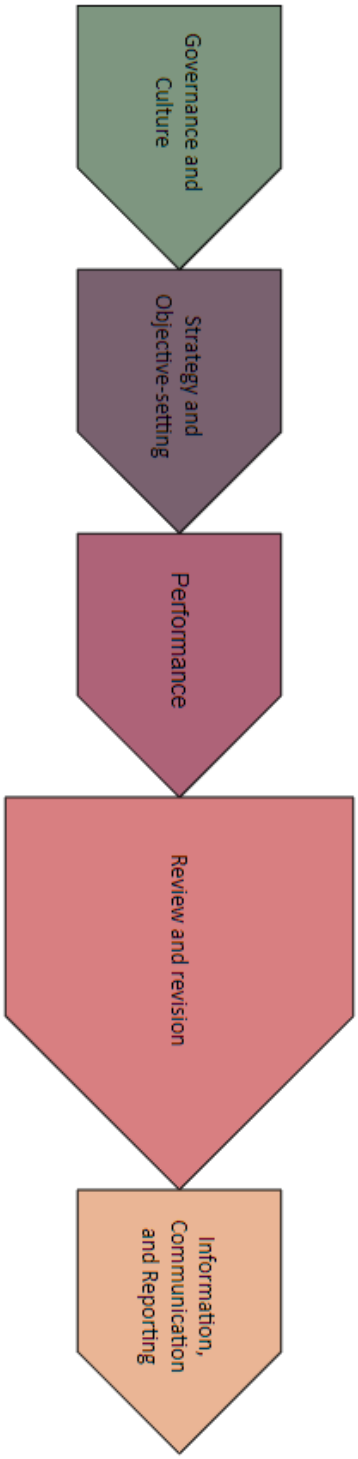


Figure 12 - Components: Review and Revision. Produced in Google Drawings.

Review and revision focuses on reviewing how the elements of ERM functions and changes over a period of time, and which revisions to implement (COSO, 2017). The review and revision section is composed of three principles, based on COSO ERM Framework on Review & Revision:

Principle 15: Assesses Substantial Change: The entity identifies and evaluates changes that may potentially have a significant effect on strategy and business objectives (COSO, 2017).

Principle 16: Reviews Risk and Performance: The entity reviews risks and performance (COSO, 2017).

Principle 17: Pursues Improvement in Enterprise Risk Management: The entity corrects and enhances their ERM (COSO, 2017).

The sub-chapter contains the following activities:

Principle 15: Assesses Substantial Change:

- Determine changes in the entity's internal and external environment that can significantly affect the entity's strategy or business objectives.

Principle 16: Reviews Risk and Performance:

- Periodically evaluate ERM related activities in order to assess and revise future ERM processes.

Principle 17: Pursues Improvement in Enterprise Risk Management:

- Integrate a culture of learning and continuing improvement.

3.5.1 Assesses Substantial Change

Entities can often anticipate shifts and changes in risk when setting new, or changing, strategies and business objectives, but there are often several overlooked changes occurring to the entity which has prominent effects generated from the entity's internal and external environment in addition to adjustments in culture (COSO, 2017). Table 10 shows an example of internal and external environment changes which may affect the entity's current strategy or business objectives (COSO, 2017).

Table 10 - Environmental changes affecting strategy or business objectives.

Environment	Example of changes occurring to the entity
Internal Environment	
Rapid growth	IT systems not able to meet risk information requirements.
Innovation	Modification of risk responses, extra training needed.
Changes in leadership and personnel	New employee not understanding entity culture or only focuses on performance numbers.
External Environment	
Changing regulatory or economic environment	Increased competitive pressure, changes in requirements.
Changing stakeholder expectations	

Note - Examples retrieved from COSO (2017)

COSO (2017) recommends directing a "post-mortem" in the aftermaths of a risk event to assess the entity's reaction to the passed risk in order to learn what to implement in case of future events.

3.5.2 Reviews Risk and Performance

Integrating Reviews into Business Practices

After determining the changes surrounding the entity's environment, the entity should evaluate or revise their chosen ERM process using a question-based approach. When reviewing the entity's performance, the management, or a specified committee, should seek answers in questions like (COSO, 2017):

- Has the entity's performance been conducted as previously anticipated and did it accomplish its short/long-time targets?
- Has the entity taken enough risk to achieve its targets?
- Are there any risks taking place at the present time which is affecting the entity's performance?
- Has the entity been successful in acquiring sufficient knowledge to lessen the uncertainty of identified risks?

If the entity has deemed any of the answers not being within the entity's acceptable variation of performance, it may be required to (COSO, 2017):

- Review business objectives by changing or renouncing current practices.
- Review culture to see if the entity is embracing its intended risk culture.
- Review strategy or re-evaluating alternative strategies discovered previously.
- Review changes to communication and reporting (COSO & wbcsd, 2018) by inviting evaluation from relevant stakeholders engaged in the entity's risk practices (Aven & Thekdi, 2019).

With the increased knowledge the entity now has of its performance, the entity may also (COSO, 2017):

- Revise target performance
- Reassess severities of risk results
- Review prioritisation of risks
- Revise risk responses
- Revise risk appetite

3.5.3 Pursues Improvement in Enterprise Risk Management

By integrating a culture of continuing improvement, the entity can improve efficiency and the benefits from ERM at all organisational levels and furthermore, aid in achieving the entity's mission and vision. There are several areas where the entity can find opportunities to improve efficiency and ERM benefits, for instance (COSO, 2017):

- With new technology
- Analysing past shortcomings in performance
- Organisational changes
- New ways of communication
- Upgrading to the next ERM maturity level to further enhance benefits from ERM (Aven & Thekdi, 2019).

3.6 Information, Communication & Reporting

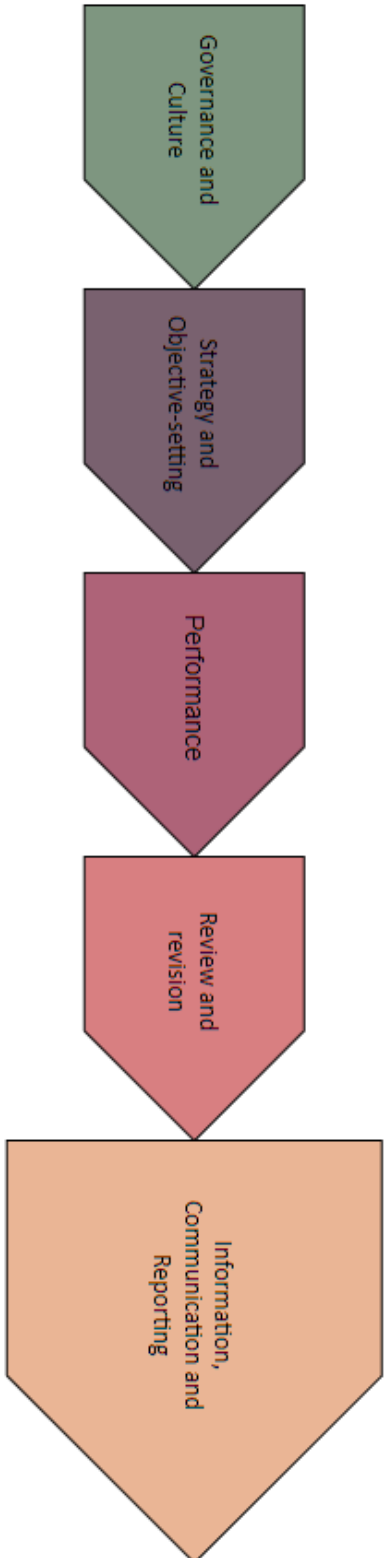


Figure 13 - Components: Information, Communication, and Reporting. Produced in Google Drawings

The last section of the COSO ERM Framework is information, communication, and reporting, which focuses on attaining the right information and transforming this information to relevant knowledge that can help the entity attain its mission and vision. The elements of ERM functions and changes over a period of time, and which revisions to implement (COSO, 2017). The review and revision section is composed of three principles, based on COSO ERM Framework on Information, Communication, and Reporting:

Principle 18: Leverages Information and Technology: The entity takes advantage of its information system to support ERM (COSO, 2017).

Principle 19: Communicates Risk Information: The entity uses channels of communication to support ERM (COSO, 2017).

Principle 20: Reports on Risk, Culture, and Performance: The entity regularly report risk, culture, and performance at multiple organisational levels across the entity (COSO, 2017).

The sub-chapter contains the following activities:

Principle 18: Leverages Information and Technology:

- Establish a system to consider the relevancy of gathered information in order to avoid information overload.

Principle 19: Communicates Risk Information:

- Create information channels where personnel can submit awareness and information on ERM to internal stakeholders.
- Use established information channels to invite constructive feedback from external stakeholders.
- Establish a system for open and transparent communication channels between the board and the management.

Principle 20: Reports on Risk, Culture, and Performance:

- Develop a system for reports to keep relevant stakeholders informed on information that could benefit them in the interest of fulfilling their functions and obligations.

3.6.1 Leverages Information and Technology

Relevant information is needed by the entity in order to maintain the understanding and advancements of the entity's present and future risk profile (COSO, 2017). The entity should therefore consider:

- If the information available is relevant.
- What kind of information system the entity is utilising.
- The cost of acquiring relevant information.

When discussing relevant information, the entity may look up the data acquisition categories presented in Table 7 in the guide. Incomplete or inaccurate data can, as mentioned earlier, hinder the management in making appropriate judgements, and estimations (COSO, 2017).

3.6.2 Communicates Risk Information

Communication with Stakeholders

The entity should use some form of informative channels to provide the stakeholders with relevant information in regard to making decisions. The information submitted by the management should clearly communicate reminders, promote awareness, and general information about ERM for the stakeholders, as well as the management's expectations of the stakeholders with regard to following ERM (COSO, 2017). Open communication where stakeholders can (anonymously if needed) comment and discuss ERM related activities and applications should be provided.

Furthermore, the entity should open channels of communication for groups of stakeholders (both internal and external) engaged in risk practises, where they can discuss and learn from previous experiences before sharing with the rest of the entity (COSO, 2017). External stakeholders can provide valuable information about customer satisfaction and how to tailor experiences to suit customers differently.

Communicates with the Board

For the board to sufficiently encourage and challenge the management without the management feeling constrained, a dynamic, constructive, and pedagogical dialogue must exist between the two groups. Entity boards often use pre-planned meetings and on-site visits as a way to engage with the management of the entity. Using technological channels of communication, the board can keep an oversight and show openness to conversations on risk information that have not yet got defined risk responses in place as well as discussions on the ERM process and how to improve the entity's ERM (COSO, 2017).

3.6.3 Reports on Risk, Culture, and Performance: Identifying Report Users and Their Roles

For the entity to achieve its mission and vision, it is essential that appropriate stakeholders know the information that is relevant to them and their work. To avoid spending valuable time, reports are made to inform relevant readers in a clear way of news, details, and data deemed beneficial for their work fulfilling the entity's strategy and business objectives in due frequency depending on the severity and priority of the risk. Report uses are comprised of (COSO, 2017):

- The board and the management of the entity.
- Relevant risk owners responsible for the management of defined risks.
- Assurance providers.
- External stakeholders, such as regulators.

Table 11 - Project plan – Implementing ERM

Project plan

Project name: Implementing enterprise risk management

Number		Responsible	Execution	Estimated time	Start date	End date
1	Governance and Culture					
1.1	Exercises Board Risk Oversight					
1.1.1	Ensure all board members fully understand the industry of the entity and keep themselves updated at all time of changes in business context.	Board of directors	Board of directors			
1.1.2	Ensure the board is made up of independent professionals to avoid conflicts of interest.	Board of directors	Board of directors			
1.1.3	Review periodically that the board consist of a group with relevant skills and knowledge in order to provide entity oversight.	Board of directors	Board of directors			
1.2	Establishes Operating Structure					
1.2.1	Define the entity's regulatory and non-regulatory risk and safety guidelines.	CEO	Risk manager			
1.2.2	Consider a range of factors when developing the entity's operating structure.	Board of directors	CEO			
1.2.3	Establish an ERM committee to get insight on risks developing from different organisational units.	CEO	Risk manager			
1.3	Defines Desired Culture					
1.3.1	Assess internal and external factors to shape the entity's culture.	Board of directors	CEO			
1.3.2	Produce a simple visual representation which can function as a helpful guide to employees.	CEO	Risk manager			
1.3.3	Periodically assess the entity's risk culture after major changes in the entity.	CEO	Risk manager			
1.3.4	Produce clear and detailed definitions on various risk strategies (cautionary principles, robustness-, resilience-, and discursive strategies).	CEO	Risk manager			

1.3.5	Ensure compliance from the leaders top down by communicating the entity's desired culture and working as role models.	Board of directors	Risk manager
1.4	Demonstrates Commitment to Core Values		
1.4.1	Promote openness and transparency in regard to risk related subjects.	CEO	Risk manager
1.4.2	Create a system for which personnel can easily send deviations and improvement suggestions anonymously.	Risk manager	Risk manager
1.4.3	Encourage personnel to speak up about all hazardous behaviour in a polite manner no matter the level of the wrongdoer.	Risk manager	Risk manager
1.5	Attracts, Develops, and Retains Capable Individuals		
1.5.1	Establish a system to provide personnel with guidance and motivation to show that the entity is committed to their welfare.	HR manager	HR manager
1.5.2	Create a system for periodic reviews of every personnel's well efficiency, education, and wellbeing.	HR manager	HR manager
2	Strategy and Objective-setting		
2.1	Analyses Business Context		
2.1.1	Use external and internal environment characteristics to realise and establish the entity’s business context.	Board of directors	CEO/CFO
2.2	Defines Risk Appetite		
2.2.1	Create a risk to performance ratio, risk profile, to gain a rough draft for describing the entity’s risk appetite.	CEO/CFO	Risk manager
2.2.2	Use the risk culture decided upon previously to see how much variation the entity is willing to undergo in regard to value creation.	CEO/CFO	Risk manager
2.2.3	Find the entity's target level and risk capacity to create a risk appetite for the entity.	CEO/CFO	Risk manager
2.2.4	Define a total knowledge approach used for classifying knowledge throughout the ERM process.	Risk manager	Risk manager
2.3	Evaluates Alternate Strategies		
2.3.1	Choose a strategy that reflects the entity’s risk appetite, based on the strength of knowledge of the strategies in question.	CEO/CFO	CEO/CFO
2.3.2	Set up periodical strategy-setting evaluations to keep an overview of short-term and long-term strategies	Risk manager	Risk manager
2.4	Formulates Business Objectives		
2.4.1	Use the entity’s strategy and risk appetite to formulate specific, measurable, attainable, and relevant business objectives.	CEO/CFO	Risk manager
3	Performance		

3.1	Identifies Risk		
3.1.1	Select categories of risk which resonates with your entity.	Risk manager	Risk manager
3.1.2	Create a designated group of employees trained on risk management and practitioners to identify new, emerging, and changing risks.	Risk manager	Risk manager
3.1.3	Utilise and continually update the entity's risk inventory to determine new, emerging, and changing risks several time each year.	Risk manager	Risk manager
3.1.4	Identify threats/hazards/opportunities that can impact the entity's strategy and business objectives.	Risk manager	Risk manager
3.1.5	Establish and use an entity sentence structure to precisely define risks.	Risk manager	Risk manager
3.1.6	Use cause analysis to find the risk drivers threatening the entity's strategy or business objectives.	Risk manager	Risk manager
3.1.7	Employ a specialised approach to cause analysis emphasising knowledge and surprises to risks with higher levels of uncertainties.	Risk manager	Risk manager
3.2	Assesses Severity of Risk		
3.2.1	Classify the impacts affecting the entity by grouping into classifications in which the entity values.	Risk manager	Risk manager
3.2.2	Analyse likelihoods qualitatively or quantitatively by referencing the strategy and business objectives of the entity.	Risk manager	Risk manager
3.2.3	Enhance likelihoods and reduce uncertainty by including strength of knowledge and where the total knowledge comes from.	Risk manager	Risk manager
3.2.4	Create an extended risk picture for an overall look of all identified risks.	Risk manager	Risk manager
3.2.5	Display uncertain risks in an extended risk matrix to provide further judgement when prioritising and reviewing risks.	Risk manager	Risk manager
3.3	Prioritises Risk		
3.3.1	Create a set of risk criteria in order to compare the identified risks to the entity's risk appetite.	CEO/CFO	Risk manager
3.3.2	Evaluate and prioritise risks at the level where the risk is owned.	CEO/CFO	Risk manager
3.4	Implements Risk Responses		
3.4.1	Decide upon risk responses based on the entity's business context, obligations, regulations, risk appetite, severity, and prioritisation.	CEO/CFO	CEO/CFO
3.4.2	Use a layered approach to assess which measures to implement based on cost and uncertainties.	CEO/CFO	Risk manager
3.5	Develops Portfolio View		

3.5	Periodically evaluate how risks owned by different organisational units can affect strategy and business objectives.	CEO/CFO	Risk manager
4	Review and Revision		
4.1	Assesses Substantial Change		
4.1.1	Determine changes in the entity's internal and external environment that can significantly affect the entity's strategy or business objectives.	Board of directors	CEO
4.2	Reviews Risk and Performance		
4.2.1	Periodically evaluate ERM related activities in order to assess and revise future ERM processes.	Board of directors	CEO
4.3	Pursues Improvement in Enterprise Risk Management		
4.3.1	Integrate a culture of learning and continuing improvement.	CEO	CEO
5	Information, communication and reporting		
5.1	Leverages information and Technology		
5.1.1	Establish a system to consider the relevancy of gathered information in order to avoid information overload.	CEO/CFO	Risk manager
5.2	Communicates Risk Information		
5.2.1	Create information channels where personnel can submit awareness and information on ERM to internal stakeholders.	Risk manager	Risk manager
5.2.2	Use established information channels to invite constructive feedback from external stakeholders.	Board of directors	CEO
5.2.3	Establish a system for open and transparent communication channels between the board and the management.	CEO/CFO	Risk manager
5.3	Reports on Risk, Culture, and Performance		
5.3.1	Develop a system for reports to keep relevant stakeholders informed on information that could benefit them in the interest of fulfilling their functions and obligations.	CEO/CFO	Risk manager

4 Example of Application

In the following chapter, an example of the application of parts of the guide will be given. The example is based on a group report written by a group of university students, including myself, in the course SAM510 Risikobasert styring in the spring of 2019. The report is called *Hvorfor bør vannverkseier sikre sine høydebasseng mot tilsiktet forurensing av drikkevann* (why should the owner of a water supply secure their water reservoir against intentional contamination of drinking water) which is open and can be accessed through Ove Njå at the University of Stavanger. The report consists of a risk assessment which includes a qualitative and quantitative analysis. For the example presented below, the qualitative coarse risk analysis will be used.

The following example will address the enhanced performance section of the COSO loop in the order which has been presented previously in chapter 3. Risks are identified, assessed with regards to severity and likelihood, a judgement of the strength of knowledge of data is reviewed, and finally a risk response is chosen accommodated by suggestions for minimising the risks in question.

The water reservoir in question is real and owned by a Norwegian commune which shall remain anonymous. The knowledge this analysis is based on are expert, specialist, and employee expertise in the form of interviews provided by the Norwegian food safety authority, Norwegian Water (Norsk Vann) (a water industry association in Norway (Aasand, 2018)), a consulting specialist in the field of limnology as well as knowledge from two employees of the commune.

4.1 Introduction

Each Norwegian municipality are responsible for their own communal water supply pipes or pipelines. Often these pipes go through elevated water basins or reservoirs (henceforth called reservoirs) in order to, for the greatest part, ensure sufficient water supply to towns or cities in case of fires or if the main water source is temporarily inaccessible (Folkehelseinstituttet, 2008).

During a recent review of a town's operational risk inventory a team of professionals, consisting of one risk specialist, one offsite and one onsite employee working directly with the town water supply on a day to day basis, were commissioned to identify intentional threatening risks towards the town's reservoirs.

4.2 Identifies Risk

The team rephrased the tasked into *the possibility of an intentional threat to the safety or security of the town's reservoirs and the associated impacts on the supply of safe drinking water.*

The team decided to use a simplified SWIFT process, where they divided the reservoir into components to identify events made intentionally that may lead to a hazardous situation with regard to the drinking water or the physical structure of the reservoir itself. The team produced a list of eight threatening scenarios presented in Table 12.

Table 12 - Application example: Eight scenarios

Scenario number	Description
1	An individual performs an act of mapping the area around the reservoirs.
2	An unfaithful server steals, distributes, destructs, or sabotages values connected to the reservoirs.
3	An individual contaminates the drinking water in the reservoirs.
4	An individual performs physical damage on the reservoirs.
5	An individual uses violence or threatening behaviour to gain access to valuables connected to the reservoir.
6	An individual vandalises the reservoirs or the physical security of the reservoir.
7	An individual makes threats of sabotage or contamination of the drinking water in the reservoir.
8	An individual breaks into the reservoir

Note - Scenarios are inspired by Norwegian Water's scenarios page 22 (Riis & Hareide, 2017)

Furthermore, the team asked themselves a series of questions relevant to their task and scenarios.

- *How can this threat/hazard damage the entity's strategy or objectives?*
  The ministry of Health and Care Services produced in 2017 a drinking water regulation, with an objective to protect human health by demanding safe delivery of adequate quantities of healthy drinking water which is clear and without prominent odour, flavour, or colour (omsorgsdepartementet, 2017). An individual contaminating the drinking water in the reservoir will directly threaten the regulated objectives, whereas performing physical damage to the reservoir may threaten the objectives with more uncertainty. More so uncertain towards the main objectives are cases where an individual threatens, maps out, or breaks into the reservoir, but the events signalise a threat to the safety of the drinking water, which threatens the strategy towards fulfilling the entity's objectives. Because of the likelihoods of the last-mentioned events may lead to further events which can affect the objectives, the team decides to keep these eight scenarios and deem them plausible as threats to the entity's strategy and objectives.
- *How can this threat/hazard develop further in the future?*
  These events can all become steppingstones for other individuals who would want to threaten the safety of the town's water supply.

- *What kind of opportunities can the entity salvage from previously identified threats/hazards?*
  The team can use information from past identified events to see how they can improve on the technology of their security systems. By for example installing CCTV, they will have 24-hour surveillance without having to employ a guard to manually check the premises. By setting up automatic water testing facilities inside the reservoir building there can be more frequent testing of water quality without compromising time since the employees are not required to leave their main offices in another part of the town.
- *What kind of unlikely threats/hazards can the entity face?*
  There is a general agreement that an intentional contamination is one of the more unlikely threats than may happen, but also one of the most critical. There has yet not been any fatalities in regard to intentional water contamination in Norway (Scandpower, Aquateam, COWI, & forskingsinstitutt., 2003).

By brainstorming the team identified some causes to why an individual or individuals would want to harm or damage the town's drinking water or reservoir, for example for scenario 1, an individual would want to map out the area with the hope of harming or damaging human life, environment or materials around the reservoir at a later point. An intentional contamination of drinking water, as described in scenario 3, is or can be, caused by an individual who has a desire to harm lives, which can be done for multiple reasons, for example for their own enjoyment or to make a point towards the commune who have done them wrong in the past. In the following of the analysis, special attention will be given to scenario 3 in order to shorten the example.

4.3 Assesses severity of risk

The impact classifications produced by the Norwegian Food Safety Authority (Mattilsynet) are used in this part of the analysis and can be viewed in Appendix 7.4 D. In the following a table of the severities for scenario 3 will be presented as well as a short reasoning for each chosen level.

Table 13 - Application example: Severity levels

Theme		Severity level (after 2 days)	Severity level (after 7 days)
a.	**Quality**	3	4
b.	**Delivery**	2	2
c.	**Public Perception**	2	3
d.	**Human life**	3	4

Note - Severity levels taken from report "Hvorfor bør vannverkseier sikre sine høydebasseng mot tilsiktet forurensing av drikkevann".

Consequences related to the contamination of drinking water is mainly related to quality, where the objective of a healthy drinking water as defined by the Ministry of Care Services (Omsorgsdepartementet) is violated. The impact level for quality is therefore classified as a level 3, whereas if no measures are taken in due time, the impact level changes to level 4 and is therefore described as a serious breach of the objective.

If the contamination is not discovered, there will be no impact on the delivery. After discovery, users may discover short disruptions to the water supply, but is not deemed severe enough to get more than a level 2 on impact for both two and seven days.

The public perception may be threatened if it is revealed a lack of security or lack of priority from the commune to prevent contaminations. The public perception is further weakened the longer the contamination endures and is therefore given a severity level 3 after seven days.

A contamination of drinking water can after two days produce illnesses in the users of that particular reservoir and is therefore seen as hazardous for human health. The classification of level 3 is given, which is high due to the possibility of users either neglecting the hazard or not receiving sufficient warnings from the authorities. The impact level is set at level 4 after seven days in the case where the contamination is not discovered and the water ends up severely affecting the health of many people, and in the worst case leads to fatalities both in private homes or in health care facilities (i.e. hospitals).

4.4 Assessment of likelihood

Likelihoods are based on the Norwegian Food Safety Authority (Mattilsynet) matrix which can be found in Appendix 7.4 D, and is divided into three criteria:

a. Is the event known in the industry? If yes, has the commune experienced the event in the past?
b. Does professional judgement and cautionary principles dictate that the event may happen in the future?
c. Do threat assessments say that the event is likely?

Scenario 3 is indeed known by the industry and the communes, but the number of contaminations to reservoirs is extremely rare word wide (Scandpower et al., 2003) and have not yet caused a fatality in Norway (criteria a). The commune in question have not experienced an intentional contamination first-hand. Scenario 3 is known by professionals where they consider it to be likely within 10-50 years in light of the cautionary principle (criteria b). A threat assessment has been made in the original report but will not be presented in this example. Scenario 3 is categorised under the threats terror and sabotage, where contamination is viewed in the terror category as unlikely, and sabotage as likely or medium likely (criteria c). These reasons total to a likelihood level 2 (medium).

4.5 A judgement of strength of knowledge

In this example, the commune has in advance chosen a selective approach to total knowledge, which will affect the overall judgement of the strength of knowledge. Data integrity and system understanding are set as important criteria and are therefore prioritised as such.

4.5.1 Assumptions

There exist strong assumptions across the different respondents that if an individual has decided to break into a reservoir, they will succeed. The reason for this being that the Norwegian water supply system being out of date and not built to accommodate present threats (anonymous expert, personal communication, March 2019).

Furthermore, many of the respondents assume the difficulty of acquiring necessary contaminants in order to contaminate the drinking water in a reservoir. However, regarding the availability of contaminants or toxins, one does not have to contaminate with illegal drugs. One can assume that an individual with the desire to harm people could easily contaminate drinking water with human or animal faeces, nitrates from fertilisers (Bjørnå, 2018) (easily acquired as a farmer) or metals. There exists strong support for assumptions of human beings becoming ill, or in the worst-case die, by drinking contaminated water, giving human lives and quality a strong classification of knowledge.

There is weak knowledge regarding delivery because there are so many different variables involved. If the reservoir is a side-pool (sidebasseng) the current contaminated reservoir pipes going in and out can be shut down, and therefore not compromise day-to-day delivery. A flow-pool (gjennomstrømningsbasseng) however, which stands between the water source and inhabitants/users will have some delivery shut offs in the case of a contamination (Folkehelseinstituttet, 2008). The time of the delivery shut off will depend on each commune, where the contamination comes from and how it is treated.

There are weak assumptions regarding public perception.

4.5.2 Data availability

There is weak data availability associated with reservoirs in the different communes in Norway. The means of acquiring data has been through personal data exchanges with the commune in question. The Norwegian institute of public health (folkehelseinstituttet) released in 2008 a series called *Vannforsyningens ABC* (the ABC of water supply) containing general information about the Norwegian water supply system. However, details about specific reservoirs can only be acquired through the commune itself, either in person or shared through their webpages.

There is, however, medium to strong data availability on effects of water contamination on human lives.

4.5.3 Data integrity

There is strong data integrity for information sourced by employees and historical data in regard to quality and delivery.

There is medium data integrity for the effect of water contamination on human life because of the vastness of different sources and contaminants.

There is weak data integrity for information about public perception on a water contamination.

4.5.4 Consensus

There exists strong expert agreement on the difficulty of breaking into a reservoir, but there is weak expert agreement on the likelihood of an intentional contamination of drinking water. Some respondents have deemed it likely that it will happen at some point, while other respondents consider the event to be severely unlikely and is therefore an event not accounted for in their risk related analyses. Because of disagreements of respondents regarding contamination of drinking water the classification will be considered weak.

4.5.5 System understanding

There exists strong understanding of the systems the reservoirs contain and how they work. There is also a strong understanding of the basic security surrounding the reservoir, its benefits and shortcomings especially regarding delivery.

4.6 Extended risk picture

A table with extended risk picture is presented in the following.

Table 14 - Application example: Extended risk picture

Identified risk	Impact group	Impact level (2 days)	Impact level (7 days)	Likelihood	Uncertainty	Total SoK
Scenario 3: An individual contaminates the drinking water in the reservoirs.	e. Quality	3	4	2 (medium)	Low	strong
	f. Delivery	2	2		Medium	strong
	g. Public Perception	2	3		High	weak
	h. Human life	3	4		High	medium

4.7 Implement risk response

The team considers the objective to provide healthy and clean water of upmost importance and can choose to either avoid or reduce the risk towards scenario 3. Avoidance of an event is very easy to say, but difficult to achieve when the scenario involves an external individual/saboteur. The team should therefore work in order to reduce the likelihood of an

individual gaining access to the reservoir. Implementing measures to reduce unauthorised intrusion into the area, such as CCTV or loud alarms can act as a hindrance into the field. Other active measures involving human relations, such as employing professional security guards can also be implemented if the commune has required resources.

Per today, the commune tests their reservoir once a week, with testing taking from three up to five days (employee from commune in question, interview, 21.03.19), which means that a contamination of water would not be detected before the situation becoming critical unless the users of the water informed the commune. The team suggests testing reservoir water more often in order to stay on top of the situation if a contamination would occur.

Furthermore, the commune can also implement organisational measures by for example teaching the population what to look for in terms of symptoms in case of a contamination, as well as how to safely boil water. Sending out information by SMS or similar would benefit the duration it takes to inform the user population of the drinking water in question.

5 Discussion

This next chapter demonstrates a discussion on the main differences between COSO (2017) and the guide presented in chapter 3. The chapter below is outlined in the order of COSO's components.

5.1 Governance and culture

COSO (2017) devotes a page under principle 3 to the application of judgement, where it is stated that judgements are used when there is a limited amount of information or data for support, when strategy, business objectives, performance or risk profile goes though unusual changes, and during disturbing times. Judgement is presented in a way of the management using their personal experiences by showing for example over- or under-confidence or communication styles, leading to organisational bias and decisions made which are not in line with the entity's core values, resulting in lower confidence from stakeholders (COSO, 2017). Whiles being aware of judgements being applied is important, the guide takes the judging data one step further by adding an extensive judgement of knowledge to the third component of the framework – performance. A limitation to changing the placement of the issue is that it may seem more like an afterthought or that it is only important to review judgement during an analysis, and not in prior stages of implementing ERM. However, considering judgement is mentioned a few times before the performance component, and should be reviewed in every part of an ERM application process.

When reviewing the component of governance and culture in COSO (2017), the subject of accountability kept appearing throughout principle 4 – *demonstrates commitment to core values*. "(..) demonstrating to personnel that lack of accountability is not tolerated.", "(about adherence to core values), and rewards are allocated or disciplinary action is applied as appropriate" and "(..) an employee being issued a warning to being put on probation to even being terminated" are all statements cited from COSO (2017) and are concerns not included in the enhanced guide. This is done on purpose in order to not take a stance regarding workplace discipline. It is important for all personnel to understand and be expected to follow the entity's core values. However, this guide will not recommend disciplinary methods which can lead to workplace aggression and punishments, but instead recommend guiding and educating personnel to adhere to entity rules and regulations (Fredericksen & McCorkle, 2013). At the same time, it is important to stress an emphasis on the consequences to not adhering to the entity's core values, and the effects on the entity as a whole when these values are not expressed especially from a top down point of view. In 2009, BP, formerly British Petroleum, had a specific core value with the title *Responsible*, "We are committed to the safety of our people and the communities and societies in which we operate. We aim for no accidents, no harm to people and no damage to the environment." (BP, 2009). According to the Norwegian encyclopaedia, it was revealed that platform inspections had been both superficial and shorter than the established processes suggested. About 25 percent of the required monthly inspections were not performed. It is

not in the scope of this thesis to speculate as to why it was chosen not to follow official processes, but these events ended in the Deepwater Horizon accident in 2010, where 11 people lost their lives. It also led to large spills of oil and extensive environmental damage, great damage to the company's reputation and a price tag of over $ 65 billion (Smith-Solbakken, 2020). It is therefore crucial for the management to stress the point that core values do not only have to be expressed in an official policy, but must also be complied by all management, with the leaders as role models.

5.2 Strategy and objective setting

An entity defining and using its risk appetite is considered a central part regarding creation, preservation, and realisation of value (COSO, 2017). COSO (2017) offers a range of possibilities for an entity establishing their desired risk appetite, ranging from generic terms (low or high risk appetite), to numerous quantitative measures coordinated with the entity's strategy and objective targets (for example risk acceptance criteria). However, given that the guide is of beginner maturity, less priority is given to defining a detailed risk appetite, and therefore considers the generic terms mentioned earlier as satisfactory. As the entity's ERM process matures, a growth of the risk appetite should be of priority in order to continue the dynamic improvement when forming the entity's risk profile. A limitation to not spending much time on the definition of the entity's risk appetite can be regarding risk appetite as less importance, and therefore ignoring, over- or underestimating its influence on target performance. This may lead to, amongst others, the entity not realising its potential by selecting a low risk profile and wasting opportunities, or the entity going over their risk capacity, which can result in losing value that the entity has earned.

The addition of selecting the entity's approach to judging knowledge, namely total knowledge, based on strategy, business context, and objectives suggested in Aven and Thekdi (2018) represents the start of assessing uncertainties in an ERM process. If the business context of an entity penalises them greatly for inaccurate, insufficient, or misinterpretation of their judgement of knowledge, a pessimistic or conservative approach could be preferable. However, if, as in the application example in chapter 4, the entity sees some criteria as more important than others (in this instance data integrity and system understanding), a selective approach to total knowledge would be more beneficial to the entity in question. The management's chosen approach can help create a picture of what kind of uncertainties the entity is facing and where it may protrude most.

5.3 Performance

By dividing risks into groups or themes, the analyst is able to create a more comprehensive list of threats and opportunities affecting the entity's strategy or objectives. In the application example in chapter 4, the analysis team considered intentional threatening risks towards a specific commune's water reservoirs. By focusing the analysis on one specific area and type of behaviour, the team managed to review multiple aspects, circumstances, and types of hazardous behaviours in a short amount of time. When looking at Table 3 one can

draw a systematic line directly to the category: Operational, and in that way cover the largest possible amount of threats, hazards, and opportunities. A simple representation of the process is given below.

$$Risk\ Inventory \rightarrow Operational \rightarrow Security\ Related\ Events \rightarrow Water\ Supply \rightarrow Water\ Reservoir \rightarrow Intentional$$

In order to continue on the same path, the team can analyse *unintentional* threats, hazards, and opportunities regarding the commune's water reservoir and so forth. The method can be limited by lack of time, depending on resources provided and who is conducting the analyses. If the analysis is performed by a CRO or similar in a managerial position, their time may be better spent elsewhere if they are heavily loaded with projects. A suggestion would be a CRO or risk manager to map out systematic lines similar to the process presented earlier, and from there the analysis being conducted by a project team of different skill sets who are known with the day-to-day operations of the objects being analysed, before it is saved in a risk portfolio for all employees to access. On the other side, an over emphasis on finding *all* risk that can threaten the entity may result in spending too much time on unimportant risks and not enough time on looking at the big picture. The entity must create a balance between finding new risks which are both relevant and finding the uncertain or unknown risks which may threaten the entity in the future. A way to create a balance here, if the entity chooses to prioritise it, is to find all threatening risks with the process stated earlier, and then further analysing the most important and aggressive risks, as well as risks which influence each other.

When storing risks in a portfolio where a number of employees with different backgrounds provide their inputs, it is important for the writers to have a homogenous language. Using the same neutral wording and terminologies can remove bias (COSO, 2017) by not incorporating root causes or blame on workers, services, or technology. By using the process line described above and a general phrasing of the risk itself, stakeholders or anyone with a need for looking through the entity's risk portfolio can easily find the groups, subgroups, and subject they are looking for without getting lost in the various formulations provided in the risk portfolio. In the example in the previous chapter, the commune or town can choose to file the risk under safety, reservoir, or drinking water depending on the entity's focus and choice. This can become confusing if all employees do not understand the system in which the risks are filed, and it may in this way become more difficult to locate or track down the risks you are looking for. A suggestion for this could be delegating the filing of the risk to the administration for processing. Commissioning extra work on the administration can on the other hand overwork their caseload, leading to imprecise or faulty efforts. Nevertheless, assigning the archiving of the risk analyses to one single person or group can help correct small archiving mistakes which can be easily made by personnel who are less familiar with the organisation of the entity's portfolio.

One large addition in the guide in relation to the original framework is the supplemented questions one is to ask when identifying threats, hazards, and opportunities. COSO (2017) recites, under principle 10, where new, emerging, and changing risks can occur from, but are mentioned as examples. The guide in this thesis composes questions one is to ask themselves when identifying risks in order to make the analyst stop and think. By focusing on specific questions, the analyst can produce a more comprehensive list of threats, hazards, and opportunities than they may have identified otherwise. At the same time, the questions provide an important aspect of risk definition which is only mentioned a few times but not covered in depth in COSO (2017), namely unlikely or unknown threats, hazards, and opportunities. Entities can experience unknowns frequently but having defined and thought about possible unlikely events may lessen the shock and encourage quicker recovery, as well as time to identify feasible opportunities which can be salvaged. The questions are a way of gathering one's thoughts to specific areas or risks and are not designed to be dwelled upon for a long time. The answers to the questions may be responded to in keywords or short sentences for the sake of saving time.

COSO (2017) states under principle 10 that one should describe risks with accuracy and promotes a one sentence description as referred to earlier in this chapter. At the same time, COSO (2017) also mentions that one should describe the risk itself instead of other factors, such as root causes. However, when reciting the positive effects of precise risk identification, COSO (2017) states that precise risk identification «Helps the organisation identify the typical root causes and impacts, and therefore select and deploy the most appropriate risk responses» (COSO, 2017, p. 71). Even though the quotation may seem plausible, it is curious to see that the framework does not include any kind of cause analysis before jumping directly on to assessing severity. A reason for this may be giving more room to connect the risks to strategy, objectives, and performance, which can be interpreted to be one of the central parts or areas of ERM. The enhanced guide does, however, include cause analysis into the risk assessment, with a list of methods which can be used, as well as techniques and methods highlighting unknowns in order to acquire more knowledge on underlying issues that may seem small, but can affect other units of the entity on a larger scale. For example, it would not be completely unlikely that a farmer who is angry at the state or commune for some reason (taking their land, for example, to construct a new and more effective motorway) takes it out on the government by contaminating the drinking water in said commune, as in the application example, in order to either harm or make the commune delay their road work.

Another supplement in the guide has been the addition of impact classifications in order to divide and assess how one single risk can affect different areas of the entity. COSO (2017) does use some impact classification in their table «*Example 8.2: Aligning Business Objectives, Risk, and Severity Measures*» (COSO, 2017, p. 76), where they state the rating of one impact type and its likelihood. A list of impact types or classifications which also corresponds to the business objective being analysed can help the analyst see interdependencies, as well as

seeing which risks has *stackable* impacts which in themselves do not cause harm, but together can possibly affect the entity. For example, COSO (2017) uses an example of an entity not being able to develop new products which can result in a moderate impact on customer satisfaction. It is not mentioned in the example, however, that not being able to produce new products may lead to a decrease in earnings because of the lower customer satisfaction and possible reduction in customer or brand loyalty. For this reason, the guide has an added section where one defines impact classifications and impact levels to each risk, making it easier to visualise which parts of the operation is affected most in order to prioritise what aspects are most crucial to act upon first.

There are several approaches to assessing the severity of identified risks, in both qualitative and quantitative methods. When considering quantitative methods, COSO (2017) refers to probabilistic and non—probabilistic models, where the former is exampled with the examples: value at risk, cash flow at risk and operational loss distributions (a statistical approach based on value at risk) (A. Frachot, Georges, & Roncalli, 2001), which are all examples of probabilistic models based on expected numbers. It is not within the scope of this thesis to discuss consequences of relying too much on expected numbers, but it must be said that if these types of methods are to be utilised, some judgement of strength of knowledge should be included in order to assess the "trueness" of the numbers and assumptions used during analysis. COSO (2017) does state that « (..) management may rely on a degree of judgement and expertise when conducting the modelling. Regardless of the approach used, any assumptions should be clearly stated» (COSO, 2017, p. 75). The statements given by COSO (2017) senses a step in the right direction regarding justifications and stating assumptions, but it does not make judgement of who or what the knowledge is provided by, how well understood the phenomena or system is, and agreement amongst experts. A new section of judging strength of knowledge is therefore included in the enhanced guide heavily based Aven and Thekdi (2020) and implemented in the application example. Dividing into data acquisition categories proved to be successful in the example mentioned by giving the analyst the means to reflect upon the credibility of the information provided by respondents. In the end, a list of total knowledge was produced and added to the extended risk picture giving the reader a more complete and realistic view on the choices of impact levels. A limitation of the technique would be that it takes extended time, but at the same time knowing how credible ones sources are, especially in a time where information can be provided by anyone online, should be high on an anyone's priority list not only during a risk assessment, but also in life.

Costs and benefits are considered in COSO (2017) to be a significant factor in choosing a response to identified risks. However, selecting appropriate expected numbers to uncertain and/or non-monetary values are both difficult and often chosen in the eye of the analyst themselves (meaning that the analyst has their own perception and their own judgements on risk) (Abrahamsen, Aven, Vinnem, & Wienche, 2004). For this reason, a layered approach

is recommended, as it not only focuses on the costs and benefits of implementation, but also evaluates other concerns, like uncertainties and strategy.

5.4 Review & Revision

COSO (2017) says that all entities, even the ones with a suitable ERM practice, can become even more effective by pursuing continual improvement. It is important to learn from one's experiences by reviewing, revising and following up risks, but at the same time, learning *how* to become more efficient also takes time and values. An entity having a whole ERM department could spend all their time and resources on improving their ERM process continually, but most entities, especially those in a beginner maturity, have ERM as a process on top of their existing workload. However, learning and improving is a vital part of risk management. It is by collecting and assessing knowledge that one can decipher the uncertainties that are threatening the entity. Regarding this thesis, however, a main method in enhancing the entity's ERM process is by going up to the next maturity level described by Aven and Thekdi (2020).

5.5 Information, Communication and Reporting

Both the guide and COSO (2017) agree on the importance of openness in the flow of information as well as transparency throughout the entity. The entity must have channels, preferably with a choice to be anonymous, where personnel can freely report deviations and suggestions for improvement regarding ERM, but also the rest of the entity. It must be stated, however, that this does not mean that the personnel have mandates in all decisions made in the entity, but that they can be extra sets of eyes and eyes for the entity to function as a whole unit.

In addition to the information going from the personnel to the management, there must also be open communication from the management to personnel, as well as a channel for the management to be able to express uncertainties to the entire company. Large uncertainties from the management will and does affect personnel in their day to day activities, and it is important that the management are comfortable to sometimes say "I do not know. It is uncertain" is need be. Risk communication on this level is not, however, in the scope of this thesis but is an interesting topic which can be viewed in different works, for example in the article *Risk communication in the light of different risk perspectives* by Veland and Aven (Veland & Aven, 2013).

6 Conclusion

This thesis has reviewed COSO's *Enterprise Risk Management – Integrating with Strategy and Performance*, collected methods in incorporating uncertainty-based principles in risk management, produced a guide in using said methods inside COSO's framework for a beginner maturity level and evaluated both the differences and practicalities of the guide presented in chapter 3 in comparison to the original COSO framework.

The guide in chapter 3 has shown a simplified and concretised procedure in how to implement an ERM process, with the purpose of reducing COSO (2017) down to the basics. A small or growing entity, especially an entity which experiences increased risks as a result of expanded performance or an uncertain business context being subject to frequent changes from external sources, can often be understaffed or have limited time and resources to devote to having a full ERM team, which COSO (2017) insinuates. This thesis eliminates this problem by exhibiting a clear activity plan with responsibilities incorporated in order to allocate the correct authority, but also to show where it is appropriate to delegate assignments to other groups or personnel. In addition to presenting an activity plan, the guide also suggests incorporating elements from the topic of uncertainties, based on Aven and Thekdi (2020), and has therefore added these into the guide in order to produce a more cohesive and forward-thinking view on emerging risks.

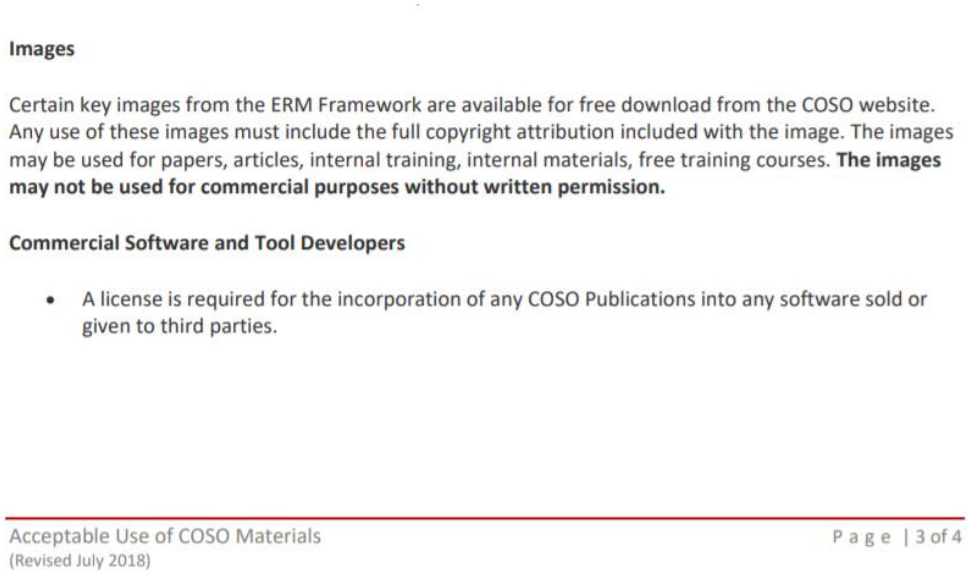
Special notice should also be addressed to the human factor in implementing such a large and all-encompassing procedure to an already functioning entity. Implementing new or changed methods, especially when the method affects all aspects of an entity is not always easy or straight forward. Therefore, it is important for the entity, as a whole, to understand *why* changes are happening. The board, management and leaders are the role models to all personnel regarding risk, safety, and realising value, and they are the ones who have to be the greatest advocates for ERM in order to establish desired culture.

COSO (2017) mentions that there is no "one size fits all" when it comes to ERM, and this thesis concludes with the same message, but the guide provided is concluded to may be beneficial in implementing EMR in some entities which can identify with a beginner maturity level of risk management. It is recommended to use the original COSO (2017) and Aven and Thekdi (2020) as references if there is desire to go beyond said maturity level.

7 Appendix

7.1 A – Copyright

Copyright for the use of images from COSO (2017).



Images

Certain key images from the ERM Framework are available for free download from the COSO website. Any use of these images must include the full copyright attribution included with the image. The images may be used for papers, articles, internal training, internal materials, free training courses. **The images may not be used for commercial purposes without written permission.**

Commercial Software and Tool Developers

- A license is required for the incorporation of any COSO Publications into any software sold or given to third parties.

Acceptable Use of COSO Materials
(Revised July 2018)
Page | 3 of 4

7.2 B – Taxonomy

From the book *Enterprise risk management – Advances on its foundation and practice* by Aven and Thekdi (2020), table 3.1 Taxonomy of ERM maturity.

	Characteristic	*Beginner*	*Intermediate*	*Advanced*
Resources				
	R.1. Dedicated risk manager		✓	✓
	R.2 Dedicated risk management business unit (proportional to size/importance of organization)			✓
	R.3 Documented risk guidelines and policies, available to all organizational stakeholders			✓
	R.4 Clear and detailed risk strategies (risk-informed strategies, cautionary/precautionary/robustness/resilience strategies, and discursive strategies)	✓	✓	✓
	R.5 Resources for regular risk management benchmarking and reporting		✓	✓
Expertise				
	E.1 Some employees trained on risk management practices	✓	✓	✓
	E.2 All employees trained on risk management practices, with training aligned with each role's function in risk management processes		✓	✓
Culture				
	C.1. Agreement among board and other leadership on the organization's risk appetite	✓	✓	✓
	C.2 Regular assessment and accountability at all levels of the organization, to ensure risk policies are properly implemented	✓	✓	✓
	C.3 Risk perception studies to identify major risk concerns, including social, cultural, and psychological factors in risk judgment		✓	✓
	C.4 Implementation of open, transparent, and timely risk communication procedures	✓	✓	✓
	C.5 Invite feedback from stakeholders engaged in the risk practices, and incorporate in risk policies as needed	✓	✓	✓
Practices				
	P.1 Meets local and industry-specific regulations	✓	✓	✓

P.2 Meets local and industry-specific non-regulatory risk and safety guidelines	✓	✓	✓
P.3 Knowledge-dependent prioritization of risk informed by formal tools	✓	✓	✓
P.4 Formal procedures for balancing risk concerns, such as cost-benefit methods, see comment below		✓	✓
P.5 Formal procedures for identifying appropriate risk control, risk treatment, risk response strategies that are in agreement with the overall risk appetite of the organization		✓	✓
P.7 Active stakeholder involvement in risk management processes		✓	✓
P.8 Formal processes for assessing risk for high uncertainty and black swan surprises			✓
P.9 Continuously monitor and audit the ERM process, while adapting to changing conditions and stakeholder feedback	✓	✓	✓

7.3 C – Strength of knowledge

Examples of methods of assessing the strength of knowledge, from appendix in Aven and Thekdi (2020).

The knowledge K is judged as weak if one or more of the following conditions are true:

w1) The assumptions made represent strong simplifications.
w2) Data/information are/is non-existent or highly unreliable/irrelevant.
w3) There is strong disagreement among experts.
w4) The phenomena involved are poorly understood; models are non-existent or known/believed to give poor predictions.
w5) The knowledge K has not been examined (for example with respect to unknown knowns)

If, on the other hand, all (whenever they are relevant) of the following conditions are met, the knowledge is considered strong:

s1) The assumptions made are seen as very reasonable.
s2) Large amounts of reliable and relevant data/information are available.
s3) There is broad agreement among experts.
s4) The phenomena involved are well understood; the models used are known to give predictions with the required accuracy.
s5) The knowledge K has been thoroughly examined.

Cases in between are classified as medium strength of knowledge. To obtain a wider strong knowledge category, the requirement that all of the criteria s1)-s5) need to be fulfilled (whenever they are relevant) could, for example, be replaced by a criterion expressing that at least one (or two, three or four) of the criteria s1)-s5) need to be fulfilled and, at the same time, none of the criteria w1)-w5) are fulfilled.

A simplified version of these criteria can be obtained by applying the same score for strong but assigning the medium and weak scores when a suitable number of conditions are not met, for example medium score if one or two of the conditions s1)-s5) are not met and weak score otherwise, i.e. when three, four or five of the conditions are not met.

The above system is based on Flage and Aven (2009) and Aven and Flage (2018). For an adjusted similar scheme addressing security issues, see Askeland et al. (2017). An alternative related approach is the so-called NUSAP system (NUSAP: Numeral, Unit, Spread, Assessment, and Pedigree) (Funtowicz and Ravetz 1990, 1993, Kloprogge et al 2005,2011, Laes et al 2011, van der Sluijs et al 2005a,2005b).

7.4 D - Mattilsynet

Impact and likelihood classifications produced by the Norwegian Food Safety Authority (Mattilsynet).

S-NIVÅ	KRITERIER
S1: Liten sannsynlighet	a: Hendelsen er ukjent i bransjen b: Faglig skjønn tilsier at hendelsen ikke helt kan utelukkes c: Trusselvurdering tilsier at hendelsen er lite sannsynlig
S2: Middels sannsynlighet	a: Bransjen kjenner til at hendelsen har inntruffet de siste 5 år b: Faglig skjønn og føre-var hensyn tilsier at det er riktig å ta høyde for at hendelsen kan oppstå i vannverket de neste 10-50 år c: Trusselvurdering tilsier at hendelsen er middels sannsynlig
S3: Stor sannsynlighet	a: Det er kjent i bransjen at hendelsen forekommer årlig b: Vannverket har selv opplevd enkeltstående tilfeller, eller hendelsen har nesten inntruffet c: Faglig skjønn og føre-var hensyn tilsier at hendelsen kan oppstå i vannverket i løpet av de neste 1-10 år d: Trusselvurdering tilsier at hendelsen har stor sannsynlighet
S4: Svært stor sannsynlighet	a: Hendelsen forekommer fra tid til annen i vannverket b: Trusselvurdering tilsier at hendelsen har svært stor sannsynlighet

K-NIVÅ	KRITERIER
K1: Liten konsekvens	a: Kvalitet: Kvalitet påvirkes noe, men krav overholdes b: Leveranse: Ubetydelig påvirkning c: Omdømme & økonomi: Omdømme ikke truet, eller økonomisk tap mindre enn 5% av årlig driftskostnader
K2: Middels konsekvens	a: Kvalitet: Kortvarig, mindre brudd på gjeldende krav b: Leveranse: Kortvarig (timer) svikt i forsyning til enkelte områder c: Omdømme & økonomi: Omdømme truet, eller økonomisk tap 5-10% av årlig driftskostnader
K3: Stor konsekvens	a: Kvalitet: Brudd på gjeldende krav, ulempe for helse b: Leveranse: Langvarig svikt (dager) i forsyning til enkelte områder c: Omdømme & økonomi: Omdømme kortvarig tapt, eller økonomisk tap 10-20% av årlig driftskostnader
K4: Svært stor konsekvens	a: Kvalitet: Alvorlig brudd på gjeldende krav, fare for liv og helse, drikkevannsforskriften § 9 andre ledd trer i kraft b: Leveranse: Langvarig svikt som rammer flertallet av abonnentene c: Omdømme & økonomi: Omdømme langvarig tapt, eller økonomisk tap større enn 20% av årlig driftskostnader

8 Reference list

A. Frachot, Georges, P., & Roncalli, T. (2001). *Loss Distribution Approach for operational risk∗*. Retrieved from http://thierry-roncalli.com/download/lda.pdf

Aasand, F. I. (2018). About Norway's water industry. Retrieved from https://www.norskvann.no/index.php/om-norsk-vann/information-in-english

Abrahamsen, Aven, Vinnem, & Wienche. (2004). Safety management and the use of expected values. *Risk Decision and Policy*(9), 347-357.

Aven, T. (2014). *Risk, Surprises and black swans: fundamental ideas and concepts in risk assessment and risk management*. Oxfordshire, England: Routledge.

Aven, T. (2015). *Risk Analysis*. United Kingdom: John Wiley & Sons, Ltd.

Aven, T., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., . . . Zio, E. (2018). Risk Analysis : Fundamental Principles. *SRA*.

Aven, T., & Thekdi, S. (2019). *Enterprise risk management - Advances on its foundation and practice*: Routledge.

Bjørnå, F. (Ed.) (2018). SNL.

BP. (2009). *Sustainability review*. Retrieved from https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/sustainability/archive/archived-reports-and-translations/2009/bp_sustainability_review_2009.pdf

COSO. (1985-2020). Guidance Retrieved from https://www.coso.org/Pages/guidance.aspx

COSO. (2014). Enterprise Risk Management - Integrated Framework - executive summary. In.

COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance. In.

COSO, & wbcsd. (2018). *Enterprise Risk Management -Applying enterprise risk management to environmental, social and governance-related risks*. In.

COSO, w. (2018). *Enterprise Risk Management -Applying enterprise risk management to environmental, social and governance-related risks*. In.

Dickinson, G. (2001). Enterprise Risk Management: Its Origins and Conceptual

Foundation. *The Geneva Papers on Risk and Insurance, 26*, 360-366.

Folkehelseinstituttet. (2008). *Vannforsyningens ABC*

Kapittel E - Vannforsyningsnett. Retrieved from Folkehelseinstituttet: PDF attached

Fredericksen, E. D., & McCorkle, S. (2013). Explaining Organizational Responses to Workplace Aggression. *Sage Journals, 42*(2), 223-238. doi:https://doi.org/10.1177/0091026013487050

omsorgsdepartementet, H.-o. (2017). Forskrift om vannforsyning og drikkevann (drikkevannsforskriften). In. Lovdata.

R.Moeller, R. (2011). *COSO Enterprise Risk Management - Establishing Effective Governance, Risk, and Compliance Processes*. Hoboken, New Jersey: John Wiley & Sons.

Riis, L., & Hareide, A. (2017). *Sikring av vannforsyning mot tilsiktede uønskede hendelser*. Retrieved from Norsk Vann:

Scandpower, Aquateam, COWI, H., & forskingsinstitutt., F. (2003). *Sårbarhet i vannforsyningen (SIV).* Retrieved from

Smith-Solbakken, M. (2020). Deelwater Horizon-ulykken. In *SNL*.

UC Berkeley. (2011). 1980-82 Early 1980s Recession. *Slaying the Dragon og Debt - Fiscal Politics & Policy from the 1970s to the Present.* Retrieved from https://bancroft.berkeley.edu/ROHO/projects/debt/1980srecession.html

Veland, & Aven. (2013). Risk communication in the light of different risk perspectives. *Reliability Engineering System Safety, 110*, 34-40.